

Privacy in eVoting

(joint work with Erik de Vink and Sjouke Mauw)

Hugo Jonker

h.l.jonker@tue.nl

TU/e overview

lr	ntro	duc	tion

- overview
- Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

- voting in the "real world"
 - privacy in voting
- voting electronically (digitally / over the internet)
 - ♦ (aside) irregularities
 - privacy in evoting
- formalising privacy
 - characterising receipts
 - receipt-freeness as anonymity
 - current / future work

TU/e typical elections

Introduction

- Real world voting
- typical elections
- preventing cheating
- privacy
- eVoting
- Receipt-freeness
- Characterising receipts
- Strong RF
- Current / future work

- set of candidates
- set of voters
- one vote for one candidate per voter
- result is multiset of cast votes
- E.g. national elections in the Netherlands.

TU/e preventing cheating

Introduction

Real world voting

• typical elections

• preventing cheating

privacy

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

Cheating in elections is prevented by law, procedures and regulations, e.g.:

At all times during the elections, the chairman and two members of the voting bureau are present *Kieswet, Artikel J lid 12 sub 1*

This provides (some) protection against incorrect voting, multiple voting, incorrect counting, etc. etc.

TU/e privacy

Introduction

- Real world voting
- typical elections
- preventing cheating
- privacy
- eVoting
- Receipt-freeness
- Characterising receipts
- Strong RF
- Current / future work

per-district:

- record kept of who votes
- paper ballots: mixed, so somewhat ok (note: UK elections)
 voting machines: unclear
- district size: average of $\pm 1,400$ voters

TU/e pro's & con's

Introduction

Real world voting

eVoting

●pro's & con's

irregularities

• properties

• privacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

advantages:

disadvantages:

Hugo Jonker, Process Algebra Meetings, January 31st, 2007

TU/e pro's & con's

Introduction

Real world voting

eVoting

● pro's & con's

• irregularities

• properties

privacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

advantages:

- **•** more voter convenience ($\stackrel{?}{\Longrightarrow}$ greater turnout)
- less overhead
- quicker counting
- large scale updates are easy

disadvantages:

TU/e pro's & con's

Introduction

Real world voting

eVoting

● pro's & con's

• irregularities

propertiesprivacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

advantages:

- **•** more voter convenience ($\stackrel{?}{\Longrightarrow}$ greater turnout)
- less overhead
- quicker counting
- Iarge scale updates are easy
- disadvantages:
- costlier
- re-invent the wheel:
 - danger of introducing new flaws
 - risk of forgetting about known flaws
- Iarge scale updates are easy

TU/e irregularities

Introduction

Real world voting

eVoting

• pro's & con's

irregularitiesproperties

proportion
 privacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

As an aside, some insights / anecdotes on:

- Sdu voting machine reveals votes through radiation
- Nedap voting machines not secure
- elections irregularities in Eindhoven

TU/e properties

Introduction

Real world voting

eVoting

• pro's & con's

• irregularities

propertiesprivacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

established voting properties include:

- democracy
- eligibility
- accuracy
- verifiability
 - individual
 - universal
- fairness

TU/e privacy

Introduction

Real world voting

eVoting

• pro's & con's

irregularities

propertiesprivacy

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

Anonymity vote is private w.r.t. an observer

- receipt-freeness no proof
- strong receipt-freeness no elimination of possibilities
- coercion-resistance
 - no randomisation
 - no abstention
 - no simulation

TU/e intuition

Introduction

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

A receipt proves how a voter voted.

TU/e intuition

Introduction

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

A receipt proves how a voter voted.

Examples:

- Everyone signs their vote.

TU/e intuition

Introduction

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

A receipt proves how a voter voted.

Examples:

- Everyone signs their vote.
- In Italy, simultaneous elections were held for various posts, using one ballot. The order of posts listed is up to the voter, and is preserved. An attacker (El Mafiosi) can assign each voter a specific order of posts. Benaloh & Tuinstra

In	strc	vdı.	inti	on
- 11	iuu	JUL	มนเ	υu

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

More precisely: a receipt r proves that a voter v cast a vote for candidate c.

Introduction

Real world voting

eVoting

_					
Re	cei	pt-	fre	en	ess

intuition

requirements

Characterising receipts

Strong RF

Current / future work

More precisely: a receipt r proves that a voter v cast a vote for candidate c.

R1: r authenticates v

Introduction

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

More precisely: a receipt r proves that a voter v cast a vote for candidate c.

