Constrained Systems

Benoît Cogliati
Thales DIS France

Ashwin Jha
RUB

Jordan Naccache
uni.lu

Mridul Nandi
ISI Kolkata

Abishanka Saha
TU/e

ASK 2026
19 March, 2026

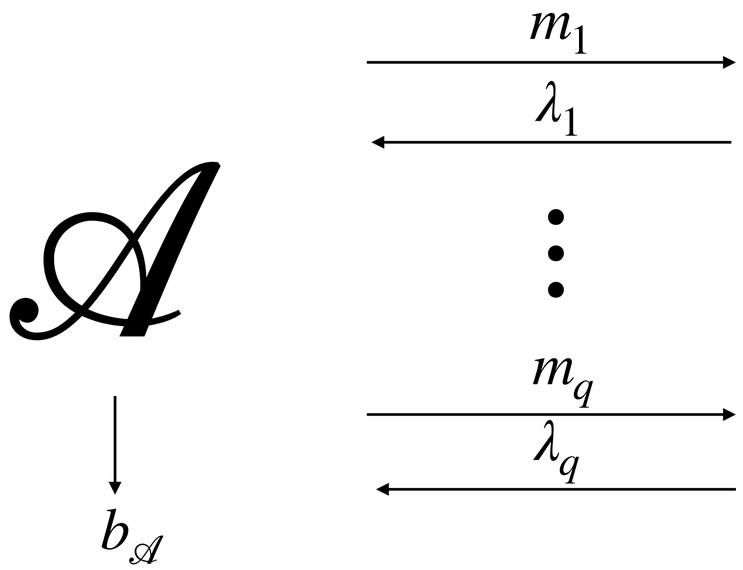
Pseudorandom Function

An *efficient* keyed function $f_K \colon \mathscr{D} \to \{0,1\}^n$ that *behaves* like a uniform random function.

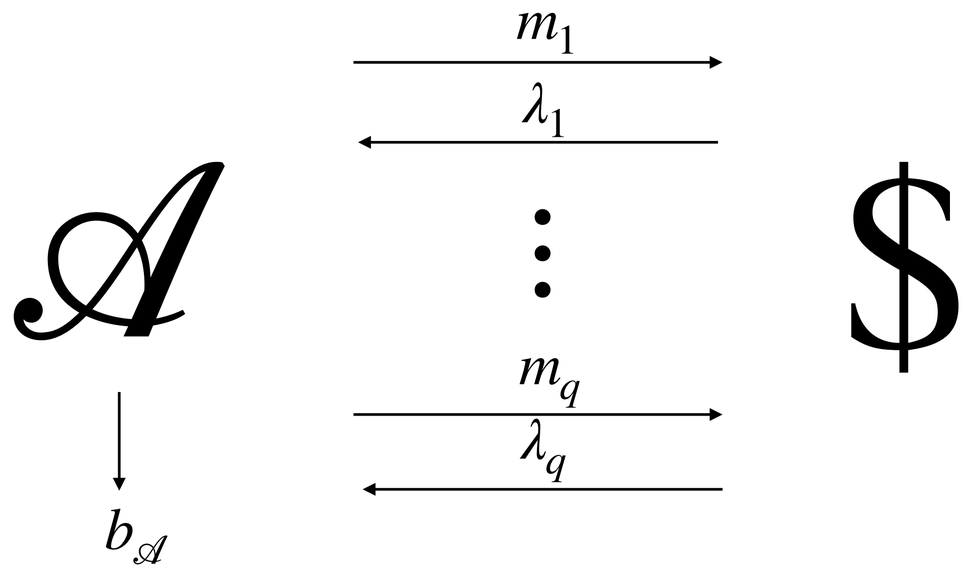
Pseudorandom Function

An *efficient* keyed function $f_K \colon \mathcal{D} \to \{0,1\}^n$ that *behaves* like a uniform random function.

Real world



Ideal world



$$\mathbf{Adv}^{\$}_{f}(q) := \max_{\mathcal{A}} \left| \Pr\left(b_{\mathcal{A}} = 1 \text{ in the real world}\right) - \Pr\left(b_{\mathcal{A}} = 1 \text{ in the ideal world}\right) \right|$$

Pseudorandom Function

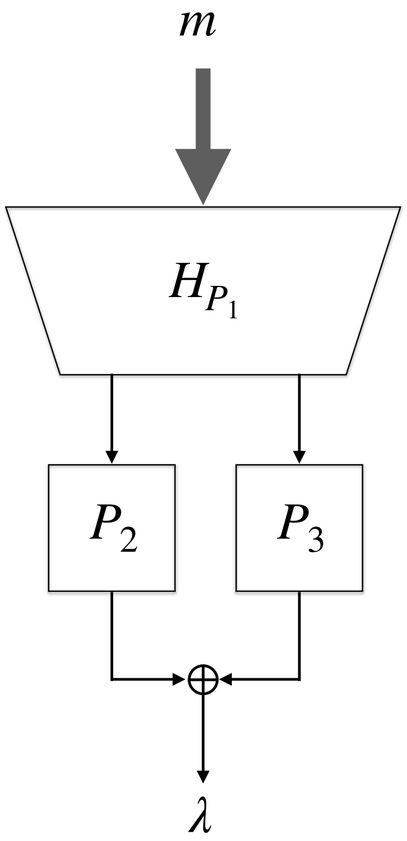
- Versatile building block:

  HMAC, CMAC, LightMAC, GCM, SIV, HKDF, CTR-DRBG

- Block ciphers are PRF up to $\approx \sqrt{2^n}$ queries.
- Growing demand for *beyond-the-birthday-bound* (BBB) PRFs.
- BBB PRFs require specialised modes/paradigms:
  - Block cipher-based: Sum of Permutations, Truncation, *Double block Hash then Sum*.
  - Permutation-based: *Sum of Even-Mansour*, pEDM, pPMAC_plus.

