Traceable Receipt-Free Encryption

Henri Devillez, Olivier Pereira, Thomas Peters

UCLouvain, Louvain-la-Neuve, Belgium

Asiacrypt '22 – December 2022

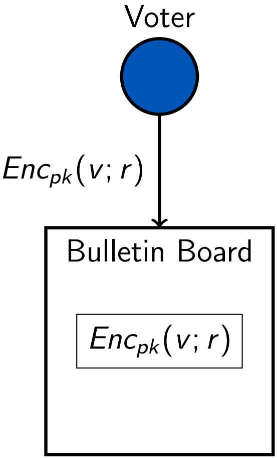
Motivation: Non-interactive vote submission

Verifiability

Bulletin Board + ZKP

Ballot Privacy

NM-CPA encryption

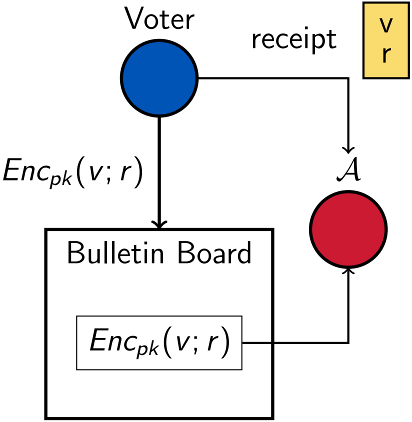


Receipt-Freeness

Other privacy issue

Voter can prove how she votes by disclosing (v, r)

Ballot privacy is not enough



Rerandomization countermeasure

Achieving RF

No opening vs
Multiple openings

Rerandomization countermeasure

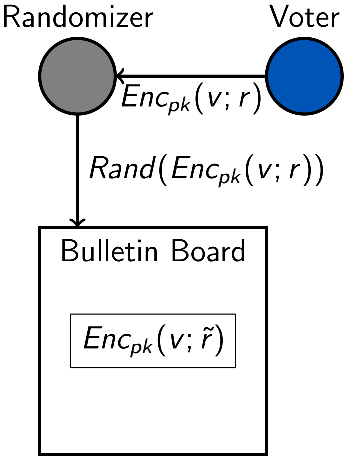
Achieving RF

No opening vs Multiple openings

Rerandomization of ciphertext

Verifiability

Unmalleable with respect to vote



A Non-Interactive Receipt-Free protocol

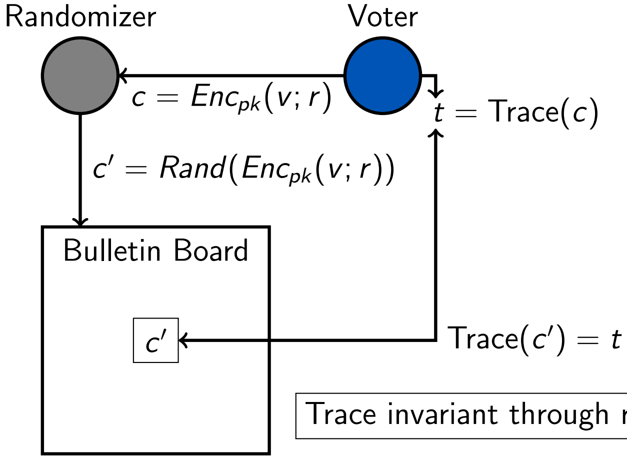
Existing solutions

1. Hirt et al: Randomizer sends a designated verifier proof
2. Blazy et al, Belenios-RF: Based on Signatures on Randomizable Ciphertexts
    - RCCA security is not enough
    - Registration to obtain the signature key
    - efficiency: bit-by-bit encryption