R1: r authenticates v

R2: r proves that v chose candidate c

requirements TU/e

Introduction
Real world voting
eVoting
Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

More precisely: a receipt r proves that a voter v cast a vote for candidate c.

- \blacksquare R1: r authenticates v
- **R2:** r proves that v chose candidate c
- **R3:** r proves that v cast her vote

Introduction

Real world voting

eVoting

Receipt-freeness

intuition

requirements

Characterising receipts

Strong RF

Current / future work

More precisely: a receipt r proves that a voter v cast a vote for candidate c.

- **R1:** r authenticates v
- **R2:** r proves that v chose candidate c
- **R3:** r proves that v cast her vote

Note:

- Specific for this type of elections
- Quite strict

TU/e ingredients

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms
suitable terms

Strong RF

Current / future work

- voters $v \in \mathcal{V}$, choices $c \in \mathcal{C}$
- ballots \mathcal{B} and results (multisets of choices) $\mathcal{M}(\mathcal{C})$
- a set of received ballots *RB*, from which the result will be computed
- a choice function $\Gamma \colon \mathcal{V} \to \mathcal{C}$, which specifies how the voters vote

TU/e ingredients

Introduction	

Real world voting

eVoting

- Receipt-freeness
- Characterising receipts

ingredients

- decomposing receipts
- receipts as terms
 suitable terms
- Strong RF
- Current / future work

- voters $v \in \mathcal{V}$, choices $c \in \mathcal{C}$
- ballots \mathcal{B} and results (multisets of choices) $\mathcal{M}(\mathcal{C})$
- a set of received ballots *RB*, from which the result will be computed
- a choice function $\Gamma \colon \mathcal{V} \to \mathcal{C}$, which specifies how the voters vote
- \blacksquare the set of receipts $\mathcal R$
- Terms(v), the set of all terms that a voter $v \in \mathcal{V}$ can generate
- authentication terms $\mathcal{AT}(v)$: $t \in \mathcal{AT}(v) \implies \forall w \neq v : t \notin Terms(w)$
- $auth: \mathcal{AT} \to \mathcal{V}$, the unique voter that created an AT

duction	
world voting	
ng	$\blacksquare \alpha : \mathcal{R}$
ipt-freeness	$\blacksquare \beta : \mathcal{R}$
acterising receipts	$\bullet \gamma : \mathcal{R}$
composing receipts	
eipts as terms	
table terms	Formai
ig RF	
ent / future work	

Intro

Real

eVot

Rece

Chai ing de

Stror

Curr

he following functions are used to decompose receipts:

 $\alpha \colon \mathcal{R} \to \mathcal{AT}$, extract authentication term from receipt $\beta \colon \mathcal{R} \to \mathcal{RB}$, extract ballot from receipt $\gamma \colon \mathcal{R} \to \mathcal{C}$, extract candidate from receipt

Formalisation of the requirements:

 Introduction
 Infection

 Real world voting
 $\alpha: \mathcal{R} - \alpha$

 eVoting
 $\alpha: \mathcal{R} - \alpha$

 Receipt-freeness
 $\beta: \mathcal{R} - \alpha$

 Characterising receipts
 $\gamma: \mathcal{R} - \alpha$

 • ingredients
 $\varphi: \mathcal{R} - \alpha$

 • decomposing receipts
 $\varphi: \mathcal{R} - \alpha$

 • suitable terms
 Formalis

 Strong RF
 $\mathbb{R}1: \alpha(\alpha)$

The following functions are used to decompose receipts:

α: R → AT, extract authentication term from receipt
β: R → RB, extract ballot from receipt
γ: R → C, extract candidate from receipt

Formalisation of the requirements:

```
• R1: \alpha(r) \in \mathcal{AT}(v)
```

Introduction
Real world voting
eVoting
Receipt-freeness
Characterising receipts
ingredients
decomposing receipts
receipts as terms
suitable terms

Strong RF

Current / future work

The following functions are used to decompose receipts:

α: R → AT, extract authentication term from receipt
β: R → RB, extract ballot from receipt
γ: R → C, extract candidate from receipt

Formalisation of the requirements:

```
R1: \alpha(r) \in \mathcal{AT}(v)
R2: \gamma(r) = \Gamma(v)
```

Introduction
Real world voting
eVoting
Receipt-freeness
Characterising receipts
ingredients
decomposing receipts
receipts as terms
suitable terms

Strong RF

Current / future work

The following functions are used to decompose receipts:

