Single Key Variant of PMAC_Plus

Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, Liting Zhang

Fast Software Encryption, 2018, Bruges

7th March, 2018

Contribution of the Paper

1k-PMAC_Plus: Single Key Variant of PMAC_Plus

- First Single Key Beyond Birthday Bound (BBB) Secure Rate-1 Block-cipher based PRF.
- Achieves Better Security Bound than Existing Bound for PMAC_Plus

Message Authentication Protocol

- Alice and Bob shares a secret key K.
- Alice generates tag $T = F_K(M)$ and send (M, T) pair to Bob.
- Bob verifies whether tag is valid or not.

Message Authentication Protocol

- Alice and Bob shares a secret key K.
- Alice generates tag $T = F_K(M)$ and send (M, T) pair to Bob.
- Bob verifies whether tag is valid or not.

Security

It is hard for Eve to generate T' for a message M'.

Security Definitions

MAC Security

- Adversary can not generate fresh valid (message,tag) pairs.
- $\mathbf{Adv}_{\mathsf{F}}^{\mathrm{mac}}(A) := Pr_K[A^{F_K} \text{ forges }] \leq \epsilon$

Security Definitions

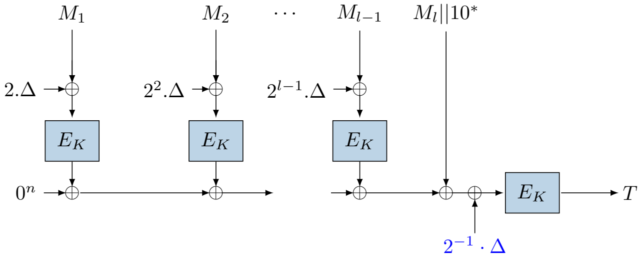
MAC Security

- Adversary can not generate fresh valid (message,tag) pairs.
- $\mathbf{Adv}_{\mathsf{F}}^{\mathrm{mac}}(A) := Pr_K[A^{F_K} \text{ forges }] \leq \epsilon$

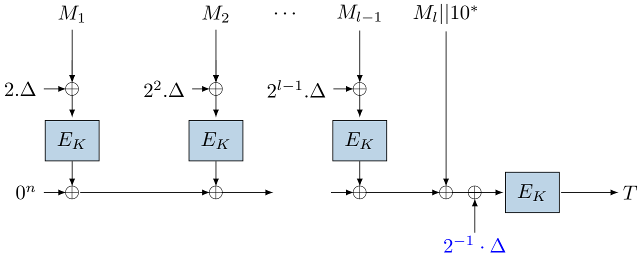
PRF Security

- Adversary can not distinguish from a function chosen uniformly at random.
- $\mathbf{Adv}_{\mathsf{F}}^{\mathrm{prf}}(A) := |Pr_K[A^{F_K} = 1] - Pr_{\$}[A^{\$} = 1]| \leq \epsilon$

Parallelizable MAC (PMAC) By Black and Rogaway

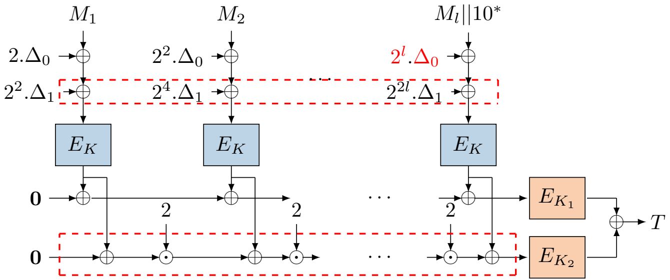


Parallelizable MAC (PMAC) By Black and Rogaway



Security of PMAC: $5\sigma q/2^n$ by Nandi et al. (JMC, 2008),
Tightness: Gaži et al. (IACR Trans. 2016)

PMAC_Plus by Yasuda, CRYPTO 2011



Beyond Birthday Bound secure block cipher based PRF.

Features of PMAC_Plus

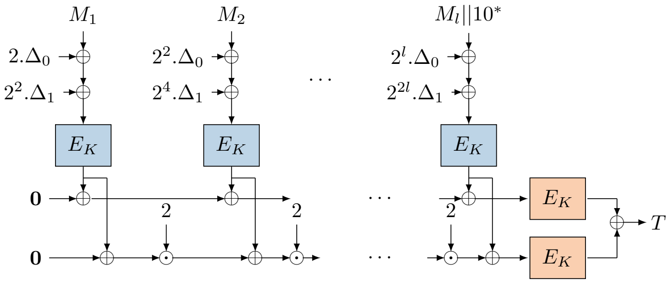
- Parallel rate 1 Construction.
- Two layers of input masking
- Two layers of linear output mixing and hence the internal state size becomes doubled.
- Three independent block cipher keys
- Offers $O(\frac{q^3\ell^3}{2^{2n}})$ PRF security bound.