Our solution

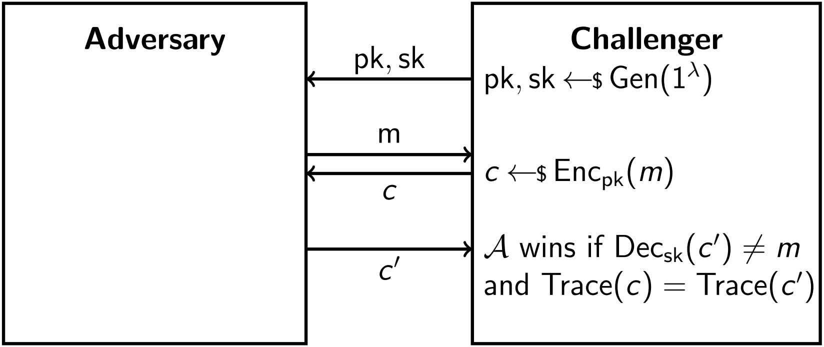
- Identify the exact security notion required for RF
- Efficient: support encryption of group elements

Tracing ciphertexts



Trace invariant through randomization

Traceable Encryption



Adversary

Challenger

pk, sk

$\mathsf{pk}, \mathsf{sk} \leftarrow\!\!\$\, \mathsf{Gen}(1^\lambda)$

m

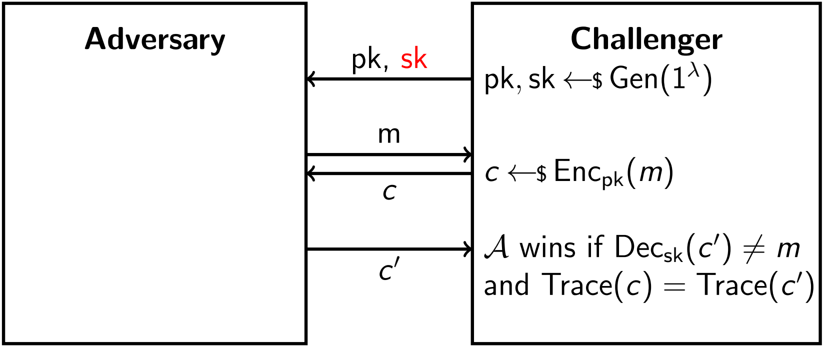
c

$c \leftarrow\!\!\$\, \mathsf{Enc}_{\mathsf{pk}}(m)$

c'

$\mathcal{A}$ wins if $\mathsf{Dec}_{\mathsf{sk}}(c') \neq m$ and $\mathsf{Trace}(c) = \mathsf{Trace}(c')$

Traceable Encryption



Adversary

Challenger

pk, sk

$\mathsf{pk}, \mathsf{sk} \leftarrow\!\!\$\ \mathsf{Gen}(1^\lambda)$

m

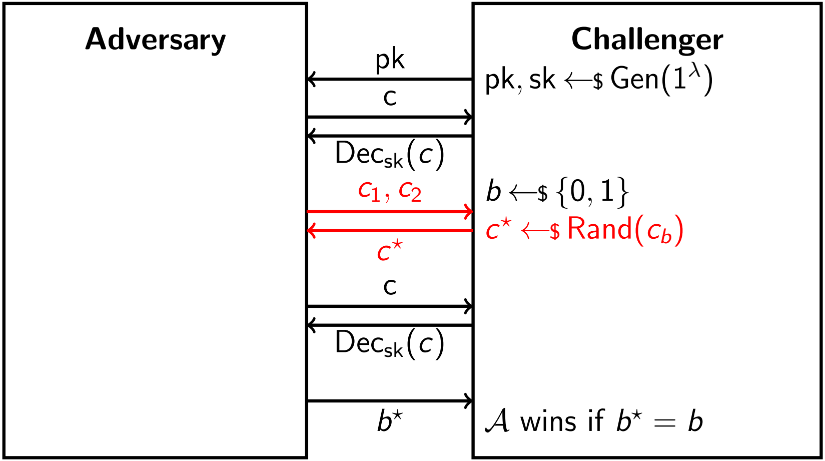
$c \leftarrow\!\!\$\ \mathsf{Enc}_{\mathsf{pk}}(m)$

c

c'

