Challenges in eHealth: From Enabling to Enforcing Privacy

Naipeng Dong*, Hugo Jonker, and Jun Pang

Faculty of Sciences, Technology and Communication,
University of Luxembourg, Luxembourg

Abstract. Privacy has been recognised as a fundamental requirement for electronic health-care (eHealth) systems. Various proposals to achieve privacy have been put forth in literature, most of which approach patient privacy as either an access control or authentication problem.
In this paper, we investigate privacy in eHealth as a communication problem, since typical eHealth systems in future will be highly distributed and require interoperability of many sub-systems. In addition, we research privacy needs for others than patients. In our study, we have identified two key privacy challenges in eHealth: *enforced privacy* and *enforced respecting privacy*. We propose to use formal techniques to understand and define these new privacy notions in a precise and unambiguous manner, and to build an efficient verification framework to ensure privacy properties for eHealth systems.

1 Introduction

The inefficiency of traditional paper-based health-care and the development of information communication technologies, in particular cloud computing, mobile, and satellite communications, give electronic health-care (eHealth for short) a great opportunity to grow as an important part of people's daily life. eHealth systems aim to provide effective support for secure sharing of information and resources across different health-care settings, and workflows among different health-care providers. The services of such systems for the general public are intended to be more secure, more effective, more efficient, more patient-centered and more timely. However, the attractive advantages of eHealth systems entail many scientific challenges. One of the foremost of these are the privacy issues raised by adapting electronic storage and communication, due to the sensitive nature of health data. Indeed, privacy in eHealth has been recognised as one of the paramount requirements necessary for adoption by the general public [1, 2].

Various proposals to achieve privacy in eHealth have been put forth in literature, most of which focus on patient privacy (notable exceptions: [3–5]) and approach it as an access control or authentication problem. First, eHealth systems have a large number of different stake-holders, for instance, patients, doctors, pharmacists, organisations for social security and public safety, health insurance

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

companies, etc. These parties all have different or even conflicting privacy requirements. The virtually exclusive focus on patient privacy in literature has left the question of privacy requirements of other parties, doctors in particular, wide open. The fact that some parties, e.g. pharmacists, cannot be fully trusted causes adversely impacts privacy [4].

Second, eHealth systems must provide assurance of privacy and address privacy issues at different system levels – architectural design, access control, communication protocols, etc. This inherent difficulty is aggravated as privacy of sensitive information is a complex issue and subject to (individual) application of professional ethics, regulations and guidelines. Currently, (patient) privacy is usually described in terms of protection of information and in terms of controlling access to services. Thus, it is commonly achieved in practice by means of a form of access control or authentication (e.g., see [6–10]). However, typical eHealth systems, especially in future, will be highly distributed and require interoperability of many sub-systems. Improperly designed communication protocols for such interoperability will cause information leakage and hence breach users' privacy. So far, security and privacy of communication protocols in eHealth systems is seldom studied in literature.

In this paper, we research privacy in eHealth as a communication problem and investigate which privacy requirements are essential for both patients and doctors, not only focusing on protecting private health data of patients. We have identified two critical privacy requirements as key challenges for the field: *enforced privacy* (e.g. a doctor cannot prove to a pharmaceutical company which medicine he prescribed) and *enforced respecting privacy* (e.g. a patient cannot reveal which doctor prescribed her medicine). We also propose to use formal techniques to understand and interpret these new privacy notions in a precise and unambiguous manner, and to build an efficient verification framework for analysing privacy properties of eHealth systems. We believe this step is crucial, as the formal assurance of key properties including privacy in such systems will increase users, especially patients, confidence and reduce their reluctance and skepticism towards new eHealth systems.

2 Privacy in eHealth

Privacy in eHealth systems has attracted a lot of research effort and many different methods to enable privacy have been proposed. We classify related work into two categories, as they either focus on patient privacy (Section 2.1) or doctor privacy (Section 2.2). We present our observations in Section 2.3.

2.1 Enabling patient privacy

The importance of patient privacy in eHealth is traditionally seen as vital to establishing a good doctor-patient relationship. This is even more pertinent with the emergence of the Electronic Patient Record [6]. As in most of the literature, a necessary early stage of eHealth is to transfer paper-based health-care process

to digital-based. The most important changes on this stage are made on patients information, mainly health-care records. Privacy policies are considered as the standard way to express requirements for patient privacy. There are three main approaches to support patient privacy: access control, architectural design, and the use of cryptography.