Double block Hash then Sum

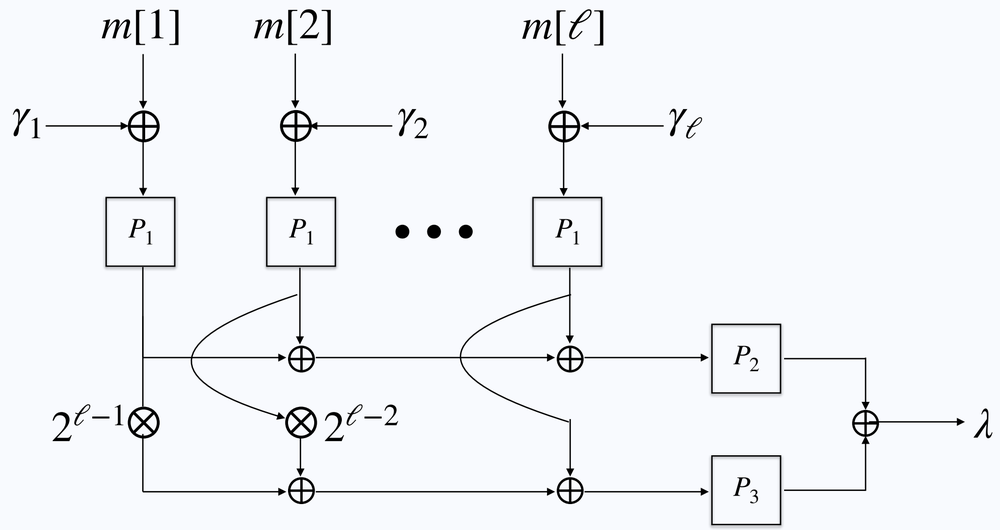
[DDNP 2018]



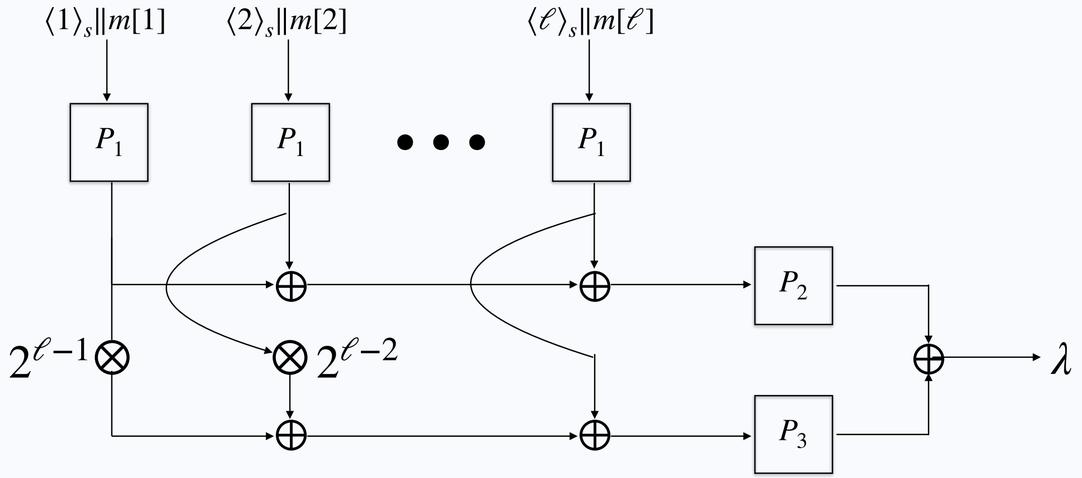
- Secret $P_1, P_2, P_3 \leftarrow_{\$} \mathsf{Perm}(n)$
- $H_{P_1} : \{0,1\}^* \rightarrow \{0,1\}^n \times \{0,1\}^n$

Double block Hash then Sum

Instantiations



PMAC+ [Yasuda 2011]

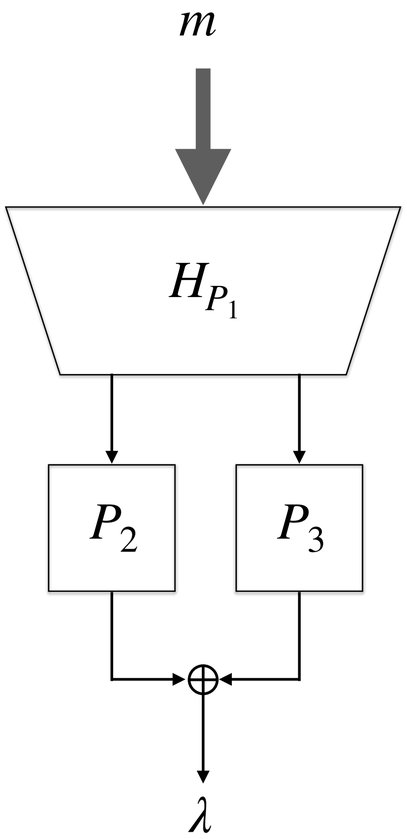


LightMAC+ [Naito 2017]

Other Examples: Sum-ECBC [Yasuda 2010], 3kf9 [ZWSW 2012].

