On Non-Uniform Security for Black-box Non-Interactive CCA Commitments

Rachit Garg
UT Austin

Dakshita Khurana
UIUC

George Lu
UT Austin

Brent Waters
UT Austin
NTT Research

Date: Apr 26, 2023

Commitments

Commitments

ALICE

BOB

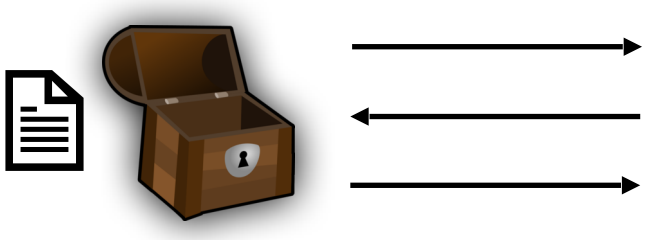
Commitments

ALICE

BOB

Commitments

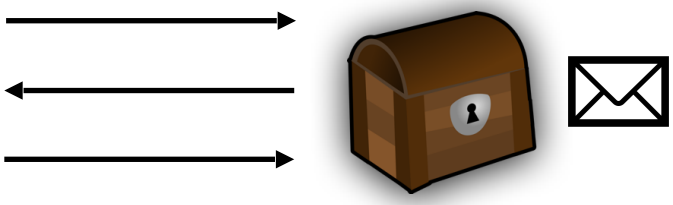
ALICE



BOB

Commitments

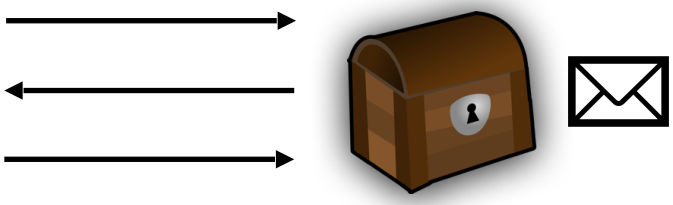
ALICE



BOB

Commitments

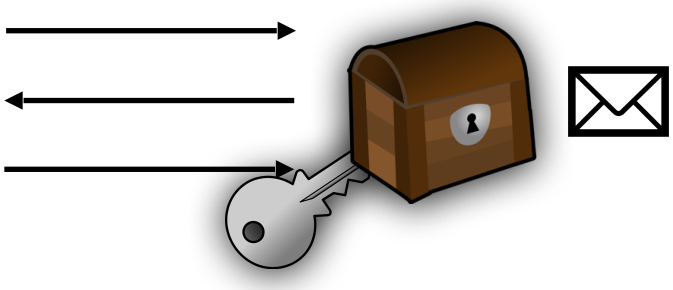
ALICE



BOB

Commitments

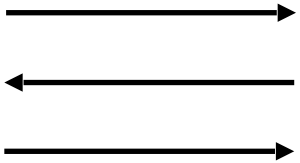
ALICE



BOB

Commitments

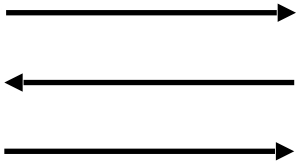
ALICE



BOB

Commitments

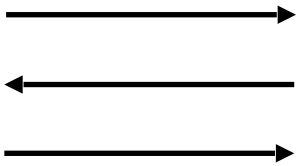
ALICE



BOB

Commitments

ALICE

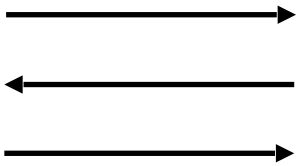


Hiding

BOB

Commitments

ALICE



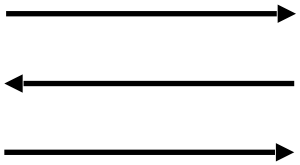
Hiding

BOB

Binding

Commitments

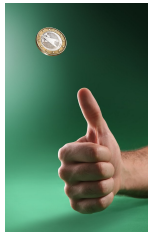
ALICE



Hiding

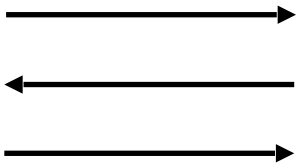
BOB

Binding



Commitments

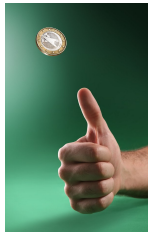
ALICE