Patient privacy by access control. To ensure privacy of electronic health-care records, a necessary part is to ensure privacy during the access procedure of these records. Anderson listed several privacy threats to personal health information, thus claimed that privacy policy for access control should be required in eHealth systems [6]. A technique to achieve access control is to make proper rules to avoid leaking private information to those who should not have access to it. Louwerse claimed that consent access control is required besides of access control based on "need-to-know" principles [7]. Evered and Bögeholz showed that access control for eHealth systems are too complex for per-method access control and proposed an access control mechanism for complex eHealth systems [9]. A tailored role-based access control (rBAC) with explicitly denial is proposed by Reid et al. [8] for distributed eHealth systems. Most traditional privacy policies and access control focused on data between medical institutions. However, eHealth systems also consist of non-medical institutions which may cause privacy problems. This leads Hung to propose the use of rBAC to ensure privacy of non-medical institutions [10]. Detailed access control techniques for eHealth systems are studied as well, for instance, in a wireless access environment [11] and between data owner and different service providers [12].

Patient privacy by architectural design. eHealth systems are complex in the sense that many different roles are involved, for instance patients, doctors, pharmacists, medical administration, social security, insurance companies, legal administration, etc. Each role has their own sub-systems or components. To this aspect, eHealth systems can be considered as a large network of *systems of systems* of different departments and laboratories, including administrative system components, laboratory information systems, radiology information systems, pharmacy information systems, and financial business management systems. To design such complicated systems, architectural design is an essential step to make a system function correctly. Since privacy is an important challenge in eHealth systems, keeping privacy in mind when design the architecture of such systems is a promising way to ensure privacy [13]. Ko et al. considered privacy issues when building a wireless sensor networks for health-care [14]. Some eHealth system architectures are specially designed with a particular privacy issue in mind. For example, Maglogiannis et al. proposed an architecture that enhances patients' location privacy [15]. There also exist architectures, which use different privacy protecting techniques at different layers of a system. For example, Chiu et al. studied privacy requirements for cross-institution image protecting and designed a system combining access control principles, rBAC, authentication, and etc. [16].

Patient privacy by cryptography. Cryptography is considered as a necessary tool to solve privacy issues raised by information technologies in eHealth systems [17]. Cryptography based authentication is proposed to satisfy the security and privacy requirements for cross-institutional electronic patient-records [18, 16]. In particular, credential transfer systems are proposed to keep users' identities anonymous [19]. Layouni et al. proposed a system using credential systems to allow patients to selectively disclose their identity, thus this system guarantees that no health data is sent to the monitoring center without the patients' prior approval [20]. Concerning doctor privacy, group signatures are used to keep doctors' identities anonymous [4]. More recently, several cryptographic primitives are used in order to guarantee a number of security and privacy requirements in [5], including zero-knowledge proof, digital credential, signed proof of knowledge, bit-commitments.

2.2 Ensuring doctor privacy

A relatively understudied aspect is the relevance of doctor privacy. Matyáš [3] investigated a method of ensuring doctor privacy while enabling analysis of prescription information. However, this work does not motivate why doctors' privacy should be respected. Later Ateniese et al. [4] observed that pharmaceutical companies might want to provide financial incentives to doctors for prescribing their medicines. To prevent this, they proposed an anonymous prescription scheme that uses group signatures to keep the doctor's identity private. Finally, De Decker et al. [5] noted that preserving doctor privacy is not sufficient to prevent such bribery: pharmacists could act as *go-betweens*, revealing the doctor's identity to the briber. They proposed a privacy-preserving health-care scheme that incorporates the roles of pharmacist and health insurer as well as doctor and patient.

2.3 Observations

From the above analysis,[1] we observe that current approaches to privacy in eHealth mostly focus on patient privacy and try to solve it as an access control or authentication problem. However, eHealth systems involve many different roles, and they have their own privacy concerns. We believe that at least doctor privacy is as important as patient privacy and should be studied in more depth to avoid situations like doctor bribery as described in Section 2.2. It is also clear from the analysis that privacy in eHealth systems need to be addressed at different layers: cryptography employment guarantees privacy at the foundation layer, access control ensures privacy at the service layer; privacy by design considers privacy at the system/architecture layer. Since eHealth systems are complex [21], and require communication of many sub-systems, we study privacy in eHealth as a communication problem – message exchanges in communication protocols may cause information leakage and thus breach privacy of the communicating parties.