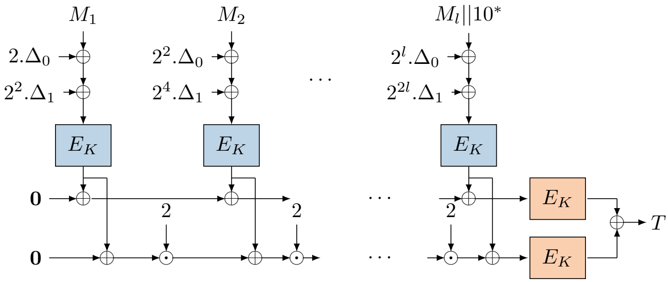
Features of PMAC_Plus

- Parallel rate 1 Construction.
- Two layers of input masking
- Two layers of linear output mixing and hence the internal state size becomes doubled.
- Three independent block cipher keys
- Offers $O(\frac{q^3\ell^3}{2^{2n}})$ PRF security bound.

[Yasuda, CRYPTO 2011]: "This raises a challenge to come up with a 1-key rate-1 MAC construction which is secure beyond the birthday bound"

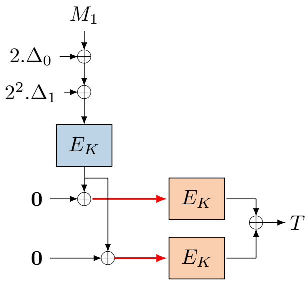
Designing towards 1k-PMAC_Plus: Step I





Same Construction, Single Key: Is it secure?

Designing towards 1k-PMAC_Plus: Step I

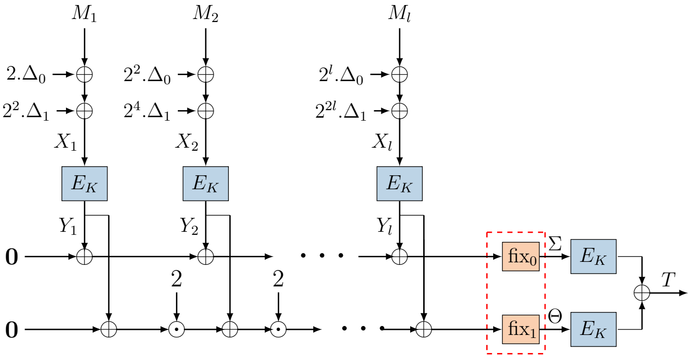


Distinguishing Attack with One Query:

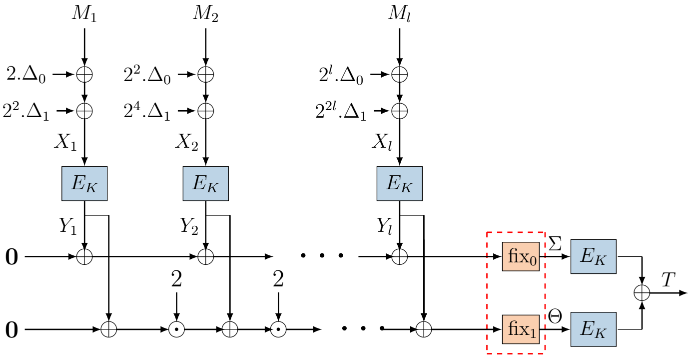
Single block query $\Longrightarrow$ $(T = 0)$

Designing towards 1k-PMAC_Plus: Step II

Domain Separation for the two lanes:

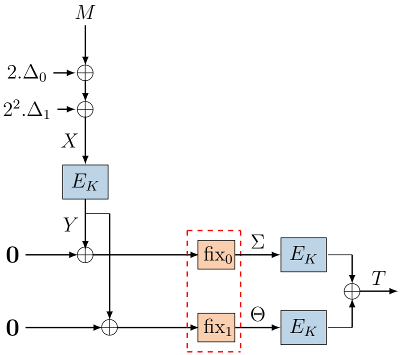


Domain Separation for the two lanes:



Is this secure beyond the birthday bound?

Designing towards 1k-PMAC_Plus: Step II

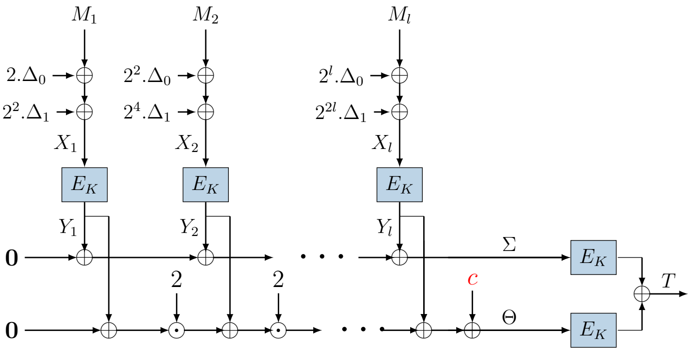


Birthday Bound Distinguishing Attack:

- Make single block queries until a collision occurs.
- Append a block and distinguish.

