Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations

Naipeng Dong*   Hugo Jonker   Jun Pang

Abstract

Protecting privacy against bribery and coercion is a necessary requirement in electronic services, like e-voting, e-auction and e-health. To capture this requirement, domain-specific privacy properties have been proposed in the literature. We generalise these properties as *enforced privacy*: a system enforces a user's privacy even when the user collaborates with the adversary. On top of that, we take into account third parties' influence on the privacy of a target user. The third parties help to break the target user's privacy when collaborating with the adversary and help to protect the target user's privacy when cooperating with the target user. We propose *independency of privacy* to capture the negative privacy impact that third parties can have, and *coalition privacy* to capture their positive privacy impact. We formally define these privacy notions in the applied pi calculus and build a hierarchy showing the relations among the notions.

1 Introduction

Privacy is of great importance to electronic services such as e-voting, e-auction, and e-health. A large amount of research has been done in this area. In the literature, an important focus is privacy in communication protocols, since most electronic services use the Internet. To capture privacy in protocols, a wide variety of privacy properties have been proposed, such as anonymity, untraceability, quantified privacy, etc. (e.g., see [3, 9, 24, 32, 33]). We focus on a subset of such properties – non-quantified (binary) data privacy, i.e., properties that are either satisfied or not (as opposed to providing a quantitative answer).

Classical data privacy assumes that users want to keep their privacy [3, 9, 32]. However, a user may want to reveal information to the adversary due to bribery or coercion. Systems providing electronic services need to protect against such threats (e.g., [2, 5, 13, 26]). This was first achieved in voting: a system in which a voter could not undo his privacy after voting (preventing vote selling) [5], and later, a system in which a voter, coerced to communicate continuously with the adversary, cannot undo his privacy [26]. These ideas were lifted to an e-auction system [2] and an e-health system [13]. Following this development of stronger systems, domain-specific formalisations of privacy properties against bribery and coercion were proposed in the literature: receipt-freeness and coercion-resistance in e-voting [14], e-auction [16], and e-health [18]. In order to address these privacy concerns domain-independently, we propose a generic notion of *enforced privacy*: a user's privacy is preserved even if the user collaborates with the adversary by sharing information.

The notions of data privacy and (enforced) privacy focus on a target user and ignore the impact that other users can have on his privacy. However, a third party may help the adversary break privacy of the target user (*collaboration*), e.g., revealing his vote may enable the adversary to deduce another voter's vote. On the other hand, a third party may help the target user to maintain his privacy (*coalition*), e.g., a non-coerced voter (who happens to vote as the adversary desires) can swap receipts with a coerced voter, providing the coerced voter "proof" of compliance while being free to vote as he pleases.

Accounting for the privacy effect of third parties is particularly necessary in domains where many untrusted roles are involved. Such roles may potentially reveal information to the adversary, e.g., pharmacists in e-health may be able to reveal prescription behaviour of doctors. In order to ensure doctor prescribing-privacy, an e-health system must prevent this situation [13, 17]. This requirement has been expressed and formalised as independency-of-prescribing-privacy [18]: a doctor's prescribing-privacy is preserved even if pharmacists share information with the adversary. In voting, a similar privacy property, vote-independence [20], was proposed to ensure a voter's vote-privacy even if another voter is coerced by the adversary. In this paper, we generalise these properties as *independency of privacy*: the help of a set of third parties does not enable the adversary to break a target user's privacy. This notion is generic in the sense that first, a third party may have the same role as the target user (as in vote-independence), or a different role (as in independency-of-prescribing-privacy); second, the collaboration can be instantiated as coercion, but is not limited to that; third, this notion is domain-independent, i.e., it is not restricted a specific domain like e-voting or e-health.

The converse, that is, the privacy effect of third parties helping the target user by sharing information with the target user, has not been well studied. To capture privacy in this situation, we propose the notion of *coalition privacy*: a target user's privacy is preserved with the help of a set of third parties sharing information with the target user. In particular, we use this notion to also capture the situation where third parties are involved but no information is shared between the target user and third parties. In this case, the mere *existence* of the third parties can help to create a situation where privacy is preserved. For example, vote-privacy [14] requires a non-unanimous result – there must be at least one voter voting differently. He then ensures that the other voters' privacy is not trivially broken.

In addition to identifying these privacy notions, we formalise them in a new formal framework. Cryptographic protocols are well known to be error-prone and formal approaches have shown to be efficient in addressing this problem, e.g., see [10, 30]. Thus, formalising

*Supported by a grant from the Fonds National de la Recherche (Luxembourg).

privacy notions is a necessary step to verify the privacy claims of a protocol. Our framework is based on the applied pi calculus as it provides an intuitive way for modelling privacy properties and cryptographic protocols. In addition, it is supported by the ProVerif [6] tool, which allows us to verify many privacy properties automatically [8, 11].

Inspired by the frameworks in the applied pi calculus by Arapinis et al. [3] and Delaune et al. [14], our framework allows us to give domain-independent formalisations of all of the identified (enforced) privacy notions. We define a standard form of protocols which is able to represent any protocol. To formally define enforced privacy properties and independency of privacy properties, we model *collaboration* between users and the adversary in a more generic way. It allows us to specify which information is shared and how it is shared. Thus, our framework provides the necessary flexibility for modelling various types of collaboration. Bribery and coercion can be considered as collaboration between the target user and the adversary, and their formalisations as proposed by Delaune et al. [14] are essentially instances of our collaboration specification: bribery is one-way complete information sharing from the target user to the adversary; coercion is another specific collaboration where the target user shares *all* his private information while the adversary provides information for the target user. To model coalition privacy properties, we propose the notion of *coalition* in our framework to formally capture the behaviour and shared information among a target user and a set of third parties.

In our framework, the foundational property data-privacy, is formalised in a classical way as strong secrecy: equivalence of two processes where a variable is instantiated differently [7]. This formalisation captures privacy notions like anonymity [3] which is formalised as equivalence of two process with different identities. Based on this property, we formalise enforced-privacy, coalition-independency-of-privacy and their combination coalition-independency-of-enforced-privacy using the formalisation of collaboration. Using the formalisation of coalition, four corresponding coalition privacy properties are formalised. In particular, we can show that various domain-specific privacy formalisations such as vote-privacy [27] in e-voting, bidding-privacy [16] in e-auction, and prescribing-privacy [18] in e-health, are instances of coalition-privacy, receipt-freeness and coercion-resistance in e-voting [14, 21] are instances of the property coalition-enforced-privacy, and independency-of-prescribing-privacy [18] and vote-independence [20] are instances of coalition-independency-of-privacy (cf. Sect. 6).[1]

Finally, we formally discuss how the formalised privacy properties are related in a privacy hierarchy. We show that data privacy notions considered in an existing hierarchy of privacy in voting [22] are instances of properties in our hierarchy. The main difference between the two is that our hierarchy is domain-independent and focuses on privacy in the presence of third parties.

Contributions. The main contributions of this paper are:

- We generalise privacy against bribery and coercion to a domain-independent notion *enforced privacy* to capture privacy of users collaborating with the adversary.
- We propose the notion of *independency of privacy* to capture the privacy effects of third parties collaborating with the adversary. Third parties can be any set of users excluding the target user, unlike the existing domain-specific notions which usually limit the roles and the number of third parties.
- We propose the notion of *coalition privacy* to capture the privacy effects in the presence of defending third parties. This opens a new direction of privacy notions which take into account communication among third parties and the target user.
- We present a formal framework in which we can precisely model how users collaborate with the adversary and how users form a coalition against the adversary in the applied pi calculus. The framework leads to a generic formalisation of the identified privacy notions. Furthermore, we prove the relations between the formalised notions and build a privacy hierarchy.

2 Adversary Model and Privacy Notions

To study privacy, we need to make explicit against *whom* privacy is protected – who is the adversary. Our adversary is based on the Dolev-Yao adversary [15] who can eavesdrop, block and inject messages on the network. Moreover, he can extract data from messages and compose new messages from known data. The adversary can generate fresh data as needed and can initiate a conversation with any user. The adversary's initial knowledge contains public information, such as public keys.[2]

We distinguish between two classes of privacy-affecting behaviour: the target user (collaborating with the adversary or not), and the behaviour of third parties. Third parties may be *neutral*, collaborating with the adversary (*attacking*), or collaborating with the target user (*defending*) – thus we also consider the situation where some are attacking and some are defending. A target user who collaborates with the adversary is not under the adversary's direct control, contrary to a compromised user who genuinely shares initial private information with the adversary. A *neutral* third party, like an honest user, follows the protocol specification exactly. Thus, such a third party neither actively helps nor actively harms the target user's privacy. A *defending* third party helps the target user to preserve his privacy. An *attacking* third party communicates with the adversary to break the target user's privacy. Note that we do not consider a third party that attacks and defends the target user simultaneously. Given this classification, a target user will find himself one of the following four situations w.r.t. third parties: 1) all are neutral; 2) some are attacking; 3) some are defending; and 4) some are attacking, some are defending. In the latter three cases, the remaining third parties (if any) are considered neutral.

[1] Note that quantified enforced privacy properties in voting [25] are not captured in our framework.

[2] Note that the Dolev-Yao adversary is not assumed to fully control authenticated users. Bribed or coerced users cannot be modelled as part of the adversary, as they are not trusted by the adversary. In addition, it is necessary to model which information and how users share the information, especially those obtained from channels hidden from the adversary.

Table 1: Privacy notions

target user collaborates with adversary	third parties			
	all neutral	*some attacking*	*some defending*	*some defending some attacking*
no	priv	ipriv	cpriv	cipriv
yes	epriv	iepriv	cepriv	ciepriv

Combining the various behaviours of the third parties with those of the target user gives rise to eight privacy properties (see Tab. 1). These properties hold when the adversary cannot break a user's privacy. In more details, the adversary cannot link the target user to his data:

1. data-privacy (priv): when the target user is honest.
   E.g., the adversary cannot link the contents of an encrypted email to the user.

2. enforced-privacy (epriv): when the target user seems to collaborate with the adversary.
   E.g., a voter should not be able to prove to a vote-buyer how he voted.

3. independency-of-privacy (ipriv): when (some) third parties collaborate with the adversary.
   E.g., in e-health the adversary cannot link a doctor to his prescriptions, despite the help of a pharmacist.

4. independency-of-enforced-privacy (iepriv): even when the target user seems to, and some third parties actually do collaborate with the adversary.
   E.g., the adversary should not be able to link a doctor to his prescriptions (to prevent bribes), even when both the pharmacist and the doctor are helping him.

5. coalition-privacy (cpriv): when (some) third parties collaborate with the target user.
   E.g., in location-based services, the user's real location is hidden amongst the locations of the helping users.

6. coalition-enforced-privacy (cepriv): even when the target user seemingly collaborates with the adversary, provided (some) third parties help to defend the user.
   E.g., in anonymous routing, a sender remains anonymous if he synchronises with a group of senders, even if he seems to collaborate.

7. coalition-independency-of-privacy (cipriv): even when some (attacking) third parties collaborate with the adversary, provided some other (defending) third parties collaborate with the target user.
   E.g., the adversary cannot link an RFID chip to its identity, even though some malicious readers are helping the adversary, provided other RFID tags behave exactly as the target one.

8. coalition-independency-of-enforced-privacy (ciepriv): even when the target user seems to, and some third parties actually do collaborate with the adversary, provided that other third parties work to defend the target user.
   E.g., in electronic road pricing, other users may hide a user's route from the adversary, even if the user seems to collaborate and malicious routers relay information on passing cars to the adversary.

The examples above illustrate that similar privacy concerns arise in many different domains – e-voting, e-health, location-based services, RFID, electronic road pricing, etc. So far, attempts at formalising privacy have usually been domain-specific (e.g., [3, 9, 12, 14, 16, 18, 21, 27, 33]). We advocate a domain-independent approach to privacy, and develop a formal framework to achieve this in Sect. 3.

3 Formal Framework

In this section, we propose a framework to formalise the privacy properties from Tab. 1 in the applied pi calculus. We briefly introduce the language and notions used in this paper (Sect. 3.1). For the simplicity of formalisation, we define a standard form of protocols – *well-formed* protocols (Sect. 3.2), inspired by the formal framework for modelling anonymity [3]. Based on this, we introduce the property *data-privacy* which acts as the foundation of other properties (Sect. 3.3). To formalise enforced privacy and independency of privacy properties, we formally define collaboration between a set of users and the adversary (Sect. 3.4), inspired by the formal framework for modelling bribery and coercion in voting [14]. Finally, to formalise coalition privacy properties, we formally define coalition among a set of users (Sect. 3.5).

3.1 The applied pi calculus

The applied pi calculus [1] assumes an infinite set of *names* to model data and communication channels, an infinite set of *variables* and a finite set of *function symbols* each with an associated arity to capture cryptographic primitives. A constant is defined as a function symbol with arity zero. *Terms* are defined as either names, or variables or function symbols applied on other terms to capture communicated

Figure 1: Applied pi processes

$$\begin{array}{lll}
P, Q, R ::= & & \text{plain processes} \\
& 0 & \text{null process} \\
& P \mid Q & \text{parallel composition} \\
& !P & \text{replication} \\
& \nu \mathtt{n}.P & \text{name restriction} \\
& \text{if } M =_E N \text{ then } P \text{ else } Q & \text{conditional} \\
& \mathsf{in}(v, x).P & \text{message input} \\
& \mathsf{out}(v, M).P & \text{message output} \\
\\
A, B, C ::= & & \text{extended processes} \\
& P & \text{plain process} \\
& A \mid B & \text{parallel composition} \\
& \nu \mathtt{n}.A & \text{name restriction} \\
& \nu x.A & \text{variable restriction} \\
& \{M/x\} & \text{active substitution}
\end{array}$$

messages. We denote the variables in a term N as $\mathsf{Var}(N)$. A set of equations on terms are defined as an equational theory E. $M =_E N$ denotes that term M and N are equivalent according to the equational theory. In addition, the applied pi calculus assumes a set of base types (e.g., the universal type *Data*) and a type system (sort system) for terms generated by the base set. Terms are assumed to be well-typed and syntactic substitutions preserve types. Based on the above notions, processes are defined as in Fig. 1 where M, N are terms, $\mathtt{n}$ is a name, x is a variable and v is a metavariable, standing either for a name or a variable.

A name is *bound* if it is under restriction. A variable is *bound* by restrictions or inputs. Names and variables are *free* if they are not delimited by restrictions or by inputs. The sets of free names, free variables, bound names and bound variables of a process A are denoted as $\mathsf{fn}(A)$, $\mathsf{fv}(A)$, $\mathsf{bn}(A)$ and $\mathsf{bv}(A)$, respectively. A term is *ground* when it does not contain variables. A process is *closed* if it does not contain free variables. $\{M/x\}$ is a substitution which replaces variable x with term M. The active substitutions in extended processes allow us to map an extended process A to its frame $\mathsf{frame}(A)$ by replacing every plain process in A with 0. A *frame* is defined as an extended process built up from 0 and active substitutions by parallel composition and restrictions. The *domain* of a frame B, denoted as $\mathsf{dom}(B)$, is the set of variables for which the frame defines a substitution. A *context* $\mathcal{C}[\_]$ is defined as a process with a hole, which may be filled with any process. Finally, we abbreviate $\nu\mathtt{n}_1 \cdots \nu\mathtt{n}_n$ as $\nu\widetilde{\mathtt{n}}$, $\nu\mathtt{n}_1 \cdots \nu\mathtt{n}_{i-1}.\nu\mathtt{n}_{i+1}.\cdots.\nu\mathtt{n}_n$ as $\nu\widetilde{\mathtt{n}}/\mathtt{n}_i$, and $\{M_1/x_1\}\cdots\{M_n/x_n\}$ as $\{M_1/x_1, \cdots, M_n/x_n\}$.

The operational semantics of the applied pi calculus is defined by: 1) structural equivalence of processes ($\equiv$), which defines when two processes that only differ in structure are equivalent; 2) internal reduction ($\rightarrow$), which covers sub-processes communication and *if-then-else* evaluation; and 3. labelled reduction ($\xrightarrow{\alpha}$), which covers the communication between the adversary and the protocol. The transition $A \xrightarrow{\alpha} B$ means that process A performs action α and continues as process B. Action α is either reading a term M from the process's context, or sending a name or a variable of base type to the context. We use $\rightarrow^*$ to denote one or more transitions.

Several equivalence relations on processes are defined in the applied pi calculus. We mainly use labelled bisimilarity $\approx_\ell$ [1], which is based on static equivalence $\approx_s$ of processes: labelled bisimilarity compares the dynamic behaviour of processes, while static equivalence compares the static states of processes (as represented by their frames).

Definition 1 (static equivalence)**.** *Closed frames B and B' are statically equivalent, $B \approx_s B'$, if (1) $\mathsf{dom}(B) = \mathsf{dom}(B')$; (2) $\forall$ terms M, N: $M =_E N$ in $B \Longleftrightarrow M =_E N$ in B'. Extended processes A, A' are statically equivalent, $A \approx_s A'$, if their frames are statically equivalent: $\mathsf{frame}(A) \approx_s \mathsf{frame}(A')$.*

Definition 2 (labelled bisimilarity)**.** Labelled bisimilarity ($\approx_\ell$) *is defined as the largest symmetric relation $\mathcal{R}$ on closed extended processes, such that $A\,\mathcal{R}\,B$ implies: (1) $A \approx_s B$; (2) if $A \rightarrow A'$ then $B \rightarrow^* B'$ and $A'\,\mathcal{R}\,B'$ for some B'; (3) if $A \xrightarrow{\alpha} A'$ and $\mathsf{fv}(\alpha) \subseteq \mathsf{dom}(A)$ and $\mathsf{bn}(\alpha) \cap \mathsf{fn}(B) = \emptyset$; then $B \rightarrow^* \xrightarrow{\alpha} \rightarrow^* B'$ and $A'\,\mathcal{R}\,B'$ for some B'.*

3.2 Well-formed protocols

In the applied pi calculus, a protocol is normally modelled as a plain process. For the simplicity of formalising privacy properties, we define a standard form of a protocol [3] and any protocol can be written in this form.