[1] Note that our literature study is not intended to be exhaustive.

Privacy properties have been studied in the literature and include anonymity, unlinkabiltiy, untraceability, and etc. All these notions play a role in eHealth systems and provide different strength of privacy that can be *enabled*. However, enabling privacy is far from enough. In many cases, a system needs to enforce users' privacy instead of user pursuing it, which we call *enforced privacy*.

3 Enforced privacy in other domains

In literature, enforced privacy is studied firstly in electronic voting. Benaloh and Tuinstra [22] introduced the notion of *receipt-freeness*, which expresses that a voter cannot gain any information to prove to an adversary (someone trying to force the voter to cast a specific vote) that he voted in a certain way. This notion preserves privacy of a voter even when a voter actively seeks to renounce that privacy, as in the case of vote-buying. Another stronger notion of privacy is coercion-resistance [23], stating that a voter cannot cooperate with the intruder to prove how he voted. These strong notions of privacy actually capture the essential idea that privacy must be enforced by a system upon its users, instead enabling it. Enforced privacy has also been studied in the other domains. For instance, a number of papers [24, 25] have identified a need for enforced privacy (receipt-freeness) in online auctions. However, enforced privacy has received a little attention in eHealth. In this paper, we advocate the importance of enforced privacy in eHealth (see Section 4) and discuss our approach to formally understand and verify it (see Section 5).

4 Key privacy challenges

In this section, we identify two key privacy challenges in eHealth: *enforced privacy* (e.g. a doctor cannot prove to a pharmaceutical company which medicine he prescribed) and *enforced respecting privacy* (e.g. a patient cannot reveal which doctor prescribed her medicine).

4.1 Challenge I: enforced privacy

Enforced privacy plays an important role in eHealth systems, especially for doctors. A typical scenario can be described as follows. A pharmaceutical company may want to persuade a doctor to favor a certain kind of medicine by bribing or coercing. To prevent this, a doctor should not be able to prove his prescription to a pharmaceutical company (or an adversary). It means that doctors' privacy should be enforced by eHealth systems. Generally speaking, a doctor should not be able to prove his prescription to a third party except for the trusted authorities. However, enforced privacy might not be necessary for patients as patients should have full control of their own private information, and can disclose their information (partially) to any party if needed.

Enforced privacy in eHealth is rarely studied. In general, it is worthy to investigate which roles in an eHealth system require the notion of enforced privacy.

It is also interesting to study which cryptographic techniques can be employed to enforce privacy. In this case, techniques used in other domains to guarantee receipt-freeness and coercion-resistance can be the first proposals, for example, chameleon bit commitments used in the online auction protocol [24]. In our research, we focus on formal definition of enforced privacy and efficient techniques to verify enforced privacy in eHealth. Due to the complexity of eHealth systems, all these remain as scientific challenges.

4.2 Challenge II: enforced respecting privacy

Different from voting systems and online auction protocols where privacy is mainly concerned about one role (voter and bidder, respectively), eHealth systems involved many more different roles. Therefore, one party can be bribed or coerced to reveal his private information to break another parity's privacy. In literature, it is shown that doctor's prescription pattern should be protected, which means anyone, except for a doctor himself or trusted third parties, should not link the doctor to his prescriptions. In order to obtain a doctor's prescription pattern, an adversary may bribe some other parties, such as patients or pharmacists, to reveal their private information to get a doctor's prescription. This leads us to a requirement of enforcing third party to respect a doctor's privacy, which means a third party should not be able to prove to others the link between a doctor and his prescription. In general, we identify this privacy requirement as enforced respecting privacy.

A party besides of the adversary and the party whose privacy should be enforced is considered as a third party. The notion of enforced respecting privacy implicitly covers two situations. First, the third party may reveal his private information to help the party who is willing to prove his privacy to the adversary. One example is that a patient cooperating with a bribed doctor to prove to a pharmaceutical company how the doctor prescribes. Second, the third party is bribed or coerced to reveal his private information to the adversary and the revealed information breaches privacy of a party whose privacy should be enforced. The aforementioned example still applies, while instead the doctor is honest and wants to protect his prescription pattern.

