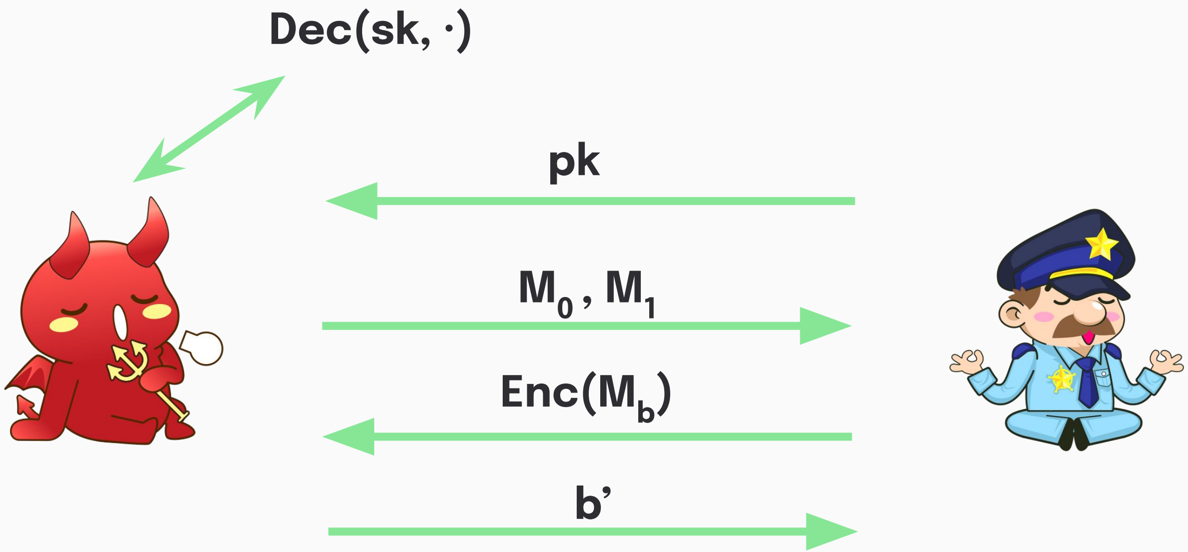
Almost Tightly-Secure Re-Randomizable and Replayable CCA-secure Public Key Encryption

Antonio Faonio, Dennis Hofheinz, **Luigi Russo**

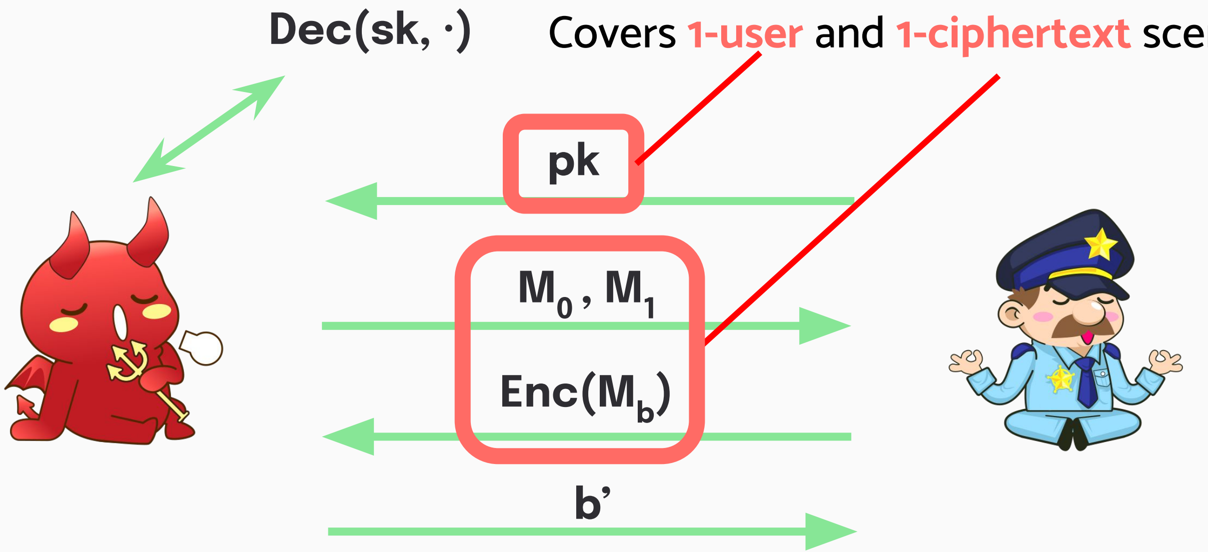
Public Key Encryption

Standard Security Notion: chosen-ciphertext (**IND-CCA**)