Definition 3 (well-formed protocols)**.** *A protocol with p roles is well-formed if it is a closed plain process P_w of the form:*

$$\begin{array}{rcl}
P_w & = & \nu\widetilde{\mathtt{c}}.(genkey \mid !R_1 \mid \cdots \mid !R_p) \\
R_i & = & \nu\mathtt{id}_i.\nu\mathtt{data}_i.init_i.!(\nu\mathtt{s}_i.\nu\mathtt{sdata}_i.sinit_i.main_i) \quad (\forall i \in \{1, \cdots, p\})
\end{array}$$

where

1. *P_w is canonical [3]: names and variables in the process never appear both bound and free, and each name and variable is bound at most once;*

2. *data is typed, channels are ground, private channels are never sent on any channel;*

3. *$\nu\widetilde{\mathtt{c}}$, $\nu\mathtt{data}_i$ and $\nu\mathtt{sdata}_i$ may be null;*

4. *$init_i$ and $sinit_i$ are sequential processes;*

5. *$genkey$, $init_i$, $sinit_i$ and $main_i$ can be any process (possibly null) such that P_w is a closed plain process.*

In process P_w, $\widetilde{\mathtt{c}}$ are channel names; $genkey$ is a sub- process in which shared data (e.g., keys shared between two roles) are generated and distributed; R_i $(1 \le i \le p)$ is a role. To distinguish instances taking the same role R_i, each instance is dynamically associated with a distinct identity $\nu\mathtt{id}_i$; $\mathtt{data}_i$ is private data of an instance; $init_i$ models the initialisation of an instance; $(\nu\mathtt{s}_i.\nu\mathtt{sdata}_i.sinit_i.main_i)$ models a session of an instance. To distinguish sessions of the same instance, each session is dynamically associated to a distinct identity $(\nu\mathtt{s}_i)$; $\mathtt{sdata}_i$ is private data of a session; $sinit_i$ models the initialisation of a session; $main_i$ models the behaviour of a session.

Note that this standard form does not limit the type of protocols we consider. A role may include a number of sub-roles so that a user may take more than one part in a protocol. The identities do not have to be used in the process. All of $\nu\widetilde{\mathtt{c}}$, $\nu\mathtt{data}_i$ and $\nu\mathtt{sdata}_i$ may be null and $genkey$, $init_i$, $sinit_i$ and $main_i$ can be any process (possibly null) such that P_w is a closed plain process. Any process can be written in a canonical form by α-conversion [3]. Thus, any protocol can be written as a well-formed protocol.

3.3 Data-privacy

We formally define the property data-privacy that acts as the foundation upon which other properties are built. To do so, we need to make explicit *which data* is protected. Thus, the property data-privacy always specifies the target data. In process P_w, the target data τ is a bound name which belongs to a role (the target role R_i), i.e., $\tau \in \mathsf{bn}(R_i)$. For the sake of simplicity, we (re)write the role R_i in the form of

$$R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i,$$

where $\hat{R}_i$ is a plain process which has two variables id_i and τ. Note that by α-conversion we can always transform any role R_i into the above form. When $\tau \in \mathtt{data}_i$,

$$\hat{R}_i = \nu\mathtt{data}_i/\tau.init_i.!(\nu\mathtt{s}_i.\nu\mathtt{sdata}_i.sinit_i.main_i).$$

When τ is session data in session $\mathtt{s}$, i.e., $\tau \in \mathtt{sdata}'_i$,

$$\hat{R}_i = \nu\mathtt{data}_i.init_i.(!(\nu\mathtt{s}_i.\nu\mathtt{sdata}_i.sinit_i.main_i) \mid (\nu\mathtt{s}.\nu\mathtt{sdata}'_i/\tau.sinit'_i.main'_i)).$$

In case that only information in session $\mathtt{s}$ is shared with the adversary or third parties, we require that $\mathtt{s} \notin \mathsf{bn}(P_w)$, $\nu\mathtt{sdata}'_i/\tau.sinit'_i.main'_i$ is obtained by applying α-conversion on bound names and variables in the original process $\nu\mathtt{sdata}_i/\tau.sinit_i.main_i$.

Intuitively, data-privacy w.r.t. τ of protocol P_w, is the unlinkability of an honest user taking role R_i and his instantiation of the target data τ. An honest user taking role R_i is modelled as process R_i. We denote a particular user – the *target user process*, as $\check{R}_i\{\mathsf{id}/id_i\}$ where $R_i = \nu\mathtt{id}_i.\check{R}_i$, variable id_i is instantiated with a constant id. $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$ denote an instance of the target user in which the target user instantiates the target data with t where t denotes any data which can be used to replace the target data. The unlinkability is modelled as strong secrecy [7] of the target data: the adversary cannot distinguish an execution of R_i where $\tau = \mathtt{t}_1$ from an execution where $\tau = \mathtt{t}_2$, for $\mathtt{t}_1 \neq \mathtt{t}_2$.

Definition 4. *A well-formed protocol P_w satisfies data-privacy (*priv*) w.r.t. data τ ($\tau \in \mathsf{bn}(R_i)$), if*

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}].$$

In the definition, id is a constant, $\mathtt{t}_1$ and $\mathtt{t}_2$ are free names. Since $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, process $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}$ is an instance of role R_i where the identity is id and the target data is $\mathtt{t}_1$. The context $\mathcal{C}_{P_w}[\_]$ models neutral third parties. Thus, $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}]$ is an instance of the protocol P_w, similarly for $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}]$. The only difference between these two instances is the instantiation of the target data τ. Thus, this definition captures data-privacy by using the relation $\approx_\ell$: the adversary cannot distinguish a user process with different target data.

3.4 Modelling Collaboration with the Adversary

Based on data-privacy, we are able to formalise other properties. In order to define enforced privacy properties where the target user collaborates with the adversary and independency privacy properties where a set of third parties collaborate with the adversary, we need to model *collaboration* of users (a target user/third parties) with the adversary.

The process of a set of users is modelled as processes of each user in parallel. Since a user process is modelled as a role in a well-formed protocol and each user process can be any role, the set of users of a well-formed protocol P_w is formally defined as a plain process $R_U = R_{u_1} \mid \cdots \mid R_{u_m}, \forall i \in \{1, \ldots, m\}, R_{u_i} \in \{R_1, \ldots, R_p\}$.

Inspired by the formal definition of coercion in [14], the collaboration between a user and the adversary is formalised as a transformation of the user process. We extend it as a transformation of the process of a set of users. Note that a user need not always share *all* his information, e.g., a bribed user in a social network may reveal his relation with another user, but not his password. To be able to specify which information is shared, we formally define the set of information that a user has. Information of a user is expressed as a set of terms in the user process. Since the user processes are canonical in a well-formed protocol, bound names and variables are different in each user process. Thus, we can express information of a set of users as a set of terms appearing in the process of the set of users. Terms appearing in a plain process R_U are given by $\mathsf{Term}(R_U)$.

$$\begin{array}{rcl}
\mathsf{Term}(0) & = & \emptyset \\
\mathsf{Term}(P \mid Q) & = & \mathsf{Term}(P) \cup \mathsf{Term}(Q) \\
\mathsf{Term}(!P) & = & \mathsf{Term}(P) \\
\mathsf{Term}(\nu \mathtt{n}.P) & = & \{\mathtt{n}\} \cup \mathsf{Term}(P) \\
\mathsf{Term}(\mathsf{in}(v,x).P) & = & \{x\} \cup \mathsf{Term}(P) \\
\mathsf{Term}(\mathsf{out}(v,M).P) & = & \{M\} \cup \mathsf{Term}(P) \\
\mathsf{Term}(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q) & = & \mathsf{Term}(P) \cup \mathsf{Term}(Q)
\end{array}$$

A collaboration specification then specifies which terms of a process are shared and how they are shared.

Definition 5 (collaboration specification)**.** *A* collaboration specification *of a process R_U is a tuple $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$. $\Psi \subseteq \mathsf{Term}(R_U)$ denotes the set of terms sent to the adversary each of which is of base type, $\Phi \subseteq \mathsf{Term}(R_U)$ represents terms to be replaced by information provided by the adversary, c_{out} is a fresh channel for sending information to the adversary, and c_{in} is a fresh channel for reading information from the adversary, i.e., $\mathsf{c}_{out}, \mathsf{c}_{in} \notin \mathsf{fn}(R_U) \cup \mathsf{bn}(R_U)$.*

Given a plain process R_U and a collaboration specification $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ of the process, the transformation of R_U is given by $R_U^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}$.

Definition 6 (collaboration behaviour)**.** *Let R_U be a plain process, and $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ be a collaboration specification of R_U. Collaboration behaviour of R_U according to $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ is defined as:*

- $0^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}\ 0,$
- $(P \mid Q)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}\ P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \mid Q^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle},$
- $(!P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}\ !P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle},$
- $(\nu \mathtt{n}.P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}$
  $\begin{cases} \nu \mathtt{n}.\mathsf{out}(\mathsf{c}_{out}, \mathtt{n}).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{if } \mathtt{n} \in \Psi \\ \nu \mathtt{n}.P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{otherwise}, \end{cases}$
- $(\mathsf{in}(v,x).P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}$
  $\begin{cases} \mathsf{in}(v,x).\mathsf{out}(\mathsf{c}_{out}, x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{if } x \in \Psi \\ \mathsf{in}(v,x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{otherwise}, \end{cases}$
- $(\mathsf{out}(v,M).P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}$
  $\begin{cases} \mathsf{in}(\mathsf{c}_{in}, x).\mathsf{out}(v,x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{if } M \in \Phi \\ \qquad \textit{where } x \textit{ is a fresh variable}, & \\ \mathsf{out}(v,M).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} & \textit{otherwise}, \end{cases}$
- $(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \ \hat{=}$
  $\mathsf{in}(\mathsf{c}_{in}, x).\mathit{if}\ x = \mathsf{true}\ \mathit{then}\ P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\ \mathit{else}\ Q^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}$
  where x is a fresh variable and true *is a constant.*

Note that we only specify user behaviour in a collaboration with the adversary. The adversary's behaviour may be omitted, as in the applied pi calculus the adversary is considered as the environment and does not need to be explicitly modelled. Our approach to reasoning about the adversary's behaviour in a collaboration (e.g., enforcing a voter to cast a particular vote) follows the line of the definition of coercion-resistance in [14]. Namely, a context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}(\_ | Q)$ models a specific way of collaboration of the adversary, where Q models the the adversary's behaviour in the context. In this way, we separate the adversary's behaviour of distinguishing two processes, which is modelled by the environment, from the behaviour of collaborating with users which is modelled by the context.

3.5 Modelling User Coalitions

To define coalition privacy properties, we need to formally define a *coalition* between a target user and a set of defending third parties. The notion collaboration from the previous section cannot be adopted directly, as it does not specify the adversary's behaviour, whereas a coalition must specify the behaviour of *all* involved users. We extend the formalisation of collaboration to model coalition among users.

Given a set of users $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$, a coalition of the users specifies communication between (potentially) each pair of users. For every communication, a coalition specification needs to make explicit who the sender and receiver are (unlike collaboration). Similar to the specification of collaboration, a coalition specification makes explicit which data is sent on which channel. To make the behaviour of both communicating parties explicit, we need to specify how the term in a communication is referred to in the receiver's process. A communication in a coalition is specified as a tuple $\langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle$ where $R_{u_i}, R_{u_j} \in \{R_{u_1}, \ldots, R_{u_m}\}$ ($R_{u_i} \neq R_{u_j}$) are the sender and receiver process, respectively; $M \in \mathsf{Term}(R_{u_i})$ is the data sent in the communication; $\mathsf{c} \notin \mathsf{fn}(R_U) \cup \mathsf{bn}(R_U)$ is a fresh channel used in the communication; $y \notin \mathsf{fv}(R_U) \cup \mathsf{bv}(R_U)$ is the variable used by the receiver to refer to the term M. A coalition specifies a set of communications of this type (denoted as Θ). For the simplicity of modelling, we assume that for each communication, the coalition uses a distinct channel and distinct variable, i.e., $\forall \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta$ and $\langle R'_{u_i}, R'_{u_j}, M', \mathsf{c}', y'\rangle \in \Theta$ we have $\mathsf{c} \neq \mathsf{c}' \wedge y \neq y'$.

A coalition specifies a set of terms which are communicated by the originating user process and are replaced in the coalition. In addition, a coalition needs to define how a term is replaced. In a collaboration, the adversary is assumed to be able to compute and prepare this, but in a coalition, no user can compute and prepare information for other users. Thus, this ability has to be explicitly specified in a coalition as a set of substitutions $\Delta = \{\{N/M\} \mid M \in \mathsf{Term}(R_U)\}$. The new term N are calculated from a set of terms $N_1, \ldots, N_n$ which are generated by the user, read in by the original process, or read in from coalition members. A successful coalition requires that there are no such situations where N cannot be calculated in the user process when M needs to be replaced.

Moreover, in a coalition, we allow the coalition to decide values of conditional evaluations (similar to collaboration, where the adversary decides this). Since no user in a coalition has the ability to specify the values of evaluations, these need to be assigned specifically. In addition, to add more flexibility, we allow a coalition to specify which evaluations are decided by the coalition and which are not. The evaluations of a plain user process R_U is $\mathsf{Eval}(R_U)$.

$$
\begin{array}{rcl}
\mathsf{Eval}(0) & = & \emptyset \\
\mathsf{Eval}(P \mid Q) & = & \mathsf{Eval}(P) \cup \mathsf{Eval}(Q) \\
\mathsf{Eval}(!P) & = & \mathsf{Eval}(P) \\
\mathsf{Eval}(\nu \mathtt{n}.P) & = & \mathsf{Eval}(P) \\
\mathsf{Eval}(\mathsf{in}(v,x).P) & = & \mathsf{Eval}(P) \\
\mathsf{Eval}(\mathsf{out}(v,M).P) & = & \mathsf{Eval}(P) \\
\mathsf{Eval}(\textit{if } M =_E N \textit{ then } P \textit{ else } Q) & = & \{M =_E N\} \cup \mathsf{Eval}(P) \cup \mathsf{Eval}(Q)
\end{array}
$$

The assignments of evaluations are specified as a set $\Pi \subseteq \{(e, b) \mid e \in \mathsf{Eval}(R_U) \wedge b \in \{\mathsf{true}, \mathsf{false}\}\}$.

Definition 7 (coalition specification)**.** *A coalition*[3] *of a set of users R_U is specified as a tuple $\langle \Theta, \Delta, \Pi\rangle$ where Θ is a set of communication, Δ is a set of substitutions and Π is an assignment for a set of evaluations.*

With the above setting, given a set of users R_U and a coalition specification $\langle \Theta, \Delta, \Pi\rangle$ on users, the behaviour of a user in the coalition is modelled as a coalition transformation of the user's original process.

Definition 8 (coalition behaviour)**.** *Let $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$ be a plain process of a set of users, $\langle \Theta, \Delta, \Pi\rangle$ be a coalition specification of process R_U, $R \in \{R_{u_1}, \cdots, R_{u_m}\}$ be a plain user process, the transformation of the process R in the coalition is given by $R^{\langle \Theta, \Delta, \Pi\rangle}$:*

$$R^{\langle \Theta, \Delta, \Pi\rangle} = \nu\eta.(R^{\langle \Gamma, \Delta, \Pi\rangle} \mid \mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell))$$

where $\eta = \{\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell\}$, $\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell$ are fresh, $\Gamma = \{\langle R, R_{u_j}, M, \mathsf{c}, y\rangle \mid \langle R, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$, $\{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R_{u_i}, R, M, \mathsf{c}, y\rangle \in \Theta\}$, $y'_1, \ldots, y'_\ell$ are fresh variables. Each variable is read in from a distinct channel in $\{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\}$ and sent out over a distinct channel in $\{\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell\}$. Thus we have the following set ξ represents the association $\xi = \{(\mathsf{c}_1, y'_1, \mathsf{c}'_1), \ldots, (\mathsf{c}_\ell, y'_\ell, \mathsf{c}'_\ell)\}$.
$R^{\langle \Gamma, \Delta, \Pi\rangle}$ is given by:

- $0_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=} 0,$
- $(P \mid Q)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=} P_F^{\langle \Gamma, \Delta, \Pi\rangle} \mid Q_F^{\langle \Gamma, \Delta, \Pi\rangle},$
- $(!P)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=} !P_F^{\langle \Gamma, \Delta, \Pi\rangle},$
- $(\nu \mathtt{n}.P)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=}$
$$\begin{cases} \nu \mathtt{n}.\mathsf{out}(\mathsf{c}_1, \mathtt{n}).\ldots.\mathsf{out}(\mathsf{c}_\ell, \mathtt{n}).P_F^{\langle \Gamma, \Delta, \Pi\rangle} \\ \qquad\qquad \textit{if } \{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R, R_{u_j}, \mathtt{n}, \mathsf{c}, y\rangle \in \Gamma\} \\ \nu \mathtt{n}.P_F^{\langle \Gamma, \Delta, \Pi\rangle} \qquad\qquad \textit{otherwise}, \end{cases}$$
- $(\mathsf{in}(v,x).P)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=}$
$$\begin{cases} \mathsf{in}(v,x).\mathsf{out}(\mathsf{c}_1, x).\ldots.\mathsf{out}(\mathsf{c}_\ell, x).P_F^{\langle \Gamma, \Delta, \Pi\rangle} \\ \qquad\qquad \textit{if } \{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R, R_{u_j}, x, \mathsf{c}, y\rangle \in \Gamma\} \\ \mathsf{in}(v,x).P_F^{\langle \Gamma, \Delta, \Pi\rangle} \qquad\qquad \textit{otherwise}, \end{cases}$$
- $(\mathsf{out}(v,M).P)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=}$
$$\begin{cases} \mathsf{in}(\mathsf{c}'_1, y_1).\cdots.\mathsf{in}(\mathsf{c}'_\ell, y_\ell).\mathsf{out}(v, \mathsf{f}(N_1, \ldots, N_n)).P_{F\setminus\{y_1, \ldots, y_\ell\}}^{\langle \Gamma, \Delta, \Pi\rangle} \\ \qquad\qquad \textit{if } \{N/M\} \in \Delta, \{y_1, \ldots, y_\ell\} \subseteq F \cup \mathsf{Var}(N), \\ \qquad\qquad \forall i \in \{1, \ldots, \ell\}, \langle R_i, R, \mathsf{c}_i M, y_i\rangle \in \Theta \wedge (\mathsf{c}_i, y'_i, \mathsf{c}'_i) \in \xi \\ \mathsf{out}(v,M).P_F^{\langle \Gamma, \Delta, \Pi\rangle} \qquad\qquad \textit{otherwise}, \end{cases}$$
- $(\textit{if } M =_E N \textit{ then } P \textit{ else } Q)_F^{\langle \Gamma, \Delta, \Pi\rangle} \hat{=}$
$$\begin{cases} P_F^{\langle \Gamma, \Delta, \Pi\rangle} & \textit{if } (M =_E N, \mathsf{true}) \in \Pi \\ Q_F^{\langle \Gamma, \Delta, \Pi\rangle} & \textit{if } (M =_E N, \mathsf{false}) \in \Pi \\ \textit{if } M =_E N \textit{ then } P_F^{\langle \Gamma, \Delta, \Pi\rangle} \textit{ else } Q_F^{\langle \Gamma, \Delta, \Pi\rangle} & \textit{otherwise} \end{cases}$$

with F initially equals to $\{y_1, \ldots, y_\ell \mid \langle R_{u_i}, R, M, \mathsf{c}, y\rangle \in \Theta\}$.