We want to emphasise that enforced respecting privacy is different from enforced privacy, e.g. receipt-freeness and coercion-resistance, in voting and online auction, since a party revealing his private information does not aim to break his own privacy but another party's privacy. This is also different from the case when an adversary controls a set of untrusted parties. Besides, it is too strong to make the assumption that the adversary has full control of a party, or the party fully cooperates with the adversary. Because it is impractical for the adversary to control, for example, all pharmacists. Enforced respecting privacy is a new notion of privacy, which has not been studied in literature. We believe it is important to eHealth systems as well and stands in its own as a challenge.

5 Our approach

We propose to use formal methods to understand and define the new privacy notions in eHealth and to build an efficient verification framework to ensure privacy properties for eHealth systems.

5.1 The need for formal methods

In literature, many research efforts have been devoted to ensure enforced privacy properties for electronic voting. Several schemes that claim receipt-freeness (e.g. [22, 26]) have been proposed and later shown to have receipts [27, 28]. Resolving this kind of situation underlines the need for formal methods, which are mathematically based techniques to specify and verify systems.

5.2 Current approaches to enforced privacy

Several formalisations of enforced privacy properties in voting have been proposed. Delaune et al. [29] developed their formalisation of receipt-freeness and coercion-resistance based on observational equivalences in the applied pi calculus [30]. Automatic verification techniques within the applied pi calculus framework have been proposed by Backes et al. [31]. Their approach focuses on remote electronic voting protocols, and mainly deals with coercion-resistance. Baskar et al. [32] define a language to specify voting protocols and use an epistemic logic to reason about receipt-freeness. Although it is relatively easy to express privacy properties based on logic of knowledge, it is rather difficult to develop verification techniques within such a logical framework. Jonker et al. [33] introduced a formal framework combining knowledge reasoning and trace equivalences to model and reason about receipt-freeness for voting protocols and provided a quantitative definition of voter-controlled privacy. Künsters et al. [34] gave a game theoretic definition of coercion-resistance as a voter has a counter strategy to cheat the adversary. Based on the work of Delaune et al. [29], Dong et al. [35] formalised receipt-freeness in online auction.

5.3 A case study

Currently, we are formalising enforced privacy and enforced respecting privacy in the applied pi calculus as observational equivalences and studying their applicability in the protocol proposed by De Decker et al. [5]. One advantage of using the applied pi calculus is that it is supported by an automatic verification tool ProVerif [36], which takes the applied pi model and properties as input and checks whether the properties can be proved on the model. In this case study, the following key properties are verified:

- secrecy of private information of patients and doctors: to prevent secret information from being intercepted;

– authentication of patients and doctors: to guarantee the communication is truly between the one a participant wants to talk to;
– patient and doctor anonymity: to keep patients' and doctors' identity secret;
– patient untraceability: to prevent the possibility to identify two separate sessions executed by a same patient;
– patient-prescription unlinkability: to guarantee the prescription is not linked to a patient even if the patient's identity is not revealed;
– doctor-prescription unlinkability: to guarantee a doctor's prescription pattern is not revealed;
– doctor enforced privacy: to prevent a doctor from being bribed by a pharmaceutical company, i.e. the doctor cannot prove which medicine he prescribed;
– doctor enforced respecting privacy: to guarantee a doctor's prescription pattern is not revealed, even if other parties cooperating with the adversary.

5.4 Future directions

We give a few direction we want to pursuit in the future. The formalisation of enforced privacy in voting based on observational equivalences [29] provides users with a fixed defensive strategy. This strategy entails the bribed or coerced voter being teamed up with another voter, such that one of their two cast votes matches the adversary's wishes. The adversary cannot determine who has cast the matching vote. This forming of defensive coalitions was introduced as a modelling trick to ensure observational equivalence between a trace where a voter votes according to the coercers desires and one where he does not. In general, we envisage more applications for coalition-forming in the formal understanding of enforced privacy. On one hand, different parties may form larger coalitions and so have a more robust defensive model. On the other hand, privacy with respect to an adversary conspiring with multiple parties is inherently lower than the privacy with respect to an adversary without such a coalition or with a smaller coalition. Hence, a game theoretic approach combined with observational equivalences is an interesting approach to enforce and enforced respecting privacy.