Double block Hash then Sum

PRF Security

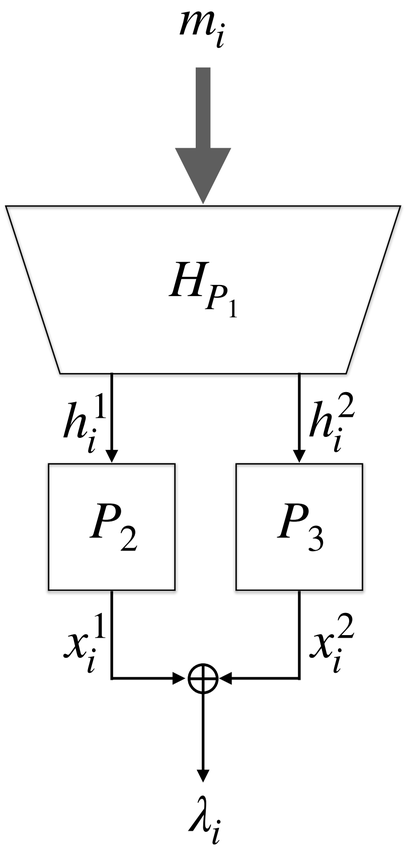


Theorem [LNS 2018, KLL 2020, JN 2020]

$$\mathbf{Adv}^{\$}_{\mathsf{DbHtS}}(q) = \Theta\left(\frac{q^4}{2^{3n}}\right)$$

Double block Hash then Sum

PRF Security Proof via Combinatorial Lower Bounds

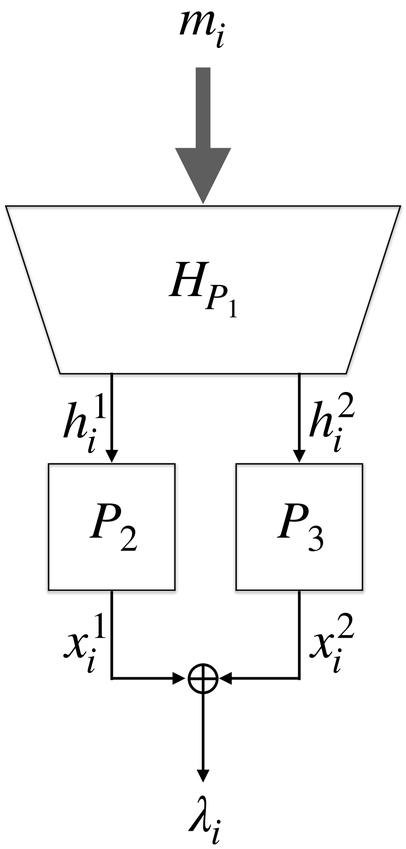


$$\Longrightarrow \quad \begin{aligned} x_1^1 \oplus x_1^2 &= \lambda_1 \\ x_2^1 \oplus x_2^2 &= \lambda_2 \\ &\vdots \\ x_q^1 \oplus x_q^2 &= \lambda_q \end{aligned}$$

Constraint: $x_i^b = x_j^b \iff h_i^b = h_j^b$

Double block Hash then Sum

PRF Security Proof via Combinatorial Lower Bounds



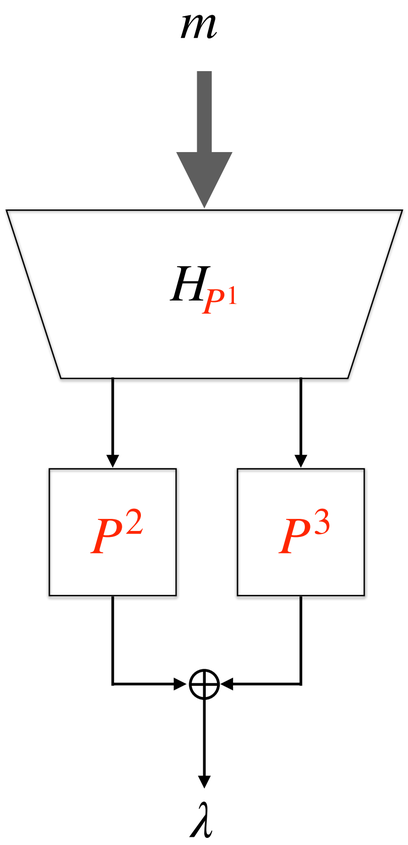
$$\Longrightarrow \quad \begin{aligned} x_1^1 \oplus x_1^2 &= \lambda_1 \\ x_2^1 \oplus x_2^2 &= \lambda_2 \\ &\vdots \\ x_q^1 \oplus x_q^2 &= \lambda_q \end{aligned}$$

Constraint: $x_i^b = x_j^b \iff h_i^b = h_j^b$

Goal: Upper bound $\mathbf{Adv}^{\$}_{\mathsf{DbHtS}}(q)$ $\Longrightarrow$ **Goal:** Lower bound the number of solutions to the system of equations under the given constraint.