[3] This model does not include the coalition strategies in which the target users and defending third parties are able to generate new data, initiate new sessions, establishing new secrets, etc.

Process $\mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)$ models the receiving behaviour of process R in the coalition. The coalition specifies which channel is use to receive data. The received data on a channel are referred to as a distinct fresh variable. The received data is sent out over a distinct private channel. The association of channels and variables is modelled in ξ. This sending behaviour is used for the process $R^{\langle \Gamma, \Delta, \Pi \rangle}$ to read the data when it is needed. Process $R^{\langle \Gamma, \Delta, \Pi \rangle}$ models the sending behaviour, substitution of terms, assignments of evaluations. F captures the variables which are in $\{y_1, \ldots, y_\ell\}$ and has not been read in yet.

Given a set of users R_U and a coalition specification $\langle \Theta, \Delta, \Pi \rangle$ for them, the coalition is now modelled as $R_U^{\langle \Theta, \Delta, \Pi \rangle} = \nu \Omega.(R_{u_1}^{\langle \Theta, \Delta, \Pi \rangle} \mid \cdots \mid R_{u_m}^{\langle \Theta, \Delta, \Pi \rangle})$ where $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$.

Remark. We extend the definition *hiding on channel* by Delaune et al. [14] to allow hiding on a set of channels. They define process R hiding channel c as $R^{\backslash (\mathsf{c}, \cdot)} = \nu \mathsf{c}.(R \mid !\mathsf{in}(\mathsf{c}, x))$. We extend this as follows.

Definition 9 (hiding on multiple channels)**.** *Given a process R and a set of channels $\tilde{\mathsf{c}} = \{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\}$, hiding on the set of channels is defined as $R^{\backslash (\tilde{\mathsf{c}}, \cdot)} = \nu \tilde{\mathsf{c}}.(R \mid !\mathsf{in}(\mathsf{c}_1, x_1) \mid \cdots \mid !\mathsf{in}(\mathsf{c}_n, x_\ell))$ ($x_1, \ldots, x_\ell \notin \mathsf{bv}(R) \cup \mathsf{fv}(R)$).*

4 Formalising the Privacy Notions

Based on the framework defined in Sect. 3, we formally define (enforced) privacy properties in the presence of third parties. Based on the formalisation of data-privacy (see Def. 4), we first define enforced-privacy where the target user collaborates with the adversary (Sect. 4.1). Taking attacking third parties into account, we define independency-of-privacy (Sect. 4.2) and independency-of-enforced-privacy (Sect. 4.3). Finally, we take defending third parties into account (Sect. 4.4), and define the identified corresponding coalition privacy properties (Sect. 4.4.1 to Sect. 4.4.4).

4.1 Enforced-privacy

Enforced-privacy is the unlinkability of a target user to his data even when the user collaborates with the adversary. Different collaborations impact privacy differently, so when we say a protocol satisfies enforced-privacy, it always refers to a specific collaboration specification.

As in receipt-freeness and coercion-resistance [14], the target user's privacy is considered to be satisfied, when the target user is able to lie about his target data, and the adversary cannot tell whether he has lied. Thus, when a protocol P_w satisfies enforced-privacy w.r.t. a target data τ (which belongs to role R_i) and a collaboration specification $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ defined on process $\hat{R}_i$ (where $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$), there exists a process P_f for the target user to execute, such that the adversary cannot distinguish between real collaboration with $\tau = \mathtt{t}_1$ and fake collaboration (by means of process P_f) with $\tau = \mathtt{t}_2$.[4]

Definition 10. *A well-formed protocol P_w satisfies enforced-privacy (*epriv*) w.r.t. τ and $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, if there exists a closed plain process P_f such that for any context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}]$, we have*

$$1.\ \mathcal{C}[P_f]^{\backslash (\mathsf{c}_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\},$$
$$2.\ \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]],$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ is a collaboration specification defined on $\hat{R}_i$, and t is a free name representing a piece of data.

The behaviour of the collaborating target user is modelled as $\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}$. The behaviour of the adversary in the collaboration is implicitly modelled as Q in the context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$. Thus a specific collaboration is modelled as $\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]$. Note that sometimes the target data in the collaboration is not decided by $\{t/\tau\}$, but by the context $\mathcal{C}[\_]$. Thus, the instantiation of the target data with a specific data $\mathtt{t}_1$ is modelled as the equivalence relation $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}]$. The first equivalence shows that even if the context $\mathcal{C}[\_]$ is able to decide the target data, the target user can still actually instantiate the target data with $\mathtt{t}_2$ by executing the process P_f. The second equivalence shows that the adversary cannot distinguish the target user following the collaboration in process $\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}$ from executing the process P_f, in the context of the adversary collaboration $\mathcal{C}[\_]$.

4.2 Independency-of-privacy

Next, we account for attacking third parties. Based on data-privacy, we define independency-of-privacy to capture privacy when a set of third parties collaborate with the adversary. As different sets of third parties may differently influence the target user's privacy, and since different collaboration amongst the same third parties leads to different privacy properties, independency-of-privacy is defined with respect to a set of third parties and a collaboration specification between them and the adversary.

[4] In the epistemic notion of coercion-resistance, enforced-privacy can be defined as the existence of a *counter-strategy* for the target user to achieve his own goal, but the adversary cannot distinguish it from the target user following the adversary's instructions [28].

Definition 11 (third parties)**.** *Given a well-formed protocol P_w and an instance of the target user $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$, a set of third parties is defined as a set of users $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$ where $\forall i \in \{1, \cdots, m\}, R_{u_i} \neq \hat{R}_i\{\mathsf{id}/id, t/\tau\}$. We use R_T to denote a set of attacking third parties and R_D to denote a set of defending third parties.*

The collaboration between a set of attacking third parties R_T and the adversary is expressed as a collaboration specification $\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle$ defined on process R_T. The behaviour of the third parties in the collaboration is modelled as $R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}$.

Inspired by the formal definitions of independency-of-prescribing-privacy [18] and vote-independence [20], independency-of-privacy is defined as follows: a well-formed protocol P_w satisfies independency-of-privacy w.r.t. $\tau \in \mathsf{bn}(R_i)$ and $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle)$, if the adversary cannot distinguish the honest target user executing role R_i with $\tau = \mathtt{t}_1$ from the same user with $\tau = \mathtt{t}_2$, even when the set of third parties R_T collaborates with the adversary according to collaboration specification $\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle$.

Definition 12. *A well-formed protocol P_w satisfies independency-of-privacy (*ipriv*) w.r.t. data τ and attacking third parties $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle)$ if*

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}],$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle$ is a collaboration specification of process R_T.

Process $R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}$ models collaboration between R_T and the adversary. If the equivalence holds, then despite this collaboration, adversary cannot distinguish $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}$ in which the target user uses $\tau = \mathtt{t}_1$ from $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}$ in which the target user uses $\tau = \mathtt{t}_2$.

4.3 Independency-of-enforced-privacy

We define independency-of-enforced-privacy (iepriv for short) based on enforced-privacy in a similar fashion as independency-of-privacy. As iepriv combines enforced-privacy and independency-of-privacy, it depends on target data and collaboration. More precisely, iepriv of a protocol P_w is defined w.r.t. target data $\tau \in \mathsf{bn}(R_i)$, a collaboration specification $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$ defined on process $\hat{R}_i$ with $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, and a set of attacking third parties together with a collaboration specification defined on the third parties processes $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle)$. A well-formed protocol P_w satisfies iepriv w.r.t. $\tau, \langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$, and $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle)$, if there exists a closed plain process P_f for the target user to execute, such that, despite the help of third parties R_T according to $\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle$, the adversary cannot distinguish between the target user collaborating with $\tau = \mathtt{t}_1$, and him really using $\tau = \mathtt{t}_2$ but faking collaboration for $\tau = \mathtt{t}_1$ by P_f.

Definition 13. *A well-formed protocol P_w satisfies independency-of-enforced-privacy (*iepriv*) w.r.t. data τ, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$, and $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle)$, if there exists a closed plain process P_f, such that for any $\mathcal{C}[\_] = \nu\mathtt{c}_{out}.\nu\mathtt{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T]$, we have*

1. $\mathcal{C}[P_f]^{\backslash(\mathtt{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}$,
2. $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}]$,

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$ is a collaboration specification for $\hat{R}_i$, t is a free name representing a piece of data, and $\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle$ is a collaboration specification of process R_T.

This definition mainly adds the collaboration of third parties $R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in}\rangle}$ to Def. 10.

4.4 Coalition privacy properties

In the previous sections, a third party user is considered as either neutral or attacking from the target user's point of view. In this section, we take into account third parties which cooperate with the target user to protect the target user's privacy. Corresponding to each privacy property defined above, we define coalition privacy properties which take into account defending third parties.

Definition 14 (defensive coalition)**.** *Given an instance of the target user $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$, a set of defending third parties R_D, and a coalition specification $\langle \Theta, \Delta, \Pi\rangle$ defined on $R_U = \hat{R}_i\{\mathsf{id}/id, t/\tau\} \mid R_D$, the coalition is modelled as $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id, t/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi\rangle}$ where $\Omega = \{\mathtt{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathtt{c}, y\rangle \in \Theta\}$. The target user's behaviour in the coalition is $\hat{R}_i\{\mathsf{id}/id, t/\tau\}^{\langle \Theta, \Delta, \Pi\rangle} = \nu\eta.((\hat{R}_i\{\mathsf{id}/id, t/\tau\})^{\langle \Gamma, \Delta, \Pi\rangle} |P_\gamma)$, where $\eta = \{\mathtt{c}'_i, \ldots, \mathtt{c}'_\ell\}$, $\Gamma = \{\langle \hat{R}_i\{\mathsf{id}/id, t/\tau\}, R_{u_j}, M, \mathtt{c}, y\rangle \mid \langle \hat{R}_i\{\mathsf{id}/id, t/\tau\}, R_{u_j}, M, \mathtt{c}, y\rangle \in \Theta\}$, $P_\gamma = \mathsf{in}(\mathtt{c}_1, y'_1).!\mathsf{out}(\mathtt{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathtt{c}_\ell, y'_\ell).!\mathsf{out}(\mathtt{c}'_\ell, y'_\ell)))$ with $\{y'_1, \ldots, y'_\ell\}$ being fresh variables, $\{\mathtt{c}_1, \ldots, \mathtt{c}_\ell\} = \{\mathtt{c} \mid \langle R_{u_i}, \hat{R}_i\{\mathsf{id}/id, t/\tau\}, M, \mathtt{c}, y\rangle \in \Theta\}$ and $\xi = \{(\mathtt{c}_1, y'_1, \mathtt{c}'_1), \ldots, (\mathtt{c}_\ell, y'_\ell, \mathtt{c}'_\ell)\}$. The third parties' behaviour in the coalition is modelled as $R_D^{\langle \Theta, \Delta, \Pi\rangle}$.*

4.4.1 Coalition-privacy

Intuitively, coalition-privacy means that a target user's privacy is preserved due to the cooperation of a set of defending third parties. A well-formed protocol P_w satisfies coalition-privacy w.r.t. $\tau \in \mathsf{bn}(R_i)$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$ ($\langle \Theta, \Delta, \Pi \rangle$ is defined on $\hat{R}_i \mid R_D$ where $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$), if the adversary cannot distinguish an honest user in role R_i using $\tau = \mathtt{t}_1$ from the user actually using $\tau = \mathtt{t}_2$ while helped by a set of defending third parties.

Definition 15. *A well-formed protocol P_w satisfies coalition-privacy (cpriv) w.r.t. data τ and coalition $(R_D, \langle \Theta, \Delta, \Pi \rangle)$ if*

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D] \approx_\ell \quad \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}],$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Theta, \Delta, \Pi \rangle$ is a coalition specification defined on $R_U = \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$, and $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$.

In the above definition, the coalition is modelled as $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}$, where the target user instantiates the target data with $\mathtt{t}_2$. The equivalence shows that the adversary cannot distinguish the target user instantiating the target data with $\mathtt{t}_2$ in the coalition from the target user instantiating the target data with $\mathtt{t}_1$. Thus, coalition-privacy captures privacy when there exists a set of third parties cooperating with the target user following a pre-defined coalition specification.

4.4.2 Coalition-enforced-privacy

Taking into account defending third parties, we define coalition-enforced-privacy based on enforced-privacy. As before, coalition-enforced-privacy specifies a target data τ and a collaboration specification of the target user $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$. As in coalition-privacy, coalition-enforced-privacy specifies a set of defending third parties R_D and a coalition specification $\langle \Theta, \Delta, \Pi \rangle$ as well. In coalition-enforced-privacy, the target user both cooperates with the adversary and defending third parties. Similar to enforced-privacy, we assume that the target user lies to the adversary if it is possible. We do not assume that the target user lies to the defending third parties, as they help the target user maintain privacy.

Intuitively, coalition-enforced-privacy means that a target user is able to lie to the adversary about his target data when helped by defending third parties – the adversary cannot tell whether the user lied. This property is modelled as the combination of coalition-privacy and enforced-privacy: a protocol P_w satisfies coalition-enforced-privacy w.r.t $\tau \in \mathsf{bn}(R_i), \langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, for $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ a collaboration specification defined on $\hat{R}_i$ with $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, and $\langle \Theta, \Delta, \Pi \rangle$ a coalition specification defined on the target user and R_D, if there exists a process P_f, such that the adversary cannot distinguish between genuine collaboration with $\tau = \mathtt{t}_1$ and faking collaboration using P_f with the help of the coalition for $\tau = \mathtt{t}_2$.

Definition 16. *A well-formed protocol P_w satisfies coalition-enforced-privacy (cepriv) w.r.t. data τ, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, if there exists a closed plain process P_f, such that for any $\mathcal{C}[\_] = \nu \mathtt{c}_{out}.\nu \mathtt{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D]$, we have*

$$\begin{array}{l} 1. \nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathtt{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi \rangle}, \\ 2. \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle})], \end{array}$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ is a collaboration specification defined on $\hat{R}_i$, t is a free name representing a piece of data, $\langle \Theta, \Delta, \Pi \rangle$ is a coalition specification defined on $R_U = \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$, $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$, $P_\gamma = \mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)))$ with $\{y'_1, \ldots, y'_\ell\}$ being fresh variables, $\{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R_{u_i}, \hat{R}_i\{\mathsf{id}/id, t/\tau\}, M, \mathsf{c}, y \rangle \in \Theta\}$, $\eta = \{\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell\}$ and $\xi = \{(\mathsf{c}_1, y'_1, \mathsf{c}'_1), \ldots, (\mathsf{c}_\ell, y'_\ell, \mathsf{c}'_\ell)\}$.

The collaboration between the target user and the adversary instantiating the target data with $\mathtt{t}_1$ is modelled by the equivalence $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}]$. The target user's actual behaviour of instantiating the target data with $\mathtt{t}_2$ in process P_f is modelled as the first equivalence. The second equivalence shows that the adversary cannot distinguish the process in which the target user follows the collaboration with the adversary from the process in which the target user lies to the adversary with the help of defending third parties.

4.4.3 Coalition-independency-of-privacy

Similarly, we define coalition-independency-of-privacy with respect to a target data τ, a set of attacking third parties with a collaboration specification $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle)$, and a set of defending third parties R_D with a coalition specification $\langle \Theta, \Delta, \Pi \rangle$. Note that we require that there is no intersection between attacking third parties and defending third parties, i.e., $R_T \cap R_D = \emptyset$, as we assume a third party cannot be both attacking and defending at the same time. A well-formed protocol P_w satisfies coalition-independency-of-privacy w.r.t. $\tau, (R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, if the adversary, even with the collaboration of a set of attacking third parties, cannot distinguish the target user instantiating $\tau = \mathtt{t}_1$ from the target user actually instantiating $\tau = \mathtt{t}_2$ in the coalition with the help of defending third parties.