Hiding

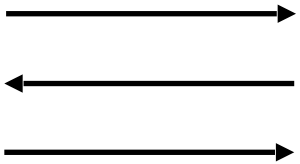
BOB

Binding



Commitments

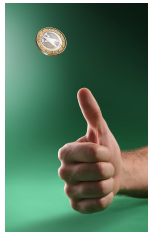
ALICE



Hiding

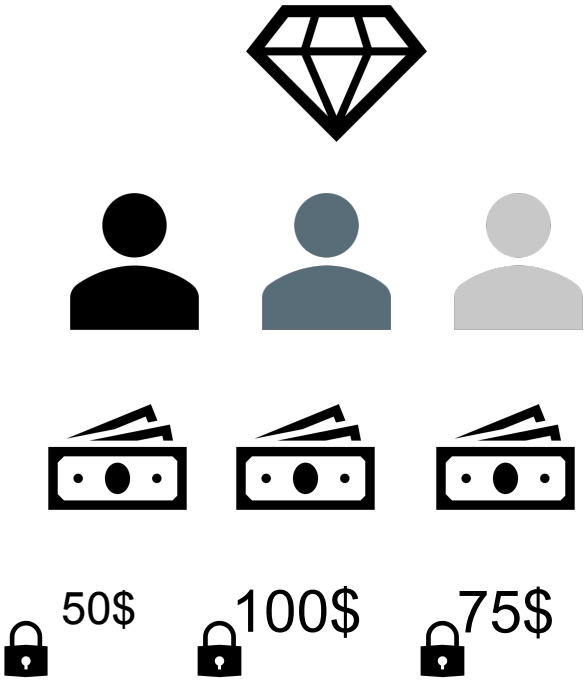
BOB

Binding

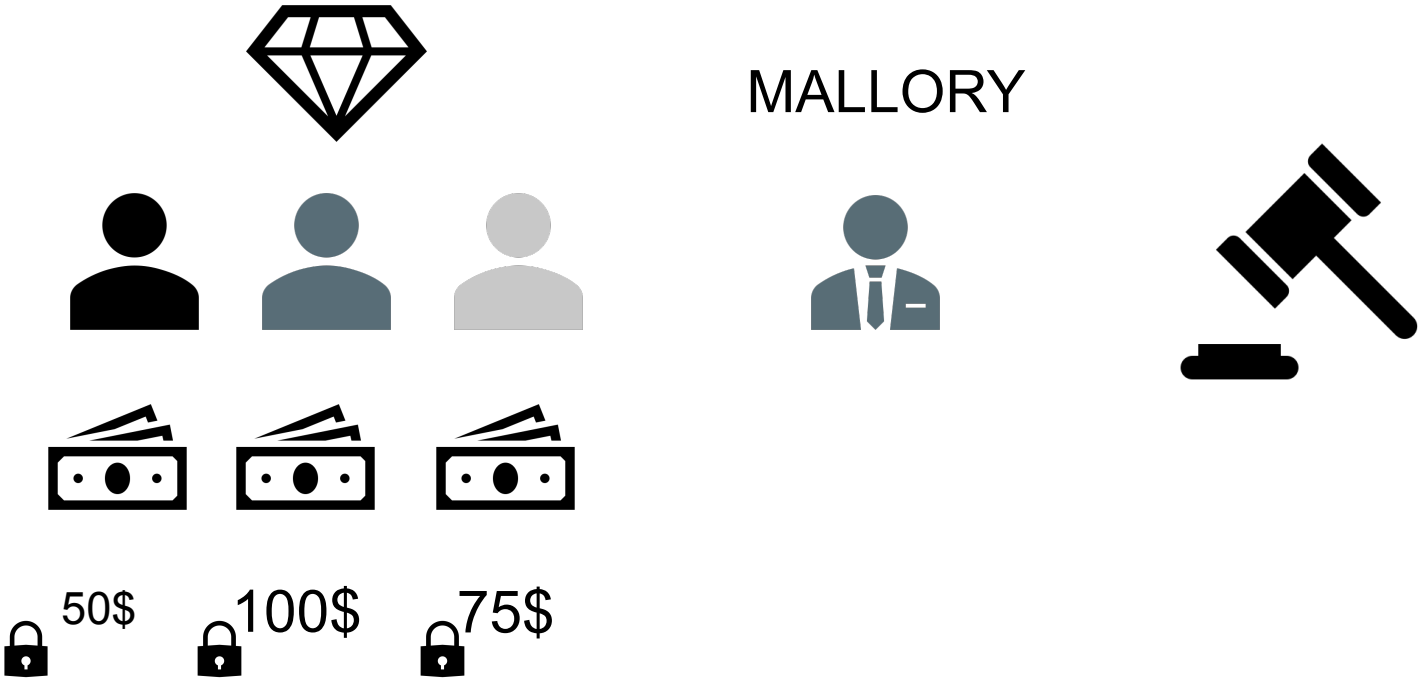


Auctions

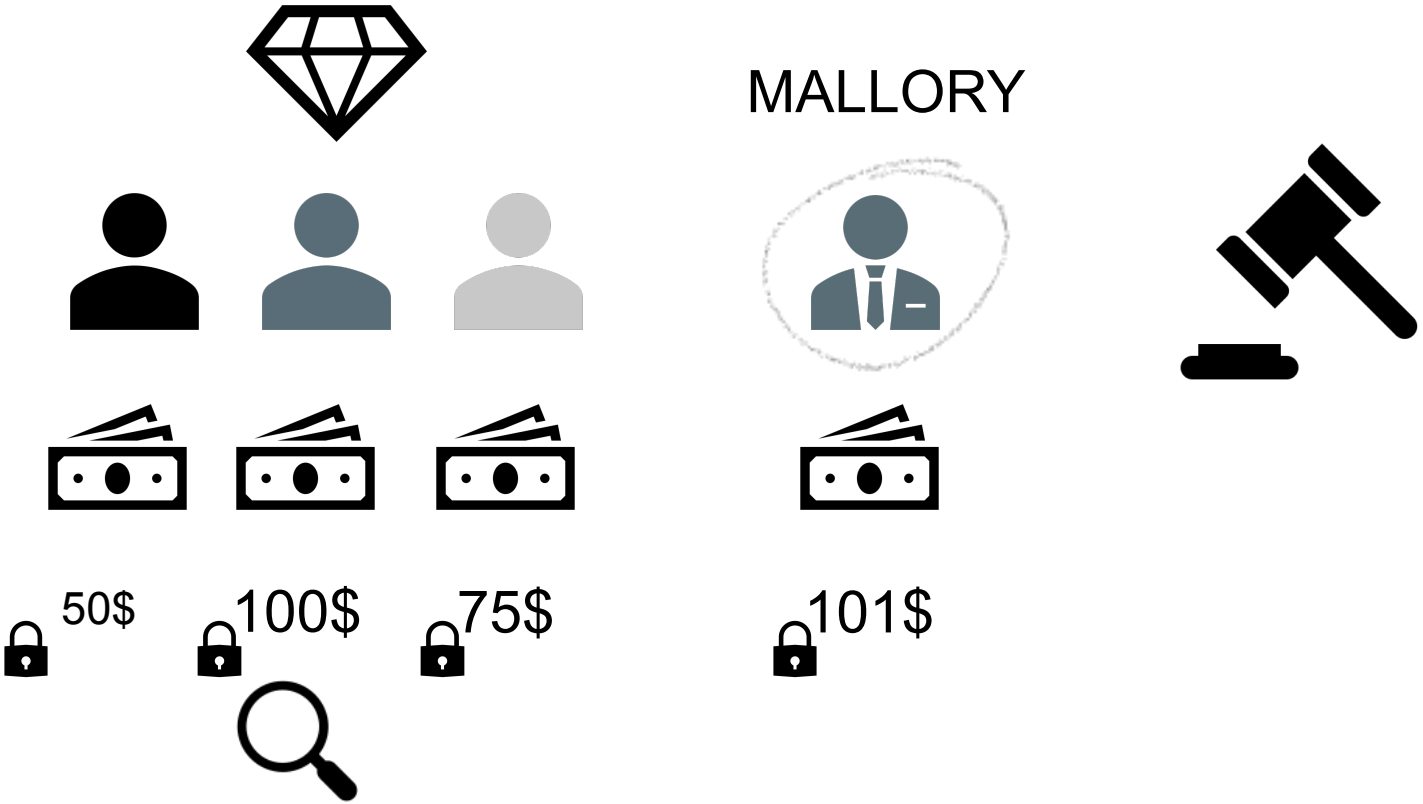
Auctions



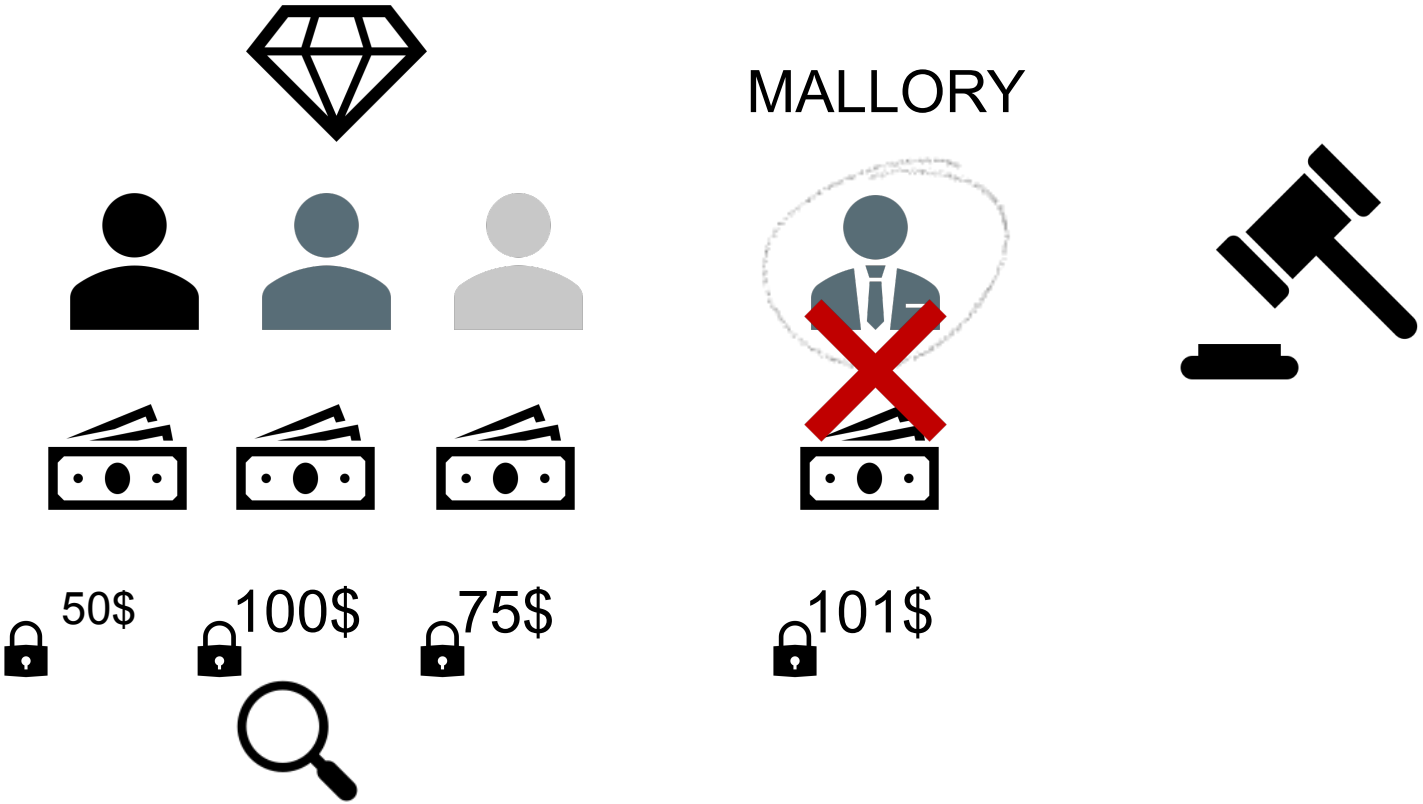
Auctions



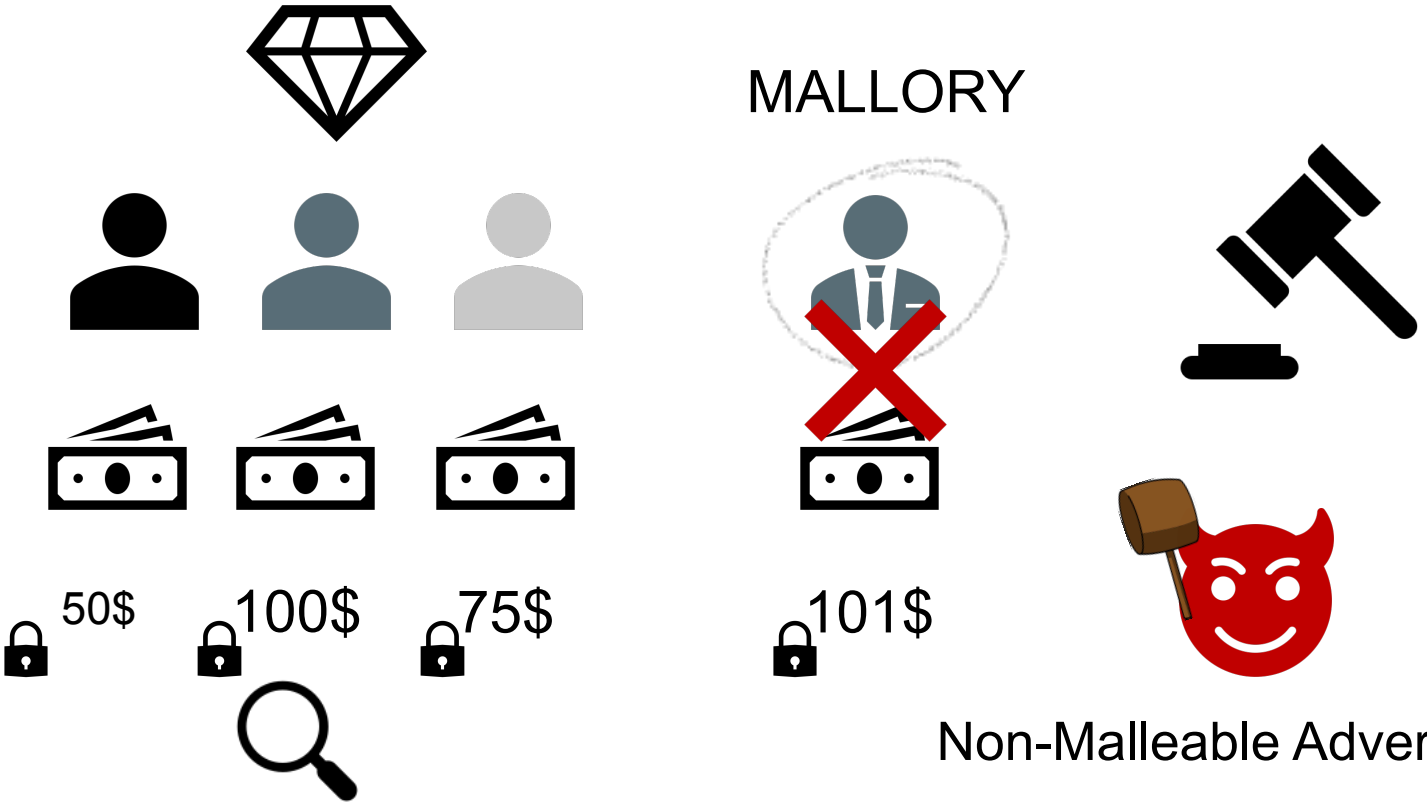
Auctions



Auctions



Auctions

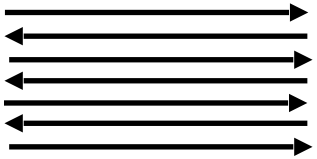


Non-Malleable Adversaries

NMC in literature

NMC in literature

$O(\log n)$

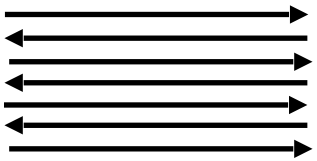


OWF

[DDN91]

NMC in literature

$O(\log n)$



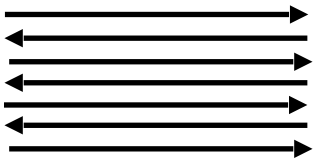
OWF

[DDN91]

[Bar02, Pas04, PR05, LPV08, Wee10, LP11, Goy11, GLOV12, GRRV14, GPR16, COSV17]

NMC in literature

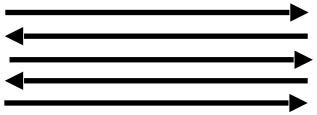
$O(\log n)$



OWF

[DDN91]

3

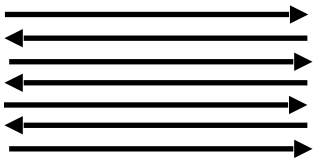


[COSV16, Khu17, GR19]

[Bar02, Pas04, PR05, LPV08, Wee10, LP11, Goy11, GLOV12, GRRV14, GPR16, COSV17]

NMC in literature

$O(\log n)$

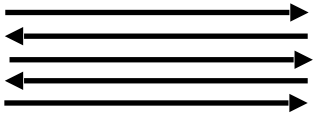