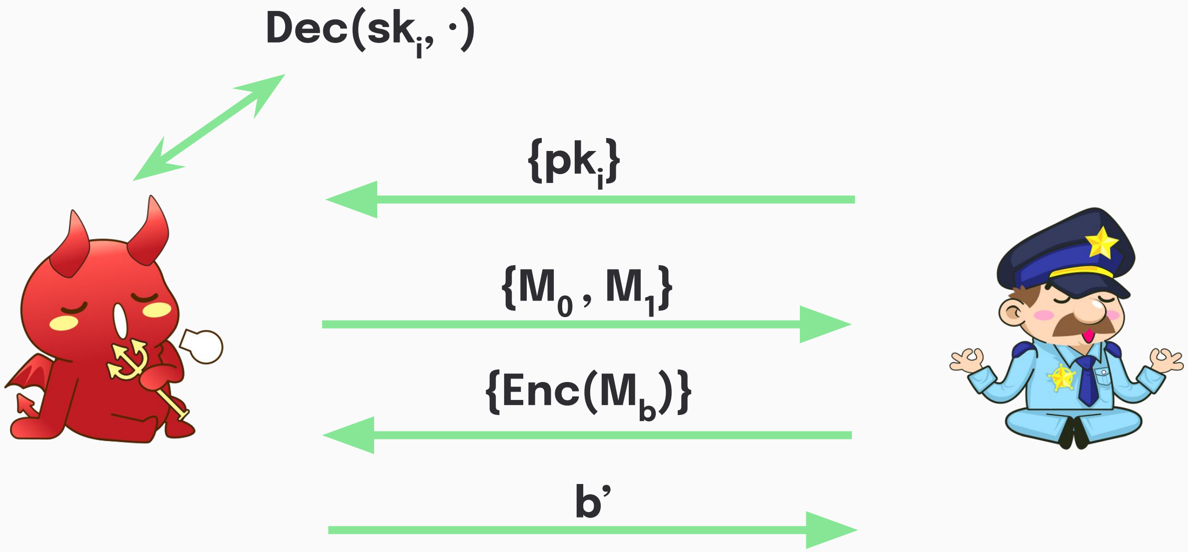


Public Key Encryption

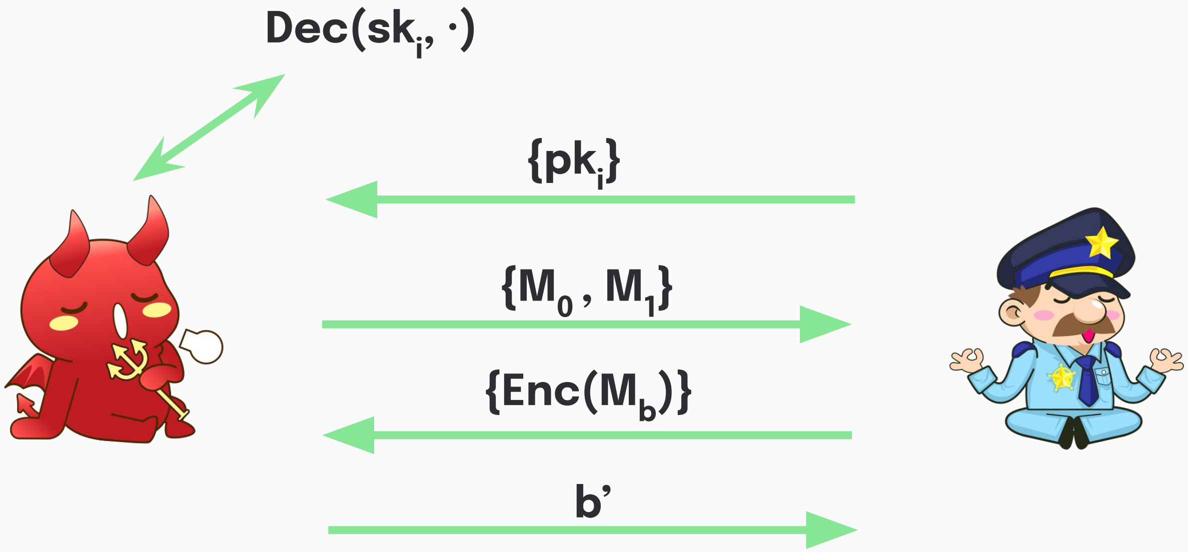
Standard Security Notion: chosen-ciphertext (**IND-CCA**)



Multi-user Multi-ciphertext CCA



Multi-user Multi-ciphertext CCA



Hybrid Argument allows to reduce multi to single!

Why is it not enough?

Hybrid Argument allows to reduce multi to single, but:

- **Security Guarantees may degrade in scenario size**
- Keylength recommendations may be influenced
- Scenario size may be **unpredictable/unknown** a priori

Tight Security

- Reduction loss is **independent** of number of ciphertexts and queries
- Keylength may be chosen regardless of the scenario size

Many schemes have been proved to have tight security
[GHKW16], [GHK17], [HLLG19], [Hof17], …

Re-Randomizable PKE

- Given a ciphertext C, it is possible to produce a fresh ciphertext C' such that **Dec(sk, C) = Dec(sk, C')**
- Rand(pk, C) → C' is efficient and uses public information

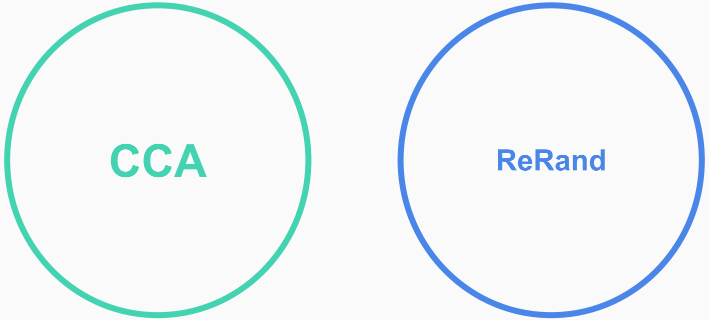
ElGamal is a Re-Randomizable PKE

CCA + Re-randomizability?