Assurance of privacy properties via formal verification is an important step in developing eHealth systems. However, automatic verification of observational equivalences is in general undecidable.[2] Recently, research has been devoted to decision procedures for observational equivalences by focusing on a fragment of the applied pi calculus [37]. It is interesting to see how this can help verification of privacy properties in eHealth. Another possible way to verification is to formalise a proof system of the applied pi calculus [38] in a theorem theorem, hence resulting a semi-automatic support for privacy verification.

6 Conclusion

eHealth systems are drawing people's attentions because of its potential advantages. However, because of several challenges, the adoption of eHealth systems

[2] The tool ProVerif provides quite limited support.

by the general public is still at an early stage. One of the key challenges is to understand privacy issues in eHealth. Current study on this topic mainly focuses on patient privacy and solves it as an access control problem. Privacy issues of other involved parties and during communications are rarely studied so far. Besides of enabling privacy in eHealth, such as protecting patients' private information, we believe that enforced privacy plays a critical role, especially for doctors. We have also identified another privacy requirement, enforced respecting privacy. Currently, our way to study privacy, enforced privacy and enforced respecting privacy in eHealth is to employ formal methods.

References

1. Meingast, M., Roosta, T., Sastry, S.S.: Security and privacy issues with health care information technology. In: Proc. 28th Annual Conference of the IEEE Engineering in Medicine and Biology Society, IEEE CS (2006) 5453–5458
2. Kotz, D., Avancha, S., Baxi, A.: A privacy framework for mobile health and home-care systems. In: Proc. Workshop on Security and Privacy in Medical and Home-Care Systems, ACM Press (2009) 1–12
3. Matyáš, V.: Protecting doctors' identity in drug prescription analysis. Health Informatics Journal (1998) 205–209
4. Ateniese, G., de Medeiros, B.: Anonymous e-prescriptions. In: Proc. ACM Workshop on Privacy in the Electronic Society, ACM Press (2002) 19–31
5. De Decker, B., Layouni, M., Vangheluwe, H., Verslype, K.: 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., Springer (2008) 118–133
6. Anderson, R.: A security policy model for clinical information systems. In: Proc. 17th IEEE Symposium on Security and Privacy, IEEE CS (1996) 30–43
7. Louwerse, K.: The electronic patient record; the management of access – case study: Leiden University hospital. International Journal of Medical Informatics **49** (1998) 39–44
8. Reid, J., Cheong, I., Henricksen, M., Smith, J.: A novel use of rBAC to protect privacy in distributed health care information systems. In: Proc. 8th Australian Conference on Information Security and Privacy. Volume 2727 of LNCS., Springer (2003) 403–415
9. Evered, M., Bögeholz, S.: A case study in access control requirements for a health information system. In: Proc. 2nd Australian Information Security Workshop. Volume 32 of Conferences in Research and Practice in Information Technology., Australian Computer Society (2004) 53–61
10. Hung, P.C.K.: Towards a privacy access control model for e-healthcare services. In: Proc. 3rd Annual Conference on Privacy, Security and Trust. (2005)
11. Currim, F., Jung, E., Xiao, X., Jo, I.: Privacy policy enforcement for health information data access. In: Proc. 1st ACM Workshop on Medical-grade Wireless Networks, ACM Press (2009) 39–44
12. Barni, M., Failla, P., Kolesnikov, V., Lazzeretti, R., Sadeghi, A.R., Schneider, T.: Secure evaluation of private linear branching programs with medical applications. In: Proc. 14th European Symposium on Research in Computer Security. Volume 5789 of LNCS., Springer (2009) 424–439