[Bar02, Pas04, PR05, LPV08, Wee10, LP11, Goy11, GLOV12, GRRV14, GPR16, COSV17]

OWF

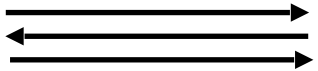
[DDN91]

3



[COSV16, Khu17, GR19]

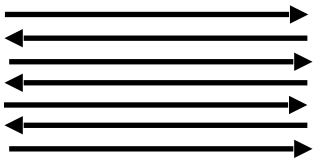
2



[LPS17, KS17]

NMC in literature

$O(\log n)$

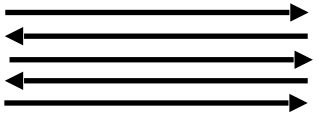


[Bar02, Pas04, PR05, LPV08, Wee10, LP11, Goy11, GLOV12, GRRV14, GPR16, COSV17]

OWF

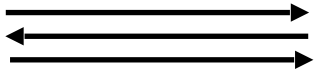
[DDN91]

3



[COSV16, Khu17, GR19]

2



[LPS17, KS17]

Non-Interactive
Without Setup!

1

[PPV08, LPS17, BL18, KK19]

Building NMC

Building NMC

Cryptography
Assumptions

Building NMC

Cryptography Assumptions $\longrightarrow$ Tagged Commitments

Building NMC

Cryptography Assumptions $\longrightarrow$ Tagged Commitments $\rightleftharpoons$ NMC Commitments

Building NMC

Cryptography Assumptions $\longrightarrow$ Tagged Commitments $\overset{*}{\rightleftharpoons}$ NMC Commitments

Building NMC

Cryptography Assumptions $\longrightarrow$ Tagged Commitments $\overset{*}{\rightleftharpoons}$ NMC Commitments