Definition 17. *A well-formed protocol P_w satisfies coalition-independency-of-privacy (*cipriv*) w.r.t. data τ, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, and $(R_D, \langle \Theta, \Delta, \Pi\rangle)$, if*

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell \quad \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi\rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}],$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification of process R_T, and $\langle \Theta, \Delta, \Pi\rangle$ is a coalition specification defined on $R_U = \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$, $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$.

4.4.4 Coalition-independency-of-enforced-privacy

Finally, we consider the case combining all situations together: the target user collaborates with the adversary following $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, a set of attacking third parties R_T collaborate with the adversary following $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$, and a set of defending third parties R_D and a coalition $\langle \Theta, \Delta, \Pi\rangle$). We formally define coalition-independency-of-enforced-privacy below.

Definition 18. *A well-formed protocol P_w satisfies coalition-independency-of-enforced-privacy (*$\mathsf{ciepriv}$*) w.r.t. data τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi\rangle)$, if there exists a closed plain process P_f such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T \mid R_D]$, we have*

$$\begin{aligned}
&1.\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \Theta, \Delta, \Pi\rangle},\\
&2.\ \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]\\
&\quad \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}],
\end{aligned}$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ is a collaboration specification defined on $\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification defined on R_T, $\langle \Theta, \Delta, \Pi\rangle$ is a coalition specification defined on $R_U = \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$, t is a free name representing a piece of data, $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$, $P_\gamma = \mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)))$ with $\{y'_1, \ldots, y'_\ell\}$ being fresh variables, $\{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R_{u_i}, \hat{R}_i\{\mathsf{id}/id, t/\tau\}, M, \mathsf{c}, y\rangle \in \Theta\}$, $\eta = \{\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell\}$ and $\xi = \{(\mathsf{c}_1, y'_1, \mathsf{c}'_1), \ldots, (\mathsf{c}_\ell, y'_\ell, \mathsf{c}'_\ell)\}$.

Remark. Each of the defined coalition privacy properties, namely cpriv, cepriv, cipriv or $\mathsf{ciepriv}$, must specify a coalition (the set of defending third parties and the coalition specification). In a protocol, a target user's privacy may be preserved or enforced with the help of different coalitions. We can formulate the coalition privacy properties by requiring the existence of such coalitions. This leads to a more general version of coalition privacy properties, where the coalition is not specified. The general version of a coalition privacy property can be easily deduced from its corresponding specific property. For instance, a generic cpriv can be defined as the existence of a set of defending third parties R_D and a coalition specification $\langle \Theta, \Delta, \Pi\rangle$, such that coalition-privacy is preserved. The general version of coalition privacy properties allow us to reason about the existence of a coalition (a strategy) such that a user's privacy is preserved. How to find such a coalition is an interesting topic for studying coalition privacy properties.

5 Relations between the Privacy Notions

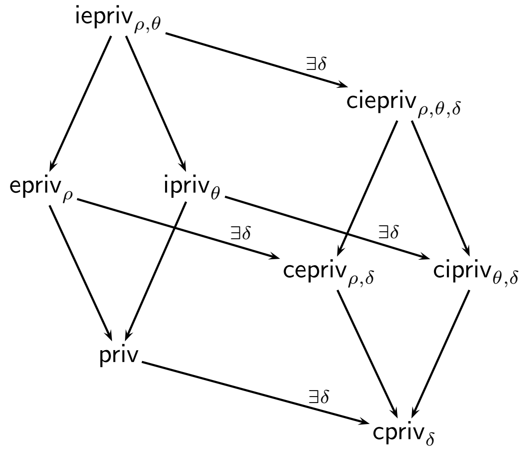
We show the relations between the privacy properties in Fig. 2: we use ρ to denote the specification of a target user's collaboration with the adversary $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, θ to denote the specification of a set of attacking third parties and their collaboration with the adversary $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, and δ to denote the specification of a set of defending third parties and their coalition with the target user $(R_D, \langle \Theta, \Delta, \Pi\rangle)$.

The left diamond in Fig. 2 shows the relations between privacy properties which do not consider defending third parties while the right diamond shows the relations between privacy properties which consider defending third parties. In the left diamond, epriv_ρ and ipriv_θ are stronger than priv, meaning that if a protocol satisfies epriv_ρ or ipriv_θ, then the protocol satisfies priv. Intuitively, if the adversary cannot break privacy with the help from the target user (in epriv_ρ) or from a set of attacking third parties (in ipriv_θ), the adversary cannot break privacy without any help (in priv). Similarly, if the adversary cannot break privacy with the help from both target user and attacking third parties (in $\mathsf{iepriv}_{\rho,\theta}$), the adversary cannot break privacy with the help from only one of them (in epriv_ρ and ipriv_θ). Thus, $\mathsf{iepriv}_{\rho,\theta}$ is stronger than both enforced-privacy$_\rho$ and ipriv_θ. This is described as Thm. 1.

Theorem 1. *(1) $\forall\theta$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{epriv}_\rho$, (2) $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$, (3) $\forall\rho$, $\mathsf{epriv}_\rho \implies \mathsf{priv}$, and (4) $\forall\theta$, $\mathsf{ipriv}_\theta \implies \mathsf{priv}$.*

Proof sketch: The proof of $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$ and $\forall\rho$, $\mathsf{epriv}_\rho \implies \mathsf{priv}$ follows the strategy of how to prove coercion-resistance $\implies$ receipt-freeness $\implies$ vote-privacy given by Delaune et al. [14]. For all ρ, when a protocol satisfies epriv_ρ, for an adversary context $\mathcal{C}[\_]$, three equivalences in Def. 10 hold. From the equivalences, we can deduce that $\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]]$. By applying the evaluation context $\nu\mathsf{c}_{out}.(\_ \ |!\mathsf{in}(\mathsf{c}_{out}, x))$ on both side of the equivalence, we prove that $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)}]$. Because of the first equivalence in Def. 10: $\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}$, we deduce the equivalence $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}]$. This coincides with the equivalence in Def. 4. Thus we prove that $\forall\rho$, $\mathsf{epriv}_\rho \implies \mathsf{priv}$. Similarly we prove $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$.

Figure 2: Relations of the privacy notions



$\forall\theta$, $\mathsf{ipriv}_\theta \Longrightarrow \mathsf{priv}$ can be proved as follows: for an adversary context $\mathcal{C}[\_] = \nu \mathsf{c}^t_{out}.\nu \mathsf{c}^t_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset \wedge \mathcal{C}_{P_w}[\mathcal{C}[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}_{P_w}[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]$), we show that $\mathsf{ipriv}_\theta \Longrightarrow \mathsf{priv}$. By applying $\mathcal{C}[\_]$ and the evaluation context $\nu \mathsf{c}^t_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}^t_{out}, x))$ on both side of the equivalence in Def. 12, we have $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_T]$. By applying rule $!P \equiv P \mid !P$, the third parties' behaviour R_T is absorbed by the environment. Thus, the equivalence in Def. 4 is satisfied. Similarly reasoning holds for proving $\forall\theta$, $\mathsf{iepriv}_{\rho,\theta} \Longrightarrow \mathsf{epriv}_\rho$. Precise proofs are available in the technical report [19]. $\square$

Moreover, the implication relations in Thm. 1 are uni-directional, in the sense that we can disprove the opposite directions by presenting counter-examples (see details in [19]). We can apply the same technique to prove the relations in the right diamond. Thus we have the following theorem.

Theorem 2. *(1)* $\forall\theta$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cepriv}_{\rho,\delta}$, *(2)* $\forall\rho$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cipriv}_{\theta,\delta}$, *(3)* $\forall\rho$, $\mathsf{cepriv}_{\rho,\delta} \Longrightarrow \mathsf{cpriv}_\delta$, *and (4)* $\forall\theta$, $\mathsf{cipriv}_{\theta,\delta} \Longrightarrow \mathsf{cpriv}_\delta$.

Each privacy property in the left diamond has a weaker corresponding property in the right diamond, meaning that if a protocol satisfies a privacy property in the left diamond, there exists a coalition such that the property satisfies the corresponding coalition privacy property in the right diamond. Intuitively, if a protocol preserves privacy of a target user without any help from third parties, the protocol can still preserve his privacy with the help from others.

Theorem 3. *(1)* $\mathsf{ciepriv}_{\rho,\theta} \Longrightarrow \exists\delta$, $\mathsf{ciepriv}_{\rho,\theta,\delta}$, *(2)* $\mathsf{epriv}_\rho \Longrightarrow \exists\delta$,$\mathsf{cepriv}_{\rho,\delta}$, *(3)* $\mathsf{ipriv}_\theta \Longrightarrow \exists\delta$, $\mathsf{cipriv}_{\theta,\delta}$, *and (4)* $\mathsf{priv} \Longrightarrow \exists\delta$, cpriv_δ.

Proof sketch: When a protocol satisfies priv, the equivalence in Def. 4 holds. It is easy to see that the equivalence in Def. 4 coincides with the one in Def. 15 when the coalition is set empty. The same reasoning holds for proving other relations in the theorem. $\square$

Generally, given a set of defending third parties R_D, when a protocol satisfies priv, the requirement that the protocol also satisfies cpriv_δ is $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$. When the coalition is of the form $\langle\Theta, \emptyset, \emptyset\rangle$, this requirement is satisfied. However, not all coalition specifications defined on R_D can satisfy the requirement. Therefore, even when a protocol satisfies priv, some coalition specification may fail to satisfy cpriv_δ. The observation holds for other relations in Thm. 3 as well.[5]

Remark. Dreier et al. [22] build a hierarchy of privacy notions, using a modular approach, in voting considering the following dimensions: 1) No communication between the target user and the adversary, target voter forwarding information or interactive communication (coercion). The latter two cases can be instantiated by a collaboration specification. 2) All other voters are neutral, or a voter is controlled by the adversary. The second case can be instantiated as a third party collaboration specification. 3) The adversary knows any behaviour of the counterbalancing voter, or the adversary knows some behaviour of the counterbalancing voter. These two cases can be instantiated by third party collaboration. 4) The target voter is forced to abstain or not. The forced-abstain-attack is not considered in our hierarchy, since we focus on data privacy, not behavioural privacy. In addition, as stated by Jonker and Pang [24], forced abstention is trivial if the adversary has a full view of the network. We do cover *forced vote spoiling* [24] where the adversary forces the voter to produce an invalid ballot. In summary, the vote-privacy notions in the hierarchy of [22] (except for forced abstention) are instances of cpriv, cipriv, cepriv and $\mathsf{ciepriv}$. Thus, our hierarchy is more general as well as domain-independent.

6 Discussion

In this section, we briefly show that several existing domain-specific privacy properties can be instantiated as one of our privacy properties. Then, we show some directions to further extend the privacy properties. For details, see [19].

[5] Note that the requirement '$\exists\delta$' makes the coalition privacy properties in Thm. 3 coincide with their general extensions as discussed previously in Sect. 4.4.

6.1 Application

Privacy notions modelled as strong secrecy can be captured by data-privacy. For instance, anonymity [3] is data-privacy where the target data is a user's identity. Various domain-specific properties, which capture privacy in domains where data-privacy is too strong to be satisfied, can be instantiated by coalition-privacy. For instance, bidding-privacy [16] in sealed-bid e-auctions is defined as the adversary cannot determine a bidder's bidding-price, assuming the existence of a winning bid. This can be instantiated as coalition-privacy where the target data is a bid, the defending third party is the winning bidder and the coalition specification is $\langle\emptyset,\emptyset,\emptyset\rangle$. Vote-privacy [27] is defined as the adversary cannot determine a voter's vote with the existence of a counter-balancing voter. This can be instantiated as coalition-privacy where the target data is a vote, the defending third party is the counter-balancing voter and the coalition specification is $\langle\emptyset,\Delta,\emptyset\rangle$ where the substitution Δ specifies how to replace the counter-balancing voter's vote.

Enforced privacy notions like receipt-freeness or coercion-resistance can be captured by either enforced-privacy or coalition-enforced-privacy. Receipt-freeness [14] in voting can be instantiated by coalition-enforced-privacy, where the target data and the coalition are the same as in vote-privacy, and the collaboration specification is $\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$ where Ψ contains all private terms generated and read-in in the target voter process. In a similar way, coercion-resistance [14] in voting is an instance of coalition-enforced-privacy.

The two independency of privacy properties, i.e., independency-of-prescribing-privacy and independence-vote-privacy are instances of coalition-independency-of-privacy. For example, independence-vote-privacy [20] can also be considered as an instance of coalition-independency-of-privacy, where the target data and the coalition are the same as in vote-privacy, the set of attacking third parties is a third voter, and the collaboration specification of the third voter is $\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$ where Ψ are all generated and read-in terms in the third voter process.

6.2 Extension

Each property in the hierarchy can be instantiated in many different forms by specifying the parameters of the property (such as target data, collaboration, coalition). Furthermore, only the target user is allowed to lie to the adversary – we do not consider lying third parties. This can happen when third parties are coerced to collaborate with the adversary. By sharing their real information, the third parties' privacy may be broken. To protect their own privacy, third parties may lie as well. For example, in social networks, it is desirable that a user can lie to the adversary about the link between the identity and pseudonym of his friends [4]. This requirement aims to protect the unlinkability of identity and pseudonym of the user's friend. The coerced user is considered as a third party and he is assumed to lie to the adversary. Such a property can be formalised like enforced-privacy: if there exists a process P_f in which a coerced (collaboration specification $\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle$) third party R_t is able to lie such that the adversary cannot tell whether he lied or not, then the protocol enforces the target user's privacy. Formally, $\mathcal{C}_{P_w}[R_t^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle} \mid \hat{R}_i\{\mathsf{id}/id_i,\mathsf{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[P_f \mid \hat{R}_i\{\mathsf{id}/id_i,\mathsf{t}_2/\tau\}]$. Other properties, such as ipriv, iepriv, cipriv and ciepriv, can be extended in a similar way.

7 Conclusion and Future Work

In this paper, we have identified (enforced) privacy notions in the presence of third parties. We formalised the collaboration of users, including the target user and attacking third parties, with the adversary and the coalition among users (the target user with defending third parties) in a generic way. The identified privacy notions are formally defined in the applied pi calculus. We presented the relations among the properties as a privacy hierarchy. We also showed that various existing privacy properties in the literature can be instantiated as one of the properties in the hierarchy.

We have already mentioned a few interesting research directions in the paper, for example, how to find a coalition and synthesize strategy for the coalition to satisfy some coalition privacy properties for a protocol, and how to extend our privacy hierarchy to capture situations where a third party is coerced but has a strategy to lie to the adversary. One important future work is to apply our privacy notions to real-world applications such as online social networks.

Acknowledgements

Naipeng Dong is supported by a grant from the Fonds National de la Recherche (Luxembourg).

References

[1] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. 28th Symposium on Principles of Programming Languages*, pages 104–115. ACM Press, 2001.

[2] M. Abe and K. Suzuki. Receipt-free sealed-bid auction. In *Proc. 5th Conference on Information Security*, volume 2433 of *LNCS*, pages 191–199. Springer, 2002.

[3] M. Arapinis, T. Chothia, E. Ritter, and M. D. Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proc. 23rd IEEE Computer Security Foundations Symposium*, pages 107–121. IEEE CS, 2010.

[4] M. Backes, M. Maffei, and K. Pecina. A security API for distributed social networks. In *Proc. 17th Network and Distributed System Security Symposium*. The Internet Society, 2011.

[5] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *Proc. 26th Symposium on Theory of Computing*, pages 544–553. ACM Press, 1994.

[6] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. 14th IEEE Computer Security Foundations Workshop*, pages 82–96. IEEE CS, 2001.

[7] B. Blanchet. Automatic proof of strong secrecy for security protocols. In *Proc. 25th IEEE Symposium on Security and Privacy*, pages 86–100. IEEE CS, 2004.

[8] B. Blanchet, M. Abadi, and C. Fournet. Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008.

[9] J. Bohli and A. Pashalidis. Relations among privacy notions. *ACM Transactions on Information and System Security*, 14(1):4:1–4:24, 2011.

[10] R. Chadha, S. Kremer, and A. Scedrov. Formal analysis of multi-party contract signing. In *Proc. 17th IEEE Computer Security Foundations Workshop*, pages 266–279. IEEE CS, 2004.

[11] V. Cheval and B. Blanchet. Proving more observational equivalences with ProVerif. In *Proc. 2nd Conference on Principles of Security and Trust*, LNCS. Springer, 2013. To appear.

[12] Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for anonymous location based services. In *Proc. Joint Workshop on Theory of Security and Applications*, volume 6993 of *LNCS*, pages 98–112. Springer, 2011.

[13] B. De Decker, M. Layouni, H. Vangheluwe, and K. Verslype. A privacy-preserving eHealth protocol compliant with the Belgian healthcare system. In *Proc. 5th European Workshop on Public Key Infrastructures, Services and Application*, volume 5057 of *LNCS*, pages 118–133. Springer, 2008.

[14] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, 2009.

[15] D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[16] N. Dong, H. L. Jonker, and J. Pang. Analysis of a receipt-free auction protocol in the applied pi calculus. In *Proc. 7th Workshop on Formal Aspects in Security and Trust*, volume 6561 of *LNCS*, pages 223–238. Springer, 2011.

[17] N. Dong, H. L. Jonker, and J. Pang. Challenges in eHealth: From enabling to enforcing privacy, 2012.

