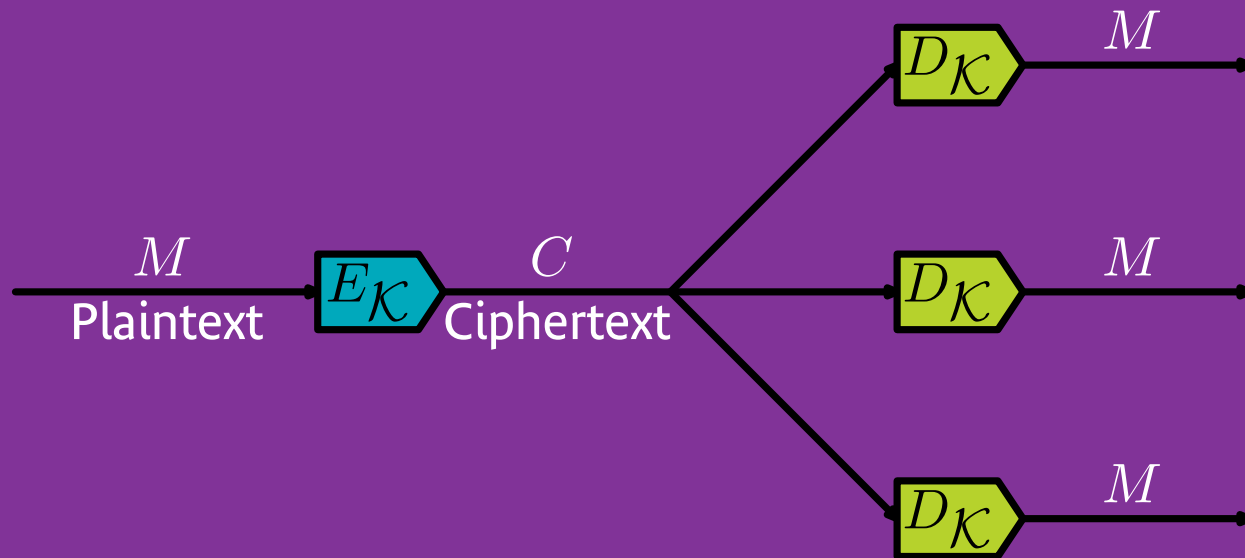


A Traceable Block Cipher

Olivier Billet, Henri Gilbert



Content Distribution *Context*



Context

Issues:

- ▶ Key Redistribution (by traitors to pirate users)
- ▶ Content Redistribution (not addressed here)

Traitor Tracing *Definitions*



Context

Definitions

- ▶ Benny Chor, Amos Fiat, Moni Naor, 1994

- ▶ Each of the N users receives a personal key \mathcal{K}_j
 - » \mathcal{K}_j enables user j to decrypt content
 - » \mathcal{K}_j uniquely identifies user j

- ▶ No coalition of k traitors will produce an untraceable key
 - » allows a pirate to decrypt content
 - » conceals all traitors' identities

Traitor Tracing



Context

Definitions

▶ Four Procedures

- » Key Generation
- » Encrypt
- » Decrypt
- » Tracing

▶ Previous Constructions

- » Combinatorial Scheme [CFN 94, NP 98]
headers $O(k \ln N)$
- » Asymmetric Algorithm [BF 99]
expansion $O(k)$

Traceable Blockcipher



Context

Definitions

Cipher

- ▶ $F_{\mathcal{K}}$ satisfies usual symmetric block cipher requirements
- ▶ generation from the meta-key \mathcal{K} of keys \mathcal{K}_j such that

$$F_{\mathcal{K}} \equiv F_{\mathcal{K}_1} \equiv \dots \equiv F_{\mathcal{K}_j} \equiv \dots \equiv F_{\mathcal{K}_N}$$