CCA-security is impossible to achieve when the PKE scheme is Re-Randomizable…

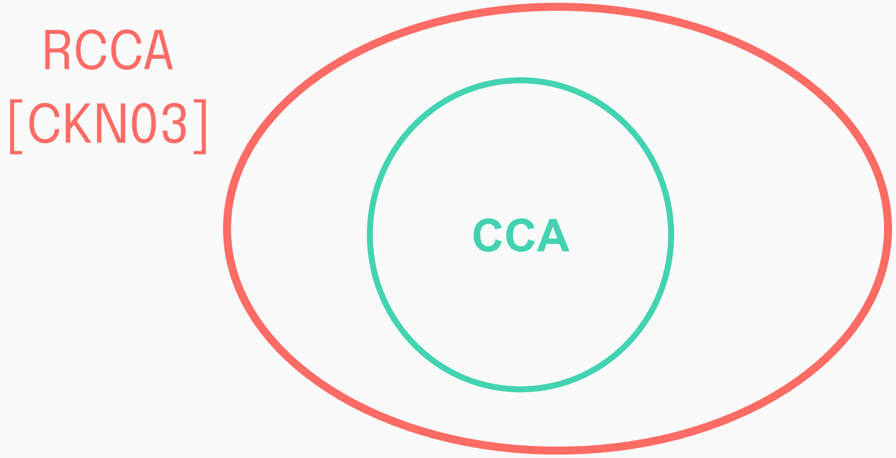
CCA + Re-randomizability?

CCA-security is impossible to achieve when the PKE scheme is Re-Randomizable…

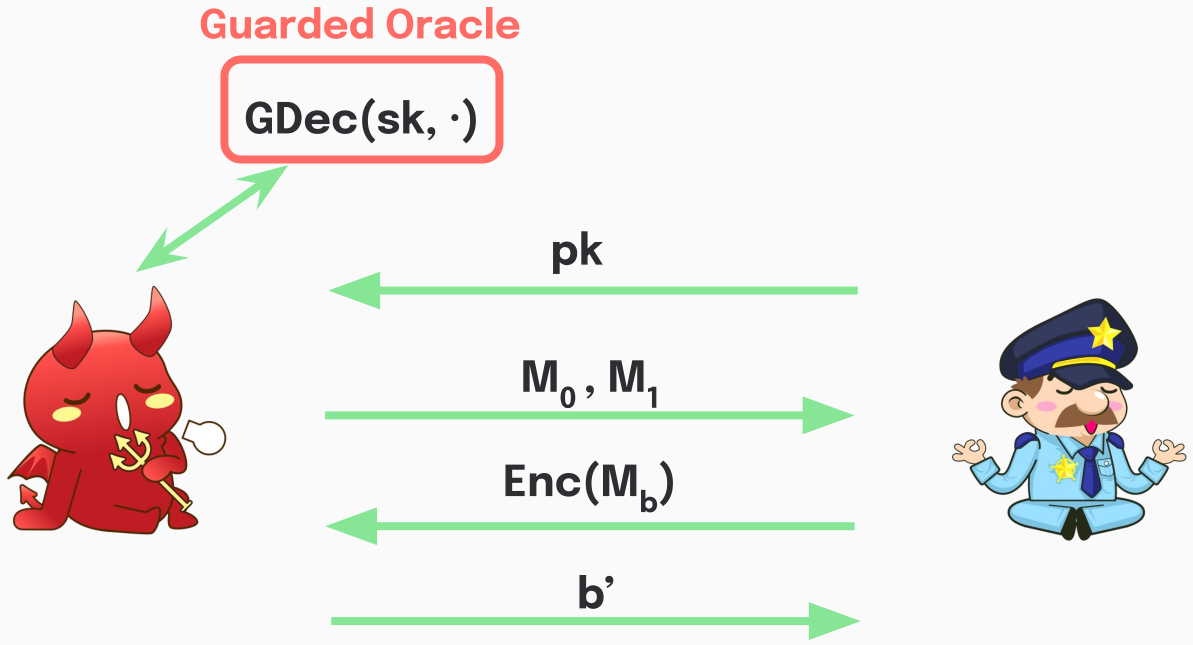


Replayable CCA Security

- sufficient to implement secure channels
- more efficient instantiations



Replayable CCA Security



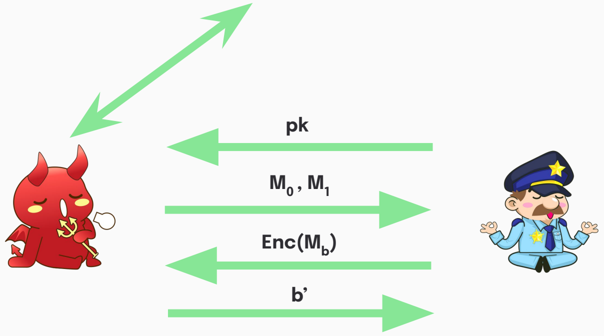
Guarded Decryption Oracle

GDec(sk, C)