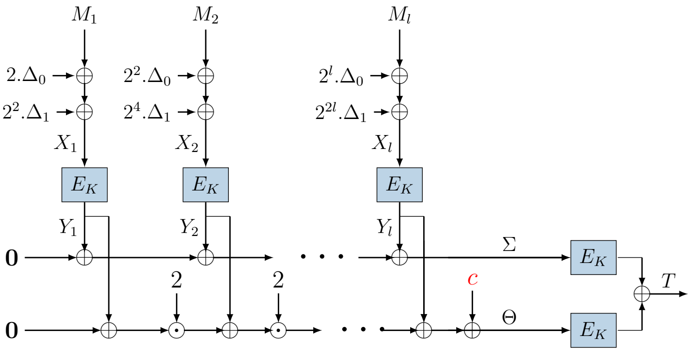
Designing towards 1k-PMAC_Plus: Step III

Xor a non-zero constant in second lane:



Is this construction secure beyond the birthday bound ?

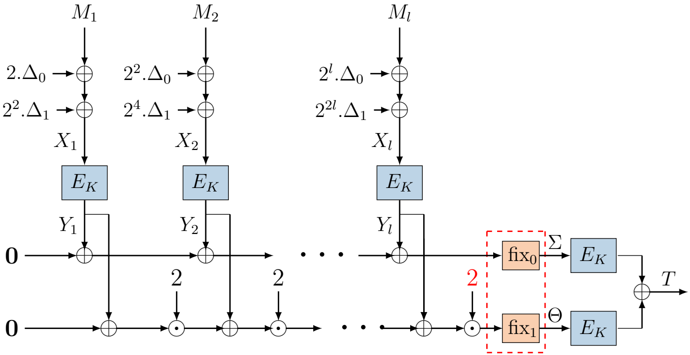
Designing towards 1k-PMAC_Plus: Step III



Birthday Bound Distinguishing Attack:

- Make $O(2^{n/2})$ many queries.
- Collision Probability in real world is substantially higher.

Multiply a non-zero constant in second lane:



1k-PMAC_Plus: first single-keyed B/C based BBB secure PRF.

Features of 1k-PMAC_Plus

1k-PMAC_Plus is structurally similar to PMAC_Plus with following minor differences:

- Second output layer is multiplied by 2.
- Requires Single block cipher key.
- Uses bit chopping function $\mathrm{fix}_0, \mathrm{fix}_1$ (Not necessary).
- Offers $O(\frac{q^3\ell^2}{2^{2n}})$ PRF security bound.

Security Result of 1k-PMAC_Plus

Theorem (Security Result)

1k-PMAC_Plus *is secure upto* $O(\sigma/2^n) + O(q\sigma^2/2^{2n})$, *where* σ *is the total number of message blocks being queried.*

Security Result of 1k-PMAC_Plus

Theorem (Security Result)

1k-PMAC_Plus *is secure upto* $O(\sigma/2^n) + O(q\sigma^2/2^{2n})$, *where* σ *is the total number of message blocks being queried.*

Proof Idea

- We prove using Coefficients-H technique:
  - Identify and bound the probability of bad transcripts (or bad events)
  - Realizing a good transcript is as likely as in the real and ideal world.

Revisiting Coefficients H Technique

Transcript

List of all queries, responses along with internal variables. We denote it as τ.

Attainable Transcript

τ is attainable if the probability of realizing that transcript in ideal world is non zero.

$\mathcal{V} := \underbrace{\mathcal{V}_g}_{\text{set of good transcripts}} \sqcup \underbrace{\mathcal{V}_b}_{\text{set of bad transcripts}}$ is the set of all attainable transcripts.

Revisiting Coefficients H Technique: Theorem

- Suppose, $\exists \epsilon_{\text{bad}} \geq 0$ s.t $\Pr[X_{\text{id}} \in \mathcal{V}_{\text{b}}] \leq \epsilon_{\text{bad}}$
- Suppose, $\exists \epsilon_{\text{ratio}} \geq 0$ s.t $\tau \in \mathcal{V}_{\text{g}}$, $\frac{p_{\text{re}}}{p_{\text{id}}} := \frac{\Pr[X_{\text{re}}=\tau]}{\Pr[X_{\text{id}}=\tau]} \geq 1 - \epsilon_{\text{ratio}}$

Then

$$\mathbf{Adv}^{\text{Ideal}}_{\text{Real}}(\mathcal{A}) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}.$$