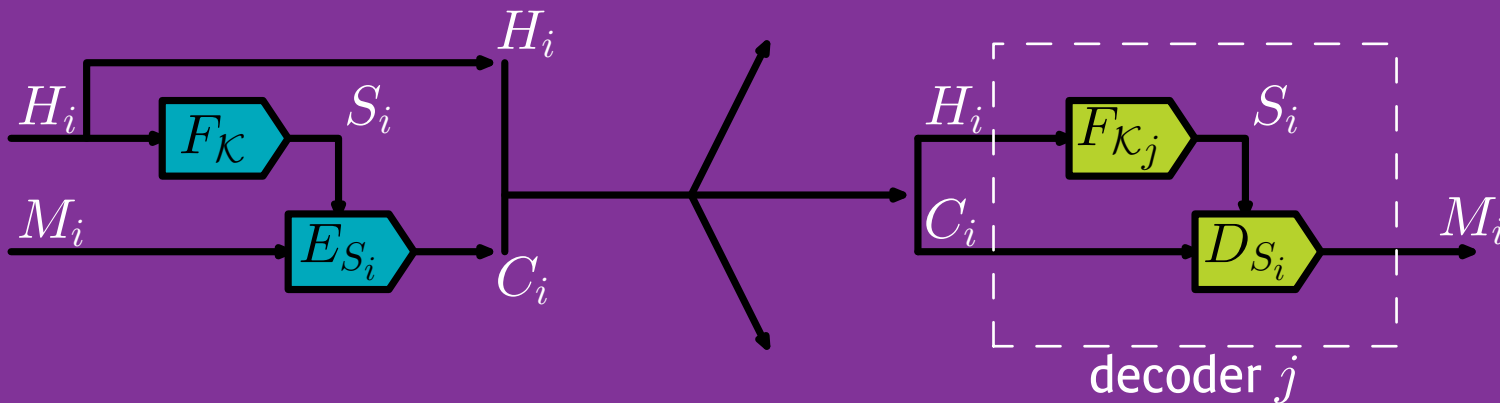
- ▶ k -traceability requirement:

an equivalent description produced from the knowledge of up to k equivalent descriptions $F_{\mathcal{K}_{j_1}}, \dots, F_{\mathcal{K}_{j_k}}$ must reveal at least one of the identities j_1, \dots, j_k