$\mathcal{A}$ wins if $\mathsf{Dec}_{\mathsf{sk}}(c') \neq m$ and $\mathsf{Trace}(c) = \mathsf{Trace}(c')$

TCCA security



Adversary

Challenger

pk

$\mathsf{pk}, \mathsf{sk} \leftarrow_{\$} \mathsf{Gen}(1^{\lambda})$

c

$\mathsf{Dec}_{\mathsf{sk}}(c)$

c_1, c_2

$b \leftarrow_{\$} \{0, 1\}$

$c^{\star} \leftarrow_{\$} \mathsf{Rand}(c_b)$

$c^{\star}$

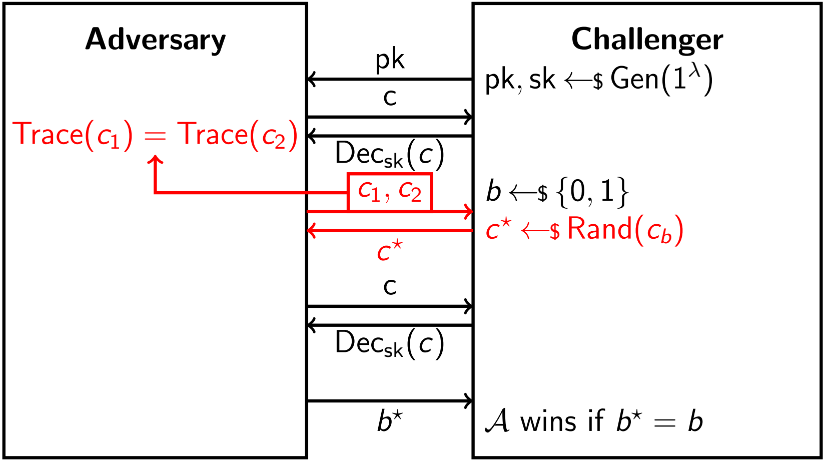
c

$\mathsf{Dec}_{\mathsf{sk}}(c)$

$b^{\star}$

$\mathcal{A}$ wins if $b^{\star} = b$

TCCA security



Adversary

Challenger

pk

$\mathsf{pk}, \mathsf{sk} \leftarrow_\$ \mathsf{Gen}(1^\lambda)$

c

$\mathsf{Dec}_{\mathsf{sk}}(c)$

$\mathsf{Trace}(c_1) = \mathsf{Trace}(c_2)$

c_1, c_2

$b \leftarrow_\$ \{0,1\}$

$c^\star \leftarrow_\$ \mathsf{Rand}(c_b)$

$c^\star$

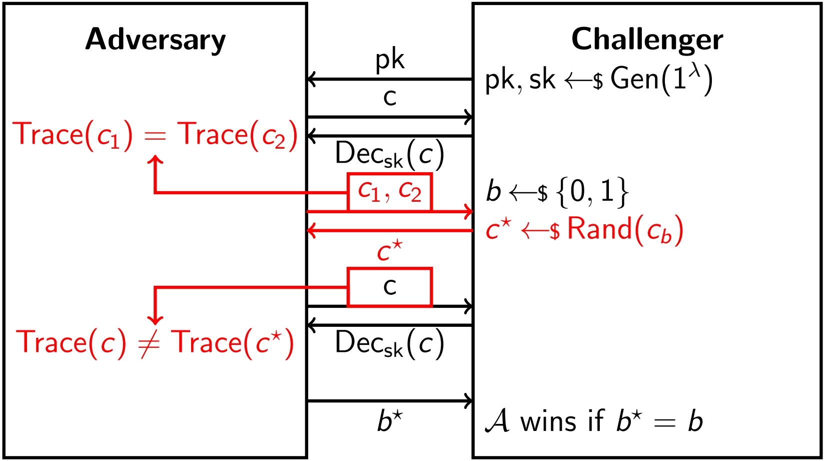
c

$\mathsf{Dec}_{\mathsf{sk}}(c)$

$b^\star$

$\mathcal{A}$ wins if $b^\star = b$

TCCA security



Adversary
Challenger
pk
$\mathsf{pk}, \mathsf{sk} \leftarrow_{\$} \mathsf{Gen}(1^\lambda)$
c
$\mathsf{Trace}(c_1) = \mathsf{Trace}(c_2)$
$\mathsf{Dec}_{\mathsf{sk}}(c)$
c_1, c_2
$b \leftarrow_{\$} \{0,1\}$
$c^\star \leftarrow_{\$} \mathsf{Rand}(c_b)$
$c^\star$
c
$\mathsf{Trace}(c) \neq \mathsf{Trace}(c^\star)$
$\mathsf{Dec}_{\mathsf{sk}}(c)$
$b^\star$
$\mathcal{A}$ wins if $b^\star = b$

Traceable Receipt-Free Encryption

TREnc: $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}) + (\mathsf{Rand}, \mathsf{Trace}, \mathsf{LGen}, \mathsf{LEnc})$

- $\mathsf{LGen}(\mathsf{pk})$ returns a link key lk and $\mathsf{LEnc}(\mathsf{pk}, \mathsf{lk}, \mathsf{m})$ returns a ciphertext
- lk determines alone the trace
