INCREMENTAL DETERMINISTIC PUBLIC-KEY ENCRYPTION

Ilya Mironov, Omkant Pandey,
Omer Reingold, Gil Segev

Microsoft Research

Incremental Deterministic Public-Key Encryption

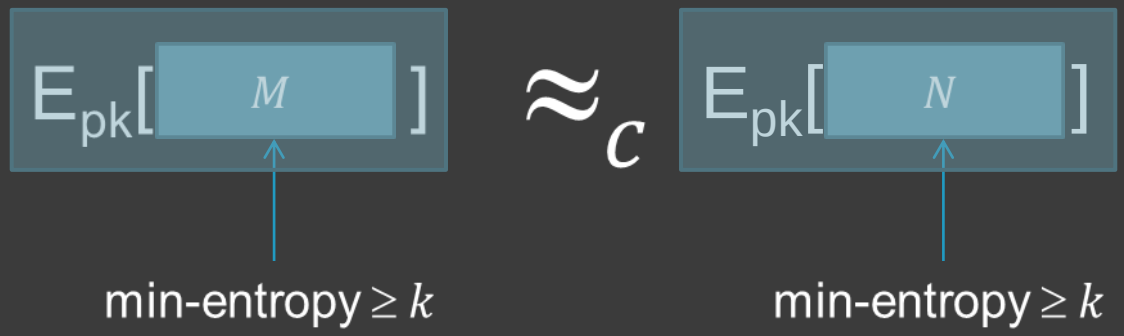
Deterministic Public-Key Encryption

k-source adversary

min-entropy $\geq k$:

Probability of any output $\leq 2^{-k}$

Deterministic Public-Key Encryption: PRIV1-IND



M and N are **independent** of PK

[Bellare, Boldyreva, O'Neill CRYPTO'07]

Is It Secure?

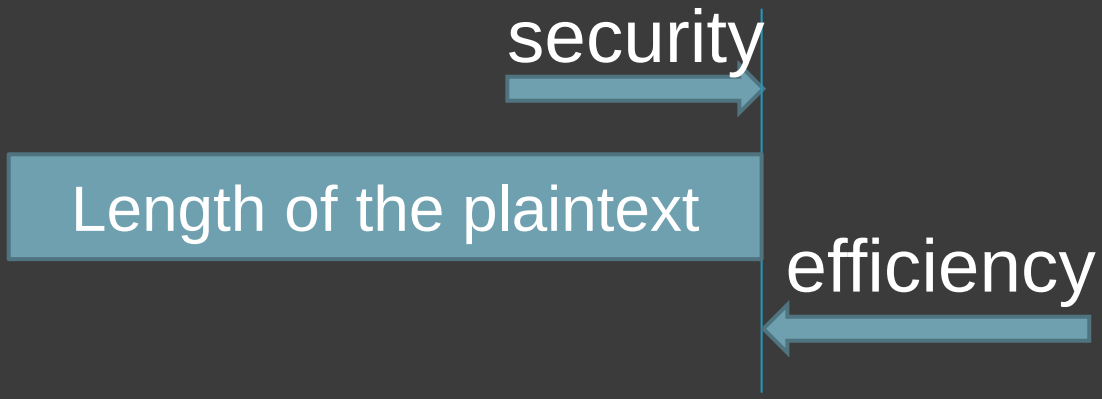
- search
- de-duplication
- deterministic KEM

Secure Deterministic Encryption

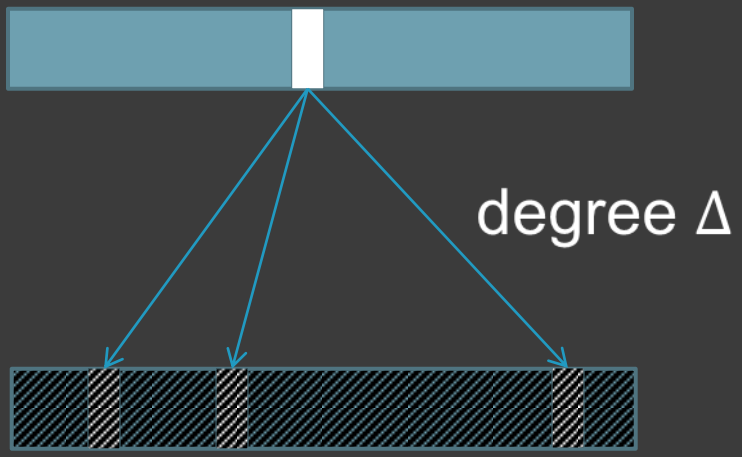
Computational assumptions

Min-entropy of the source

Long, unpredictable plaintext:
- digital photograph
- MS Word document
- entire database
- full disk


security
Length of the plaintext
efficiency

Incrementality



- Incrementality with access to plaintext: setting bit
- Incrementality without access to plaintext: flipping bit