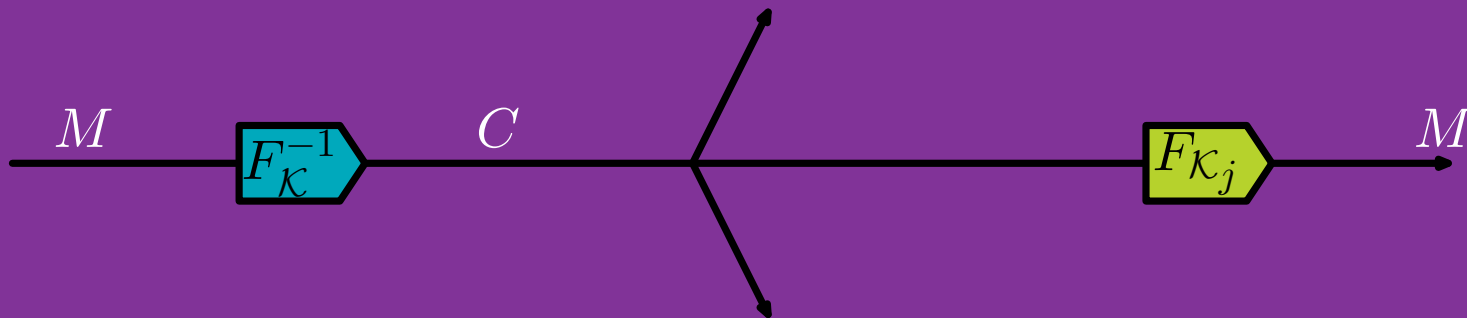
Operation Modes



▶ Mode with control words: $F_{\mathcal{K}} \equiv F_{\mathcal{K}_j}$



▶ Simple mode: $F_{\mathcal{K}}^{-1} \equiv F_{\mathcal{K}_j}$



Context

Definitions

Cipher

Modes

C^* Scheme *Matsumoto-Imai*



parameters

» $\mathbb{K} = \mathbf{GF}(q) \quad q = 2^m$

» $\mathbb{L} \simeq \mathbb{K}^n$

$$\mathbb{L} = \mathbb{K}[X]/\pi_n(X)$$

» $(1 + q^\theta) \perp (q^n - 1)$

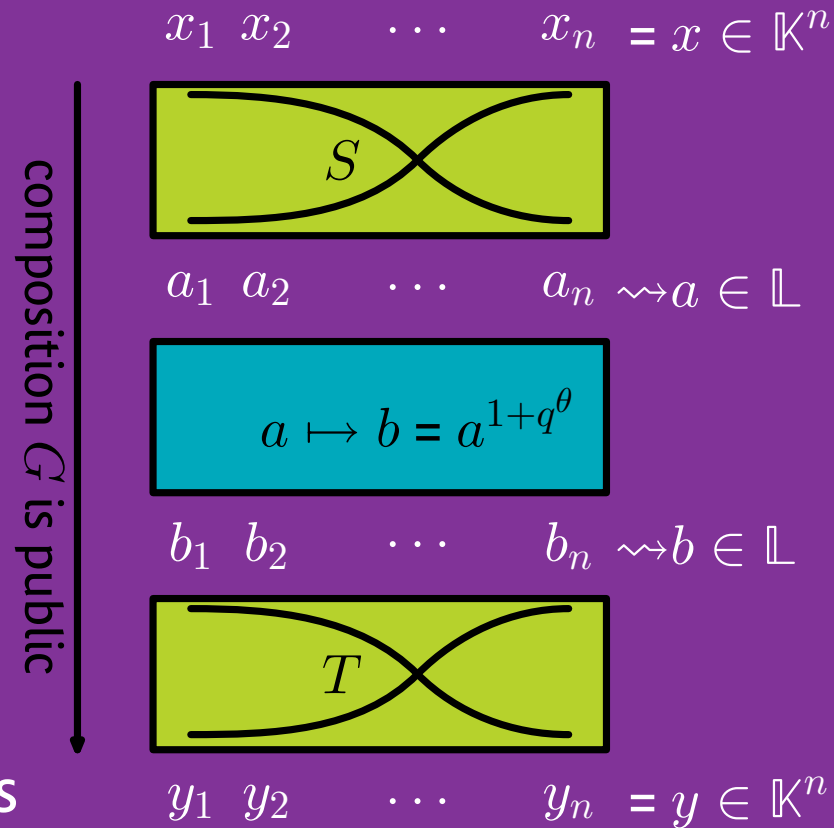
public key is a set of n quadratic equations in the variables x_i

private key is (S, T)

two invertible linear maps

encrypt with G

decrypt with $S^{-1} \circ g^{-1} \circ T^{-1}$



Context
Definitions
Cipher
Modes

C^*

Underlying Problems



► Solving systems of multivariate equations

- » find one solution (x_1, \dots, x_n) over a finite field \mathbb{K} of

$$\{y_i = P_i(x_1, \dots, x_n)\}_{i \in [1, n]}$$

- » Decision problem is NP-complete, even over $\text{GF}(2)$
- » Patarin 1995 used structure of C^* to invert it

► IP: isomorphism of polynomials

- » given two sets of polynomials $\{P\}$ and $\{Q\}$
find bijective linear maps A and B such that

$$B \circ (P_1, \dots, P_n) \circ A = (Q_1, \dots, Q_m)$$

- » IP is harder than IG
- » no polynomial algorithm is known [PGC, 1998]
- » relinearization attack for C^* degree 2 from [SK, 1999]