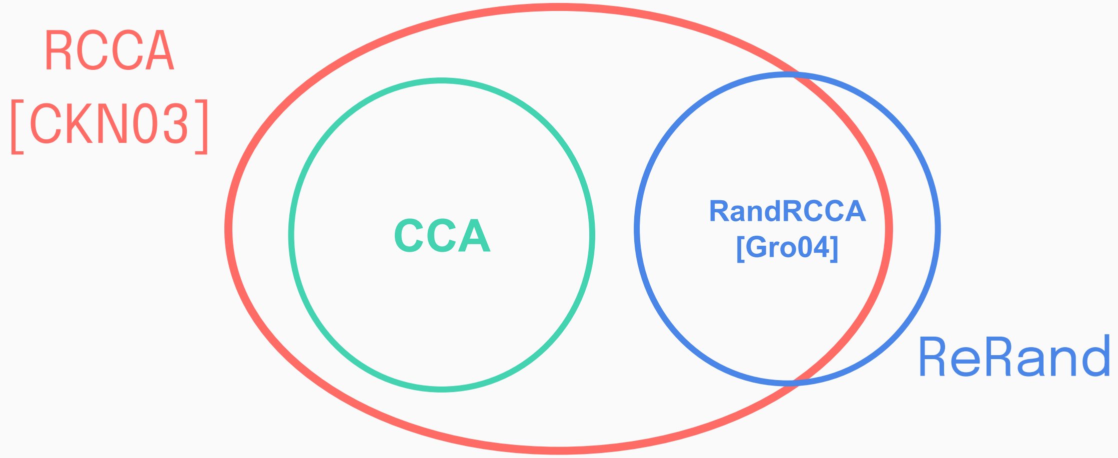
M = Dec(sk, C)

IF M $\in \{M_0, M_1\}$:
    RETURN "REPLAY"

RETURN M



RCCA + Re-randomizability



Rand RCCA Security

Rand-RCCA was introduced by [Gro04]

- Anonymous message transmissions [PR07]
- Mix-Nets [FFHR19], [PR17], [FR22]
- Controlled Functional Encryption [NAP+14]
- ...

Rand RCCA Security

Rand-RCCA was introduced by [Gro04]

- Anonymous message transmissions [PR07]
- Mix-Nets [FFHR19], [PR17], [FR22]
- Controlled Functional Encryption [NAP+14]
- ...

anonymous e-mail [Cha81], anonymous payments [JM99], electronic voting, ...

Rand RCCA Security

Multi-User Multi-Challenge Rand RCCA may be achieved through hybrid argument

But **security degrades** in settings where the **scenario size is unknown or arbitrarily large**

(anonymous e-mail, anonymous payments, e-voting, ...)


All the papers on Multi-Ciphertext Rand RCCA

Our work

Contributions

Multi-user Multi-ciphertext RCCA

How to extend RCCA definition to this scenario

Tightly-secure Scheme(s)

3 schemes under different assumptions
and with different properties

Applications

How to instantiate the first Tightly-secure MixNet ever

Rand RCCA Definition

Extending Rand RCCA to the multi-ciphertext setting is not trivial…

Naïve extensions of the guarded oracle are either **vulnerable** or **weak**

Multi-Ciphertext RandRCCA

A B

(A,B) ➔ c_1

<u>Guarded</u>

IF M ∈ {A,B}: REPLAY

Multi-Ciphertext RandRCCA

A B C D

(A,B) ➔ c_1

(C,D) ➔ c_2

Guarded

IF M ∈ {A,B}: REPLAY

IF M ∈ {C,D}: REPLAY

Multi-Ciphertext RandRCCA

A B C D

(A,B) ➔ c_1
(C,D) ➔ c_2
(E,A) ➔ c_3

Guarded

IF M ∈ {A,B}: REPLAY
IF M ∈ {C,D}: REPLAY
IF M = E: ???