Incremental Deterministic Public-Key Encryption

Our results

- Lower bound:

incrementality

$$\Delta > \frac{|P|}{k \log |C|}$$

min-entropy

- Two schemes

1. Generic Solution

Deterministic Encryption

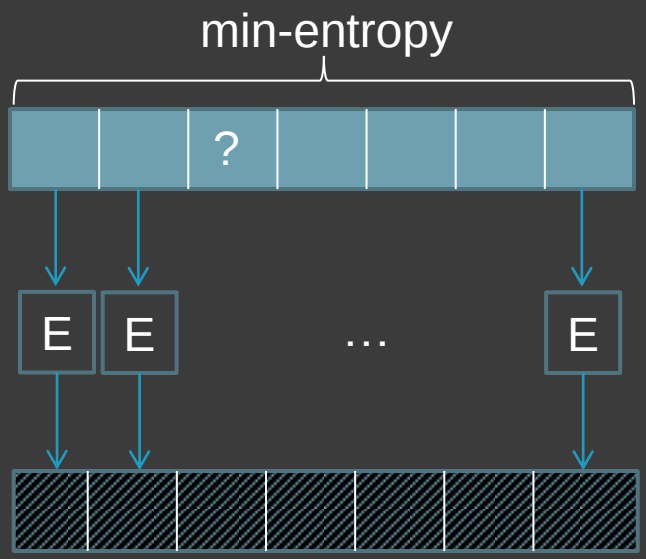
↓

Incremental Deterministic Encryption

2. DDH-based solution

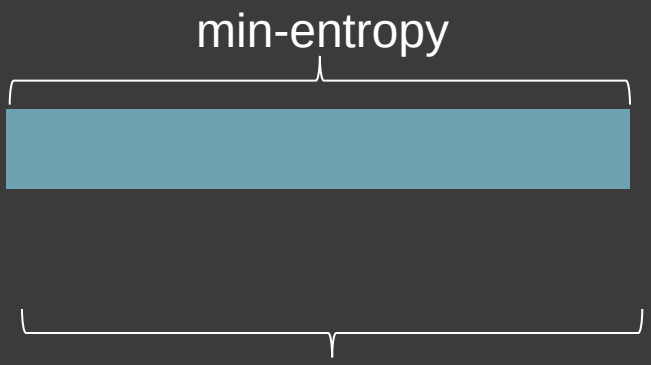
tight up to polylog factors

Naïve Generic Solution



E: deterministic encryption scheme

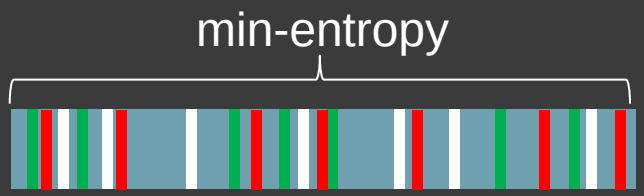
Sample-then-extract



[Nisan,Zuckerman'96] [Vadhan'04]

Generic Solution

Partition input into random subsets



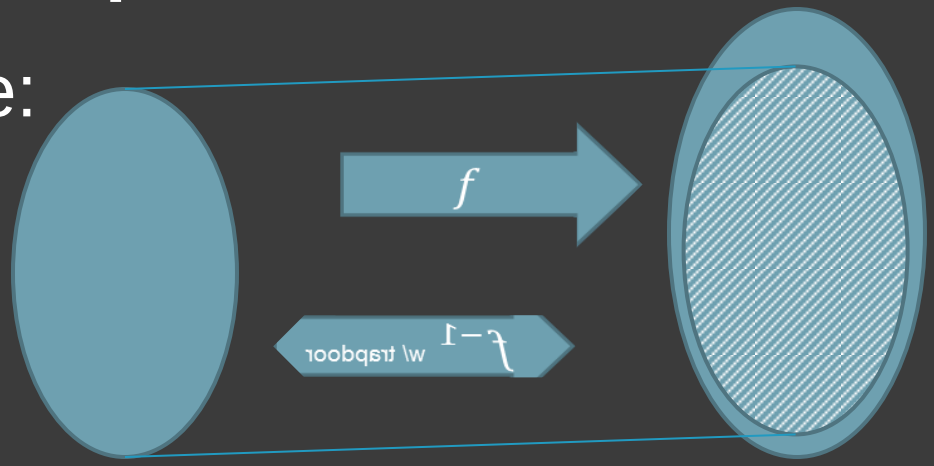
PRIV-IND $\Rightarrow$ PRIV1-IND with Incrementality