Context

Definitions

Cipher

Modes

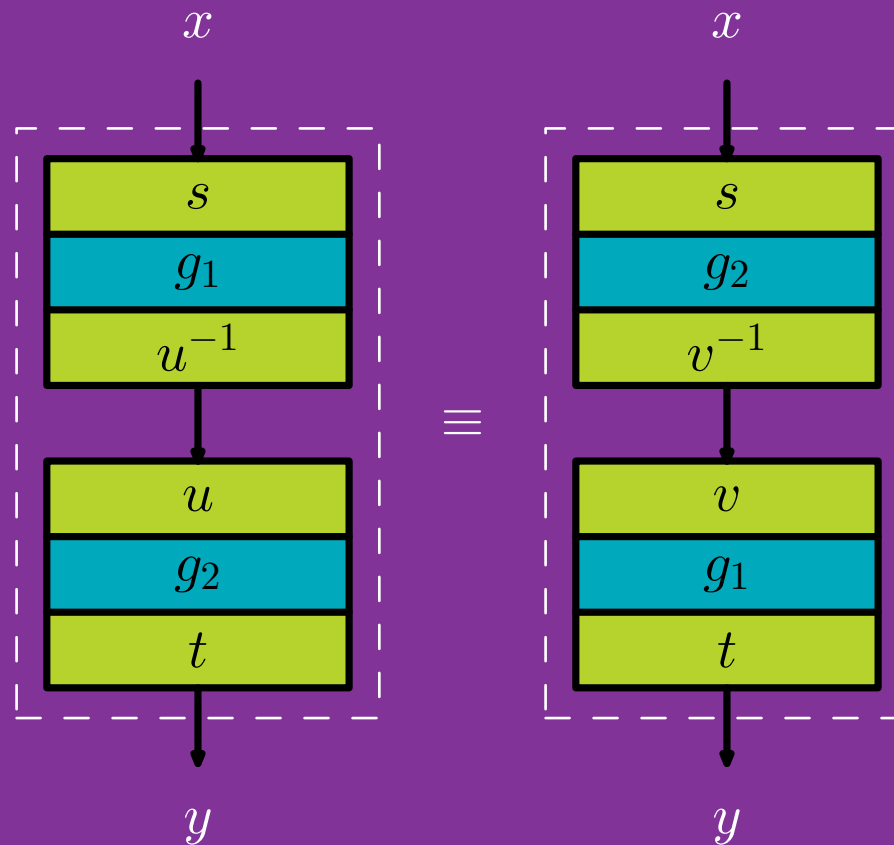
C^*

Comp. Prob.