$*$

- One time signature scheme
- **Exponentially many tags**

Tagged Commitments

Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

Perfect Binding

Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

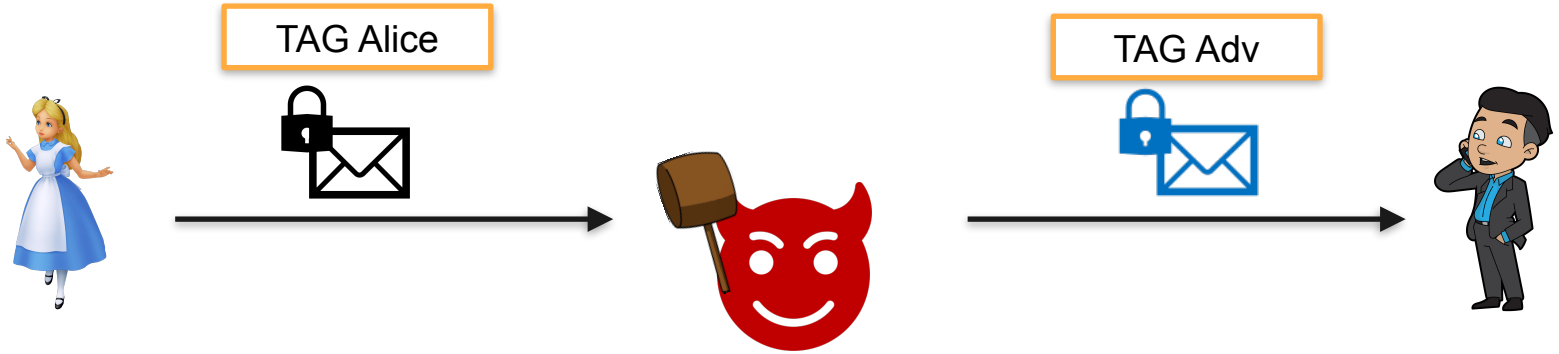
Perfect Binding

Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

Perfect Binding

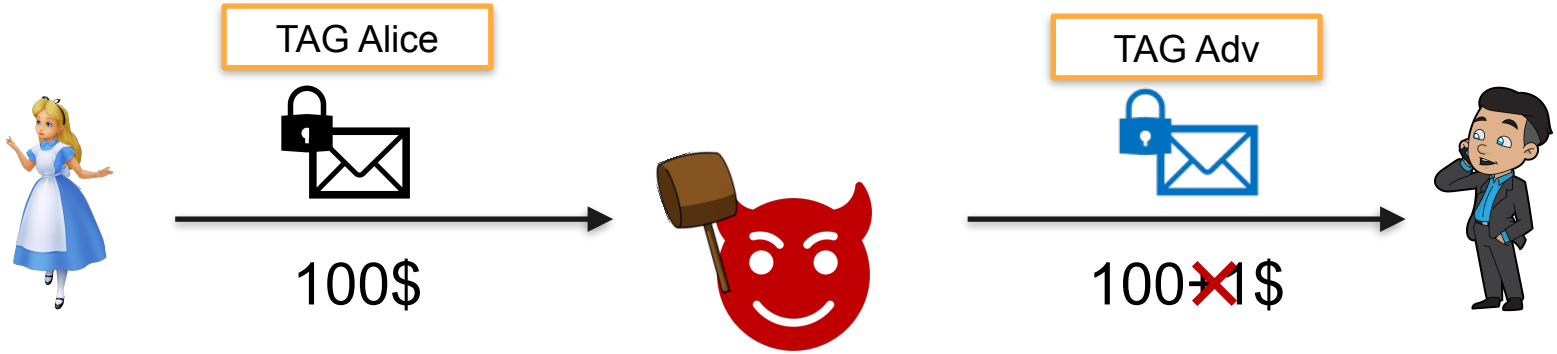


Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

Perfect Binding



Tagged Commitments

$$c \leftarrow \mathsf{Com}(1^\lambda, tag, m; r)$$

$$\{m, \perp\} \leftarrow \mathsf{Open}(tag, c, m; r)$$

Perfect Binding

TAG Alice

100$

$\mathsf{Com}(tag, m; r)$

TAG Adv

100~~→~~1$

$\mathsf{Com}(tag^*, m'; r')$

m' must not be related to m

TAG left $\neq$ TAG right

Building NI tagged commitments

PPV08, LPS17, BL18, KK19

Building NI tagged commitments

PPV08, LPS17, BL18, KK19

[KK19] Subexponential Quantum-secure and quantum-insecure commitments
[BL18] Hardness-amplifiable one-way functions
[LPS17] Assuming subexponential time lock puzzles

$c \log \log \lambda$ tags

Building NI tagged commitments

PPV08, LPS17, BL18, KK19

[KK19] Subexponential Quantum-secure and quantum-insecure commitments
[BL18] Hardness-amplifiable one-way functions
[LPS17] Assuming subexponential time lock puzzles

$c \log \log \lambda$ tags

Tag Amplification

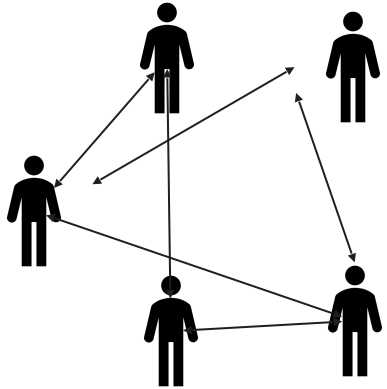
Building NI tagged commitments

PPV08, LPS17, BL18, KK19

[KK19] Subexponential Quantum-secure and quantum-insecure commitments
[BL18] Hardness-amplifiable one-way functions
[LPS17] Assuming subexponential time lock puzzles

$c \log \log \lambda$ tags

Tag Amplification



2^{λ} tags

Tag Amplification

Tag Amplification

- [KK19] **Subexponential NIWIs**

Tag Amplification

- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)

Tag Amplification

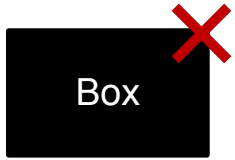
- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**

Tag Amplification

- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF

Tag Amplification

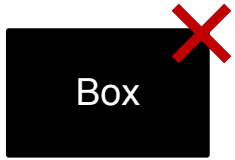
- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF



NIWIs iO

Tag Amplification

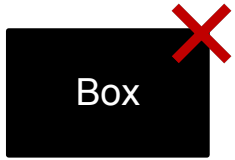
- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF



NIWIs iO

Tag Amplification

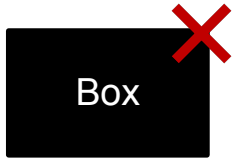
- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF
- [GKLW21] Subexponential CDH/LWE and keyless CRHFs **(for uniform)**



NIWIs iO

Tag Amplification

- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF
- [GKLW21] Subexponential CDH/LWE and keyless CRHFs **(for uniform)**



NIWIs iO

Tag Amplification

- [KK19] **Subexponential NIWIs**
- [BL18] **Subexponential NIWIs** and keyless CRHFs (for non-uniform)
- [LPS17] **Subexponential NIWIs** and keyless Collision Resistant Hash Functions **(for uniform)**
- [Khu21] **Subexponential indistinguishability obfuscation** and OWF
- [GKLW21] Subexponential CDH/LWE and keyless CRHFs **(for uniform)**

Box

NIWIs

iO

Uniform Adversaries

Our landscape

Our landscape

Non-Uniform Adversaries

Our landscape

Non-Uniform Adversaries

1. Stronger class of adversaries, better composition for MPC protocols.

Our landscape

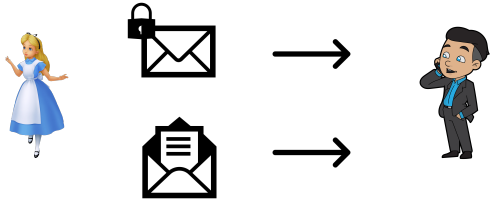
Non-Uniform Adversaries

1. Stronger class of adversaries, better composition for MPC protocols.

2. Proof technique for composing might require non-uniformity [BGJ+17].

Our landscape

Non-Interactive



Black Box Access

No Setup

No CRS
No Random Oracle

Non-Uniform Adversaries

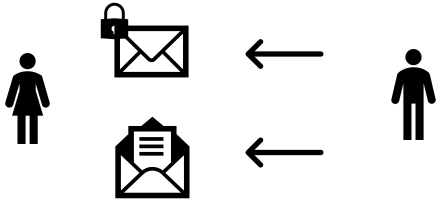
1. Stronger class of adversaries, better composition for MPC protocols.