- α: R → AT, extract authentication term from receipt
 β: R → RB, extract ballot from receipt
 γ: R → C, extract candidate from receipt
- Formalisation of the requirements:

R1:
$$\alpha(r) \in \mathcal{AT}(v)$$

R2: $\gamma(r) = \Gamma(v)$

R3:
$$\beta(r) \in \mathcal{RB}$$

Introduction Real world voting eVoting Receipt-freeness Characterising receipts • ingredients

decomposing receipts

receipts as terms
suitable terms

Strong RF

Current / future work

The following functions are used to decompose receipts:

α: R → AT, extract authentication term from receipt
β: R → RB, extract ballot from receipt
γ: R → C, extract candidate from receipt

Formalisation of the requirements:

```
■ R1: \alpha(r) \in \mathcal{AT}(v)
■ R2: \gamma(r) = \Gamma(v)
```

R3: $\beta(r) \in \mathcal{RB}$

So, for valid receipts: $auth(\alpha(r)) = v \implies \gamma(r) = \Gamma(v)$, which is satisfied by $\gamma = \Gamma \circ auth \circ \alpha$.

TU/e receipts as terms

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms
suitable terms

Strong RF

Current / future work

Intuitively, a receipt must be derivable from an actual execution of a voting protocol (i.e. receipts generated outside a protocol do not invalidate that protocol).

To facilitate detection of receipts, limit the notion of receipts to terms (i.e. $\mathcal{R} = \emptyset \lor \mathcal{R} \subseteq Terms$).

Now:

Model the protocol in ACP

Test suitability of communicated terms as receipts

Pronounce judgment

TU/e receipts as terms

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms
suitable terms

Strong RF

Current / future work

Intuitively, a receipt must be derivable from an actual execution of a voting protocol (i.e. receipts generated outside a protocol do not invalidate that protocol).

To facilitate detection of receipts, limit the notion of receipts to terms (i.e. $\mathcal{R} = \emptyset \lor \mathcal{R} \subseteq Terms$).

Now:

Model the protocol in ACP (+ tweaks)

Test suitability of communicated terms as receipts

Pronounce judgment

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms

suitable terms

Strong RF

Current / future work

Write $t \in t'$ if t is a subterm of t'.

 α, β extract terms from terms, i.e. they deal with subterms.

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms

suitable terms

Strong RF

Current / future work

Write $t \in t'$ if t is a subterm of t'.

 α,β extract terms from terms, i.e. they deal with subterms.

Lemma $\forall t \in \mathcal{R} \colon \alpha(t) \in t \land \beta(t) \in t$

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

receipts as terms

suitable terms

Strong RF

Current / future work

Write $t \in t'$ if t is a subterm of t'.

 α,β extract terms from terms, i.e. they deal with subterms.

.emma
$$\forall t \in \mathcal{R} \colon \alpha(t) \in t \land \beta(t) \in t$$

(Note that, by definition: $t \in t' \land t \in AT(v) \implies t' \in AT(v)$. So receipts are themselves authentication terms)

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

ingredients

decomposing receipts

• receipts as terms

Strong RF

• suitable terms

Current / future work

Write $t \in t'$ if t is a subterm of t'.

 α, β extract terms from terms, i.e. they deal with subterms. Lemma $\forall t \in \mathcal{R} \colon \alpha(t) \in t \land \beta(t) \in t$

(Note that, by definition: $t \in t' \land t \in AT(v) \implies t' \in AT(v)$. So receipts are themselves authentication terms)

Although this does not capture the entire notion of receipts, it turns out to be strong enough in the examined cases.

TU/e RF \approx anonymity

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

 $\bullet\,\mathrm{RF}\approx\mathrm{anonymity}$

unlinkability

Current / future work

Anonymity, 3 flavours:

sender/voter anonymity? no, voter tries to prove vote

TU/e RF \approx anonymity

Introduction	
Real world voting	

eVoting

Receipt-freeness

Characterising receipts

Strong RF

ullet RF pprox anonymity

ullet unlinkability

Current / future work

Anonymity, 3 flavours:

- sender/voter anonymity? no, voter tries to prove vote
- plausible deniability? no, sender knows how she voted

TU/e RF \approx anonymity

	A
Introduction	
Real world voting	
eVoting	
Receipt-freeness	
Characterising receipts	
Strong RF	
ullet RF $pprox$ anonymity	
unlinkability	

Current / future work

Anonymity, 3 flavours:

- sender/voter anonymity? no, voter tries to prove vote
- plausible deniability? no, sender knows how she voted
- unlinkability?
 - "no link between vote and voter"...