Commuting Blocks *Conducting Idea*



$$g_1 \circ g_2 = g_2 \circ g_1$$



⊛ use a version of C^* with higher degree $d > 2$

$$g_i : a \mapsto b = a^{1+q^{\theta_1}+\dots+q^{\theta_{d-1}}}$$

Context

Definitions

Cipher

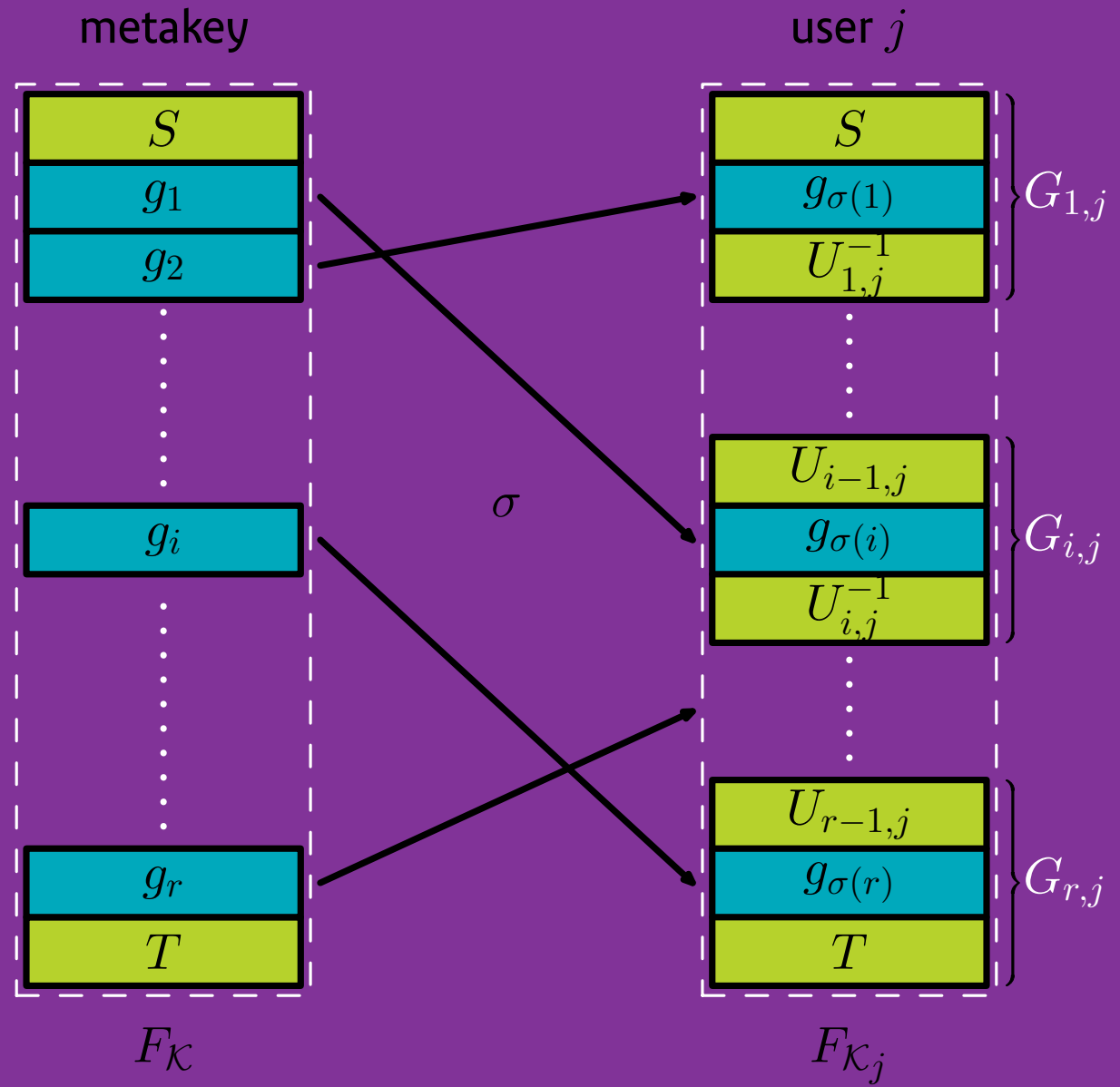
Modes

C^*

Comp. Prob.

Commuting

Commuting Blocks *Key Generation*



- Context
- Definitions
- Cipher
- Modes
- C^*
- Comp. Prob.
- Commuting**

Parameters *Example*



▶ $q = 2^{16}$ $\mathbb{K} = \text{GF}(q)$

▶ $n = 5$ block size is 80 bits

▶ $d = 4$

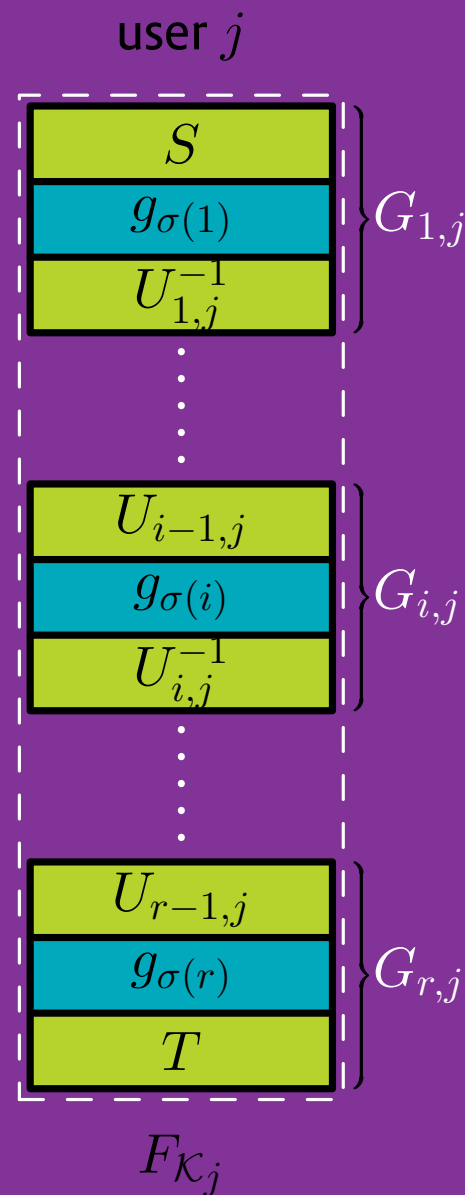
equations for $G_{i,j}$ have degree 4
about 70 monomials per equation