Multi-Ciphertext RandRCCA

A B C D

E

$(A,B) \rightarrow c_1$

$(C,D) \rightarrow c_2$

$(E,A) \rightarrow c_3$

GDec(c_3) allows to distinguish

Guarded

IF $M \in \{A,B\}$: REPLAY

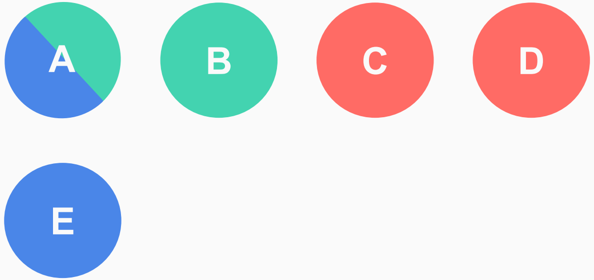
IF $M \in \{C,D\}$: REPLAY

IF $M = E$: REPLAY

Multi-Ciphertext RandRCCA

(A,B) → c_1
(C,D) → c_2
(E,A) → c_3

GDec(Rand(c_3))
to distinguish



Guarded

IF M ∈ {A,B}: REPLAY
IF M ∈ {C,D}: REPLAY
IF M ∈ {A,E}: REPLAY

Multi-Ciphertext RandRCCA

(A,B) → c_1

(C,D) → c_2

(E,A) → c_3

A B C D

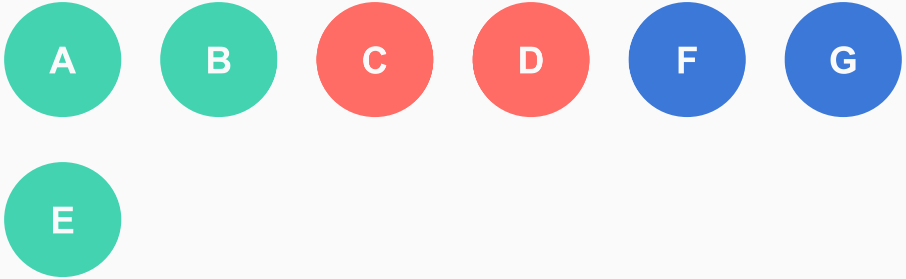
E

Guarded

IF M ∈ {A,B,E}: REPLAY

IF M ∈ {C,D}: REPLAY

Multi-Ciphertext RandRCCA



(A,B) ➔ c_1
(C,D) ➔ c_2
(E,A) ➔ c_3
(F,G) ➔ c_4

Guarded

IF M ∈ {A,B,E}: REPLAY

IF M ∈ {C,D}: REPLAY

IF M ∈ {F,G} : REPLAY

Multi-Ciphertext RandRCCA

A B C D F G

E

(A,B) ➔ c_1
(C,D) ➔ c_2
(E,A) ➔ c_3
(F,G) ➔ c_4
(C,F) ➔ c_5

Guarded

IF M ∈ {A,B,E}: REPLAY
IF M ∈ {C,D}: REPLAY
IF M ∈ {F,G} : REPLAY

Multi-Ciphertext RandRCCA

(A,B) → c_1
(C,D) → c_2
(E,A) → c_3
(F,G) → c_4
(C,F) → c_5

A B C D F G

E

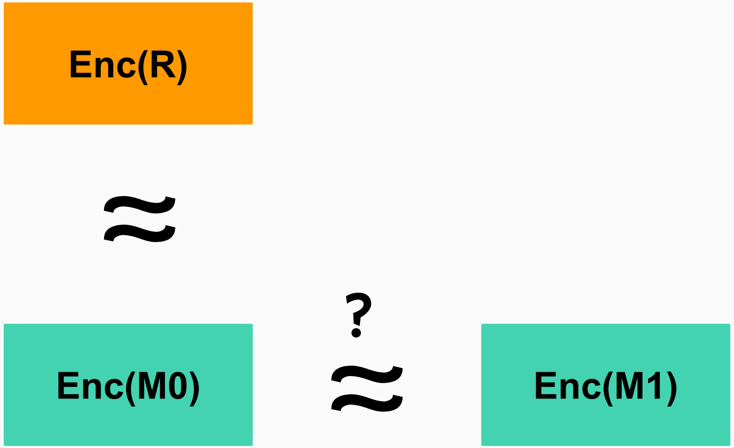
Guarded

IF M ∈ {A,B,E}: REPLAY
IF M ∈ {C,D,F,G}: REPLAY

(IND-CCA) Reduction Goal

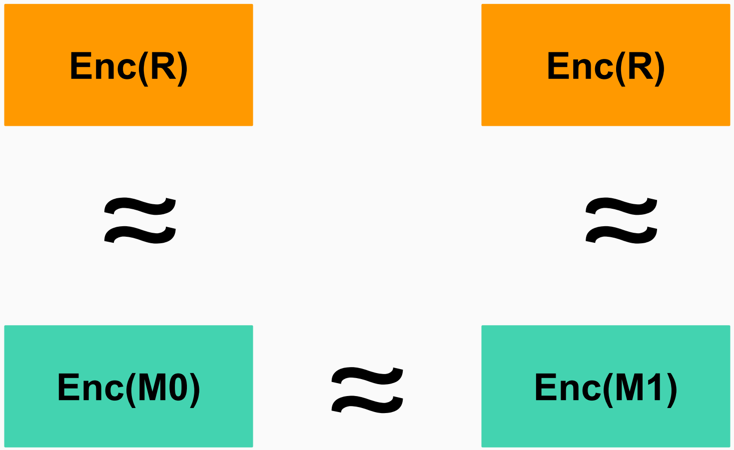
Enc(M0) $\overset{?}{\approx}$ Enc(M1)

(IND-CCA) Reduction Goal



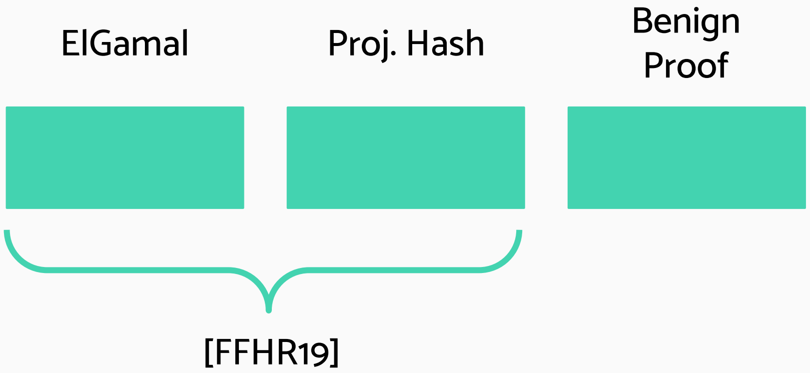
Goal: Replace challenge ciphertexts with encryption of **random msg**