[18] N. Dong, H. L. Jonker, and J. Pang. Formal analysis of privacy in an eHealth protocol. In *Proc. 17th European Symposium on Research in Computer Security*, volume 7459 of *LNCS*, pages 325–342. Springer, 2012.

[19] N. Dong, H. L. Jonker, and J. Pang. Enforcing privacy in the presence of others: Notions, formalisations and relations. Technical report, University of Luxembourg, 2013. Report is available at `http://satoss.uni.lu/projects/epriv/`.

[20] J. Dreier, P. Lafourcade, and Y. Lakhnech. Vote-independence: A powerful privacy notion for voting protocols. In *Proc. 4th Workshop on Foundations & Practice of Security*, volume 6888 of *LNCS*, pages 164–180. Springer, 2011.

[21] J. Dreier, P. Lafourcade, and Y. Lakhnech. Defining privacy for weighted votes, single and multi-voter coercion. In *Proc. 17th European Symposium on Research in Computer Security*, volume 7459 of *LNCS*, pages 451–468. Springer, 2012.

[22] J. Dreier, P. Lafourcade, and Y. Lakhnech. A formal taxonomy of privacy in voting protocols. In *Proc. International Conference on Communications*, pages 6710–6715. IEEE CS, 2012.

[23] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In *Proc. Advances in Cryptology–AUSCRYPT'92*, volume 718 of *LNCS*, pages 244–251. Springer, 1992.

[24] H. L. Jonker and J. Pang. Bulletin boards in voting systems: Modelling and measuring privacy. In *Proc. 6th Conference on Availability, Reliability and Security*, pages 294–300. IEEE CS, 2011.

[25] H. L. Jonker, J. Pang, and S. Mauw. A formal framework for quantifying voter-controlled privacy. *Journal of Algorithms in Cognition, Informatics and Logic*, 64(2-3):89–105, 2009.

[26] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *Proc. 4th ACM Workshop on Privacy in the Electronic Society*, pages 61–70. ACM Press, 2005.

[27] S. Kremer and M. D. Ryan. Analysis of an electronic voting protocol in the applied pi calculus. In *Proc. 14th European Symposium on Programming*, volume 3444 of *LNCS*, pages 186–200. Springer, 2005.

[28] R. Küsters and T. Truderung. An epistemic approach to coercion-resistance for electronic voting protocols. In *Proc. 30th IEEE Symposium on Security and Privacy*, pages 251–266. IEEE CS, 2009.

[29] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *Proc. Information Security and Cryptology–ICISC'03*, volume 2971 of *LNCS*, pages 245–258. Springer, 2003.

[30] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Proc. 2nd Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, volume 1055 of *LNCS*, pages 147–166. Springer, 1996.

[31] T. Okamoto. An electronic voting scheme. In *IFIP World Conference on IT Tools*, pages 21–30, 1996.

[32] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[33] T. van Deursen, S. Mauw, and S. Radomirović. Untraceability of RFID protocols. In *Proc. 2nd Workshop on Information Security Theory and Practices*, volume 5019 of *LNCS*, pages 1–15. Springer, 2008.

Theorem 1. *If $A \approx_\ell B$ and $B \approx_\ell C$, then $A \approx_\ell C$.*

Theorem 2. *If $A \equiv B$ and $C \equiv D$, and $A \approx_\ell C$ then $B \approx_\ell D$.*

Theorem 3. *Let Q be a closed plain process and c_{out} be a channel name such that $\mathsf{c}_{out} \notin \mathsf{fn}(Q) \cup \mathsf{bn}(Q)$. Let $\mathcal{C}_h[\_] = \nu \mathsf{c}_{out}.(\_ \mid \mathsf{in}(\mathsf{c}_{out}, x))$. We have $Q^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle \backslash (\mathsf{c}_{out}, \cdot)} = \nu \mathsf{c}_{out}.(Q^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \mid \mathsf{in}(\mathsf{c}_{out}, x)) \approx_\ell Q$ [14]*

Corollary 1. *Let Q be a closed plain process and $\langle \Gamma, \emptyset, \emptyset \rangle$ be a coalition defined on Q where Γ represents terms Q forwarding to others. Information in Γ is sent on a set of channels μ. $\mu = \{\mathsf{c}_1, \dots, \mathsf{c}_n\} = \{\mathsf{c} \mid \langle Q, R_{u_j}, M, \mathsf{c}, y \rangle \in \Gamma\}$ such that $\mathsf{c}_i \notin \mathsf{fn}(Q) \cup \mathsf{bn}(Q)$. Let $\mathcal{C}_h[\_] = \nu \mu.(\_ \mid !\mathsf{in}(\mathsf{c}_1, x_1) \mid \cdots \mid !\mathsf{in}(\mathsf{c}_n, x_n))$ ($x_1, \dots, x_n \notin \mathsf{bv}(R) \cup \mathsf{fv}(R)$). We have $Q^{\langle \Gamma, \emptyset, \emptyset \rangle \backslash (\mu, \cdot)} = \nu \mu.(Q^{\langle \Gamma, \emptyset, \emptyset \rangle} \mid !\mathsf{in}(\mathsf{c}_1, x_1) \mid \cdots \mid !\mathsf{in}(\mathsf{c}_n, x_\ell)) \approx_\ell Q$*

This can be proved by applying Thm. 3 multiple times.

Theorem 4. *Let $\mathcal{C}_1[\_] = \nu \widetilde{u_1}.(\_ \mid B_1)$ and $\mathcal{C}_2[\_] = \nu \widetilde{u_2}.(\_ \mid B_2)$ be two evaluation contexts such that $\widetilde{u_1} \cap (\mathsf{fv}(B_2) \cup \mathsf{fv}(B_2)) = \emptyset$ and $\widetilde{u_2} \cap (\mathsf{fv}(B_1) \cup \mathsf{fv}(B_1)) = \emptyset$. We have that $\mathcal{C}_1[\mathcal{C}_2[A]] \equiv \mathcal{C}_2[\mathcal{C}_1[A]]$ for any extended process A [14].*

Theorem 5. *Let $A \mid B$ be a process, c be a channel name in A, c never appears in B. $(A \mid B)^{\backslash (\mathsf{c}, \cdot)} \equiv A^{\backslash (\mathsf{c}, \cdot)} \mid B$.*

Proof.

$$(A \mid B)^{\backslash (\mathsf{c}, \cdot)} = \nu \mathsf{c}.((A \mid B) \mid !\mathsf{in}(\mathsf{c}, x))$$
$$A^{\backslash (\mathsf{c}, \cdot)} \mid B = (\nu \mathsf{c}.(A \mid !\mathsf{in}(\mathsf{c}, x))) \mid B$$

Since c never appears in B, we have (rule `NEW-PAR`)

$$(\nu \mathsf{c}.(A \mid !\mathsf{in}(\mathsf{c}, x))) \mid B \equiv \nu \mathsf{c}.((A \mid !\mathsf{in}(\mathsf{c}, x)) \mid B),$$

Because of rule `PAR-C` and rule `PAR-A`, we have

$$(A \mid B) \mid !\mathsf{in}(\mathsf{c}, x) \equiv A \mid !\mathsf{in}(\mathsf{c}, x) \mid B,$$

Thus,

$$\nu \mathsf{c}.((A \mid B) \mid !\mathsf{in}(\mathsf{c}, x)) \equiv \nu \mathsf{c}.((A \mid !\mathsf{in}(\mathsf{c}, x)) \mid B).$$

By transitivity of structural equivalence, we have

$$(A \mid B)^{\backslash (\mathsf{c}, \cdot)} \equiv A^{\backslash (\mathsf{c}, \cdot)} \mid B.$$

□

A Thm. 1

(3) $\forall \rho$, $\mathsf{epriv}_\rho \Longrightarrow \mathsf{priv}$

We prove the statement in the following two directions: 1. $\forall \rho$, $\mathsf{epriv}_\rho \Longrightarrow \mathsf{priv}$ 2. $\exists \rho$, $\mathsf{priv} \not\Longrightarrow \mathsf{epriv}_\rho$

1. $\forall \rho$, when a protocol satisfies epriv_ρ, we prove that the protocol also satisfies priv.

   For a collaboration $\rho = \langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, when a well-formed protocol P_w satisfies epriv w.r.t. τ and $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
   eq1:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}],$$
   we have
   eq2:
   $$\mathcal{C}[P_f]^{\backslash (\mathsf{c}_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\},$$
   and
   eq3:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]].$$

   1) According to Lemma 1 (transitivity of $\approx_\ell$), combining (`eq1`) and (`eq3`), we have
   eq4:
   $$\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]].$$

   2) By applying the evaluation context $\mathcal{C}_h[\_] = \nu \mathsf{c}_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}_{out}, x))$ (x is a fresh variable) on both sides of (`eq4`), we have
   eq5:
   $$\mathcal{C}_h[\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}]] \approx_\ell \mathcal{C}_h[\mathcal{C}_{P_w}[\mathcal{C}[P_f]]].$$

3) According to Lemma 4, by swapping position of context $\mathcal{C}_h[\_]$ and $\mathcal{C}_{P_w}[\_]$, the left side of ($\texttt{eq5}$) is structural equivalent to

$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}]],$$

and the right side of ($\texttt{eq5}$) is structural equivalent to $\mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}[P_f]]]$. According to Lemma 2, the above two processes are bisimilar, that is

eq6:

$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}[P_f]]].$$

4) By Lemma 3, we have the following equivalence

$$\mathcal{C}_h[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}] \approx_\ell \hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}.$$

By applying the context $\mathcal{C}_{P_w}[\_]$ on both sides of the above equivalence, we have

eq7:

$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}].$$

That is, the left side of ($\texttt{eq6}$) is equivalent to $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}]$.

5) By Lemma 3, we have $\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} = \mathcal{C}_h[\mathcal{C}[P_f]]$. Thus, we can replace the process $\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)}$ in ($\texttt{eq2}$) with $\mathcal{C}_h[\mathcal{C}[P_f]]$. That is, $\mathcal{C}_h[\mathcal{C}[P_f]] \approx_\ell \hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\}$. By applying context $\mathcal{C}_{P_w}[\_]$ on both sides of the above equivalence, we have

eq8:

$$\mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}[P_f]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\}].$$

That is, the right side of ($\texttt{eq6}$) is equivalent to $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\}]$.

6) According to Lemma 2, combining ($\texttt{eq6}$), ($\texttt{eq7}$) and ($\texttt{eq8}$), we have

eq9:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\}].$$

The equivalence ($\texttt{eq9}$) coincides with the equivalence in Def. 4. Thus, the protocol P_w satisfies priv. □

2. There exists ρ such that $\mathsf{priv} \not\Longrightarrow \mathsf{epriv}_\rho$.

   We prove the statement by showing an example in which a protocol satisfies priv but not epriv_ρ for some ρ as in Ex. 1.

   Example 1. *Protocol $Q = \nu r.\nu s.\mathsf{out}(c,\mathsf{enc}(s,r))$ where c is a public channel, satisfies* priv *w.r.t. s, but not* epriv *w.r.t. s and $\langle\{r\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$. The adversary cannot distinguish $\mathsf{enc}(s_1,r)$ and $\mathsf{enc}(s_2,r)$, thus the protocol satisfies* priv *w.r.t s. However, when Q is coerced to reveal r, there is no way for Q to cheat the adversary. Because of the perfect encryption assumption, any other nonce cannot be used to decypted $\mathsf{enc}(s,r)$, thus, the adversary will find out whether the user lied.*

(4) $\forall\theta$, $\mathsf{ipriv}_\theta \Longrightarrow \mathsf{priv}$

Note that in ipriv_θ, we assume the existence of a set of attacking third parties R_T. Thus, when we consider priv, we have the same assumption that there exists the same set of third parties R_D.

We prove the statement in the following two directions: 1. $\forall\theta$, $\mathsf{ipriv}_\theta \Longrightarrow \mathsf{priv}$ 2. $\exists\theta$, $\mathsf{priv} \not\Longrightarrow \mathsf{ipriv}_\theta$

1. $\forall\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a protocol satisfies ipriv_θ, we prove that the protocol also satisfies priv with the existence of R_T.

   For a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a well-formed protocol P_w satisfies ipriv w.r.t. τ and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, the following equivalence holds.

   eqi1:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\} \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\} \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

   Similar as in definitions of enforced privacy properties like epriv, we separate the adversary's ability of coercing from distinguishing differences of two processes, and model the ability of providing information for collaborating users as a context. Since for all contexts of the adversary which provides information for the collaborating third parties, the protocol satisfies ipriv_θ, thus, for the following context $\mathcal{C}_t[\_]$, which supplies information needed by the collaborating third parties, the protocol satisfies ipriv_θ.

$$\mathcal{C}_t[\_] = \nu\mathsf{c}^t_{out}.\nu\mathsf{c}^t_{in}.(\_ \mid Q)$$

   satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}_t[\_]) = \emptyset$ and

   eqi2:

$$\mathcal{C}_t[R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell R_T^{\langle \Psi^t,\emptyset,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle},$$

   2) By applying the context $\mathcal{C}_t[\_]$ on both sides of ($\texttt{eqi1}$), we have

   eqi3:

$$\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_1}/\tau\} \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i,\mathtt{t_2}/\tau\} \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]].$$

3) By applying the evaluation context $\mathcal{C}_h^t[\_] = \nu \mathsf{c}_{out}^t.(\_ \mid \mathsf{in}(\mathsf{c}_{out}^t, x))$ (x is a fresh variable), on both sides of (eqi3), we have
eqi4:
$$\mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$
4) According to Lemma 4, by swapping contexts $\mathcal{C}_h^t[\_]$ and $\mathcal{C}_{P_w}[\_]$, the left side of (eqi4) is structural equivalent to

$$\mathcal{C}_{P_w}[\mathcal{C}_h^t[\mathcal{C}_t[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]]$$

That is,
eqi5:
$$\mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \equiv \mathcal{C}_{P_w}[\mathcal{C}_h^t[\mathcal{C}_t[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]]$$
Since c_{out}^t and c_{in}^t are fresh channel names, they do not appear in $\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}$. According to Lemma 5, we have are able to move the position of the context $\mathcal{C}_h^t[\_]$, thus have
eqi6:
$$\mathcal{C}_{P_w}[\mathcal{C}_h^t[\mathcal{C}_t[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \equiv \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$
Thus, combining (eqi5) and (eqi6), we have
eqi7:
$$\mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \equiv \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$
5) Similarly, the right side of (eqi4) satisfies the following equivalence,
eqi8:
$$\mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \equiv \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$
6) According to Lemma 2, combining (eqi7), (eqi8) and (eqi4), we have
eqi9:
$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$
7) By applying the context $\mathcal{C}_h^t[\_]$ on both sides of (eqi2), we obtain

$$\mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]] \approx_\ell \mathcal{C}_h^t[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

According to Lemma 3, from the above equivalence, we have

$$\mathcal{C}_h^t[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell R_T.$$

By Lemma 1 (transitivity of the above two equivalences), we have
eqi10:
$$\mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]] \approx_\ell R_T.$$
8) Thus, the left side of (eqi9) satisfies the following equivalence (by applying context $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \_]$ on both sides of (eqi10))
$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T].$$
The right side of (eqi9) satisfies the following equivalence (by applying context $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid \_]$ on both sides of (eqi10))
$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T].$$
According to Lemma 1 (transitivity), from (eqi9), we have
eqi11:
$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T]$$
9) According to the definition of third parties (Def. 11), third parties are third party processes running in parallel. The context $\mathcal{C}_{P_w}[\_]$ has the following form
$$\mathcal{C}_{P_w}[\_] = \nu \widetilde{\mathsf{c}}.(genkey \mid !R_1 \mid \ldots \mid !R_p \mid \_).$$

Thus, according to rule

$$!P \equiv P \mid !P,$$

R_T can be absorbed by the context. Thus, $\mathcal{C}_{P_w}[\_ \mid R_T]$ is a type of context where there requires R_T to be present. We define $\mathcal{C}'_{P_w}[\_] = \mathcal{C}_{P_w}[\_ \mid R_T]$, where R_T has to be present in the context, we have
eqi12:
$$\mathcal{C}'_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \approx_\ell \mathcal{C}'_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\}]$$
Therefore, the protocol satisfies priv w.r.t. τ with the existence of R_T. $\square$

2. There exists θ such that $\mathsf{priv} \not\Longrightarrow \mathsf{ipriv}_\theta$.

   We prove the statement by showing an example in which a protocol satisfies priv but not ipriv_θ for some θ as in Ex. 2.

   Example 2. *The following protocol*

$$\begin{array}{rcl} P & = & Q \mid Q' \\ Q & = & \nu s.\mathsf{out}(c, s) \\ Q' & = & \mathsf{in}(c, x) \end{array}$$

   where c is an untappable channel, satisfies priv w.r.t. s, but not ipriv w.r.t. s and $(Q', \langle\{x\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle)$. Since the communication is untappable, the adversary cannot distinguish $\mathsf{enc}(s_1, r)$ from $\mathsf{enc}(s_2, r)$, thus the protocol satisfies priv w.r.t. s. However, when the communication partner Q' reveals the secret information he reads in on the untappable channel, s is revealed.

(2) $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$

Similar as proving $\forall\rho$, $\mathsf{epriv}_\rho \implies \mathsf{priv}$, we prove the statement in the following two directions: 1. $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$ 2. $\exists\rho,\theta$, $\mathsf{ipriv}_\theta \not\Longrightarrow \mathsf{iepriv}_{\rho,\theta}$

1. $\forall\rho$, when a protocol satisfies $\mathsf{iepriv}_{\rho,\theta}$ for some θ, we prove that the protocol also satisfies ipriv_θ.