Standard Model

DDH $\Rightarrow$ PRIV1-IND with Incrementality

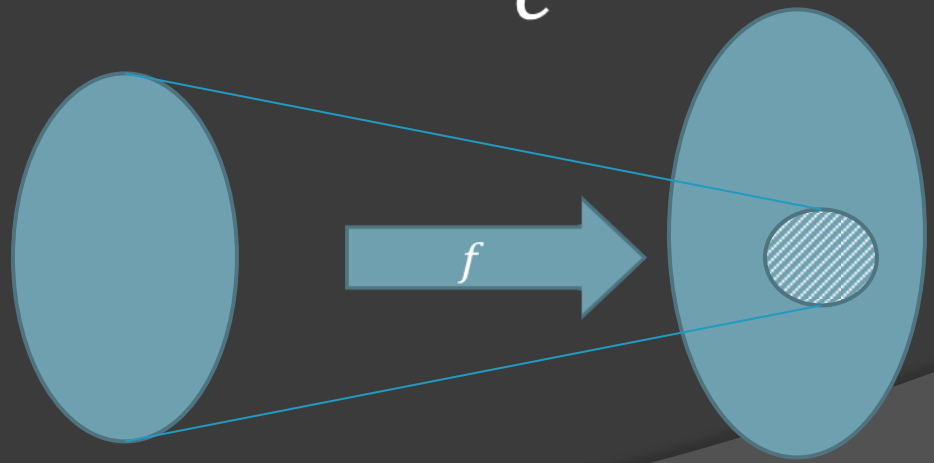
Lossy Trapdoor Functions

Injective mode:



$\approx_c$

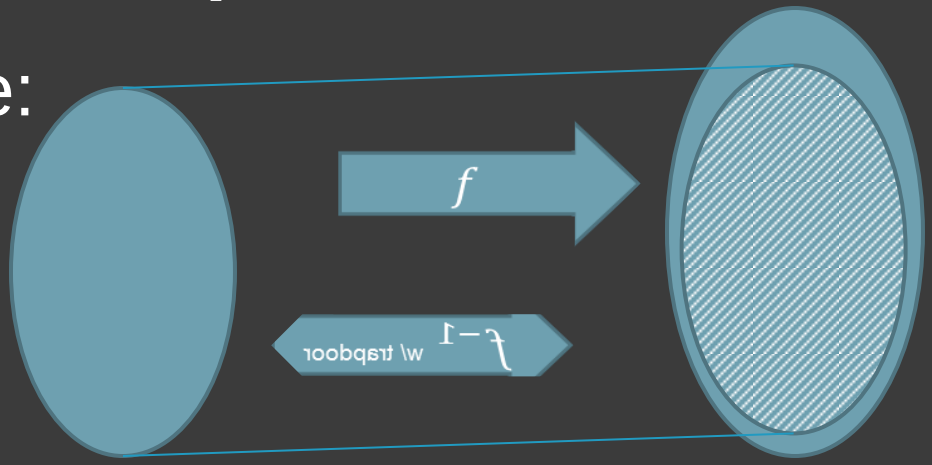
Lossy mode:



[Peikert, Waters STOC'08]