(IND-CCA) Reduction Goal



Goal: Replace challenge ciphertexts with encryption of **random msg**

Our scheme

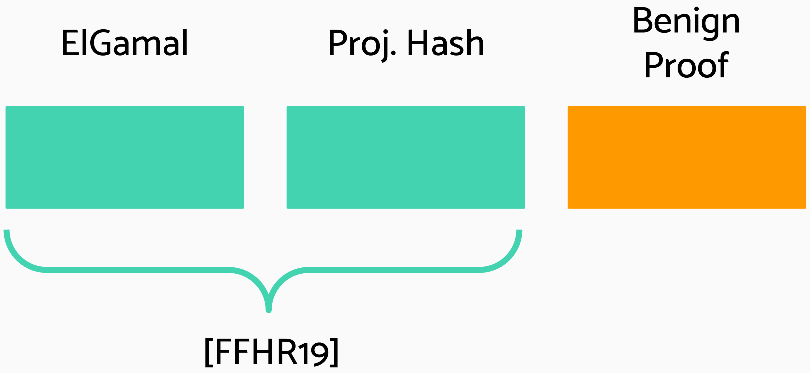


Benign Proof Requirements

1. Re-Randomizability
2. Simulation-Soundness*

ReRandomization is a linear transformation

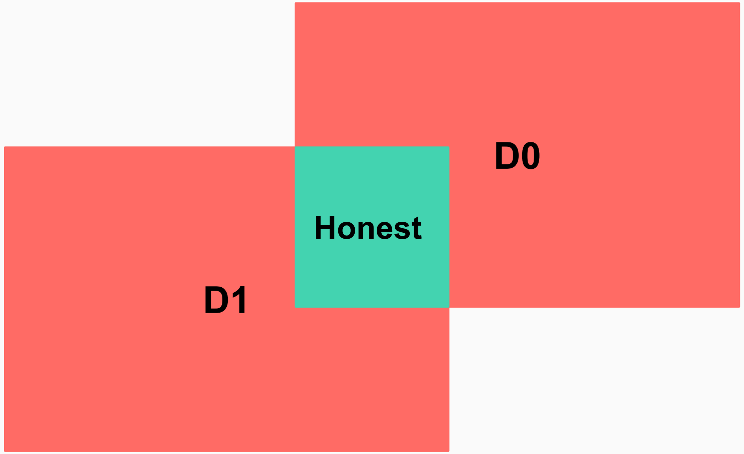
Adaptive Partitioning



Steps (simplified)

1. **Simulate benign proofs**
2. Produce ill-formed Challenge Ciphertexts
3. Adaptively inject randomness into the hash of ciphertexts*
4. Replace with random msg

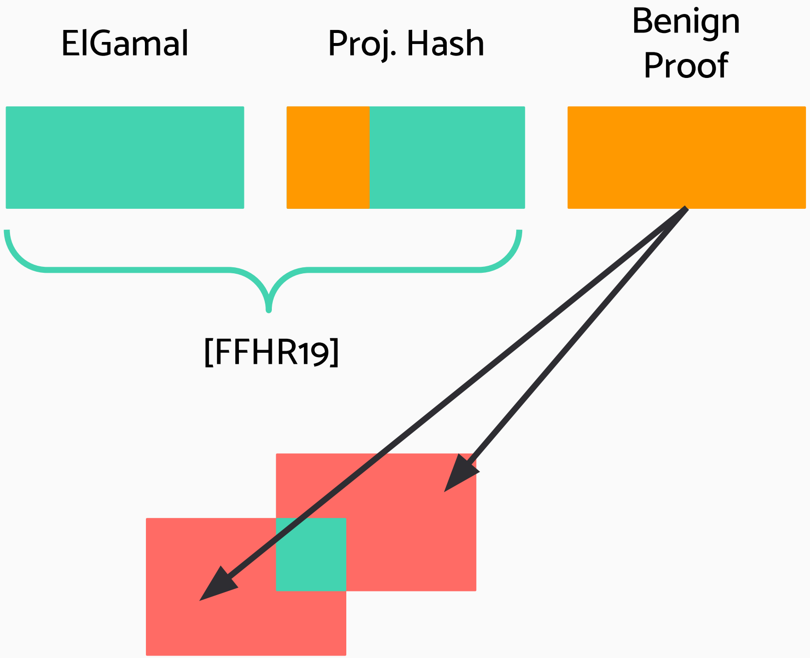
Adaptive Partitioning



Steps (simplified)

1. Simulate benign proofs
2. **Produce ill-formed Challenge Ciphertexts**
3. Adaptively inject randomness into the hash of ciphertexts*
4. Replace with random msg

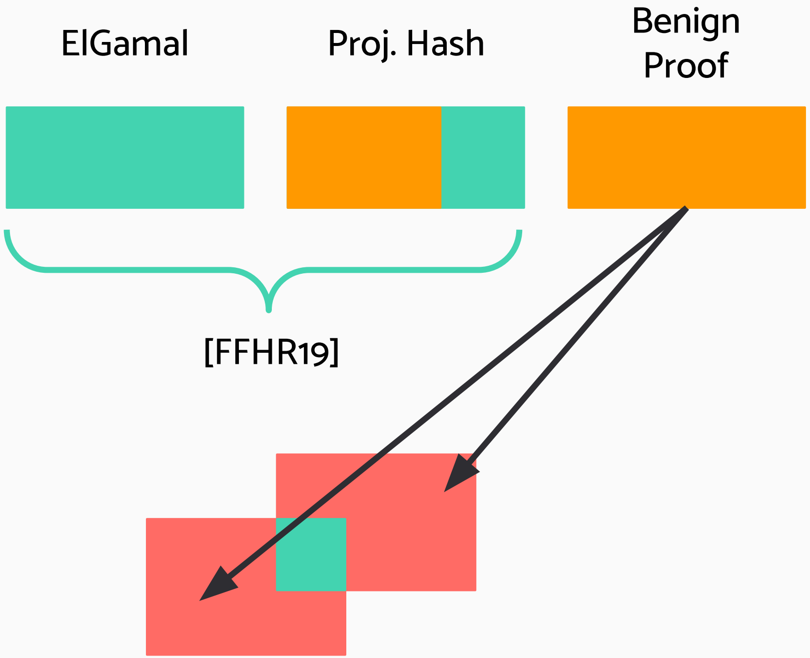
Adaptive Partitioning



Steps (simplified)