2. Proof technique for composing might require non-uniformity [BGJ+17].

Our Result

Our Result

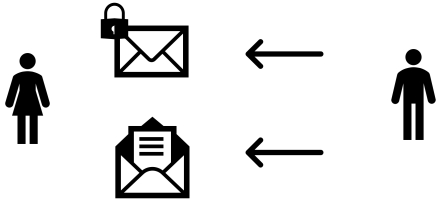
Non-Interactive



Non-Malleable

Our Result

Non-Interactive

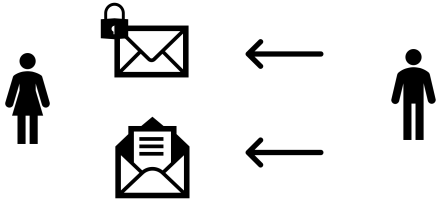


Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

Our Result

Non-Interactive



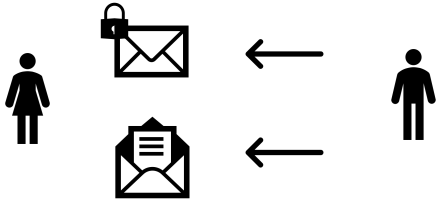
Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

ADVICE

Our Result

Non-Interactive



Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

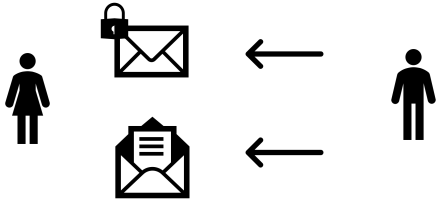
ADVICE

Box

NIZKs ~~iO~~

Our Result

Non-Interactive



Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

ADVICE

Consistency Checks

Box

NIZKs ~~iO~~

CCA Hiding

CLP10 (FOCS’10)

CCA Hiding

$\mathsf{Val}(tag, c)$

CLP10 (FOCS'10)

CCA Hiding

$\mathsf{Val}(tag, c)$

Brute force open

CLP10 (FOCS'10)

CCA Hiding

$\xleftarrow{\quad tag^* \quad}$

$\mathsf{Val}(tag, c)$

Brute force open

CLP10 (FOCS'10)

CCA Hiding

tag^*

$\mathsf{Val}(tag, c)$

Brute force open

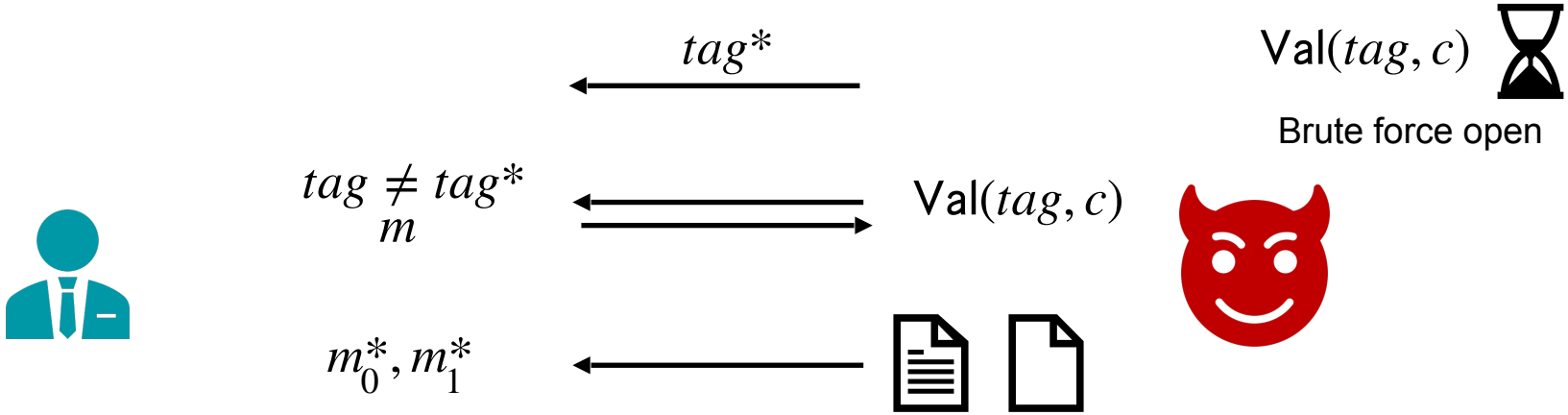
$tag \neq tag^*$

m

$\mathsf{Val}(tag, c)$

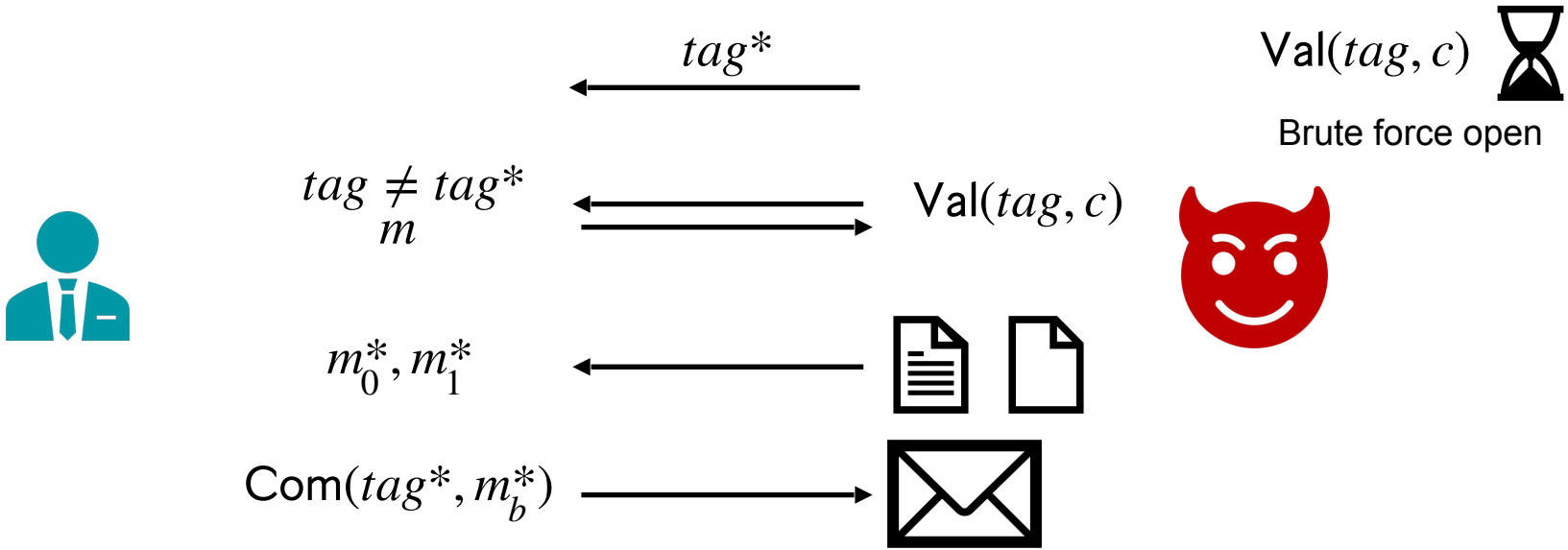
CLP10 (FOCS'10)

CCA Hiding



CLP10 (FOCS'10)

CCA Hiding



CLP10 (FOCS'10)