computing $G_{i,j}$ is at most
435 multiplications in \mathbb{K}

▶ $r = 32$ 32 rounds

$F_{\mathcal{K}_j}$ is about 14000 mult. in \mathbb{K}

▶ size for $F_{\mathcal{K}_j}$ is 22 KB



Context

Definitions

Cipher

Modes

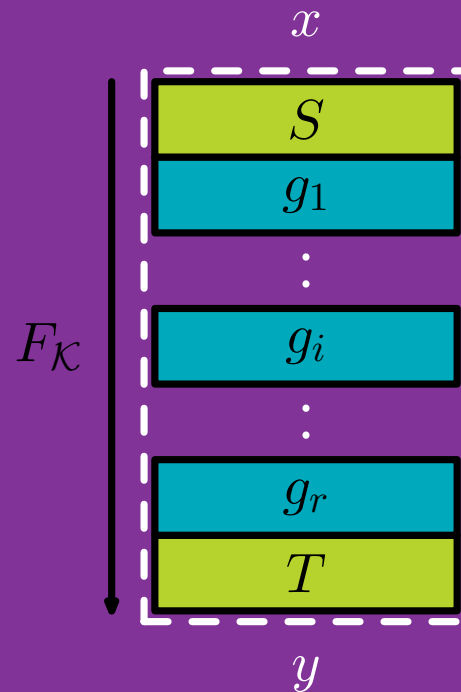
C^*

Comp. Prob.

Commuting

Parameters

Security as a Symmetric Cipher



Input/Output observation must not allow

- ▶ to recover F_K
- ▶ to interpolate F_K
- ▶ to distinguish from a random permutation

Context

Definitions

Cipher

Modes

C^*

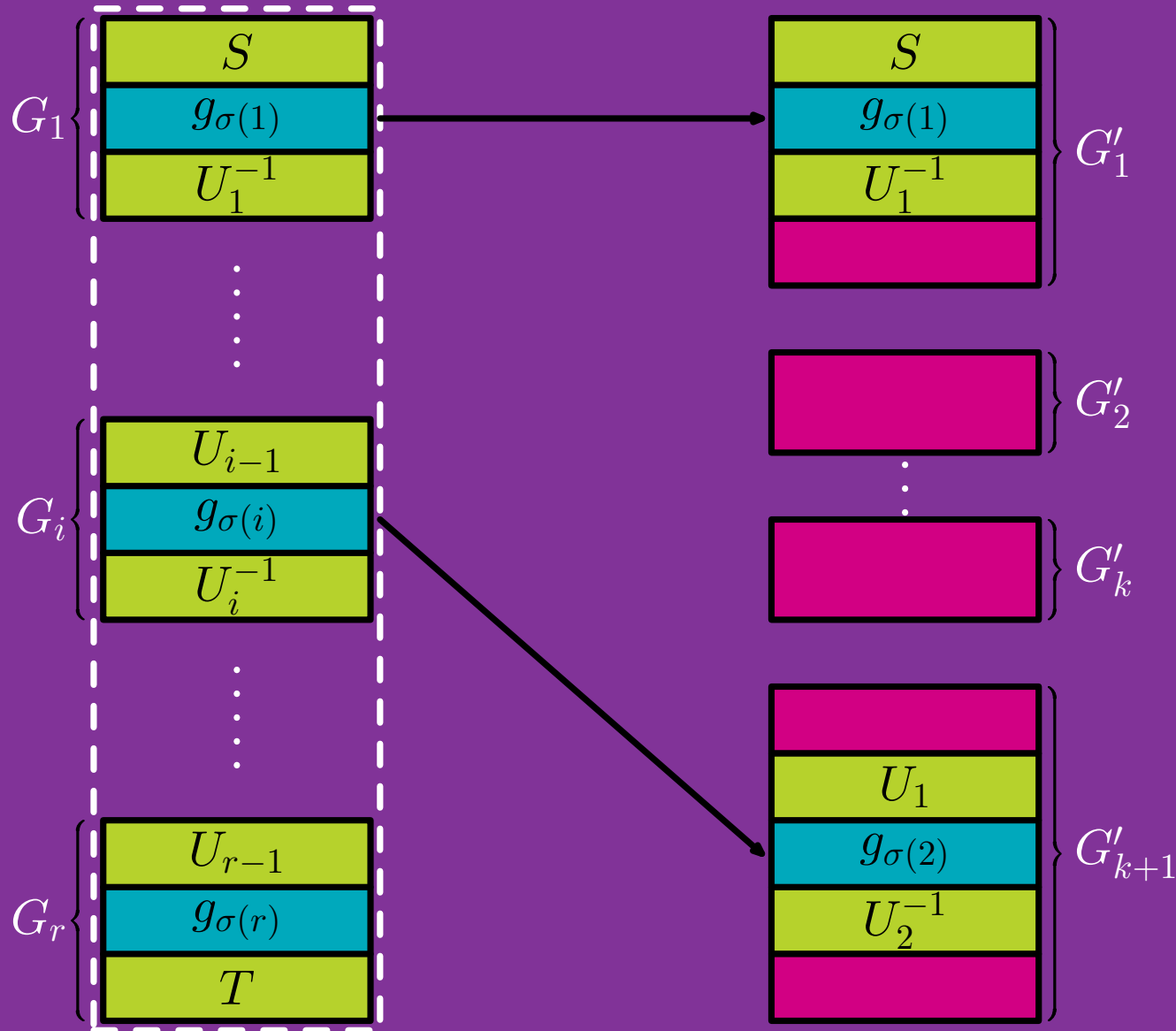
Comp. Prob.