1. Simulate benign proofs
2. Produce ill-formed Challenge Ciphertexts
3. **Adaptively inject randomness into the hash of ciphertexts***
4. Replace with random msg

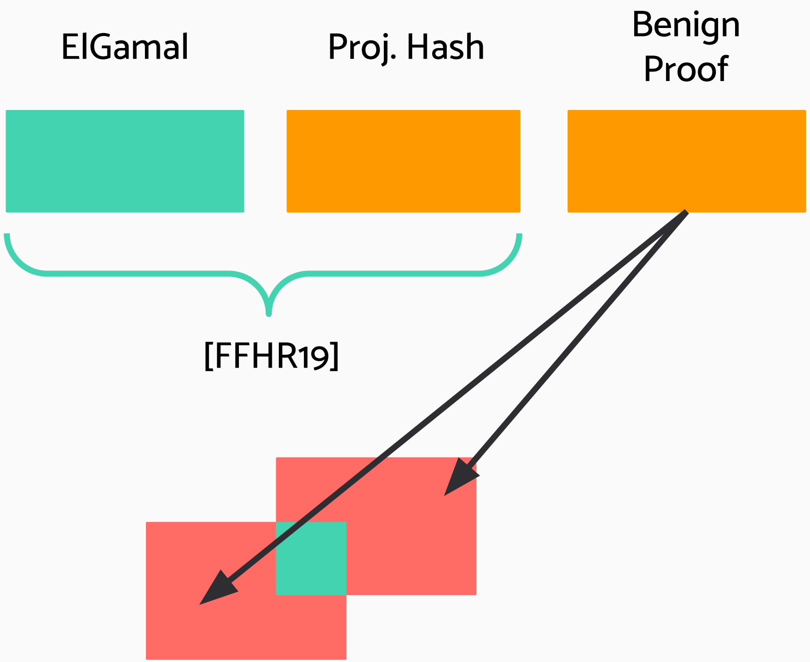
Adaptive Partitioning



Steps (simplified)

1. Simulate benign proofs
2. Produce ill-formed Challenge Ciphertexts
3. **Adaptively inject randomness into the hash of ciphertexts***
4. Replace with random msg

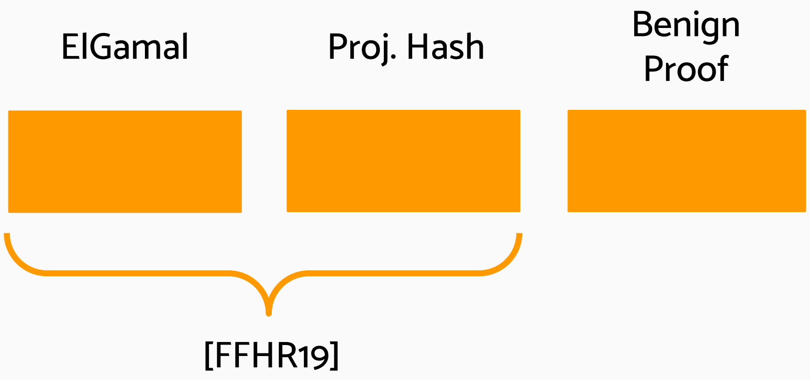
Adaptive Partitioning



Steps (simplified)

1. Simulate benign proofs
2. Produce ill-formed Challenge Ciphertexts
3. **Adaptively inject randomness into the hash of ciphertexts***
4. Replace with random msg

Adaptive Partitioning



Steps (simplified)

1. Simulate benign proofs
2. Produce ill-formed Challenge Ciphertexts
3. Adaptively inject randomness into the hash of ciphertexts*
4. **Replace with random msg**