- TCCA, traceable security and also randomizability

Construction

Generic Construction

- Use SRC and randomizable proof systems
- Stronger constructions (Link key extractability)

Direct Construction

- Pairing based solution under SXDH using a CRS

Direct construction (sketch)

- CPA encryption $c_0 = mf^\theta, c_1 = g^\theta, c_2 = h^\theta$
- Sim-sound randomizable π that $(c_1, c_2) \in< (g, h) >$
  Inspired of tag-based encryption, we use tag $\tau =$ trace
  π that $(c_1^\tau, c_2^\tau, c_1, c_2)$ in $< (g^\tau, h^\tau, g, h) >$

Challenges

- τ^* of challenge chosen at any time:
  stronger than selective-tag CCA
- Pre-challenge decryption request can use τ^*

Direct construction (sketch)

- CPA encryption $c_0 = mf^\theta, c_1 = g^\theta, c_2 = h^\theta$
- Sim-sound randomizable π that $(c_1, c_2) \in < (g, h) >$
- LHSP signature of $\begin{pmatrix} g & c_0 & c_1 \\ 1 & f & g \\ 1 & F & G \end{pmatrix}$

  key: (osk, ovk). $osk = lk$, $H(ovk) = \tau = Trace(c)$
- Groth-Sahai proofs to hide some elements
- All the parts of the construction are randomizable

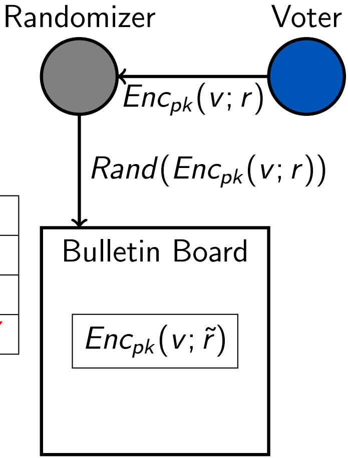
Efficiency

$$\text{Ciphertext} \in \mathbb{G}^{13} \times \hat{\mathbb{G}}^5$$

Building a RF protocol

Generic transfomation TREnc
⇒ Receipt-Free vote system

	Verifiability	Privacy	RF
Voter	✓	✓	✓
Rand.	✓	✓	✗
Tallier	✓	t-✗	t-✗



Conclusion

We proposed:

- TREnc, a new encryption primitive that capture the needs of Receipt-Free voting
- Two TREncs instances:generic & direct (under SXDH)
  Both support the encryption of group elements
- A generic transformation from a TREnc scheme to a Receipt-Free voting system