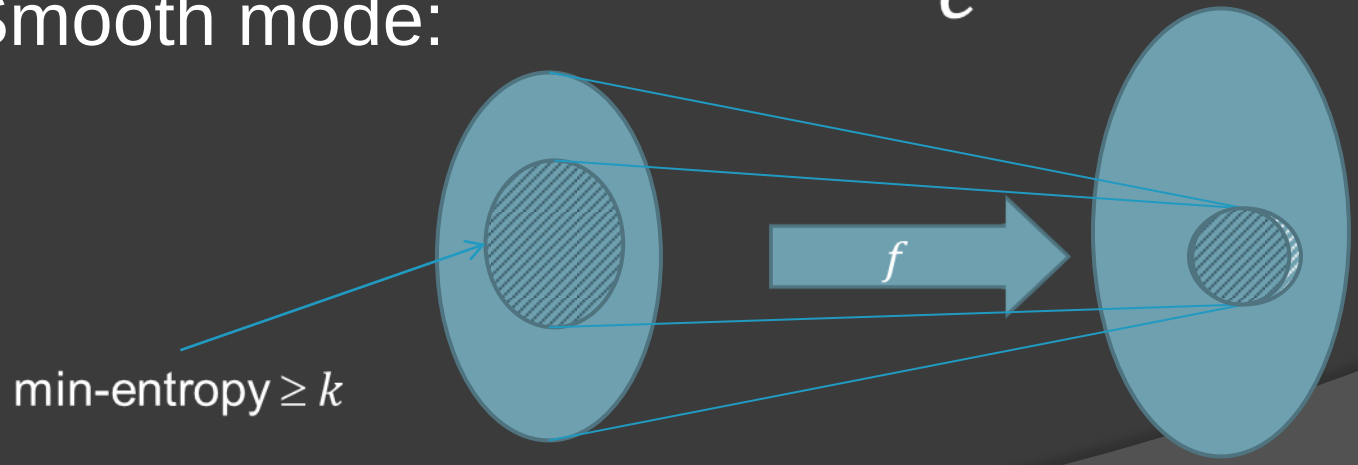
Smooth Trapdoor Functions

Injective mode:



$\approx_c$

Smooth mode:



statistically close

Smooth Trapdoor Functions $\Rightarrow$ PRIV1-IND Security

min-entropy $\geq k$ min-entropy $\geq k$

injective mode: $f(M) \approx_c f(N)$

smooth mode: $f(M) \approx f(N)$

Construction of PRIV1-IND

Lossy Trapdoor Function

Pairwise-independent permutation

Smooth Trapdoor Function

Deterministic Public-Key Encryption

[Boldyreva, Fehr, O'Neill CRYPTO'08]

Construction of PRIV1-IND

Lossy Trapdoor Function

Pairwise-independent permutation

Smooth Trapdoor Function

~~Incremental~~ Deterministic Public-Key Encryption

[Boldyreva, Fehr, O'Neill CRYPTO'08]

Construction of Lossy TDF

$\mathbb{G}$ - group of order p generated by g

$(g^A)_{ij} = (g^{a_{ij}})$

Key generation

- Sample $A \leftarrow \mathbb{Z}_p^{n \times n}$
- Output $sk = A^{-1}$ and $pk = g^A \in \mathbb{G}^{n \times n}$

Encryption

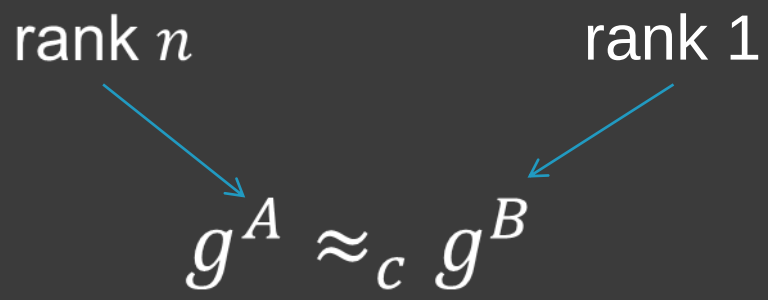
- Given $\vec{m} \in \{0,1\}^n$ output $g^{A\vec{m}} \in \mathbb{G}^n$

Decryption

- Given $g^{\vec{v}} \in \mathbb{G}^n$ compute $g^{\vec{m}} = g^{A^{-1}\vec{v}} \in \mathbb{G}^n$
- Output $\vec{m} \in \{0,1\}^n$

[Freeman, Goldreich, Kiltz, Rosen, Segev PKC'10] [Brakerski, Segev CRYPTO'11]