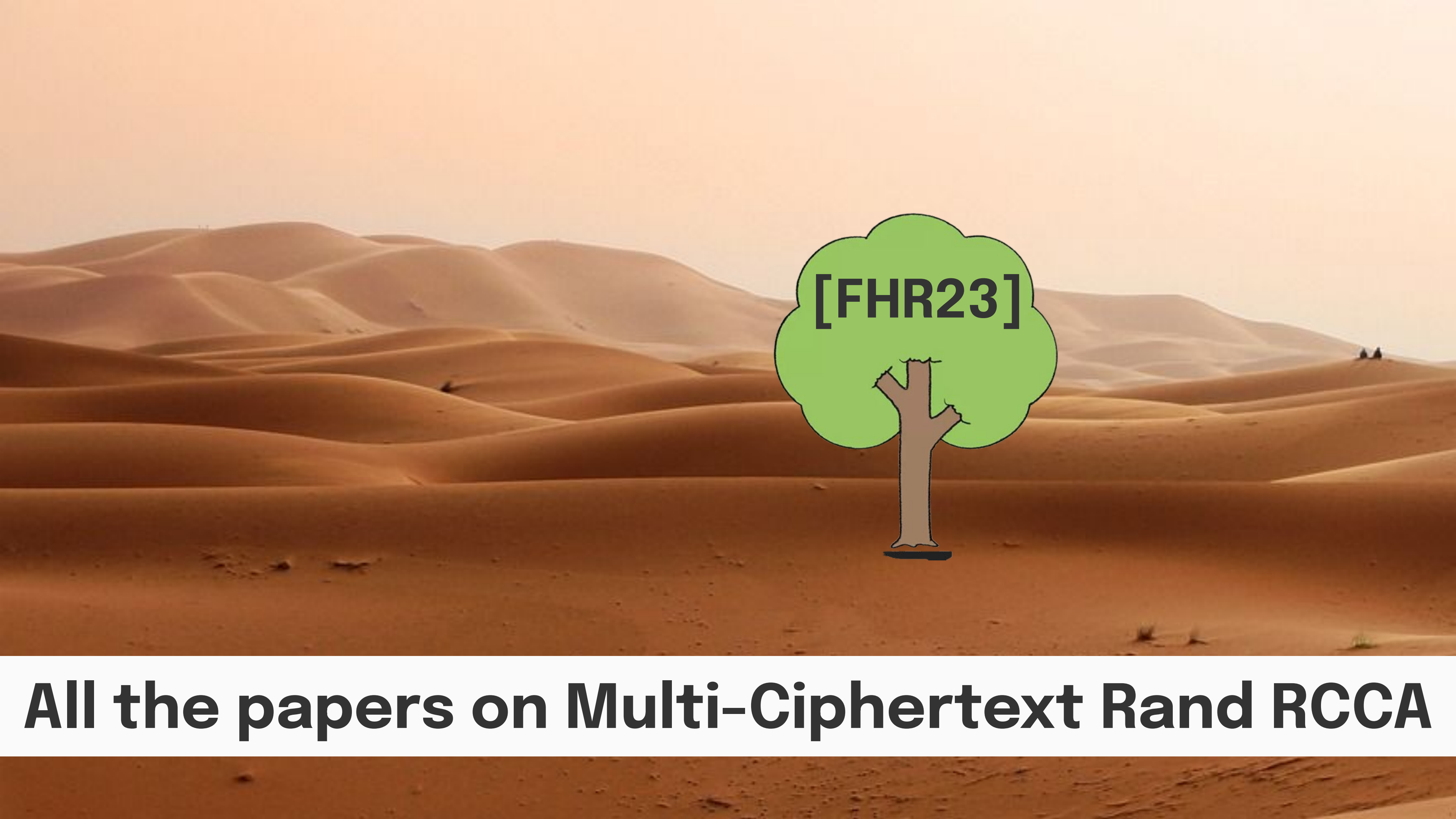
Efficiency

We compare privately-verifiable schemes only, in terms of group elements and exponentiations

	Size of C	Cost of Enc/Rand	Group Setting	Tight
[FFHR19]	3 G1 + 2 G2 + GT	4 E1 + 5 E2 + 2 ET + 5 P	Type-3	
Our work	7 G1 + 2 GT	14 E1 + 2 ET + 14 P	Type-1	✓
	Assumption: Matrix DDH			

Open Problems

- Instantiation based on type-3 pairings
- Provide a generic framework to instantiate tightly-secure Rand-RCCA PKEs
- Tightly-secure Mix-Nets from Leakage-Resilient CCA
- …


[FHR23]
All the papers on Multi-Ciphertext Rand RCCA

Thanks!

EURECOM
Sophia Antipolis

ETH zürich

ia.cr.org/2023/152

References

[CKN03] Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen. Relaxing chosen-ciphertext security. CRYPTO 2003

[FFHR19] Antonio Faonio, Dario Fiore, Javier Herranz, and Carla R`afols. Structure-preserving and re-randomizable RCCA-secure public key encryption and its applications. ASIACRYPT 2019

[FR22] Antonio Faonio and Luigi Russo. Mix-nets from re-randomizable and replayable cca-secure public-key encryption. SCN 2022

[GHK17] Romain Gay, Dennis Hofheinz, and Lisa Kohl. Kurosawa-desmedt meets tight security. CRYPTO 2017

[GHKW16] Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly CCA-secure encryption without pairings. EUROCRYPT 2016

[Gro04] Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. TCC 2004

[HLLG19] Shuai Han, Shengli Liu, Lin Lyu, and Dawu Gu. Tight leakage-resilient CCA-security from quasi-adaptive hash proof system. CRYPTO 2019

[Hof17] Dennis Hofheinz. Adaptive partitioning. EUROCRYPT 2017

[NAP+14] Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, XiaoFeng Wang, Erman Ayday, Jean-Pierre Hubaux, and Carl A. Gunter. Controlled functional encryption. ACM CCS 2014

[PR07] Manoj Prabhakaran and Mike Rosulek. Rerandomizable RCCA encryption. CRYPTO 2007

[PR17] Olivier Pereira and Ronald L. Rivest. Marked mix-nets. FC 2017 Workshops

A weak definition

A B C D

(A,B) ➔ c_1
(C,D) ➔ c_2

<u>**Guarded**</u>
IF M ∈ {A,B,C,D}:
REPLAY

Our Malleable NIDVPS

- Inspired by the work of [ABP15]: disjunction of two SPHFs for two languages based on diverse vector spaces.
- In our case the prover can generate proofs for elements that belong to the span of of matrix D.
- Soundness even in presence of simulated proofs for elements in two (possibly distinct) super-spaces of the prescribed linear space

Our Malleable NIDVPS

To prove that $[u]_1 = [D]_1 r$, compute $k^\top [D \otimes D]_T \cdot (r \otimes r)$

To verify/simulate compute $k^\top [u \otimes u]_T$

To update the proof, add
$k^\top [I \otimes D]^T \cdot [u \otimes s]_1 + k^\top [D \otimes i]_1 \cdot [s \otimes u]_1 + k^\top [D \otimes D]_T \cdot (s \otimes s)$