unlinkability TU 6

Introduction	
Real world voting	
eVoting	
Receipt-freeness	
Characterising receipts	
Strong RF	

 \bullet RF \approx anonymity

e

unlinkability

Current / future work

nlinkability of message m to sender v:

- intruder does not know that v sent m
- intruder cannot rule out that v sent any message m', where $m' \in AS$, the Anonymity Set
e unlinkability TU/

Introduction	Unlir
Real world voting	■ int
eVoting	– inu
Receipt-freeness	■ int
Characterising receipts	m'
Strong RF	
ullet RF $pprox$ anonymity	"~

Current / future work

unlinkability

hkability of message m to sender v:

- ruder does not know that v sent m
- ruder cannot rule out that v sent any message m', where $\in AS$, the Anonymity Set
- 'cannot rule out"

TU/e unlinkability

Introduction	

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

• RF \approx anonymity • unlinkability

Current / future work

Unlinkability of message m to sender v:

• intruder does not know that v sent m

■ intruder cannot rule out that v sent any message m', where $m' \in AS$, the Anonymity Set

... "cannot rule out" ...

strong rf the intruder cannot rule out *any* vote from the anonymity set.

TU/e different approaches

Current situation:

Ir	٦t	ro	d	uc	Cti	OI	n	

|--|

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

- Delaune, Kremer and Ryan proposed an approach based on bisimilarity
 - ignoring the notion of receipts
- Jonker and De Vink proposed an approach based on the characteristics of a receipt
 - founded on the notion of receipts

TU/e different approaches

Current situation:

Introduction	

```
Real world voting
```

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

• todo

- Delaune, Kremer and Ryan proposed an approach based on bisimilarity
- ignoring the notion of receipts
- Jonker and De Vink proposed an approach based on the characteristics of a receipt
 - founded on the notion of receipts

Almost reminiscant of Heisenberg vs. Schrödinger ;-)

TU/e unifying approach

Introduction
Real world voting
eVoting
Receipt-freeness
Characterising receipts
Strong RF
Current / future work
• different approaches

• unifying approach

• todo

- In the branching bisimilarity as an equivalence seems to strong e.g. order in which voters vote does not affect rf
- checking terms J&DV-style seems imprecise not a precise notion of receipts
- so unite the two! construct an appropriate equivalence notion for voting processes based on identifying receipts

TU/e todo

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

• unifying approach

● todo

Combine J&DV and DKR

How do the various privacy notions relate to eachother?

TU/e todo

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approachesunifying approach

• todo

Combine J&DV and DKR

How do the various privacy notions relate to eachother?

Further reading:

- "Formalising Receipt-Freeness", H.L. Jonker and E.P. de Vink. In Information Security Conference 2006, LNCS 4176
- "Receipt-Freeness as a special case of Anonymity in Epistemic Logic", Hugo Jonker and Wolter Pieters, WOTE 2006

TU/e todo

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- Combine J&DV and DKR
- How do the various privacy notions relate to eachother?

Further reading:

- "Formalising Receipt-Freeness", H.L. Jonker and E.P. de Vink. In Information Security Conference 2006, LNCS 4176
- "Receipt-Freeness as a special case of Anonymity in Epistemic Logic", Hugo Jonker and Wolter Pieters, WOTE 2006

Thanks for your attention

TU/e example: BT

Introduction
Real world voting
eVoting
Receipt-freeness
Characterising receipts
Strong RF
Current / future work

- different approaches
- unifying approachtodo

- Original receipt-freeness paper by Benaloh & Tuinstra
- Attack found... but not on the main scheme
- Assumes untappable channels and a voting booth
- Uses randomised encryption and "ZKP"

Process for voting authority:

Process for a voter:

TU/e example: BT

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approachesunifying approach

• todo

Original receipt-freeness paper by Benaloh & Tuinstra

Attack found... but not on the main scheme
Assumes untappable channels and a voting booth

Uses randomised encryption and "ZKP"

Process for voting authority:

$$A(v) = \sum_{x \in E(0), y \in E(1)} s_{a \to v}(\min(x, y), \max(x, y)) \cdot p_{a \to v}^*(x \in E(0) \land y \in E(1)) \cdot (r_{v \to a}(x) + r_{v \to a}(y))$$

Process for a voter:

TU/e example: BT

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approachesunifying approach

• todo

- Original receipt-freeness paper by Benaloh & Tuinstra
- Attack found... but not on the main scheme
 Assumes untappable channels and a voting booth
 Uses randomised encryption and "ZKP"