Security Argument: Lossy TDF



$g^{A\vec{m}}$ — injective $g^{B\vec{m}}$ — $\log p$ bits

Towards Incremental Smooth TDF

rank n
sparse

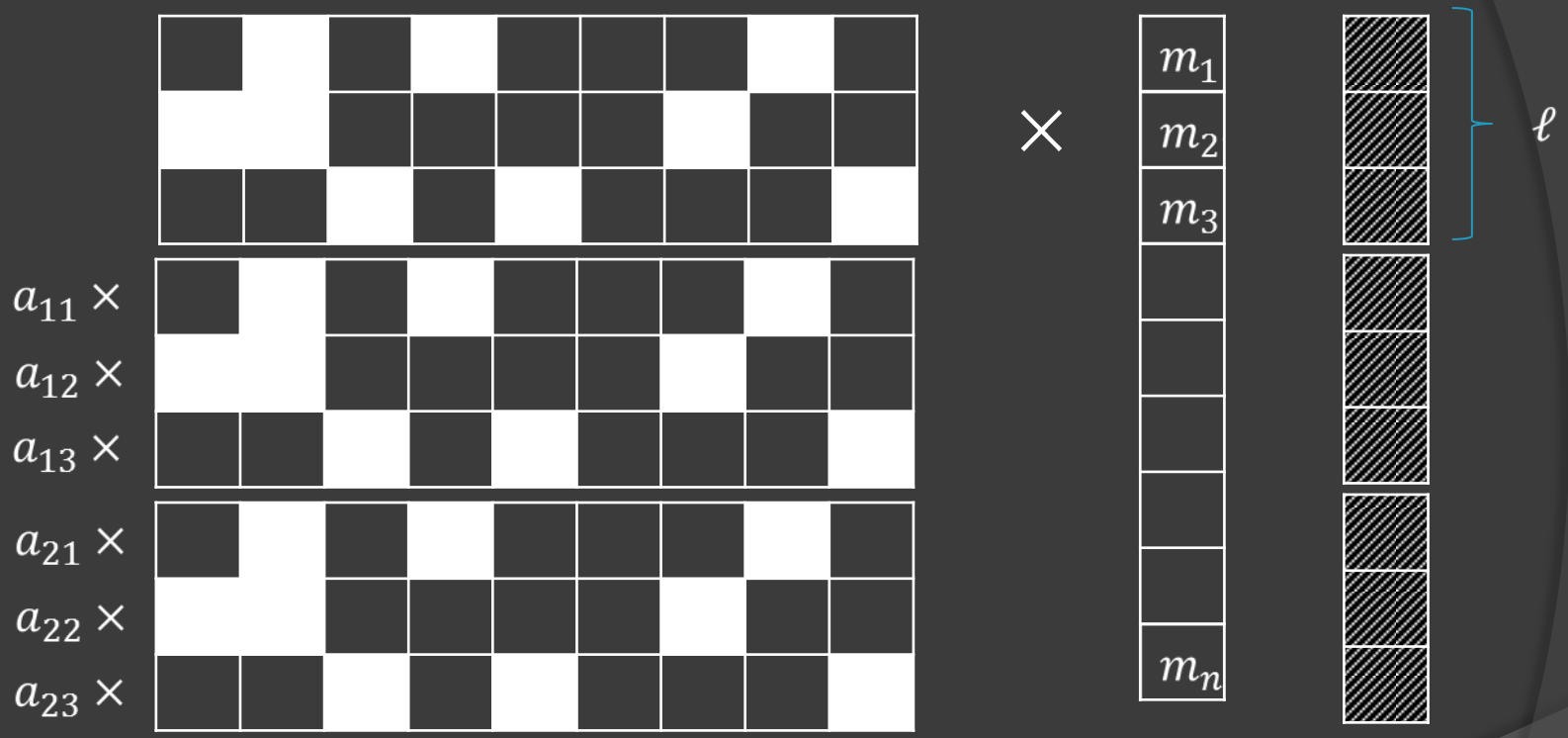
rank ℓ
sparse