13. Sneha, S., Varshney, U.: Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. Decision Support Systems **46** (2009) 606–619
14. Ko, J., Lu, C., Srivastava, M.B., Stankovic, J.A., Terzis, A., Welsh, M.: Wireless sensor networks for healthcare. Proceedings of IEEE **98** (2010) 1947–1960
15. Maglogiannis, I., Kazatzopoulos, L., Delakouridis, C., Hadjiefthymiades, S.: Enabling location privacy and medical data encryption in patient telemonitoring systems. IEEE Transactions on Information Technology in Biomedicine **13** (2009) 946–954
16. Chiu, D.K.W., Hung, P.C.K., Cheng, V.S.Y., Kafeza, E.: Protecting the exchange of medical images in healthcare process integration with web services. In: Proc. 40th Hawaii Conference on Systems Science, IEEE CS (2007) 131–140
17. Biskup, J., Bleumer, G.: Cryptographic protection of health information: cost and benefit. International Journal of Bio-Medical Computing **43** (1996) 61–67
18. van der Haak, M., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M., Wetter, T.: Data security and protection in cross-institutional electronic patient records. International Journal of Medical Informatics **70** (2003) 117–130
19. Ateniese, G., Curtmola, R., de Medeiros, B., Davis, D.: Medical information privacy assurance: Cryptographic and system aspects. In: Proc. 3rd Conference on Security in Communication Networks. Volume 2576 of Lecture Notes in Computer Science., Springer (2003) 199–218
20. Layouni, M., Verslype, K., Sandikkaya, M.T., De Decker, B., Vangheluwe, H.: Privacy-preserving telemonitoring for eHealth. In: Proc. 23rd Annual IFIP Working Conference on Data and Applications Security. Volume 5645 of LNCS., Springer (2009) 95–110
21. Tien, J.M., Goldschmidt-Clermont, P.: Healthcare: A complex service system. Journal of Systems Science and Systems Engineering **18** (2009) 257–282
22. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections (extended abstract). In: Proc. 26th Symposium on Theory of Computing, ACM Press (1994) 544–553
23. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proc. 4th ACM Workshop on Privacy in the Electronic Society, ACM Press (2005) 61–70
24. Abe, M., Suzuki, K.: Receipt-free sealed-bid auction. In: Proc. 5th Conference on Information Security. Volume 2433 of LNCS., Springer (2002) 191–199
25. Chen, X., Lee, B., Kim, K.: Receipt-free electronic auction schemes using homomorphic encryption. In: Proc. 6th Conference on Information Security and Cryptology. Volume 2971 of LNCS., Springer (2003) 259–273
26. Lee, B., Kim, K.: Receipt-free electronic voting through collaboration of voter and honest verifier. In: Proc. Japan-Korea Joint Workshop on Information Security and Cryptology. (2000) 101–108
27. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Proc. 19th Conference on the Theory and Application of Cryptographic Techniques. Volume 1807 of LNCS., Springer (2000) 539–556
28. Lee, B., Kim, K.: Receipt-free electronic voting with a tamper-resistant randomizer. In: Proc. 4th Conference on Information and Communications Security. Volume 2513 of LNCS., Springer (2002) 389–406
29. Delaune, S., Kremer, S., Ryan, M.D.: Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security **17** (2009) 435–487
30. Abadi, M., Fournet, C.: Mobile values, new names, and secure communication. In: Proc. 28th Symposium on Principles of Programming Languages, ACM Press (2001) 104–115

31. Backes, M., Hriţcu, C., Maffei, M.: Automated verification of remote electronic voting protocols in the applied pi-calculus. In: Proc. 21st IEEE Computer Security Foundations Symposium, IEEE CS (2008) 195–209
32. Baskar, A., Ramanujam, R., Suresh, S.: Knowledge-based modelling of voting protocols. In: Proc. 11th Conference on Theoretical Aspects of Rationality and Knowledge, ACM Press (2007) 62–71
33. Jonker, H.L., Mauw, S., Pang, J.: A formal framework for quantifying voter-controlled privacy. Journal of Algorithms in Cognition, Informatics and Logic **64** (2009) 89–105
34. Küsters, R., Truderung, T., Vogt, A.: A game-based definition of coercion-resistance and its applications. In: Proc. 23rd IEEE Computer Security Foundations Symposium, IEEE CS (2010) 122–136
35. Dong, N., Jonker, H.L., Pang, J.: 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., Springer (2011) 223–238
36. Blanchet, B.: An efficient cryptographic protocol verifier based on prolog rules. In: Proc. 14th IEEE Computer Security Foundations Workshop, IEEE CS (2001) 82–96
37. Cortier, V., Delaune, S.: A method for proving observational equivalence. In: Proc. 22nd IEEE Computer Security Foundations Symposium, IEEE CS (2009) 266–276
38. Liu, J., Lin, H.: Proof system for applied pi calculus. In: Proc. 6th IFIP Conference on Theoretical Computer Science. Volume 323 of IFIP., Springer (2010) 229–243