(Mirror Theory)

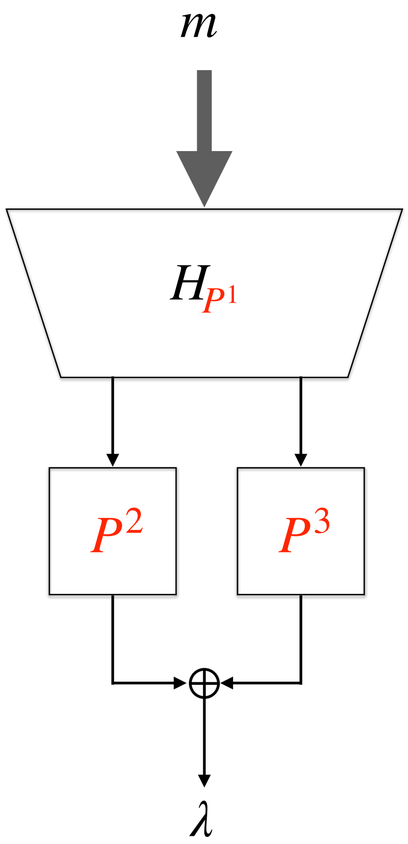
One-keyed DbHtS



- $P_i(x) := P(\langle i \rangle_2 \parallel x)$, where $P \leftarrow_{\$} \mathsf{Perm}(n)$
- $H_{P^1}\colon \{0,1\}^* \to \{0,1\}^{n-2} \times \{0,1\}^{n-2}$

One-keyed DbHtS

PRF Security: Current Status



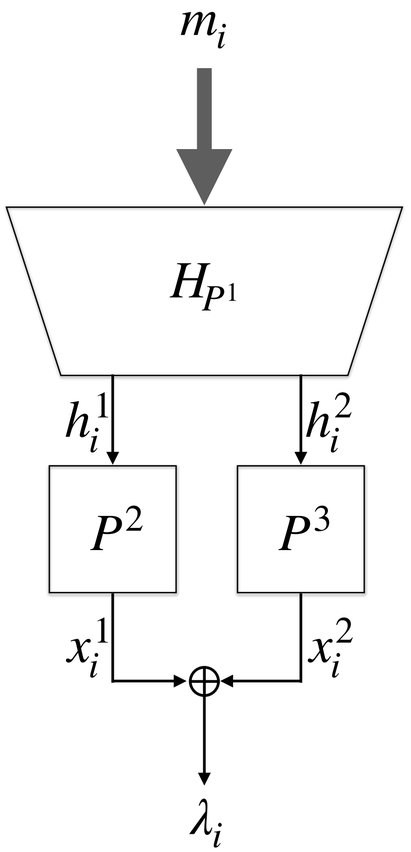
- $P_i(x) := P(\langle i \rangle_2 \,\|\, x)$, where $P \leftarrow_{\$} \mathrm{Perm}(n)$
- $H_{P^1}\colon \{0,1\}^* \to \{0,1\}^{n-2} \times \{0,1\}^{n-2}$

A clear gap in generic security analysis:

- Best attack requires $O(2^{3n/4})$ queries. [LNS 2018]
- Current lower bound is $\Omega(2^{2n/3})$. [DDNPZ 2017, SS 2022]

One-keyed DbHtS

PRF Security: Proof Bottleneck



$\Longrightarrow$

$$x_1^1 \oplus x_1^2 = \lambda_1$$
$$x_2^1 \oplus x_2^2 = \lambda_2$$
$$\vdots$$
$$x_q^1 \oplus x_q^2 = \lambda_q$$

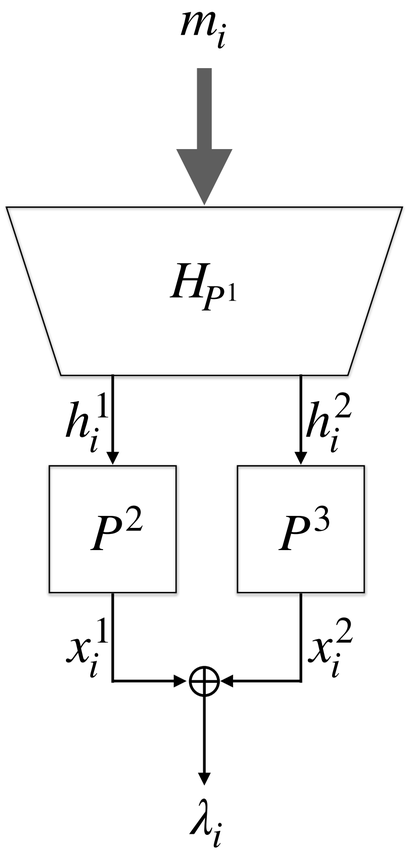
Constraint:

1. $x_i^b = x_j^b \iff h_i^b = h_j^b$

2. $x_i^1, x_i^2 \notin \mathrm{range}(P^1)$

One-keyed DbHtS

PRF Security: Proof Bottleneck



$\Longrightarrow$

$$x_1^1 \oplus x_1^2 = \lambda_1$$
$$x_2^1 \oplus x_2^2 = \lambda_2$$
$$\vdots$$
$$x_q^1 \oplus x_q^2 = \lambda_q$$

Constraint:

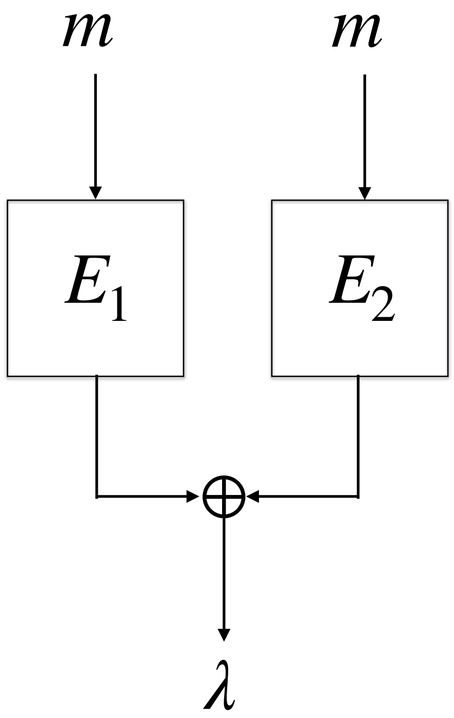
1. $x_i^b = x_j^b \iff h_i^b = h_j^b$

2. $x_i^1, x_i^2 \notin \text{range}(P^1)$

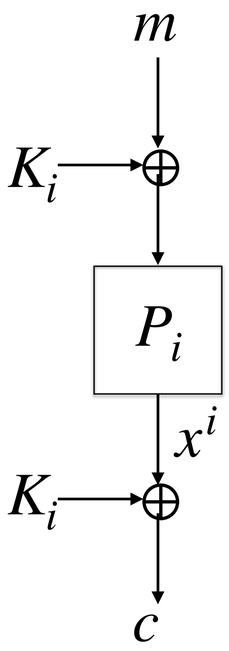
Mirror theory cannot handle “forbidden set” of values!