   For a collaboration $\rho = \langle\Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, when a well-formed protocol P_w satisfies iepriv w.r.t. τ, $\langle\Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and $(R_T, \langle\Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
   eqie1:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle\Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T],$$

   we have
   eqie2:

$$\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\},$$

   and
   eqie3:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle\Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

   We first prove the following statement: If a context which provides information for the collaborating target user $\mathcal{C}'[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q')$ satisfies $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
   eqie4:

$$\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i^{\langle\Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}],$$

   then this context satisfies (`eqie1`) when R_T exists.

   Proof. Since (`eqie4`) holds for any context of the adversary which provides information for the collaborating third parties, for a specific context $\mathcal{C}_t[\_]$ of the adversary providing information for the collaborating third parties, (`eqie4`) should hold.

$$\mathcal{C}_t[\_] = \nu\mathsf{c}^t_{out}.\nu\mathsf{c}^t_{in}.(\_ \mid Q)$$

   satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}_t[\_]) = \emptyset$ and
   eqie41:

$$\mathcal{C}_t[R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell R_T^{\langle\Psi^t,\emptyset,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle},$$

   Since (`eqie4`) holds in context $\mathcal{C}_t[\_]$, we apply context $\mathcal{C}_t[\_]$ and evaluation context $\mathcal{C}^t_h[\_] = \nu\mathsf{c}^t_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}^t_{out}, x))$ (x is a fresh variable) on both sides of (`eqie4`), we have
   eqie42:

$$\mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i^{\langle\Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i^{\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]].$$

   Similar as proving $\forall\theta$, $\mathsf{ipriv}_\theta \implies \mathsf{priv}$, by Lemma 5, we move the position of the contexts $\mathcal{C}_t[\_]$ and $\mathcal{C}^t_h[\_]$, and have
   eqie43:

$$\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i^{\langle\Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle\Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]]$$

   By applying context $\mathcal{C}^t_h[\_]$ on both sides of (`eqie41`) we have
   eqie44:

$$\mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle\Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}^t_h[R_T^{\langle\Psi^t,\emptyset,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

According to Lemma 3, we have

$$\mathcal{C}_h^t[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell R_T$$

Thus, by transitivity, combining the above equivalence and (eqie44), we have
eqie45:

$$\mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]] \approx_\ell R_T$$

By applying context $\mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \_]$ on both sides of (eqie45), we have

$$\mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T]$$

By applying context $\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \_]$ on both sides of (eqie45), we have

$$\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T]$$

Because of (eqie43), combining the above two equivalences, we have

$$\mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T]$$

Thus, the statement is proved. □

1) Since the context $\mathcal{C}^{'}[\_]$ satisfies $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
eqie51: (replacing $\mathcal{C}[\_]$ with $\mathcal{C}^{'}[\_]$ in (eqie1))

$$\mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T],$$

for $\mathcal{C}^{'}[\_]$, (eqie2) and (eqie3) should hold by replacing $\mathcal{C}[\_]$ with $\mathcal{C}^{'}[\_]$.
eqie52:

$$\mathcal{C}^{'}[P_f]^{\backslash(\mathsf{c}_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\},$$

eqie53:

$$\mathcal{C}_{P_w}[\mathcal{C}^{'}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}^{'}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

2) Combining (eqie4) and (eqie53), we have
eqie6:

$$\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}^{'}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

3) By applying evaluation context $\mathcal{C}_h[\_] = \nu \mathsf{c}_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}_{out}, x))$ (x is a fresh variable) on both sides of (eqie6), we have
eqie7:

$$\mathcal{C}_h[\mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_h[\mathcal{C}_{P_w}[\mathcal{C}^{'}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]].$$

4) By Lemma 4 and Lemma 5, we move the position of context $\mathcal{C}_h[\_]$ and have
eqie8:

$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}^{'}[P_f]] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

6) Because of Lemma 3,

$$\mathcal{C}_h[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\},$$

thus we have that the left side of (eqie8) is equivalent to

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$$

Because of (eqie52), we have

$$\mathcal{C}_h[\mathcal{C}^{'}[P_f]] = \mathcal{C}^{'}[P_f]^{\backslash(\mathsf{c}_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\}.$$

Thus, by applying context $\mathcal{C}_{P_w}[\_ \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$ on both sides of the equivalence, we have that the right side of (eqie8) is equivalent to

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$$

By Lemma 1 (transitivity), we have

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$$

The above equivalence coincides with the equivalence in ipriv (Def: 12). Thus, the protocol satisfies ipriv_θ. □

There exists ρ, θ such that $\mathsf{ipriv}_\theta \;\not\Longrightarrow\; \mathsf{iepriv}_{\rho,\theta}$.

We prove the statement by showing an example in which a protocol satisfies ipriv_θ but not $\mathsf{iepriv}_{\rho,\theta}$ for some ρ as in Ex. 3.

Example 3. *Protocol*

$$\begin{array}{rcl} P & = & Q \mid Q' \\ Q & = & \nu r.\nu s.\mathsf{out}(c, \mathsf{enc}(s, r)) \\ Q' & = & \mathsf{in}(c, x) \end{array}$$

where c is a public channel, satisfies ipriv *w.r.t. s and $(Q', \langle\{x\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle)$, but not* iepriv *w.r.t. s, $\langle\{r\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and $(Q', \langle\{x\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle)$. The revealing of information from third party Q' does not help increase the adversary's knowledge. The adversary cannot distinguish $\mathsf{enc}(s_1, r)$ and $\mathsf{enc}(s_2, r)$, even when Q' reveals information, thus the protocol satisfies* ipriv *w.r.t. s and $(Q', \langle\{x\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle)$. However, when Q is coerced to reveal r, there is no way for Q to cheat the adversary. Because of the perfect encryption assumption, any other nonce cannot be used to decrypt $\mathsf{enc}(s, r)$, thus, the adversary will find out whether the user lied. Thus, the protocol does not satisfy* iepriv *w.r.t. s, $\langle\{r\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and $(Q', \langle\{x\}, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle)$.*

(1) $\forall\theta$**,** $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{epriv}_\rho$

We prove the statement in the following two directions: 1. $\forall\theta$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{epriv}_\rho$ 2. $\exists\rho, \theta$, $\mathsf{epriv}_\rho \;\not\Longrightarrow\; \mathsf{iepriv}_{\rho,\theta}$

1. $\forall\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a protocol satisfies $\mathsf{iepriv}_{\rho,\theta}$ for some ρ, we prove that the protocol also satisfies epriv_ρ with the existence of R_T.

   For a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a well-formed protocol P_w satisfies iepriv w.r.t. τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and

   eqiee1:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T],$$

   we have

   eqiee2:
   $$\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\},$$

   eqiee3:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}].$$

   1) Since for any context of the adversary which provides information for the collaborating third parties, the equivalence (`eqiee3`) holds. Thus, for the following context $\mathcal{C}_t[\_]$ of the adversary, the equivalence still holds. $\mathcal{C}_t[\_] = \nu\mathsf{c}^t_{out}.\nu\mathsf{c}^t_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}_t[\_]) = \emptyset$ and

   eqiee4:
   $$\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}.$$

   That is, by applying the context $\mathcal{C}_t[\_]$ on both sides of (`eqiee3`), we have,

   eqiee5:
   $$\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]].$$

   2) By applying the evaluation context $\mathcal{C}^t_h[\_] = \nu\mathsf{c}^t_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}^t_{out}, x))$ (x is a fresh variable), on both sides of (`eqiee5`), we have

   eqiee6:
   $$\mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]].$$

   3) By Lemma 4 and Lemma 5, we move the position of the contexts $\mathcal{C}^t_h[\_]$ and $\mathcal{C}_t[\_]$ in (`eqiee6`) and have

   eqiee7:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]].$$

   4) By applying context $\mathcal{C}^t_h[\mathcal{C}_{P_w}[\mathcal{C}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \_]]]$ on both sides of (`eqiee4`), we have

   eqiee8:
   $$\mathcal{C}^t_h[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}^t_h[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]].$$

   5) By Lemma 5, we move the position of context $\mathcal{C}^t_h[\_]$ and have

   eqiee9:
   $$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}^t_h[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]].$$

   6) By Lemma 1 (transitivity), combining (`eqiee7`) and (`eqiee9`),we have

   eqiee10:
   $$\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \mathcal{C}^t_h[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]].$$

7) According to Lemma 3 (hide on channel), we have

$$\mathcal{C}_h^t[R_T^{\langle \Psi^t,\emptyset,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}] \approx_\ell R_T.$$

8) By Lemma 1 (transitivity), combining the above equivalence and (eqiee4), we have

$$\mathcal{C}_t[R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}] \approx_\ell R_T.$$

9) Thus, by applying context $\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid \_]$ on both sides of the above equivalence, the left side of (eqiee10) is bisimilar to

$$\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T]$$

and by applying context $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid \_]$ on both sides of the above equivalence, the right side of (eqiee10) is bisimilar to

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T].$$

Thus,

eqiee11:

$$\mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T].$$

10) Because of rule

$$!P \equiv P \mid !P,$$

R_T can be absorbed by the context. That is, $\mathcal{C}_{P_w}[\_ \mid R_T]$ is a type of context where there requires R_T to be present. We define $\mathcal{C}'_{P_w}[\_] = \mathcal{C}_{P_w}[\_ \mid R_T]$, where R_T has to be present in the context, Thus, we have

eqiee12:

$$\mathcal{C}'_{P_w}[\mathcal{C}[P_f]] \approx_\ell \mathcal{C}'_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]].$$

From (eqiee1), by replacing the context $\mathcal{C}_{P_w}[\_]$ with $\mathcal{C}'_{P_w}[\_]$, we have

eqiee13:

$$\mathcal{C}'_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}'_{P_w}[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}],$$

Therefore, for any context $\mathcal{C}[\_]$ satisfying (eqiee13), (eqiee2) and (eqiee12) hold. Thus, the protocol satisfies epriv_ρ. □

2. There exists θ, ρ such that $\mathsf{epriv}_\rho \;\not\Longrightarrow\; \mathsf{iepriv}_{\rho,\theta}$.

   We prove the statement by showing an example in which a protocol satisfies epriv_ρ but not $\mathsf{iepriv}_{\rho,\theta}$ for some θ as in Ex. 4.

   Example 4. *The following protocol*

$$\begin{array}{rcl} P & = & Q \mid Q' \\ Q & = & \nu s.\mathsf{out}(c,s) \\ Q' & = & \mathsf{in}(c,x) \end{array}$$

   where c is an untappable channel, satisfies epriv *w.r.t. s and $\langle\{s\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$, but not* iepriv *w.r.t. s, $\langle\{s\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$ and $(Q',\langle\{x\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle)$. Since the communication is untappable, Q can lie about s to be s', the adversary cannot detect whether Q lied, thus the protocol satisfies* epriv *w.r.t. s and $\langle\{s\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$. However, when the communication partner Q' reveals the secret information that he reads in on the untappable channel, s is revealed. Thus, the protocol does not satisfies* iepriv *w.r.t. s, $\langle\{s\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$ and $(Q',\langle\{x\},\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle)$.*

B Thm. 2

(3) $\forall\rho$, $\mathsf{cepriv}_{\rho,\delta} \Longrightarrow \mathsf{cpriv}_\delta$

With the above assumption, we prove the statement in the following two directions: 1. $\forall\rho$, $\mathsf{cepriv}_{\rho,\delta} \Longrightarrow \mathsf{cpriv}_\delta$ 2. $\exists\rho,\delta$, $\mathsf{cpriv}_\delta \not\Longrightarrow \mathsf{cepriv}_{\rho,\delta}$

1. $\forall\rho$, when a protocol satisfies $\mathsf{cepriv}_{\rho,\delta}$ for some δ, we prove that the protocol also satisfies cpriv_δ.

   For a collaboration $\rho = \langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$, when a well-formed protocol P_w satisfies cepriv w.r.t. τ, $\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle$ and $(R_D,\langle\Theta,\Delta,\Pi\rangle)$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and

   eqc1:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}],$$

   we have

   eqc2:

$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} | R_D)^{\langle\Theta,\Delta,\Pi\rangle},$$

eqc3:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})].$$

1) By applying context $\mathcal{C}_h[\_]$ on both side of (eqc3), we have
eqc4:
$$\mathcal{C}_h[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D]] \approx_\ell \mathcal{C}_h[\mathcal{C}_{P_w}[\nu\Omega.((\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})]].$$

2) By Lemma 5, we move the position of $\mathcal{C}_h[\_]$, and have
eqc5:
$$\mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}]] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\nu\eta.(\mathcal{C}_h[\mathcal{C}[P_f]] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})].$$

3) The context $\mathcal{C}_{P_w}[\_]$ has the following form:

$$\mathcal{C}_{P_w}[\_] = \nu\tilde{\mathsf{c}}.(genkey \mid !R_1 \mid \ldots \mid !R_p \mid \_).$$

Because of (eqc1) and rule $!P \equiv P \mid !P$, we have
eqc6:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \mid R_D].$$

4) By applying $\mathcal{C}_h[\_]$ on both side of (eqc6), we have
eqc7:
$$\mathcal{C}_h[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D]] \approx_\ell \mathcal{C}_h[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \mid R_D]].$$

5) By Lemma 5, we move the position of $\mathcal{C}_h[\_]$ and have
eqc8:
$$\mathcal{C}_{P_w}[\mathcal{C}_h[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}]] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D].$$

6) By Lemma 1, combining (eqc5) and (eqc8), we have
eqc9:
$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\nu\eta.(\mathcal{C}_h[\mathcal{C}[P_f]] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})].$$

7) By Lemma 3, we have
$$\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}$$

Thus, we have (by applying context $\mathcal{C}_{P_w}[\_ \mid R_D]$ on the above equivalence)
eqc10:
$$\mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D].$$

That is, the left side of (eqc9) is equivalent to

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D].$$

8) According to Lemma 3, we have

$$\nu\Omega.((\nu\eta.(\mathcal{C}_h[\mathcal{C}[P_f]] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle}) = \nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out}, \cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})$$

Because of (eqc2), we have
eqc11:
$$\nu\Omega.((\nu\eta.(\mathcal{C}_h[\mathcal{C}[P_f]] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi\rangle}.$$

9) By applying context $\mathcal{C}_{P_w}[\_]$ on both sides of (eqc11), we have
eqc12:
$$\mathcal{C}_{P_w}[\nu\Omega.((\nu\eta.(\mathcal{C}_h[\mathcal{C}[P_f]] \mid P_\gamma)) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle})] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi\rangle}].$$

That is, the right side of (eqc9) is equivalent to

$$\mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi\rangle}].$$

10) Combining (eqc10) and (eqc12), we have

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi\rangle}].$$

Therefore, the protocol satisfies cpriv. □

2. There exists ρ, δ such that $\mathsf{cpriv}_{\delta} \not\Longrightarrow \mathsf{cepriv}_{\rho,\delta}$.

   We prove the statement by showing an example in which a protocol satisfies cpriv_{δ} but not $\mathsf{cepriv}_{\rho,\delta}$ for some ρ, δ. As shown in Sect. 6, vote-privacy is an instance of cpriv where the defending third party is the counter-balancing voter, and the coalition is the counter-balancing voter replaces his vote to counter balance to target voter's vote, and receipt-freeness is an instance of cepriv with the same defending third party and coalition. The protocol FOO92 [23] is shown that it satisfies vote-privacy but not receipt-freeness [14].

(4) $\forall\theta$, $\mathsf{cipriv}_{\theta,\delta} \Longrightarrow \mathsf{cpriv}_{\delta}$

We prove the statement in the following two directions: 1. $\forall\theta$, $\mathsf{cipriv}_{\theta,\delta} \Longrightarrow \mathsf{cpriv}_{\delta}$ 2. $\exists\theta,\delta$, $\mathsf{cpriv}_{\delta} \not\Longrightarrow \mathsf{cipriv}_{\theta,\delta}$

1. $\forall\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a protocol satisfies $\mathsf{ipriv}_{\theta,\delta}$ for some δ, we prove that the protocol also satisfies cpriv_{δ} with the existence of R_T.

   For a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a well-formed protocol P_w satisfies cipriv w.r.t. τ, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi\rangle)$ the following equivalence holds.
   eqci1:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]$$

   Since for all context of the adversary which supplies information needed by the collaborating third parties the protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$, thus, for the following context which provides information for collaborating third parties, $\mathcal{C}_t[\_] = \nu\mathsf{c}^t_{out}.\nu\mathsf{c}^t_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}_t[\_]) = \emptyset$ and
   eqci2:

$$\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle},$$

   the protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$.
   1) By applying context $\mathcal{C}_t[\_]$ on both sides of (`eqci1`), we have
   eqci3:

$$\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}_t[\mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]].$$

   2) By applying the evaluation context $\mathcal{C}^t_h[\_] = \nu\mathsf{c}^t_{out}.(\_ \mid \mathsf{in}(\mathsf{c}^t_{out}, x))$ (x is a fresh variable), on both sides of (`eqci3`), we have
   eqci4:

$$\mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}^t_h[\mathcal{C}_t[\mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]].$$

   3) According to Lemma 4 and Lemma 5, we move the position of contexts $\mathcal{C}^t_h[\_]$ and $\mathcal{C}_t[\_]$ and have
   eqci5:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid \mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]]].$$

   4) By applying context $\mathcal{C}^t_h[\_]$ on both sides of (`eqci2`), we have

$$\mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}^t_h[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]$$

   Because of Lemma 3, we have

$$\mathcal{C}^t_h[R_T^{\langle \Psi^t, \emptyset, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell R_T$$

   Thus, by transitivity, combining the above two equivalences, we have

$$\mathcal{C}^t_h[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]] \approx_\ell R_T.$$

   Thus, by applying contexts $\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid \_]$ and $\mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid \_]$ on both sides of the above equivalence, because of transitivity via (`eqci5`), we have
   eqci6:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}) \mid R_T].$$

   5) Since R_T can be absorbed by the context $\mathcal{C}_{P_w}[\_]$, we have
   eqci7:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle})].$$

   Thus, the protocol satisfies cpriv. □

2. There exists θ such that $\mathsf{cpriv}_\delta \not\Longrightarrow \mathsf{cipriv}_{\theta,\delta}$.

   We prove the statement by showing an example in which a protocol satisfies cpriv_δ for some δ but not $\mathsf{epriv}_{\theta,\delta}$ for some θ. For instance, Dreier et al. prove that the protocol by Lee et al. [29] satisfies vote-privacy – an instance of cpriv where coalition is the counter-balancing voter votes differently from the target voter, but not vote-independence – an instance of cipriv where the coalition is the same as in cpriv and the attacking third party is the third voter [20].