Process for voting authority:

$$A(v) = \sum_{x \in E(0), y \in E(1)} s_{a \to v}(\min(x, y), \max(x, y)) \cdot p_{a \to v}^*(x \in E(0) \land y \in E(1)) \cdot (r_{v \to a}(x) + r_{v \to a}(y))$$

Process for a voter:

$$V = \sum_{x,y} r_{a \to v}(x,y) \cdot \sum_{i \in \{0,1\}} p^*_{a \to v}(x \in E(i) \land y \in E(1-i)) \cdot (\Gamma(v) = i \to s_{v \to a}(x) + \Gamma(v) = 1 - i \to s_{v \to a}(y))$$

TU/e BT: receipt-free

Introduction	

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

Let's examine the voter process:

TU/e **BT: receipt-free**

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

• different approaches

• unifying approach

● todo

Let's examine the voter process:

 $V = \sum_{x,y} r_{a \to v}(x,y) \cdot$ Not an authentication term

TU/e BT: receipt-free

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

Let's examine the voter process:

 $V = \sum_{x,y} r_{a \to v}(x,y) \cdot$

Not an authentication term

 $\sum_{i \in \{0,1\}} p_{a \to v}^* (x \in E(i) \land y \in E(1-i)).$

No ballot as a subterm

TU/e **BT: receipt-free**

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

• different approaches

• unifying approach

● todo

Let's examine the voter process:

 $V = \sum_{x,y} r_{a \to v}(x,y) \cdot$ Not an authentication term

$$\sum_{i \in \{0,1\}} p^*_{a \to v} (x \in E(i) \land y \in E(1-i)) \cdot$$
 No ballot as a subterm

$$\begin{pmatrix} \Gamma(v) = i \to s_{v \to a}(x) + \Gamma(v) = 1 - i \to s_{v \to a}(y) \end{pmatrix}$$

Subterm of first term!

TU/e BT: receipt-free

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

Let's examine the voter process:

 $V = \sum_{x,y} r_{a \to v}(x,y) \cdot$ Not an authentication term

$$\sum_{i \in \{0,1\}} p_{a \to v}^* (x \in E(i) \land y \in E(1-i)) \cdot$$
 No ballot as a subterm

$$\begin{pmatrix} \Gamma(v) = i \to s_{v \to a}(x) + \Gamma(v) = 1 - i \to s_{v \to a}(y) \end{pmatrix}$$

Subterm of first term!

None of the terms from the voter can satisfy $\alpha(t) \in t \land \beta(t) \in t$ \implies BT is receipt-free!

		1.1		11		
In	tro	Da	uc	tı	on	

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

• unifying approach

● todo

Rough sketch of the FOO protocol for voter v, admin a and counter cnt:

1. v: create a blinded, encrypted vote

In	tr	0	111	cti	on
	u.	U.	JU	υu	

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v

Introduction	
Real world voting	
eVoting	
Receipt-freeness	
Characterising receipts	
Strong RF	
Current / future work	

different approaches

unifying approach

● todo

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a

Inter duction	Ro
Introduction	
Real world voting	CO
eVotina	
	1
Receipt-freeness	1.
	2
Characterising receipts	Ζ.
	•
Strong RF	3.
Current / future work	4.
 different approaches 	••
unifying approach	

● todo

- . v: create a blinded, encrypted vote
- . $v \rightarrow a$: blinded, encrypted vote signed by v
- . $a \rightarrow v$: blinded, encrypted vote signed by a
- Let $v \rightarrow cnt$: encrypted vote signed by a

Introduction	Roi
	COU
Real world voting	000
eVoting	
	1. ι
Receipt-freeness	
Characterising receipts	2. <i>i</i>
Strong RF	3. <i>c</i>
Current / future work	Δ
different approaches	-r . (
unifying approach	E
	D (

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- **B.** $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes

Introduction
Real world voting
eVoting
Receipt-freeness
Characterising receipts
Strong RF

Current / future work

- different approachesunifying approach
- todo

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes
- 6. cnt: publish list of received votes

Introduction
Real world voting
eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes
- 6. cnt: publish list of received votes
- 7. $v \rightarrow cnt$: decryption key, index of vote in list

I	ntr	od	uc	tion	1

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes
- 6. cnt: publish list of received votes
- 7. $v \rightarrow cnt$: decryption key, index of vote in list
- 8. *cnt*: publish list of received keys

Introduction	

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

Rough sketch of the FOO protocol for voter v, admin a and counter cnt:

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes
- 6. cnt: publish list of received votes
- 7. $v \rightarrow cnt$: decryption key, index of vote in list
- 8. *cnt*: publish list of received keys

Obvious receipt... but it seems to lose its validity

Į	Inti	00	luc	tio	n

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

Rough sketch of the FOO protocol for voter v, admin a and counter cnt:

- 1. v: create a blinded, encrypted vote
- 2. $v \rightarrow a$: blinded, encrypted vote signed by v
- 3. $a \rightarrow v$: blinded, encrypted vote signed by a
- 4. $v \rightarrow cnt$: encrypted vote signed by a
- 5. cnt: collect all votes
- 6. cnt: publish list of received votes
- 7. $v \rightarrow cnt$: decryption key, index of vote in list
- 8. *cnt*: publish list of received keys

Obvious receipt... but it seems to lose its validity Timestamping \implies no it doesn't!

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
- Obvious receipt

How it works:

Introduction Real world voting eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

Used in Dutch water management board elections

- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

1. $s_{a \to v}$: key(v)

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

1. $s_{a \to v}$: key(v)

2. *a*: publish list of all possible encrypted votes, hashed: $\mathcal{L} = \bigcup_{v \in \mathcal{V}} \{ \langle h(\{c\}_{key(v)}), c \rangle \mid c \in \mathcal{C} \}$

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

- **1.** $s_{a \to v}$: key(v)
- 2. *a*: publish list of all possible encrypted votes, hashed: $\mathcal{L} = \bigcup_{v \in \mathcal{V}} \{ \langle h(\{c\}_{key(v)}), c \rangle \mid c \in \mathcal{C} \}$

3. $p_{v \to a}$: $\{\Gamma(v)\}_{key(v)}$

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

- **1.** $s_{a \to v}$: key(v)
- 2. *a*: publish list of all possible encrypted votes, hashed: $\mathcal{L} = \bigcup_{v \in \mathcal{V}} \{ \langle h(\{c\}_{key(v)}), c \rangle \mid c \in \mathcal{C} \}$

3.
$$p_{v \to a}$$
: $\{\Gamma(v)\}_{key(v)}$

4. *a*: collect all votes

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

- Current / future work
- different approaches
- unifying approachtodo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

- **1.** $s_{a \rightarrow v}$: key(v)
- 2. *a*: publish list of all possible encrypted votes, hashed: $\mathcal{L} = \bigcup_{v \in \mathcal{V}} \{ \langle h(\{c\}_{key(v)}), c \rangle \mid c \in \mathcal{C} \}$
- **3.** $p_{v \to a}$: $\{\Gamma(v)\}_{key(v)}$
- 4. *a*: collect all votes
- 5. *a*: publish outcome

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approachtodo

- Used in Dutch water management board elections
- Handled over 70,000 votes
- Uses a publicly-known hash-function and voter-specific keys
 Obvious receipt

How it works:

- **1.** $s_{a \to v}$: key(v)
- 2. *a*: publish list of all possible encrypted votes, hashed: $\mathcal{L} = \bigcup_{v \in \mathcal{V}} \{ \langle h(\{c\}_{key(v)}), c \rangle \mid c \in \mathcal{C} \}$
- 3. $p_{v \rightarrow a}$: { $\Gamma(v)$ }_{key(v)}
- 4. a: collect all votes
- 5. *a*: publish outcome

Notice a receipt?

TU/e receipts in RIES

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

To prove that v cast a vote for candidate c, it suffices to show an k such that $\langle h(\{c\}_k), c \rangle \in \mathcal{L}$.

This is precisely the voter's key!

TU/e receipts in RIES

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

• different approaches

unifying approach

● todo

To prove that v cast a vote for candidate c, it suffices to show an k such that $\langle h(\{c\}_k), c \rangle \in \mathcal{L}$.

This is precisely the voter's key!

This means the following in the formalism:

 $\bullet \ \alpha(x) = x$

 $\bullet \ \beta(x) = x$
TU/e receipts in RIES

Introduction

Real world voting

eVoting

Receipt-freeness

Characterising receipts

Strong RF

Current / future work

different approaches

unifying approach

● todo

To prove that v cast a vote for candidate c, it suffices to show an k such that $\langle h(\{c\}_k), c \rangle \in \mathcal{L}$.

This is precisely the voter's key!

This means the following in the formalism:

 $\bullet \ \alpha(x) = x$

• $\beta(x) = x \dots$ for suitable \mathcal{RB}