Sum of Even-Mansour

[CLM 2019, ST 2023]



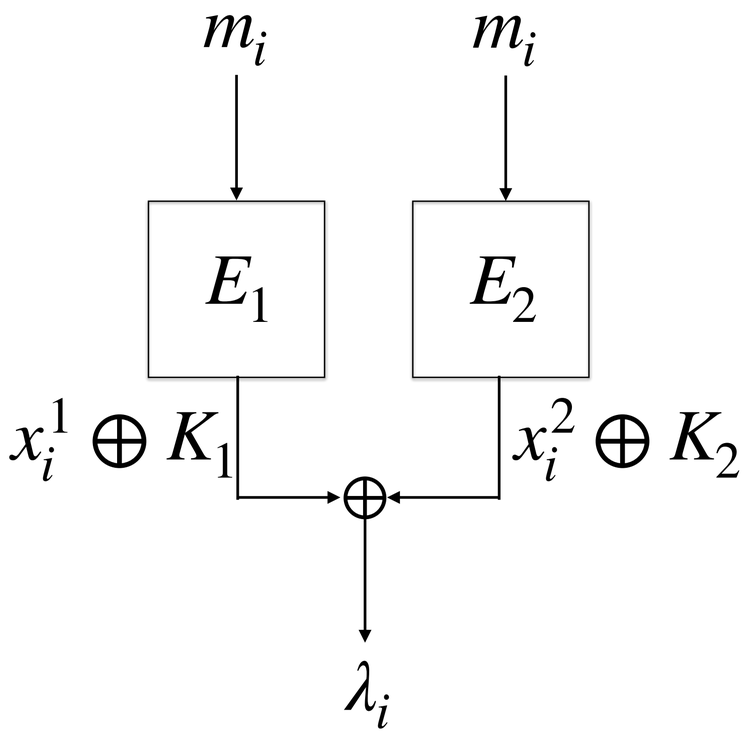
$$E_i(m) := K_i \oplus P_i(K_i \oplus m)$$



- P_i is public random permutation of $\{0,1\}^n$
- K_i is n-bit key

Sum of Even-Mansour

PRF Security: Proof Bottleneck



$$\Longrightarrow \quad \begin{aligned} x_1^1 \oplus x_1^2 &= \lambda_1 \oplus K_1 \oplus K_2 \\ x_2^1 \oplus x_2^2 &= \lambda_2 \oplus K_1 \oplus K_2 \\ &\vdots \\ x_q^1 \oplus x_q^2 &= \lambda_q \oplus K_1 \oplus K_2 \end{aligned}$$

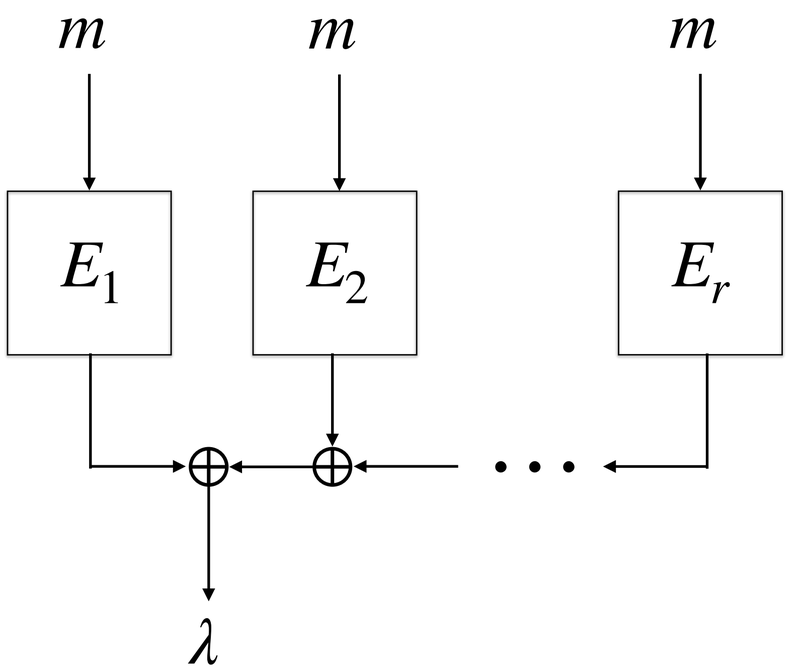
Constraint:

1. $x_i^b \neq x_j^b$

2. $x_i^b \notin \mathscr{P}_b$

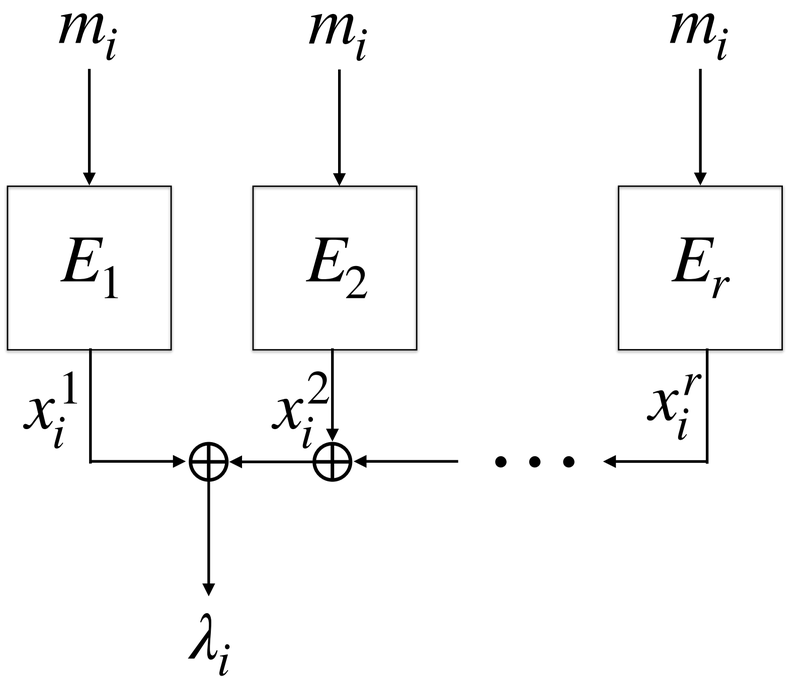
$\mathscr{P}_b$ denotes the set of permutation outputs corresponding to $\mathscr{A}$'s direct query to P_b.

Generalised SoEM (SoEM^r)



Generalised SoEM (SoEM^r)

PRF Security: Proof Bottleneck



$$\Longrightarrow$$

$$x_1^1 \oplus \cdots \oplus x_1^r = \lambda_1 \oplus c_K$$
$$x_2^1 \oplus \cdots \oplus x_2^r = \lambda_2 \oplus c_K$$
$$\vdots$$
$$x_q^1 \oplus \cdots \oplus x_q^r = \lambda_q \oplus c_K$$

Constraint:

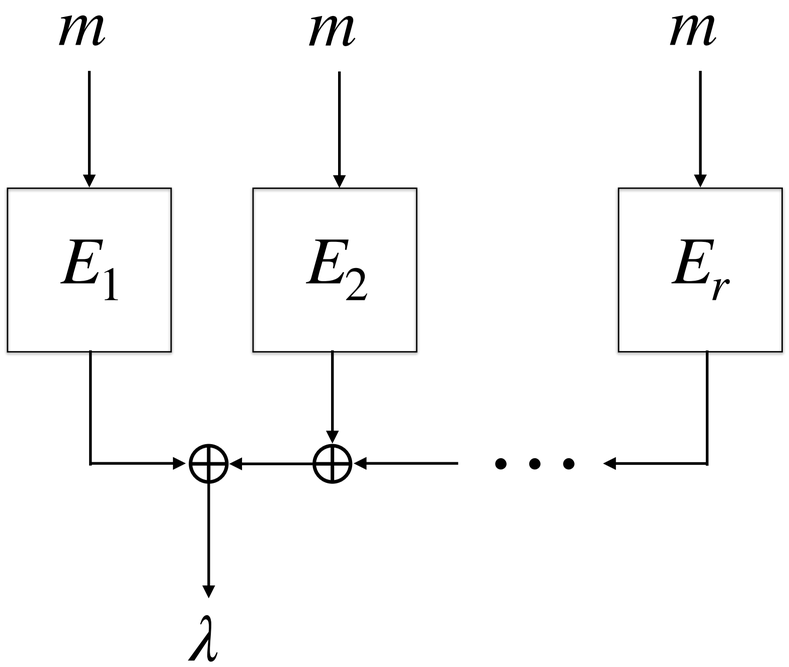
1. $x_i^b \neq x_j^b$

2. $x_i^b \notin \mathscr{P}_b$

Classical mirror theory results do not handle such constraints.

Generalised SoEM (SoEM^r)

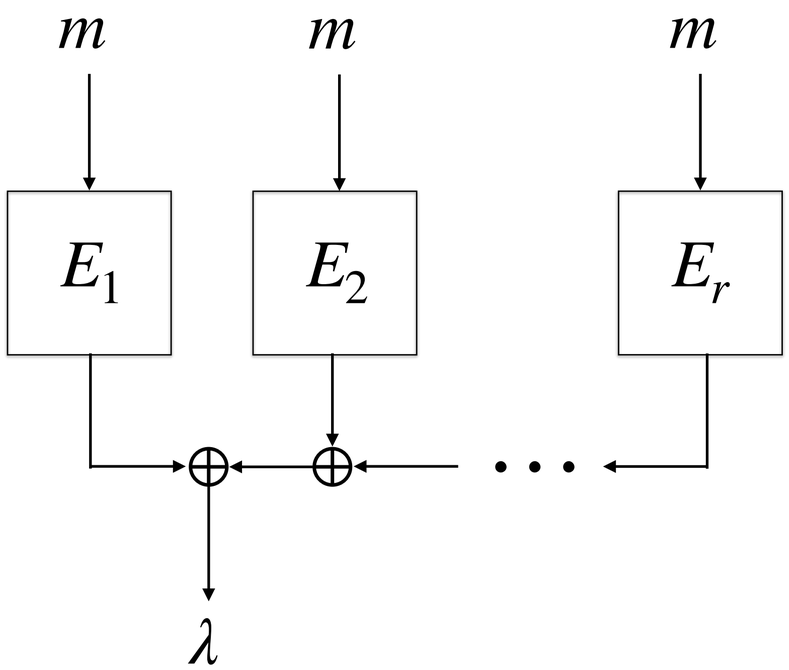
PRF Security: Current Status



- Best attack requires $O(2^{\frac{r}{r+1}n})$ queries.
- Trivial lower bound is $\Omega(2^{2n/3})$ queries.
  [CLM 2019, ST 2023]

Generalised SoEM (SoEM^r)

PRF Security: Current Status



- Best attack requires $O(2^{\frac{r}{r+1}n})$ queries
- Trivial lower bound is $\Omega(2^{2n/3})$ queries
  [CLM 2019, ST 2023]

A combinatorial result catering to these use cases is *missing*.