CCA Hiding

$\mathsf{Val}(tag, c)$

Brute force open

tag^*

$tag \neq tag^*$

m

$\mathsf{Val}(tag, c)$

m_0^*, m_1^*

$\mathsf{Com}(tag^*, m_b^*)$

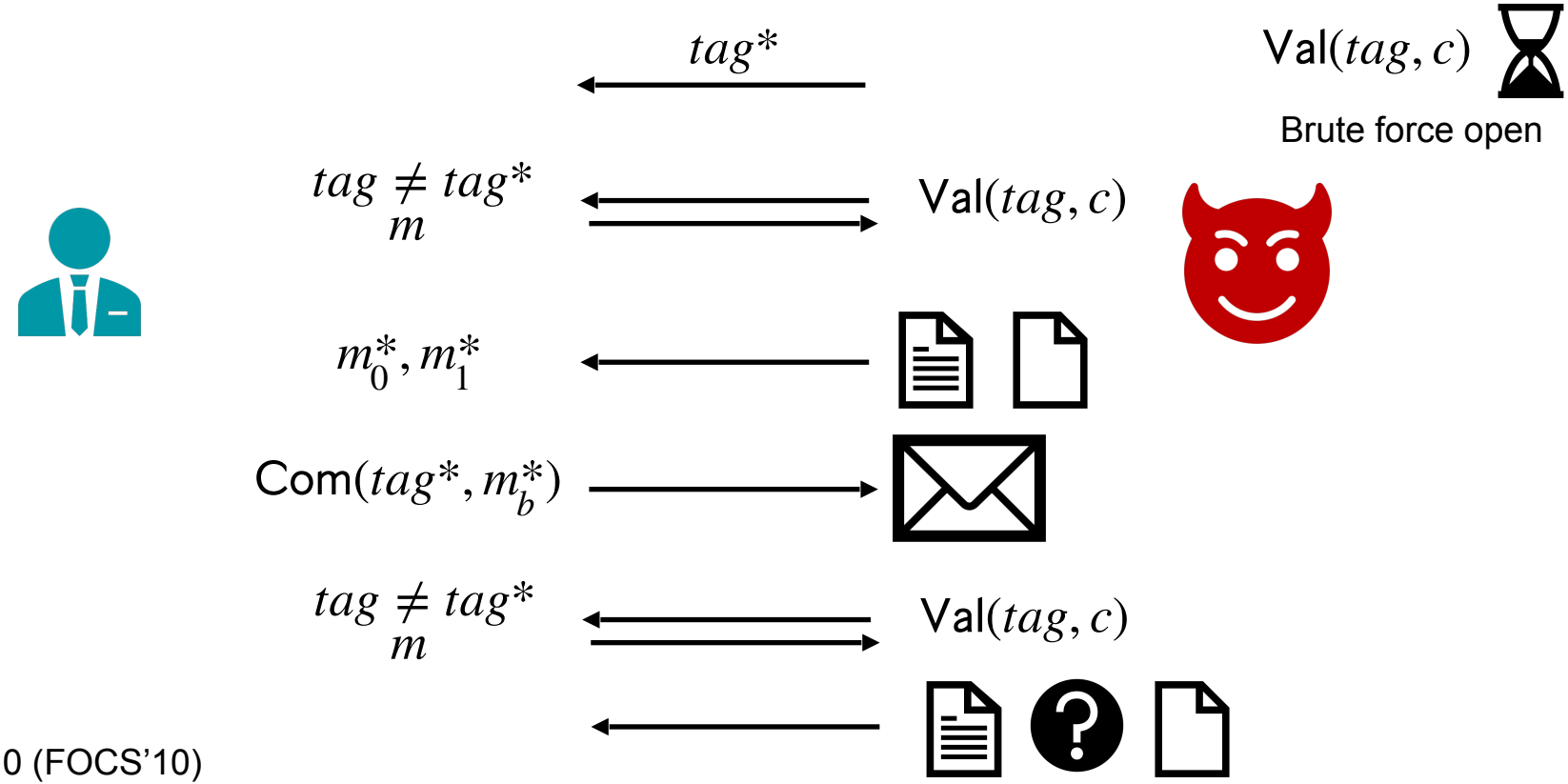
$tag \neq tag^*$

m

$\mathsf{Val}(tag, c)$

CLP10 (FOCS'10)

CCA Hiding



CLP10 (FOCS'10)

Tag Amplification

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

$\mathsf{Com}(TAG, m)$

$TAG = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

$\mathsf{Com}(TAG, m)$

$TAG = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

$\mathsf{Com}(TAG, m)$

$TAG = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1 = (1,1)$ $tag_2 = (1,2)$ $tag_3 = (0,3)$ $tag_4 = (1,4)$ $tag_5 = (1,5)$

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

$\mathsf{Com}(TAG, m)$

$TAG = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1 = (1,1)$ $tag_2 = (1,2)$ $tag_3 = (0,3)$ $tag_4 = (1,4)$ $tag_5 = (1,5)$

$\mathsf{Com}(tag_1, m)$ $\mathsf{Com}(tag_2, m)$ $\mathsf{Com}(tag_3, m)$ $\mathsf{Com}(tag_4, m)$ $\mathsf{Com}(tag_5, m)$

Tag Amplification

$$\log\log\lambda \to \log\lambda \to \lambda \to 2^{\lambda}$$

$\mathsf{Com}(TAG, m)$

$TAG = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1 = (1,1)$ $tag_2 = (1,2)$ $tag_3 = (0,3)$ $tag_4 = (1,4)$ $tag_5 = (1,5)$

$\mathsf{Com}(tag_1, m)$ $\mathsf{Com}(tag_2, m)$ $\mathsf{Com}(tag_3, m)$ $\mathsf{Com}(tag_4, m)$ $\mathsf{Com}(tag_5, m)$

Proof of consistency

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\boxed{\mathsf{Com}(tag_1^*, m)}$ $\boxed{\mathsf{Com}(tag_2^*, m)}$ $\boxed{\mathsf{Com}(tag_3^*, m)}$ $\boxed{\mathsf{Com}(tag_4^*, m)}$ $\boxed{\mathsf{Com}(tag_5^*, m)}$

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

$\mathsf{Val}(TAG, c)$ ⌛

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

$\mathsf{Val}(TAG, c)$ ⌛

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

$\mathsf{Val}(TAG, c)$

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

$\mathsf{Val}(TAG, c)$

$TAG \neq TAG^*$

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*, m)$ $\mathsf{Com}(tag_2^*, m)$ $\mathsf{Com}(tag_3^*, m)$ $\mathsf{Com}(tag_4^*, m)$ $\mathsf{Com}(tag_5^*, m)$

Proof of consistency

$\mathsf{Val}(TAG, c)$

$TAG \neq TAG^*$

1.Verify proof is consistent.
2.If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Tag Amplification

$\mathsf{Com}(TAG, m)$

$TAG^* = 11011 \in \{0,1\}^5$

$\mathsf{Com}(tag, m)$

$tag \in \{0,1\} \times [5]$

$tag_1^* = (1,1)$ $tag_2^* = (1,2)$ $tag_3^* = (0,3)$ $tag_4^* = (1,4)$ $tag_5^* = (1,5)$

$\mathsf{Com}(tag_1^*,0)$ $\mathsf{Com}(tag_2^*,0)$ $\mathsf{Com}(tag_3^*,0)$ $\mathsf{Com}(tag_4^*,0)$ $\mathsf{Com}(tag_5^*,0)$

Proof of consistency

$\mathsf{Val}(TAG, c)$

$TAG \neq TAG^*$

1.Verify proof is consistent.
2.If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Tag Amplification [GKLW21]

Tag Amplification [GKLW21]

Hybrid 0 - CCA game on big TAG

Tag Amplification [GKLW21]

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Tag Amplification [GKLW21]

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Hybrid 2 - Change challenge commitments to commitments of 0

Tag Amplification [GKLW21]

Consistency Check

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Hybrid 2 - Change challenge commitments to commitments of 0

Tag Amplification [GKLW21]

Consistency Check
Security of CHRFs

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Hybrid 2 - Change challenge commitments to commitments of 0

Tag Amplification [GKLW21]

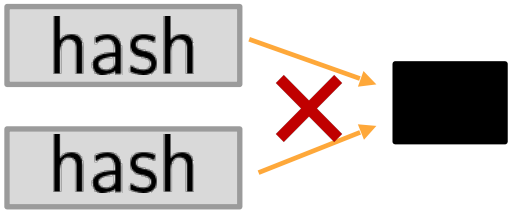
Consistency Check
Security of CHRFs

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Hybrid 2 - Change challenge commitments to commitments of 0

Keyless CRHFs - SHA256



Tag Amplification [GKLW21]

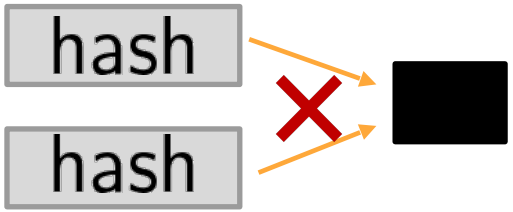
Consistency Check
Security of CHRFs

Hybrid 0 - CCA game on big TAG

Hybrid 1 - Val oracle on different tag than the challenge tag*

Hybrid 2 - Change challenge commitments to commitments of 0

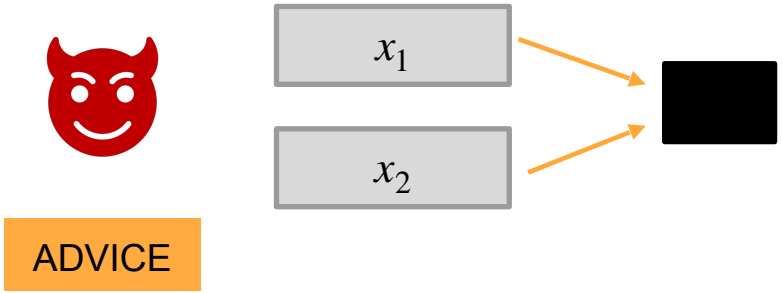
Keyless CRHFs - SHA256



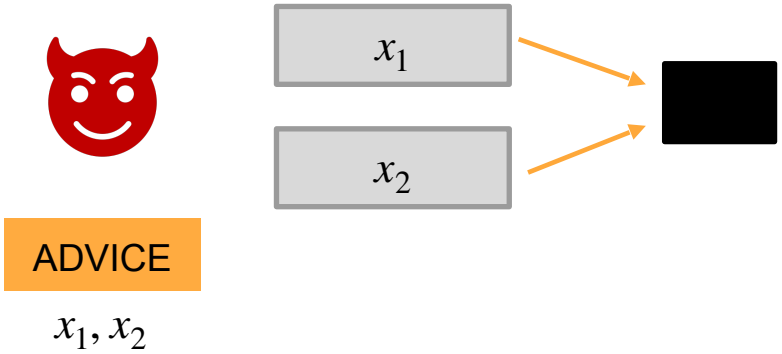
Uniform Adversaries

Non-Uniform Keyless CRHFs [BKP18,BL18]