Commuting

Parameters

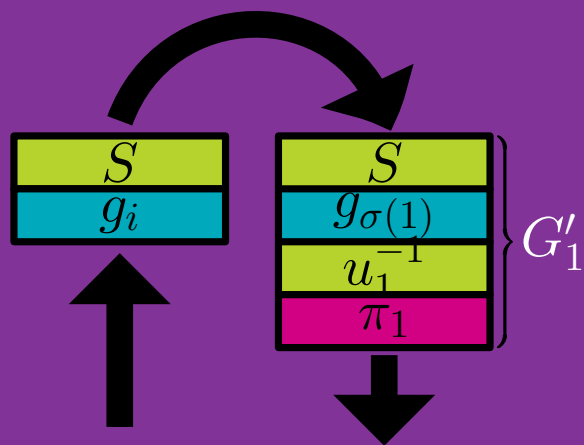
Security

Tracing One Traitor *Potential Strategy*



- Context
- Definitions
- Cipher
- Modes
- C^*
- Comp. Prob.
- Commuting
- Parameters
- Security
- Tracing**

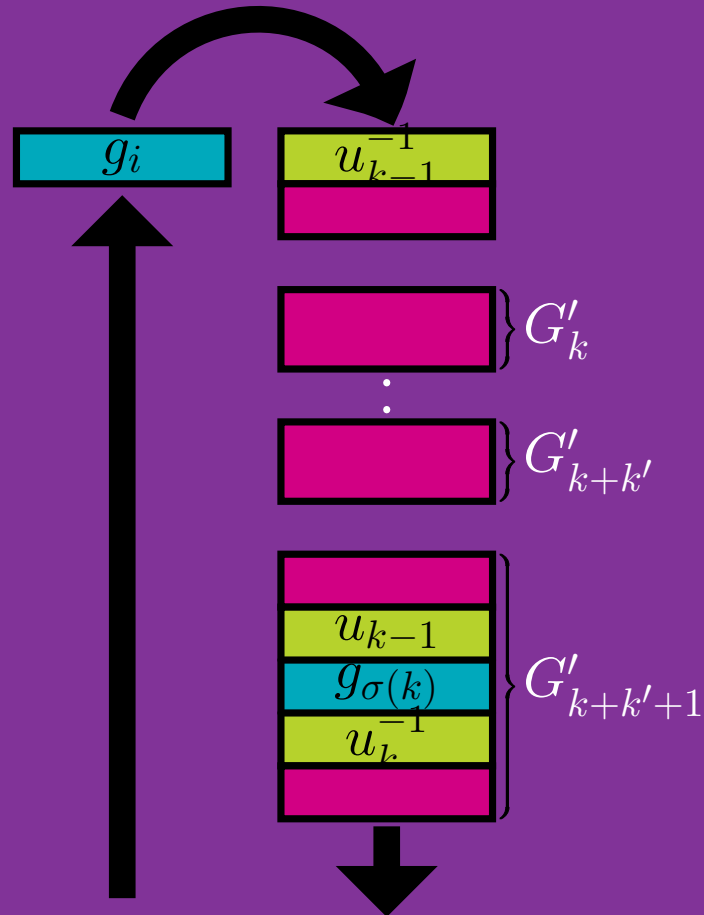
Tracing One Traitor



▶ step 1: guess $g_{\sigma(1)}$

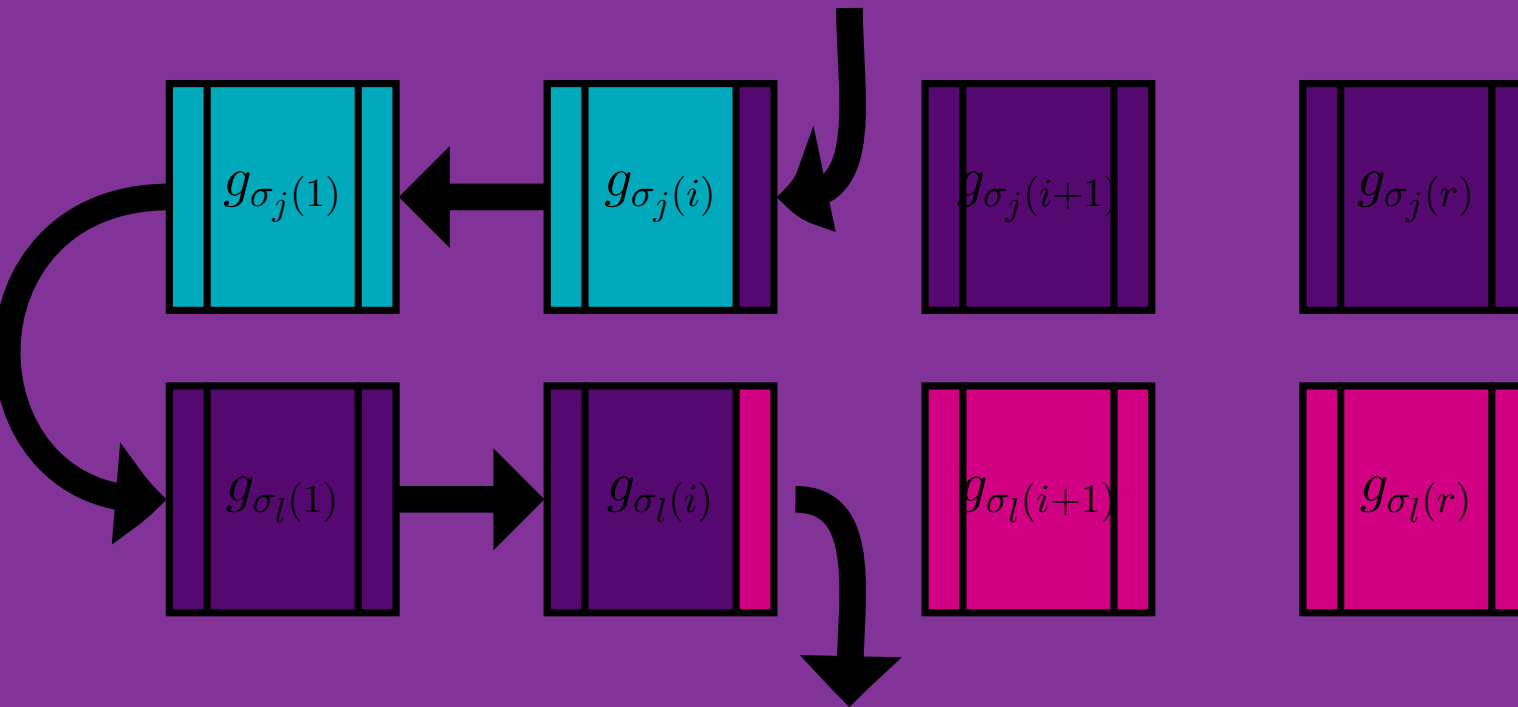
▶ step i : guess $g_{\sigma(i)}$

▶ σ is known



- Context
- Definitions
- Cipher
- Modes
- C^*
- Comp. Prob.
- Commuting
- Parameters
- Security
- Tracing**

Tracing *several* Traitors



▶ t -collision: $\{\sigma_j(i)\}_{i \in [1,t]} = \{\sigma_l(i)\}_{i \in [1,t]}$



▶ inner values reveal one identity

- Context
- Definitions
- Cipher
- Modes
- C^*
- Comp. Prob.
- Commuting
- Parameters
- Security
- Tracing**

Conclusion



▶ Properties

- » very low control word overhead: **save bandwidth**
- » good behavior with high number of traitors
- » good behavior with huge number of users: **scalable**
- » **speed** of symmetric block cipher
- » no black box yet

▶ Security

- ② IP for extended C^* with degree higher than 2

▶ Applications

- » White Box Cryptography
- » Other instantiations

Context

Definitions

Cipher

Modes

C^*

Comp. Prob.

Commuting

Parameters

Security

Tracing