(2) $\forall\rho$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cipriv}_{\theta,\delta}$

We prove the statement in the following two directions: 1. $\forall\rho$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cipriv}_{\theta,\delta}$ 2. $\exists\rho,\theta,\delta$, $\mathsf{cipriv}_{\theta,\delta} \not\Longrightarrow \mathsf{ciepriv}_{\rho,\theta,\delta}$

1. $\forall\rho$, when a protocol satisfies $\mathsf{ciepriv}_{\rho,\theta,\delta}$ for some θ,δ, we prove that the protocol also satisfies $\mathsf{cipriv}_{\theta,\delta}$.

   For a collaboration $\rho = \langle \varPsi, \varPhi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, when a well-formed protocol P_w satisfies $\mathsf{ciepriv}$ w.r.t. τ, $\langle \varPsi, \varPhi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, $(R_T, \langle \varPsi^t, \varPhi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $R_D, \langle \varTheta, \varDelta, \varPi\rangle$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w)\cap\mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and

   eqiei1:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \varPsi,\varPhi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_T \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle} \mid R_T \mid R_D],$$

   we have

   eqiei2:
$$\nu\varOmega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \approx_\ell \nu\varOmega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \varTheta,\varDelta,\varPi\rangle},$$

   eqiei3:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \varPsi,\varPhi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\varOmega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

   1) Similar as in proving $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \Longrightarrow \mathsf{ipriv}_\theta$, we can prove that if a context $\mathcal{C}'[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q')$ satisfies $\mathsf{bn}(P_w)\cap\mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and

   eqie4:
$$\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \varPsi,\varPhi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle} \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}],$$

   then this context satisfies the following equivalence (replacing $\mathcal{C}[\_]$ with $\mathcal{C}'[\_]$ in (`eqiei1`)) when R_T exists.
$$\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \varPsi,\varPhi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_T \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle} \mid R_T \mid R_D].$$

   2) Thus, for $\mathcal{C}'[\_]$, the following equivalence holds (replacing $\mathcal{C}[\_]$ with $\mathcal{C}'[\_]$ in (`eqiei2`) and (`eqiei3`)).

   eqiei5:
$$\nu\varOmega.(\nu\eta.(\mathcal{C}'[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \approx_\ell \nu\varOmega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \varTheta,\varDelta,\varPi\rangle},$$

   eqiei6:
$$\mathcal{C}_{P_w}[\mathcal{C}'[\hat{R}_i\{\mathsf{id}/id_i, t/\tau\}^{\langle \varPsi,\varPhi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\varOmega.(\nu\eta.(\mathcal{C}'[P_f] \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]$$

   3) Combining (`eqiei4`) and (`eqiei6`), we have

   eqiei7:
$$\mathcal{C}_{P_w}[\nu\varOmega.(\nu\eta.(\mathcal{C}'[P_f] \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle} \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle} \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]$$

   4) By applying evaluation context $\mathcal{C}_h[\_] = \nu\mathsf{c}_{out}.(\_ \mid !\mathsf{in}(\mathsf{c}_{out}, x))$ (x is a fresh variable) on both sides of (`eqiei7`), we have

   eqiei8:
$$\mathcal{C}_h[\mathcal{C}_{P_w}[\nu\varOmega.(\nu\eta.(\mathcal{C}'[P_f] \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]] \approx_\ell \mathcal{C}_h[\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle} \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]$$

   5) By Lemma 4 and Lemma 5, we move the position of context $\mathcal{C}_h[\_]$ and have

   eqiei9:
$$\mathcal{C}_{P_w}[\nu\varOmega.(\nu\eta.(\mathcal{C}_h[\mathcal{C}'[P_f]] \mid P_\gamma) \mid R_D^{\langle \varTheta,\varDelta,\varPi\rangle}) \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]]$$

   6) Because of Lemma 3, we have
$$\mathcal{C}_h[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}^{\langle \varPsi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}] \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\},$$

   thus, we have that the right side of (`eqiei9`) is equivalent to
$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \varPsi^t,\varPhi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

7) By applying context $\mathcal{C}_{P_w}[\_ \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$ on both sides of (eqiei2), we have

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \Theta, \Delta, \Pi \rangle} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$$

That is, the left side of (eqiei9) is equivalent to

$$\mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \Theta, \Delta, \Pi \rangle} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

Therefore, by transitivity, we have

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \Theta, \Delta, \Pi \rangle} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]$$

Therefore, the protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$. □

2. There exists ρ, θ, δ such that $\mathsf{cipriv}_{\theta,\delta} \not\Longrightarrow \mathsf{ciepriv}_{\rho,\theta,\delta}$.

   We prove the statement by showing an example in which a protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$ but not $\mathsf{ciepriv}_{\rho,\theta,\delta}$ for some ρ, θ, δ. For instance, Dreier et al. prove that the voting protocol FOO92 [23] satisfies vote-independence – an instance of cipriv where the coalition is the counter-balancing voter votes differently from the target voter and the attacking third party is the third voter, but not vote-independence with passive collaboration – an instance of ciepriv where the coalition and attacking third party are the same as in cipriv and the collaboration is forwarding private information to the adversary.

(1) $\forall\theta$**,** $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cepriv}_{\rho,\delta}$
We prove the statement in the following two directions: 1. $\forall\theta$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \Longrightarrow \mathsf{cepriv}_{\rho,\delta}$ 2. $\exists\rho,\theta,\delta$, $\mathsf{cepriv}_{\rho,\delta} \not\Longrightarrow \mathsf{ciepriv}_{\rho,\theta,\delta}$

1. $\forall\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle)$, when a protocol satisfies $\mathsf{ciepriv}_{\rho,\theta,\delta}$ for some ρ, δ, we prove that the protocol also satisfies $\mathsf{cepriv}_{\rho,\delta}$ with the existence of R_T.

   For a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle)$, when a well-formed protocol P_w satisfies ciepriv w.r.t. τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
   eqciee1:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T \mid R_D],$$

   we have
   eqciee2:

$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}|R_D)^{\langle \Theta, \Delta, \Pi \rangle},$$

   eqciee3:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}].$$

   1) Since for any context of the adversary which provides information for the collaborating third parties, the equivalence (eqciee3) holds. Thus, for the following context $\mathcal{C}_t[\_]$ of the adversary which provides information for the collaborating third parties, the equivalence (eqciee3) still holds. $\mathcal{C}_t[\_] = \nu\mathsf{c}_{out}^t.\nu\mathsf{c}_{in}^t.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}_t[\_]) = \emptyset$ and
   eqciee4:

$$\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}] \approx_\ell R_T^{\langle \Psi^t, \emptyset, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}.$$

   Therefore, by applying the context $\mathcal{C}_t[\_]$ on both sides of (eqciee3), we have,
   eqciee5:

$$\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]] \approx_\ell \mathcal{C}_t[\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]$$

   2) By applying the evaluation context $\mathcal{C}_h^t[\_] = \nu\mathsf{c}_{out}^t.(\_ \mid \mathsf{in}(\mathsf{c}_{out}^t, x))$ (x is a fresh variable), on both sides of (eqciee5), we have
   eqciee6:

$$\mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_h^t[\mathcal{C}_t[\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]]$$

   3) By Lemma 4 and Lemma 5, we move the position of context $\mathcal{C}_h^t[\_]$ and $\mathcal{C}_t[\_]$ in (eqciee6), and have
   eqciee7:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]].$$

   4) By applying context $\mathcal{C}_h^t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \_]]$ on both sides of (eqciee4), we have
   eqciee8:

$$\mathcal{C}_h^t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \mathcal{C}_t[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]]] \approx_\ell \mathcal{C}_h^t[\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \emptyset, \mathsf{c}_{out}^t, \mathsf{c}_{in}^t \rangle}]].$$

5) By Lemma 5, we move the position of context $\mathcal{C}_h^t[\_]$ in (eqciee8) and have
eqciee9:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \mathcal{C}_h^t[R_T^{\langle \Psi^t,\emptyset,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}]].$$

6) By Lemma 1, combining (eqciee7) and (eqciee9),we have
eqciee10:

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \mid \mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}]]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid \mathcal{C}_h^t[R_T^{\langle \Psi^t,\emptyset,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}]].$$

7) According to Lemma 3, we have

$$\mathcal{C}_h^t[R_T^{\langle \Psi^t,\emptyset,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}] \approx_\ell R_T.$$

8) By Lemma 1, combining the above equivalence and (eqiee4), we have

$$\mathcal{C}_h^t[\mathcal{C}_t[R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}_{out}^t,\mathsf{c}_{in}^t\rangle}]] \approx_\ell R_T.$$

9) Thus, the left side of (eqciee10) is bisimilar to

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \mid R_T]$$

and the right side of (eqiee10) is bisimilar to

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T].$$

Thus,
eqciee11:

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T].$$

10) Because of rule

$$!P \equiv P \mid !P,$$

R_T can be absorbed by the context. $\mathcal{C}_{P_w}[\_ \mid R_T]$ is a type of context where there requires R_T to be present. We define $\mathcal{C}'_{P_w}[\_] = \mathcal{C}_{P_w}[\_ \mid R_T]$, where R_T has to be present in the context, Thus, we have
eqciee12:

$$\mathcal{C}'_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle})] \approx_\ell \mathcal{C}'_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D].$$

From (eqciee1), we can obtain
eqciee13:

$$\mathcal{C}'_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell \mathcal{C}'_{P_w}[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_D],$$

Therefore, for any context $\mathcal{C}[\_]$ satisfying (eqciee13), (eqciee2) and (eqciee12) hold. Thus, the protocol satisfies cepriv_ρ. □

2. There exists θ, ρ, δ such that $\mathsf{cepriv}_{\rho,\delta} \not\Longrightarrow \mathsf{ciepriv}_{\rho,\theta,\delta}$.

   We prove the statement by showing an example in which a protocol satisfies $\mathsf{cepriv}_{\rho,\delta}$ but not $\mathsf{ciepriv}_{\rho,\theta,\delta}$ for some ρ,θ,δ. For instance, Dreier et al. prove that the voting protocol by Lee et al. [29] satisfies receipt-freeness – an instance of cepriv where the coalition is is the counter-balancing voter votes differently from the target voter and the collaboration is forwarding private information to the adversary, but not vote-independence with passive collaboration – an instance of ciepriv where the coalition and collaboration are the same as in cepriv and the defending third party is the third voter.

C Thm. 3

(4) $\mathsf{priv} \Longrightarrow \exists\delta, \mathsf{cpriv}_\delta$
We prove the statement in the following two directions: 1. $\mathsf{priv} \Longrightarrow \exists\delta, \mathsf{cpriv}_\delta$ 2. $\exists\delta, \mathsf{cpriv}_\delta \not\Longrightarrow \mathsf{priv}$

1. When a protocol satisfies priv, then there exists a coalition δ such that the protocol satisfies cpriv_δ.

   When a well-formed protocol P_w satisfies priv w.r.t. τ we have
   eqcc1:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\}].$$

   The context $\mathcal{C}_{P_w}[\_]$ has the following form

$$\mathcal{C}_{P_w}[\_] = \nu\tilde{\mathsf{c}}.(genkey \mid !R_1 \mid \cdots \mid !R_p \mid \_).$$

Because of rule

$$!P \equiv P \mid !P,$$

we have (for a set of defending third parties R_D)

eqcc2:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D].$$

Let $\delta = (R_D, \langle \emptyset, \emptyset, \emptyset \rangle)$ be a coalition,

eqcc3:

$$\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle} = \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D$$

Thus, by applying context $\mathcal{C}_{P_w}[\_]$ on both sides of (eqcc3), we have

eqcc4:

$$\mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}] = \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D]$$

Because of (eqcc2), we have

eqcc5:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}]$$

Thus, the protocol satisfies cpriv_δ. □

2. There exists δ such that $\mathsf{cpriv}_\delta \not\Longrightarrow \mathsf{priv}$.

   We prove the statement by showing an example in which a protocol satisfies cpriv_δ but not priv. For instance, FOO92 [23] is shown that it does not satisfy priv w.r.t. vote $vote$, but satisfies vote-privacy – an instance of cpriv where the coalition is the counter-balancing votes differently from the target voter [27].

(3) $\mathsf{ipriv}_\theta \Longrightarrow \exists\delta, \mathsf{cipriv}_{\theta,\delta}$

We prove the statement in the following two directions: 1. $\mathsf{ipriv}_\theta \Longrightarrow \exists\delta, \mathsf{cipriv}_{\theta,\delta}$ 2. $\exists\theta,\delta, \mathsf{cipriv}_{\theta,\delta} \not\Longrightarrow \mathsf{ipriv}_\theta$

1. When a protocol satisfies ipriv_θ for some θ, then there exists a coalition δ such that the protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$.

   For a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle)$, when a well-formed protocol P_w satisfies epriv w.r.t. τ and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle)$, the following equivalence holds.

   eqcci1:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}].$$

   Thus, we have (for a set of defending third parties R_D)

   eqcci2:

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle} \mid R_D].$$

   Let $\delta = (R_D, \langle \emptyset, \emptyset, \emptyset \rangle)$ be a coalition, then

   eqcci3:

$$\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}) = \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D$$

   Thus, we have

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}].$$

   Therefore, the protocol satisfies $\mathsf{cepriv}_{\theta,\delta}$. □

2. There exists θ, ρ such that $\mathsf{cipriv}_{\theta,\delta} \not\Longrightarrow \mathsf{ipriv}_\theta$.

   We prove the statement by showing an example in which a protocol satisfies $\mathsf{cipriv}_{\theta,\delta}$ but not ipriv_θ. For instance, voting protocols FOO92 are shown does not satisfies priv w.r.t. vote $vote$ [27], thus deos not stasifes ipriv, but satisfies vote-independence – an instance of cipriv where the coalition is the counter-balancing voter votes differently from the target voter and the attacking third party is the third voter [20].

(2) $\mathsf{epriv}_\rho \Longrightarrow \exists\delta, \mathsf{cepriv}_{\rho,\delta}$

We prove the statement in the following two directions: 1. $\mathsf{epriv}_\rho \Longrightarrow \exists\delta, \mathsf{cepriv}_{\rho,\delta}$ 2. $\exists\rho,\delta, \mathsf{cepriv}_{\rho,\delta} \not\Longrightarrow \mathsf{epriv}_\rho$

1. When a protocol satisfies epriv_ρ for some ρ, then there exists a coalition δ such that the protocol satisfies $\mathsf{cepriv}_{\rho,\delta}$.

   When a well-formed protocol P_w satisfies epriv w.r.t. τ and $\rho = \langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and

   eqcce1:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}],$$

we have
eqcce2:

$$\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\},$$

eqcce3:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f]].$$

Form (eqcce3), we have
eqcce4:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_D].$$

Let $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$ be a coalition, then
eqcce5:

$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle}) = \mathcal{C}[P_f] \mid R_D$$

By applying context $\mathcal{C}_{P_w}[\_]$ on both sides of (eqcce5) we have
eqcce6:

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle})] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_D]$$

Combining (eqcce4) and (eqcce6), by Lemma 1, we have
eqcce7:

$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle})] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D]$$

Since $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$, we have

$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle}) = \mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid R_D$$

Because of (eqcce2), we have
eqcce8:

$$\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid R_D \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D.$$

Since $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$, we have

$$\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle} = \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$$

Thus,
eqcce9:

$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle\Theta,\Delta,\Pi\rangle}) \approx_\ell \Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle\Theta,\Delta,\Pi\rangle}$$

Because of (eqcce1), we have
eqcce10:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D],$$

Therefore, for any context $\mathcal{C}[\_]$ satisfing (eqcce10), the protocol satisfies (eqcce7) and (eqcce9), thus, the protocol satisfies $\mathsf{cepriv}_{\rho,\delta}$. □

2. There exists δ, ρ such that $\mathsf{cepriv}_{\rho,\delta} \not\Longrightarrow \mathsf{epriv}_\rho$.

   We prove the statement by showing an example in which a protocol satisfies $\mathsf{cepriv}_{\rho,\delta}$ but not epriv_ρ. For instance, voting protocol by Okamoto [31] does not satisfy priv w.r.t. vote $vote$ [27] in the case of unanimous result, thus does not satisfy epriv where ρ is forwarding private information to the adversary, but satisfies receipt-freeness – an instance of cepriv where the coalition is the counter-balancing votes differently from the target voter and the collaboration is forwarding private information to the adversary [14].

$\mathsf{iepriv}_{\rho,\theta} \Longrightarrow \exists\delta, \mathsf{ciepriv}_{\rho,\theta,\delta}$
We prove the statement in the following two directions: 1. $\mathsf{iepriv}_{\rho,\theta} \Longrightarrow \exists\delta, \mathsf{ciepriv}_{\rho,\theta,\delta}$ 2. $\exists\rho,\theta,\delta, \mathsf{ciepriv}_{\rho,\theta,\delta} \not\Longrightarrow \mathsf{iepriv}_{\rho,\theta}$

1. When a protocol satisfies $\mathsf{iepriv}_{\rho,\theta}$ for some ρ,θ, then there exists a coalition δ such that the protocol satisfies $\mathsf{ciepriv}_{\rho,\theta,\delta}$.