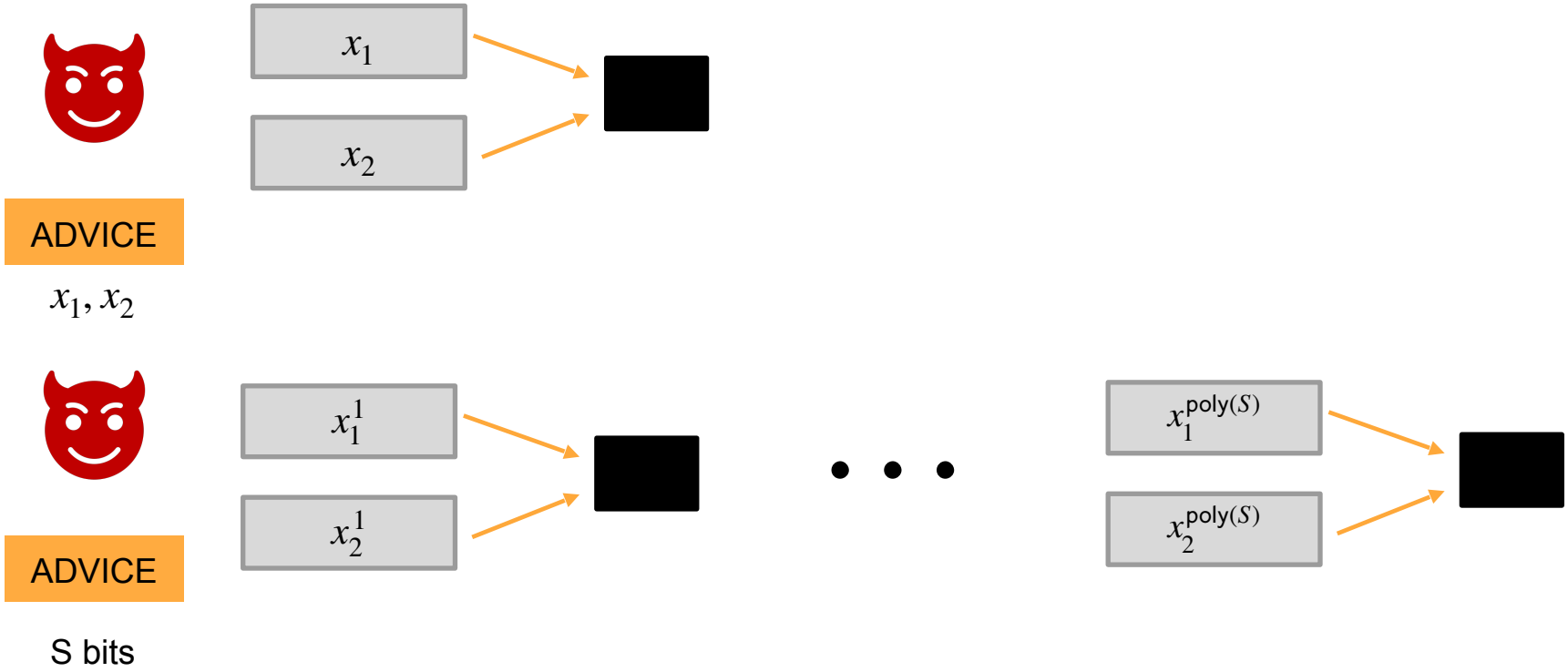
Non-Uniform Keyless CRHFs [BKP18,BL18]



Non-Uniform Keyless CRHFs [BKP18,BL18]



Non-Uniform Keyless CRHFs [BKP18,BL18]



Reduction [GKLW21]

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Reduction [GKLW21]

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Special Commitment c^*

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

Reduction [GKLW21]

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

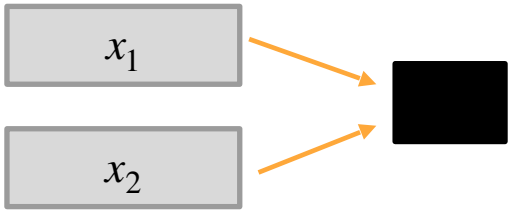
$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Special Commitment c^*

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

$$\downarrow$$



Reduction [GKLW21]

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

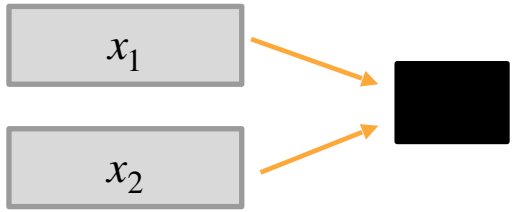
$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Special Commitment c^*

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

$$\downarrow$$



Reduction [GKLW21]

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

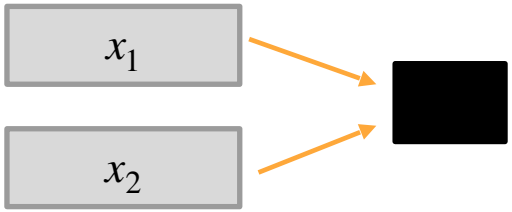
$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Special Commitment c^*

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

$$\downarrow$$



ADVICE

Can find a collision!

Reduction Idea

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

Reduction Idea

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

Reduction Idea

$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$

ADVICE

Special Commitment c_1^*

• • •

ADVICE

Special Commitment $c^*_{\mathsf{poly(S)}}$

Reduction Idea

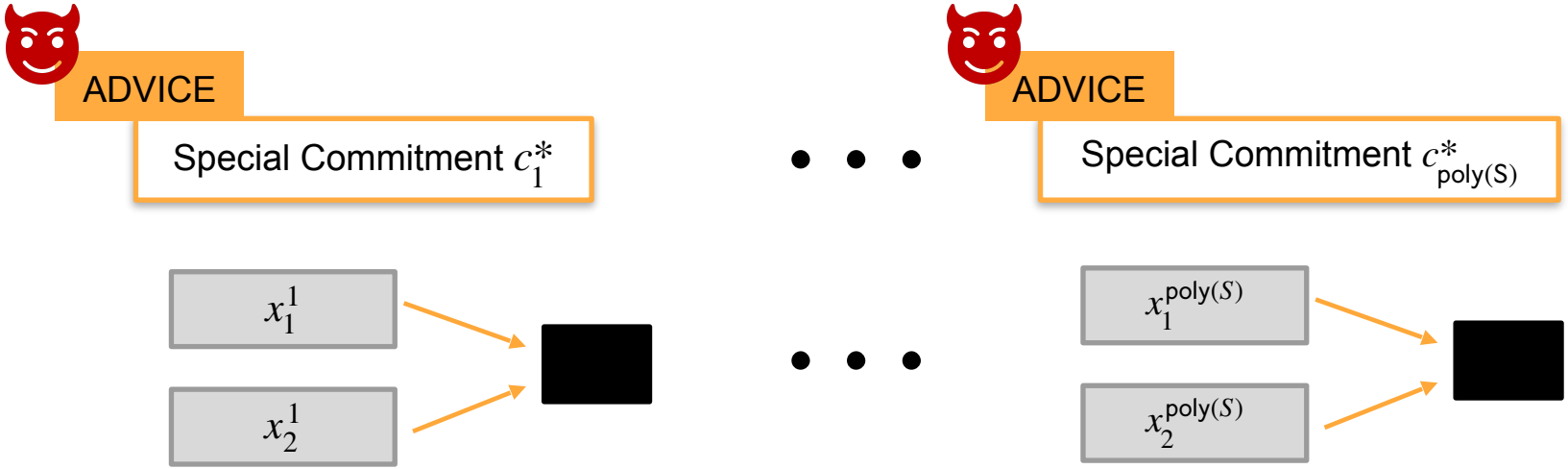
$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$