Our Contributions

- A formulation of **Constrained Systems** over arbitrary finite fields.
- Lower bounds on the number of **restricted solutions.**
  (handles “forbidden sets”)
- Two applications:
  - Tight security of 1k-DbHtS (1k-PMAC+ and 1k-LightMAC+).
  - Tight security of SoEM^r.

Constrained Systems

(q, r, t)-constrained system

A (q, r, t)-constrained system $\mathbb{S} = (A, \lambda, \mathsf{P})$ consists of:

- a system $A\mathbf{x} = \lambda$ of q equations in r variables over $\mathbb{F}_N$, and
- a partition $\mathsf{P} = \mathsf{P}_1 \sqcup \ldots \sqcup \mathsf{P}_t$ of $\mathsf{col}(A)$.

Constrained Systems

(q, r, t)-constrained system

A (q, r, t)-constrained system $\mathbb{S} = (A, \lambda, \mathsf{P})$ consists of:

- a system $A\mathbf{x} = \lambda$ of q equations in r variables over $\mathbb{F}_N$, and
- a partition $\mathsf{P} = \mathsf{P}_1 \sqcup \ldots \sqcup \mathsf{P}_t$ of $\mathsf{col}(A)$.

Two special types of constrained systems are quite frequent:

- Clique: P is the trivial partition (e.g. 1k-DbHtS).
- Partite: P partitions each $\mathsf{supp}(A_{i,\bullet})$ discretely (e.g. SoEM^r).

k-CAR Constrained Systems

- $\mathbb{S}$ is column-uniform if $A_{i,j} = A_{i',j'}$ whenever $A_{i,j}, A_{i',j'} \neq 0$ and $j, j' \in \mathsf{P}_k$.
- $\mathbb{S}$ is acyclic if:
  - $|\mathsf{supp}(A_{i\bullet}) \cap \mathsf{supp}(A_{i'\bullet})| \leq 1$, and
  - *intersection graph* of the set system $\{\mathsf{supp}(A_{1\bullet}), \ldots, \mathsf{supp}(A_{q\bullet})\}$ is *acyclic*.
- $\mathbb{S}$ is k-regular if $|\mathsf{supp}(A_{i\bullet})| = k$.

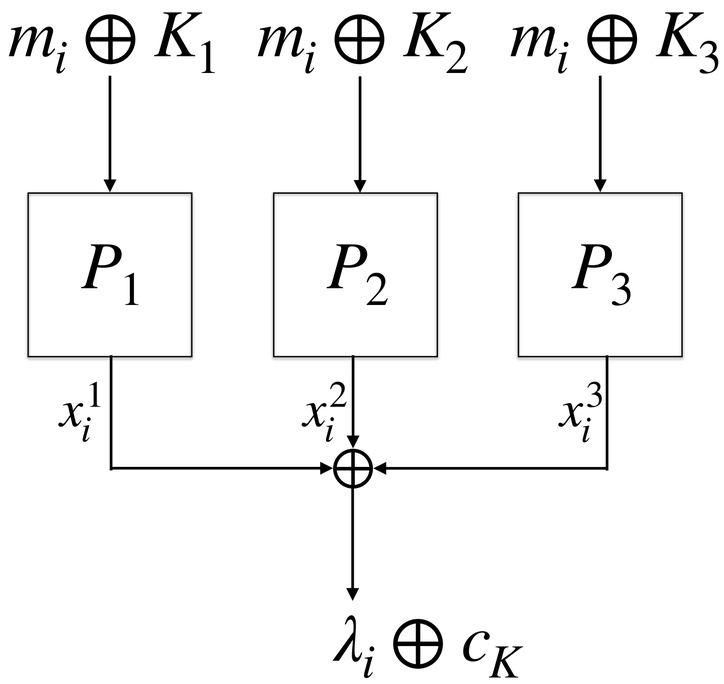
k-CAR Constrained Systems

- $\mathbb{S}$ is column-uniform if $A_{i,j} = A_{i',j'}$ whenever $A_{i,j}, A_{i',j'} \neq 0$ and $j, j' \in \mathsf{P}_k$.
- $\mathbb{S}$ is acyclic if:
  - $|\mathsf{supp}(A_{i\bullet}) \cap \mathsf{supp}(A_{i'\bullet})| \leq 1$, and
  - *intersection graph* of the set system $\{\mathsf{supp}(A_{1\bullet}), \ldots, \mathsf{supp}(A_{q\bullet})\}$ is *acyclic*.
- $\mathbb{S}$ is k-regular if $|\mathsf{supp}(A_{i\bullet})| = k$.