$$g^A \approx_c g^B$$

$g^{A\vec{m}}$ — injective

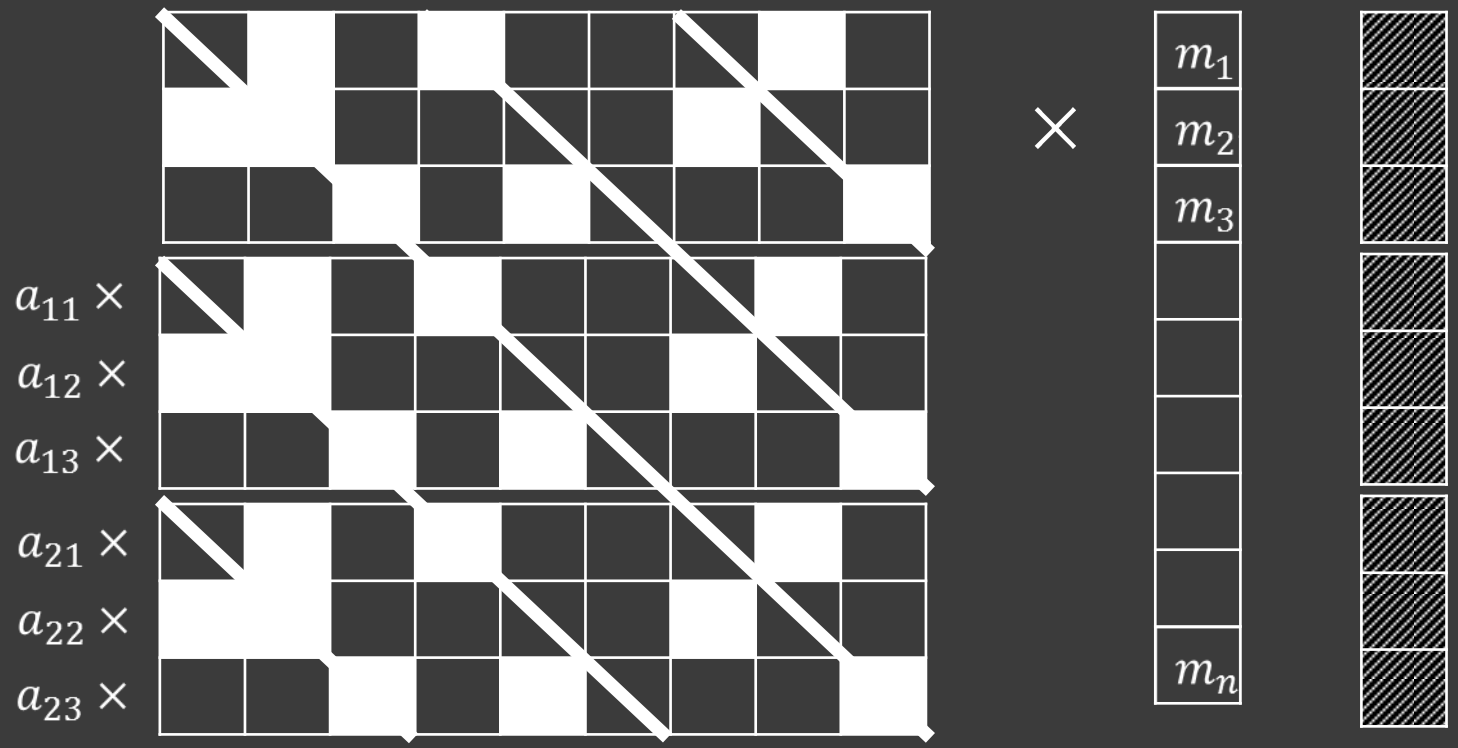
if $\vec{m}$ has min-entropy k, $g^{B\vec{m}}$ statistically close to the uniform over its range