Reduction Idea

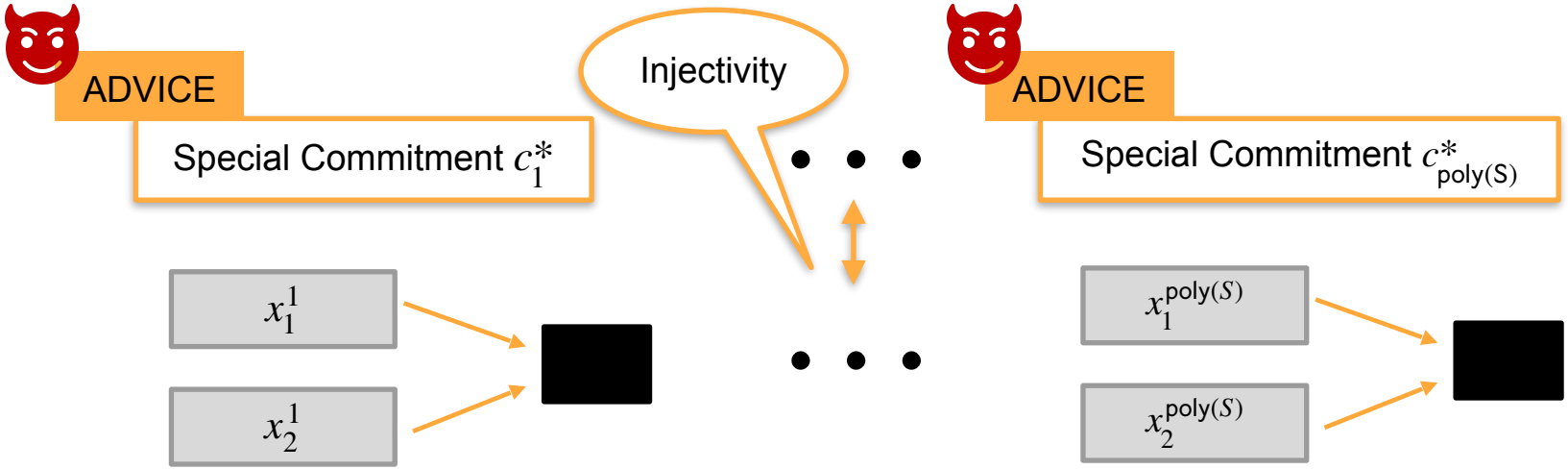
$\mathsf{Val}(TAG, c)$

1. Verify proof is consistent.
2. If valid, output $\mathsf{Val}(tag_1, c_1)$.

$\mathsf{Val}^*(TAG, c)$

1. Verify proof is consistent.
2. If valid, use $tag_j \neq tag_j^*$ output $\mathsf{Val}(tag_j, c_j)$.

$$\mathsf{Val}(TAG, c^*) \neq \mathsf{Val}^*(TAG, c^*)$$



Ingredients

Ingredients

GKLW21

Hinting PRGs [KW19]

Keyless CRHFs

Ingredients

GKLW21

Special PRG

Hinting PRGs [KW19]

Keyless CRHFs

Ingredients

GKLW21

!

Special PRG

$s \rightarrow s'_1 \cdots s'_n$

Hinting PRGs [KW19]

Keyless CRHFs

Ingredients

GKLW21

!

Special PRG

$s \rightarrow s'_1 \cdots s'_n$

Hinting PRGs [KW19]

Keyless CRHFs

Our Work

Ingredients

GKLW21

Special PRG

Hinting PRGs [KW19]

Keyless CRHFs

Our Work

Hinting PRGs w injective extension

$s \rightarrow s'_1 \quad \cdots \quad s'_n$

$s \rightarrow s'_1 \quad \cdots \quad s'_n \quad s''$

s'' is injective with s

Ingredients

GKLW21

Special PRG

$s \rightarrow s'_1 \quad \cdots \quad s'_n$

Hinting PRGs [KW19]

$s \rightarrow s'_1 \quad \cdots \quad s'_n \quad s''$

Keyless CRHFs

s'' is injective with s

Our Work

Hinting PRGs w injective extension

CDH or LWE

Ingredients

GKLW21

Special PRG

$s \rightarrow s'_1 \quad \cdots \quad s'_n$

Hinting PRGs [KW19]

$s \rightarrow s'_1 \quad \cdots \quad s'_n \quad s''$

Keyless CRHFs

s'' is injective with s

Our Work

Hinting PRGs w injective extension

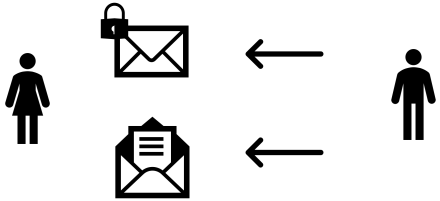
Keyless CRHFs can't find 2S collisions w S advice

CDH or LWE

Our Result

Our Result

Non-Interactive



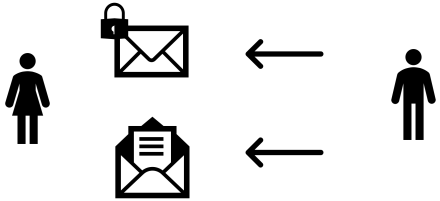
Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

ADVICE

Our Result

Non-Interactive



Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

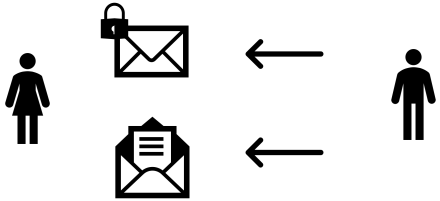
ADVICE

Hinting PRGs
w injective extension

Keyless CRHFs
can't find 2S collisions w S advice

Our Result

Non-Interactive



Non-Malleable

$c \log \log \lambda$ tags $\longrightarrow$ 2^{λ} tags

ADVICE

Hinting PRGs
w injective extension

Keyless CRHFs
can't find 2S collisions w S advice

Box

~~NIWIs~~ ~~iO~~

Open Questions

Open Questions

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

- Can we remove hinting PRGs and get it from something even simpler? (like CCA from injective TDFs) [HKW20]

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

- Can we remove hinting PRGs and get it from something even simpler? (like CCA from injective TDFs) [HKW20]

- Improve the dependence of advice on number of collisions. Can we construct from S advice and S^2 collisions?

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

- Can we remove hinting PRGs and get it from something even simpler? (like CCA from injective TDFs) [HKW20]

- Improve the dependence of advice on number of collisions. Can we construct from S advice and S^2 collisions?

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

- Can we remove hinting PRGs and get it from something even simpler? (like CCA from injective TDFs) [HKW20]

- Improve the dependence of advice on number of collisions. Can we construct from S advice and S^2 collisions?

- Recent work by [Khu21] that removed the CRHF assumption with Obfuscation. Can we hope to relax this more?

Open Questions

- Can we generalize [KW19] more? Abstract this framework of using hinting PRGs into making general statements about proving consistency checks/CCA style security.

- Can we remove hinting PRGs and get it from something even simpler? (like CCA from injective TDFs) [HKW20]

- Improve the dependence of advice on number of collisions. Can we construct from S advice and S^2 collisions?

- Recent work by [Khu21] that removed the CRHF assumption with Obfuscation. Can we hope to relax this more?

Thanks!

- [DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-Malleable Cryptography (Ex- tended Abstract). In *STOC 1991*.

- [CLP10] Ran Canetti, Huijia Lin, and Rafael Pass. Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. In *FOCS 2010.*

- [LPS17] Huijia Lin, Rafael Pass, and Pratik Soni. Two-round and non-interactive concurrent non-malleable commitments from time-lock puzzles. In *FOCS 2017*.

- [BL18] Nir Bitansky and Huijia Lin. One-message zero knowledge and non-malleable com- mitments. In *TCC 2018*.

- [KK19] Yael Tauman Kalai and Dakshita Khurana. Non-interactive non-malleability from quantum supremacy. In *Crypto 2019*.

- [GKLW21] Rachit Garg, Dakshita Khurana, George Lu, Brent Waters. Black-Box Non-Interactive Non-Malleable Commitments. In Eurocrypt 2021.