   For a collaboration of the target user $\rho = \langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and a collaboration of third parties $\theta = (R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, when a well-formed protocol P_w satisfies iepriv w.r.t. τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu\mathsf{c}_{out}.\nu\mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and
   eqccee1:

$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T],$$

   we have
   eqccee2:

$$\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\},$$

eqccee3:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}].$$

Because of (`eqccee3`), we have
eqccee4:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle} \mid R_D].$$

Let $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$ be a coalition, then
eqccee5:
$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) = \mathcal{C}[P_f] \mid R_D$$

By applying context $\mathcal{C}_{P_w}[\_ \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]$ on both sides of (`eqccee5`), we have
eqccee6:
$$\mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid R_D \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]$$

By Lemma 1, combining (`eqccee4`) and (`eqccee6`), we have
eqccee7:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle} \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \mid R_T^{\langle \Psi^t,\Phi^t,\mathsf{c}^t_{out},\mathsf{c}^t_{in}\rangle}]$$

Since $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$, we have
$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) = \mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid R_D.$$

Because of (`eqccee2`), we have
eqccee8:
$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D$$

Since $\delta = (R_D, \langle\emptyset,\emptyset,\emptyset\rangle)$, we also have
$$\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta,\Delta,\Pi\rangle} = \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D$$

Thus, we have
eqccee9:
$$\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\backslash(\mathsf{c}_{out},\cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta,\Delta,\Pi\rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\} \mid R_D)^{\langle \Theta,\Delta,\Pi\rangle}$$

Form (`eqccee1`), we have
eqccee10:
$$\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi,\Phi,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T \mid R_D] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi,\emptyset,\mathsf{c}_{out},\mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\} \mid R_T \mid R_D]$$

Therefore, for any context $\mathcal{C}[\_]$ satisfying (`eqccee10`), (`eqccee7`) and (`eqccee9`) are satisfies. Thus, the protocol satisfies $\mathsf{ciepriv}_{\rho,\theta,\delta}$. □

2. There exists θ, ρ, δ such that $\mathsf{ciepriv}_{\rho,\theta,\delta} \not\Rightarrow \mathsf{iepriv}_{\rho,\theta}$.

   We prove the statement by showing an example in which a protocol satisfies $\mathsf{ciepriv}_{\rho,\theta,\delta}$ but not $\mathsf{iepriv}_{\rho,\theta}$. For instance, voting protocol by Okamoto [31] does not satisfy priv w.r.t. vote $vote$ when all votes are unanimous. Thus, the protocol does not satisfy iepriv w.r.t. vote $vote$, ρ and θ, where ρ is the target voter forwarding information to the adversary, θ is the collaborating third voter communicating with the adversary. However, the protocol satisfies vote-independence with passive collaboration – an instance of ciepriv w.r.t. vote $vote$, ρ, θ and δ where ρ and θ are the same as in ieprivand δ is the counter-balancing voter voting differently from the target voter [20].

D Extension

D.1 Third-party-enforced-privacy

The notion of independency-of-privacy assumes that the adversary fully trusts the third parties' information. We can extend this notion to a weaker one (third-party-enforced-privacy) where the third parties are assumed to lie to the adversary if it is possible. For instance, when a third party's revealing of information harms his own privacy, the third party is willing to lie (if it is possible) to the adversary. For example, when the third party is a voter, the third party may not want to reveal his real vote. In this case, the assumption in independency-of-privacy that third parties do not lie to the adversary is too strong.

A protocol satisfies third-party-enforced-privacy if the target user's privacy is preserved under the assumption that a set of attacking third party may be coerced by the adversary and a sub-set of the third parties lie to the adversary. It can be modelled as the existence of a process in which a set of coerced third parties lie to the adversary, the adversary cannot tell whether the third parties lied, and because of the possibility of third parties lying, the adversary cannot link the target user to his sensitive data.

Definition 19 (Third-party-enforced-privacy)**.** *A well-formed protocol P_w satisfies third-party-enforced-privacy w.r.t. τ ($\tau \in \mathsf{bn}(R_i)$), $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, if there exists a closed plain process P^t_f for a sub-set of attacking third party R_{T_l} ($R_T = R_{T_l} \mid R_{T_o}$), such that,*

$$\mathcal{C}_{P_w}[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid \hat{R}_i\{\mathsf{id}/\mathtt{id}_i, \mathtt{t_1}/\tau\}] \quad \approx_\ell \quad \mathcal{C}_{P_w}[R_{T_o}^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid P^t_f \mid \hat{R}_i\{\mathsf{id}/\mathtt{id}_i, \mathtt{t_2}/\tau\}]$$

In the definition, $\hat{R}_i\{\mathsf{id}/\mathtt{id}_i\}$ is the target user, R_{T_l} is the set of attacking third parties who are willing to lie, R_{T_o} is the remaining third parties which collaborate with the adversary. The equivalence in the definition shows that even with collaboration of other attacking third parties, a set of attacking third party R_{T_l} is able to lie in process P^t_f, and the adversary cannot distinguish two situations: first the target user uses sensitive data $\mathtt{t_1}$ and the third party R_{T_l} lies in process P^t_f, second the target user uses sensitive data $\mathtt{t_2}$ and the user R_{T_l} follows process $P_f^{t\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}$, and does not lie.

Intuitively, independency-of-privacy is stronger than third-party-enforced privacy. If a protocol satisfies independency-of-privacy, then the protocol satisfies third-party-enforced-privacy. That is, the target user's privacy is preserved when the third parties do not lie to the adversary, then the target user's privacy is preserved when the third parties lie. The adversary's knowledge when the third parties are trustworthy is more than that when the third parties are not trustworthy. Example 5 shows that a protocol not satisfying independency-of-privacy may satisfy third-party-enforced-privacy.

Example 5. *A sends to B a term (A, a) through untappable channel, B is able to reveal the link between A and a. Thus, this protocol does not satisfies independency-of-privacy. In third-party-enforced-privacy, we assume that the adversary does not fully trust the third party. The adversary suspects that the third party lies to him if the third party can. Since the communication between A and B is over untappble channel, B is able to lie without being detected by the adversary. Since the adversary cannot detect whether B lied, when B forwards data a to the adversary, the adversary cannot distinguish A using a while B does not lie and A using b while B lies.*

D.2 Others

Similarly, third-party-target-enforced-privacy, coalition-third-party-enforced-privacy and coalition-third-party-target-enforced-privacy (corresponding to independency-of-enforced-privacy, coalition-independency-of-privacyand coalition-independency-of-enforced-privacy, respectively) can be defined by assuming attacking third parties may lie to the adversary.

Definition 20 (Third-party-target-enforced-privacy)**.** *A well-formed protocol P_w satisfies third-party-target-enforced-privacy (ttepriv) w.r.t. τ, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, if there exists a closed plain process P^t_f for a sub-set of attacking third parties R_{T_l} ($R_T = R_{T_l} \mid R_{T_o}$), and a closed plain process P_f, such that for any $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t_1}/\tau\}]$, we have,*

1. $\mathcal{C}[P_f]^{\setminus(\mathsf{c}_{out},\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t_2}/\tau\}$,
2. $\mathcal{C}_{P_w}[R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid \mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[R_{T_o}^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid P^t_f \mid \mathcal{C}[P_f]]$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ is a collaboration specification for $\hat{R}_i$, t is a free name representing a piece of data, and $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification of process R_T.

Definition 21. *A well-formed protocol P_w satisfies coalition-third-party-enforced-privacy (ctepriv) w.r.t. data τ, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, and $(R_D, \langle \Theta, \Delta, \Pi\rangle)$, if there exists a closed plain process P^t_f for a sub-set of attacking third parties R_{T_l} ($R_T = R_{T_l} \mid R_{T_o}$), such that*

$$\mathcal{C}_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t_1}/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t_2}/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi\rangle}) \mid R_{T_o}^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid P^t_f],$$

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification of process R_T, and $\langle \Theta, \Delta, \Pi\rangle$ is a coalition specification defined on $R_U = \hat{R}_i \mid R_D$, $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$.

Definition 22. *A well-formed protocol P_w satisfies coalition-third-party-target-enforced-privacy (cttepriv) w.r.t. data τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi\rangle)$, if there exists a closed plain process P^t_f for a sub-set of attacking third parties R_{T_l} ($R_T = R_{T_l} \mid R_{T_o}$), and a closed plain process P_f such that for any context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t_1}/\tau\}]$, we have*

1. $(\mathcal{C}[P_f]^{\setminus(\mathsf{c}_{out},\cdot)})^{\setminus(\mu,\cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t_2}/\tau\}$,
2. $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell \mathcal{C}_{P_w}[\nu\Omega.((\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi\rangle}) \mid R_{T_o}^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle} \mid P^t_f]$,

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ is a collaboration specification defined on $\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification defined on R_T, $\langle \Theta, \Delta, \Pi\rangle$ is a coalition specification defined on $R_U = \hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle} \mid R_D$, t is a free name representing a piece of data, $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$, $\mu = \{\mathsf{c} \mid \langle \hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta\}$, $P_\gamma = \mathsf{in}(\mathsf{c}_1, y_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y_\ell)$ with $\{(\mathsf{c}_1, y_1), \cdots, (\mathsf{c}_\ell, y_\ell)\} = \{(\mathsf{c}, y) \mid \langle R_{u_i}, \hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}, M, \mathsf{c}, y\rangle \in \Theta\}$.

E Application

E.0.1 Vote-privacy

Vote-privacy [27] is defined as the adversary cannot determine a voter's vote with the existence of a counter-balancing voter.

$$\mathcal{C}_{P_w}[\hat{R}_v\{\mathsf{id}/\mathtt{id}, \mathtt{t}_1/vote\} \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_v\{\mathsf{id}/\mathtt{id}, \mathtt{t}_2/vote\} \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_1/vote\}]$$

This can be instantiated as coalition-privacy w.r.t. $vote$ and $(\nu\mathtt{t}_2.(\hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}), \langle\emptyset, \{\{\mathtt{t}_1/\mathtt{t}_2\}\}, \emptyset\rangle)$ where the target data is a vote $vote$, the defending third party is the counter-balancing voter $\nu\mathtt{t}_2.(\hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\})$ and the coalition specification is $\langle\emptyset, \varDelta, \emptyset\rangle$ where the substitution $\varDelta$ specifies how to replace the counter-balancing voter's vote.

E.0.2 Bidding-privacy

Bidding-privacy [16] in sealed-bid e-auctions is defined as the adversary cannot determine a bidder's bidding-price, assuming the existence of a winning bid.

$$\mathcal{C}_{P_w}[\hat{R}_b\{\mathsf{id}/\mathtt{id}, \mathtt{t}_1/bid\} \mid \hat{R}_b\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_3/bid\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_b\{\mathsf{id}/\mathtt{id}, \mathtt{t}_2/bid\} \mid \hat{R}_b\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_3/bid\}]$$

where $\mathtt{t}_1 < \mathtt{t}_3$ and $\mathtt{t}_2 < \mathtt{t}_3$. This can be instantiated as coalition-privacy w.r.t. bid and $(\hat{R}_b\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_3/bid\}, \langle\emptyset, \emptyset, \emptyset\rangle)$ where the target data is a bid, the defending third party is the winning bidder and the coalition specification is $\langle\emptyset, \emptyset, \emptyset\rangle$.

E.0.3 Prescribing-privacy

Prescribing-privacy [18] is defined as the adversary cannot determine a doctor's prescription with the existence of a counter-balancing .

$$\mathcal{C}_{P_w}[\hat{R}_d\{\mathsf{id}/\mathtt{id}, \mathtt{t}_1/presc\} \mid \hat{R}_d\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/presc\}] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_d\{\mathsf{id}/\mathtt{id}, \mathtt{t}_2/presc\} \mid \hat{R}_d\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_1/presc\}]$$

This can be instantiated as coalition-privacy w.r.t. $presc$ and $(\nu\mathtt{t}_2.(\hat{R}_d\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}), \langle\emptyset, \{\{\mathtt{t}_1/\mathtt{t}_2\}\}, \emptyset\rangle)$ where the target data is a prescription $presc$, the defending third party is the counter-balancing doctor $\nu\mathtt{t}_2.(\hat{R}_d\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\})$ and the coalition specification is $\langle\emptyset, \varDelta, \emptyset\rangle$ where the substitution $\varDelta$ specifies how to replace the counter-balancing doctor's prescription.

E.0.4 Receipt-freeness

Receipt-freeness [14] in voting is defined as the existence of P_f such that

$$\begin{array}{l} P_f{}^{\backslash(\mathtt{c}_{out},\cdot)} \approx_\ell \hat{R}_v\{\mathsf{id}/\mathtt{id}, \mathtt{t}_2/vote\} \\ \mathcal{C}_{P_w}[\hat{R}_v^{\langle \varPsi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/\mathtt{id}, \mathtt{t}_1/vote\} \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}] \approx_\ell \mathcal{C}_{P_w}[P_f \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_1/vote\}] \end{array}$$

This can be instantiated by coalition-enforced-privacy w.r.t. $vote$ $\langle \varPsi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$ and $(\nu\mathtt{t}_2.(\hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}), \langle\emptyset, \{\{\mathtt{t}_1/\mathtt{t}_2\}\}, \emptyset\rangle)$, where the target data and the coalition are the same as in vote-privacy, and the collaboration specification is $\langle \varPsi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$ where $\varPsi$ contains all private terms generated and read-in in the target voter process. $\varPsi$ in a process R is given by $\mathsf{OutTerm}(R)$.

$$\begin{array}{rcl} \mathsf{OutTerm}(0) & = & \emptyset \\ \mathsf{OutTerm}(P \mid Q) & = & \mathsf{OutTerm}(P) \cup \mathsf{OutTerm}(Q) \\ \mathsf{OutTerm}(!P) & = & \mathsf{OutTerm}(P) \\ \mathsf{OutTerm}(\nu\mathtt{n}.P) & = & \{\mathtt{n}\} \cup \mathsf{OutTerm}(P) \quad \text{when } \mathtt{n} \text{ is name of base type,} \\ \mathsf{OutTerm}(\nu\mathtt{n}.P) & = & \mathsf{OutTerm}(P)\text{otherwise} \\ \mathsf{OutTerm}(\mathsf{in}(v,x).P) & = & \{x\} \cup \mathsf{OutTerm}(P) \quad \text{when } \mathtt{n} \text{ is name of base type,} \\ \mathsf{OutTerm}(\mathsf{in}(v,x).P) & = & \mathsf{OutTerm}(P)\text{otherwise} \\ \mathsf{OutTerm}(\mathsf{out}(v,M).P) & = & \mathsf{OutTerm}(P) \\ \multicolumn{3}{l}{\mathsf{OutTerm}(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q)} \\ & = & \mathsf{OutTerm}(P) \cup \mathsf{OutTerm}(Q) \end{array}$$

E.0.5 Coercion-resistance

Coercion-resistance [14] in voting is defined as the existence of P_f such that for any context $\mathcal{C}[\_] = \nu\mathtt{c}_{out}.\nu\mathtt{c}_{in}.(\_|Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $\mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_v^{\langle \varPsi, \varPhi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/id_i, t/vote\}]] \approx_\ell \mathcal{C}_{P_w}[\hat{R}_v^{\langle \varPsi, \emptyset, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/vote\}]$, we have

$$\begin{array}{l} \mathcal{C}[P_f]^{\backslash(\mathtt{c}_{out},\cdot)} \approx_\ell \hat{R}_v\{\mathsf{id}/\mathtt{id}, \mathtt{t}_2/vote\} \\ \mathcal{C}_{P_w}[\mathcal{C}[\hat{R}_v^{\langle \varPsi, \varPhi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle}\{\mathsf{id}/\mathtt{id}, \mathtt{t}_1/vote\}] \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_2/vote\}] \approx_\ell \mathcal{C}_{P_w}[\mathcal{C}[P_f] \mid \hat{R}_v\{\mathsf{id}'/\mathtt{id}, \mathtt{t}_1/vote\}] \end{array}$$

This can be considered as an instance of coalition-enforced-privacy as well, where the target data and the coalition are the same as in vote-privacy, and the cooperation specification is $\langle \mathit{\Psi}, \mathit{\Phi}, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ where $\mathit{\Psi}$ contains all private terms generated and read-in in the target voter process and $\mathit{\Phi}$ contains all the send out terms. $\mathit{\Phi}$ in a process R is given by $\mathsf{ReplaceTerm}(R)$.

$$\begin{array}{rcl}
\mathsf{ReplaceTerm}(0) & = & \emptyset \\
\mathsf{ReplaceTerm}(P \mid Q) & = & \mathsf{ReplaceTerm}(P) \cup \mathsf{ReplaceTerm}(Q) \\
\mathsf{ReplaceTerm}(!P) & = & \mathsf{ReplaceTerm}(P) \\
\mathsf{ReplaceTerm}(\nu \mathtt{n}.P) & = & \mathsf{ReplaceTerm}(P) \\
\mathsf{ReplaceTerm}(\mathsf{in}(v, x).P) & = & \mathsf{ReplaceTerm}(P) \\
\mathsf{ReplaceTerm}(\mathsf{out}(v, M).P) & = & \{M\} \cup \mathsf{ReplaceTerm}(P) \\
\multicolumn{3}{l}{\mathsf{ReplaceTerm}(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q)} \\
 & = & \mathsf{ReplaceTerm}(P) \cup \mathsf{ReplaceTerm}(Q)
\end{array}$$