Most cryptographic applications satisfy Column-uniform, Acyclic, and k-Regular properties.

k-CAR Constrained Systems

The case of SoEM^3



k-CAR Constrained Systems

The case of SoEM^3

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$\mathsf{P} = \{\{1,4,7,10,13\}, \{2,5,8,11,14\}, \{3,6,9,12,15\}\}$

- Assume $q = 5$ and no *construction-primitive* collisions.
- Resulting $(5,15,3)$-constrained system $\mathbb{S}$ is:
  - partite (x_i^b belongs to block P_b).
  - column-uniform (each non-zero entry is 1).
  - acyclic (each column has a single non-zero entry).
  - 3-regular (each equation has exactly 3 variables).

Restricted Solutions of a Constrained Systems

$\overline{\mathscr{R}}$-restricted solutions

A solution y of $\mathbb{S}$ with respect to forbidden sets $\mathscr{R} = (\mathscr{R}_1, \ldots, \mathscr{R}_t)$ satisfies:

- $Ay = \lambda$, (satisfies the system)
- $j \neq j' \in \mathsf{P}_i \implies y_j \neq y_{j'}$, (avoids intra-block collisions)
- $y_j \notin \mathscr{R}_i$ for all $j \in \mathsf{P}_i$. (avoids forbidden values)

Expected number of solutions (random λ):

$$\mathbb{E}(\mathbb{S} \mid \mathscr{R}) = \frac{\prod_{i=1}^{t} (N - s_i)_{r_i}}{N^q}, \text{ where } r_i = |\mathsf{P}_i|, s_i = |\mathscr{R}_i|.$$

Goal: Show that the number of solutions, $(\mathbb{S} \mid \mathscr{R})$, is close to $\mathbb{E}(\mathbb{S} \mid \mathscr{R})$.

Restricted Solutions of a Constrained Systems

$\overline{\mathscr{R}}$-restricted solutions

A solution y of $\mathbb{S}$ with respect to forbidden sets $\mathscr{R} = (\mathscr{R}_1, \ldots, \mathscr{R}_t)$ satisfies:

- $Ay = \lambda$, (satisfies the system)
- $j \neq j' \in \mathsf{P}_i \implies y_j \neq y_{j'}$, (avoids intra-block collisions)
- $y_j \notin \mathscr{R}_i$ for all $j \in \mathsf{P}_i$. (avoids forbidden values)

Expected number of solutions (random λ):

$$\mathbb{E}(\mathbb{S} \mid \mathscr{R}) = \frac{\prod_{i=1}^{t} (N - s_i)_{r_i}}{N^q}, \text{ where } r_i = |\mathsf{P}_i|, s_i = |\mathscr{R}_i|.$$

Goal: Show that the number of solutions, $(\mathbb{S} \mid \mathscr{R})$, is close to $\mathbb{E}(\mathbb{S} \mid \mathscr{R})$.

Mirror theory bounds deal with the special case of $\mathscr{R}_i = \emptyset$.

Main Results for k-CAR Systems

Partite Case:

$$\frac{(\mathbb{S} \mid \mathscr{R})}{\mathbb{E}(\mathbb{S} \mid \mathscr{R})} \geq \left(1 - \frac{\mu(\lambda, \mathscr{R})}{N^{k-1}} - \frac{q^{k+1}}{N^k}\right)$$

Clique Case:

$$\frac{(\mathbb{S} \mid \mathscr{R})}{\mathbb{E}(\mathbb{S} \mid \mathscr{R})} \geq \left(1 - \frac{\mu(\lambda, \mathscr{R})}{N^{k-1}} - \frac{q^{k+1}}{N^k} - \sum_{i \in \mathsf{NI}(\mathbb{S})} \frac{r_i^2}{N}\right)$$

$\mu(\lambda, \mathscr{R}) := |\{(a_1, \ldots, a_t) \in \mathscr{R}_1 \times \ldots \times \mathscr{R}_t : \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_t a_t \in \lambda\}|$ where α_i is the matrix element associated with P_i.

Main Results for k-CAR Systems

Partite Case (random λ):*

$$\frac{(\mathbb{S} \mid \mathscr{R})}{\mathbb{E}(\mathbb{S} \mid \mathscr{R})} \geq \left(1 - \frac{q^{k+1}}{N^k}\right)$$

Clique Case (random λ):*

$$\frac{(\mathbb{S} \mid \mathscr{R})}{\mathbb{E}(\mathbb{S} \mid \mathscr{R})} \geq \left(1 - \frac{q^{k+1}}{N^k} - \sum_{i \in \mathsf{NI}(\mathbb{S})} \frac{r_i^2}{N}\right)$$

* Using smoothness of non-trivial Fourier coefficients of random sets.

Applications

- PRF security of SoEM^r:

$$\mathbf{Adv}^{\$}_{\mathsf{SoEM}^r}(q,p) = O\left(\frac{q\,(p+q)^r}{N^r}\right).$$

- PRF security of 1k-DbHtS:

$$\mathbf{Adv}^{\$}_{\text{1k-DbHtS}}(q) = O\left(\frac{q^2}{N^{1.5}}\right).$$

(dedicated analysis of the 2-regular systems over $\mathbb{F}_{2^n}$ and a second moment trick)

- Dedicated hash analysis for 1k-PMAC+ and 1k-LightMAC+.

Open Problems

- PRF security of other single-keyed DbHtS instances.
- Avoiding domain-separation in 1k-PMAC+ and 1k-LightMAC+.
- Do the bounds hold unconditionally? (cf. randomness of λ)
- Tightness of bounds for moderate to large forbidden sets.

Open Problems

- PRF security of other single-keyed DbHtS instances.
- Avoiding domain-separation in 1k-PMAC+ and 1k-LightMAC+.
- Do the bounds hold unconditionally? (cf. randomness of λ)
- Tightness of bounds for moderate to large forbidden sets.

Thank you