Towards Incremental Smooth TDF

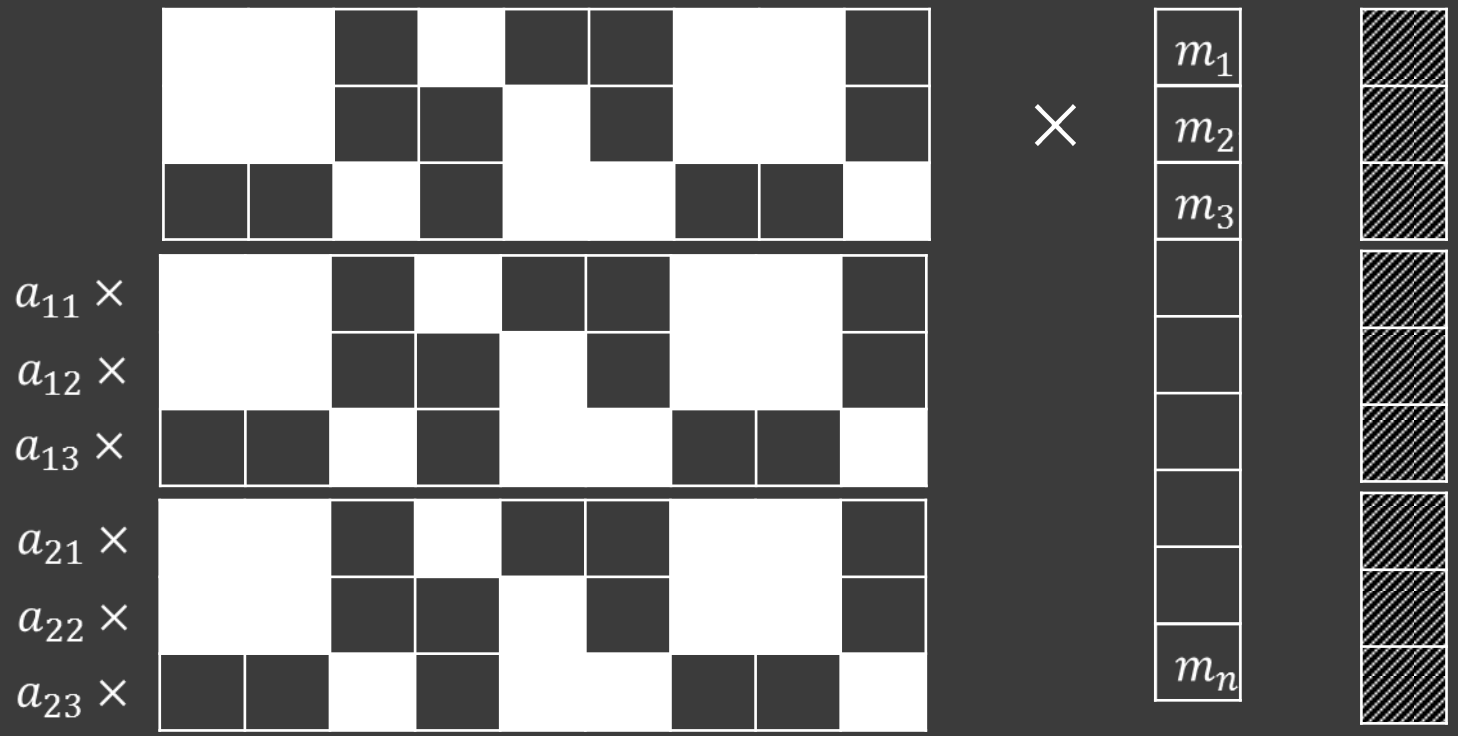


Sample-then-extract + Leftover Hash Lemma

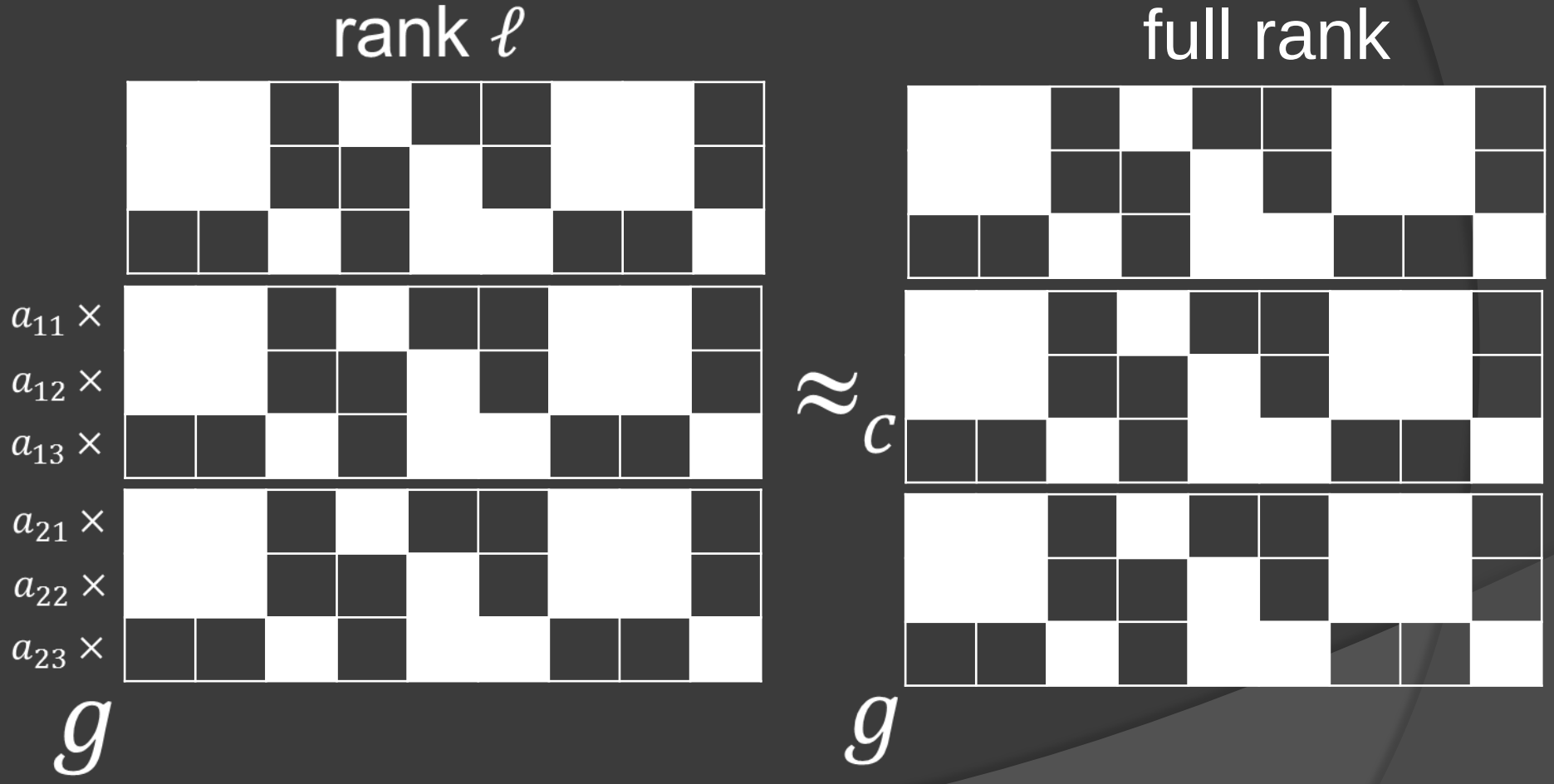
Towards Incremental Smooth TDF



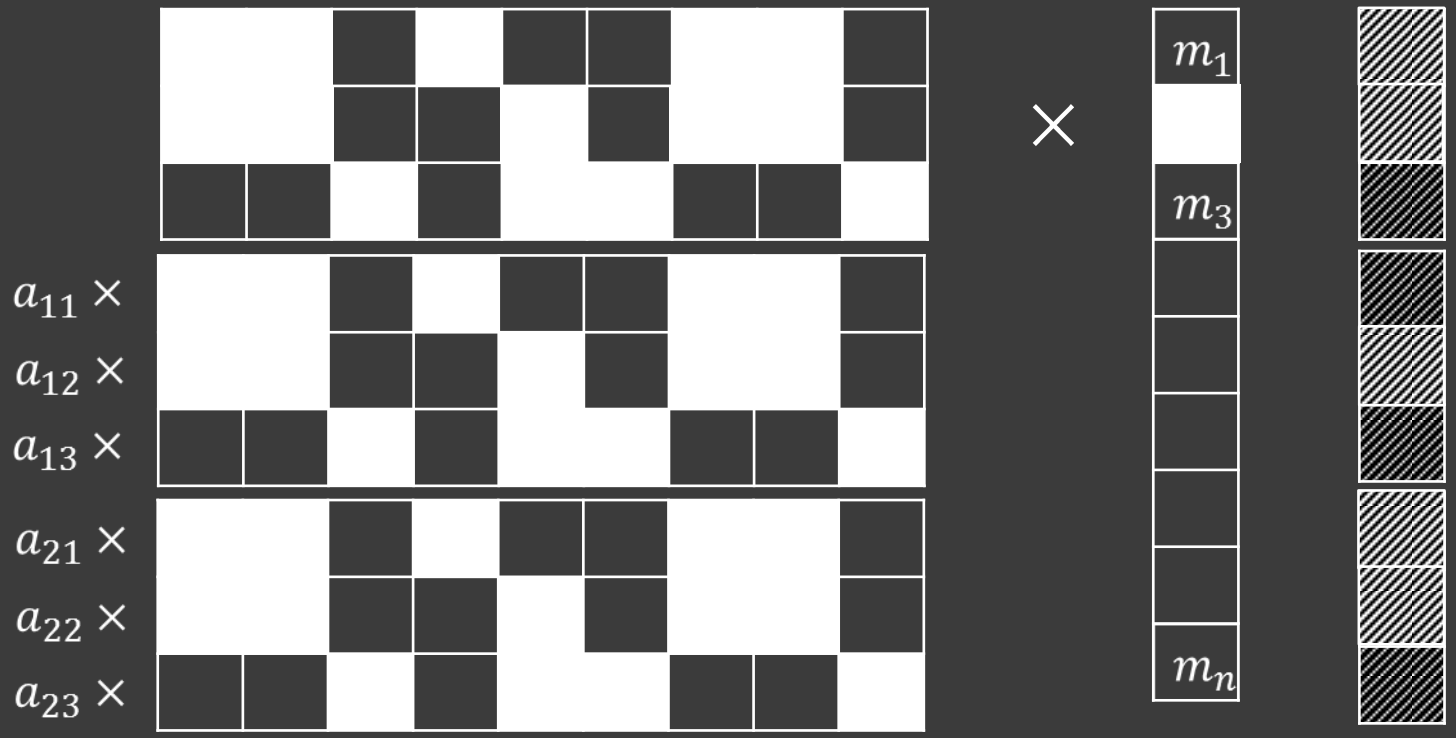
Towards Incremental Smooth TDF



Smooth vs Injective Mode



Incrementality



Open Problems

Incremental Deterministic Encryption:

- Stronger security: PRIV-IND (multiple messages)
- Length-preserving in the standard model

Deterministic Encryption:

- Relaxing the definition to allow dependency on the public key