Revisiting Coefficients H Technique: Theorem

- Suppose, $\exists \epsilon_{\text{bad}} \geq 0$ s.t $\Pr[X_{\text{id}} \in \mathcal{V}_{\text{b}}] \leq \epsilon_{\text{bad}}$
- Suppose, $\exists \epsilon_{\text{ratio}} \geq 0$ s.t $\tau \in \mathcal{V}_{\text{g}}$, $\frac{p_{\text{re}}}{p_{\text{id}}} := \frac{\Pr[X_{\text{re}}=\tau]}{\Pr[X_{\text{id}}=\tau]} \geq 1 - \epsilon_{\text{ratio}}$

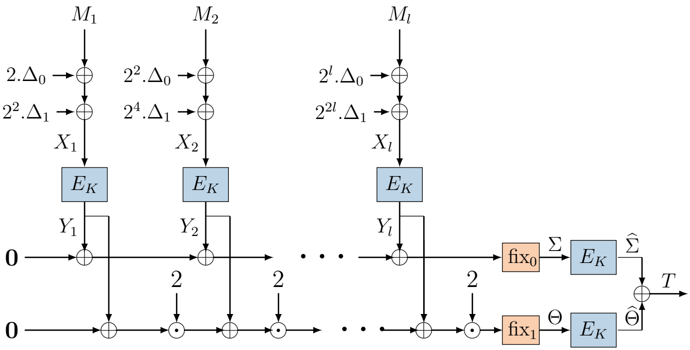
Then

$$\mathbf{Adv}_{\text{Real}}^{\text{Ideal}}(\mathcal{A}) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}.$$

Bounding PRF Advantage of 1k-PMAC_Plus

If $\text{Ideal} = \text{RF}$ and $\text{Real} = \text{1k} - \text{PMAC\_Plus}$, some keyed construction over the same domain, then

$$\mathbf{Adv}_{\text{1k}-\text{PMAC\_Plus}}^{\text{prf}}(\mathcal{A}) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}.$$



Transcripts for 1k-PMAC_Plus

$(M^i_j, X^i_j, Y^i_j, \Sigma_i, \Theta_i, \widehat{\Sigma}_i, \widehat{\Theta}_i, T_i)_i$

Bad Transcripts for 1k-PMAC_Plus

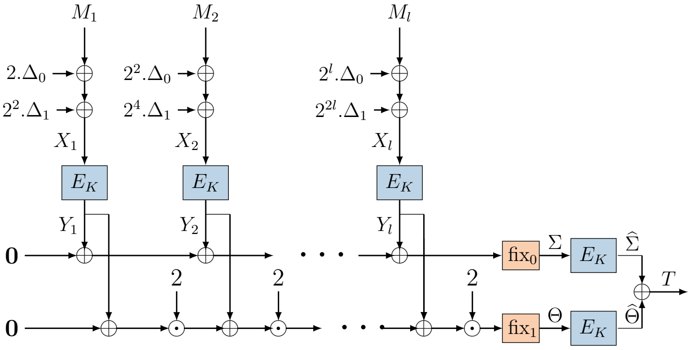
- $\exists i : \ T_i = 0.$
- $\exists i$: Both Σ_i and Θ_i is non-fresh
- Additional Bad Events due to Permutation Compatibility:
  - $\exists i$: Both Σ_i non-fresh, Θ_i is fresh, $\widehat{\Theta_i}$ is non-fresh.
  - $\exists i$: Both Θ_i non-fresh, Σ_i is fresh, $\widehat{\Sigma_i}$ is non-fresh.

Implication for Good Transcripts for 1k-PMAC_Plus

$\forall i,\ \Sigma_i$ or Θ_i is fresh and $(\Sigma_i, \Theta_i, \widehat{\Sigma}_i, \widehat{\Theta}_i)$ is permutation compatible:

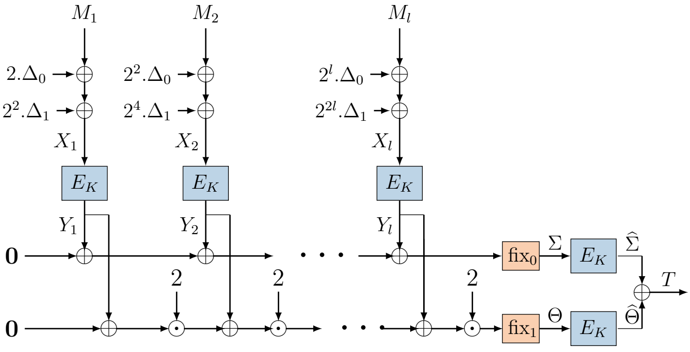
- We can use Sum of Permutation Result

Proof Idea of 1k-PMAC_Plus: Bad Events

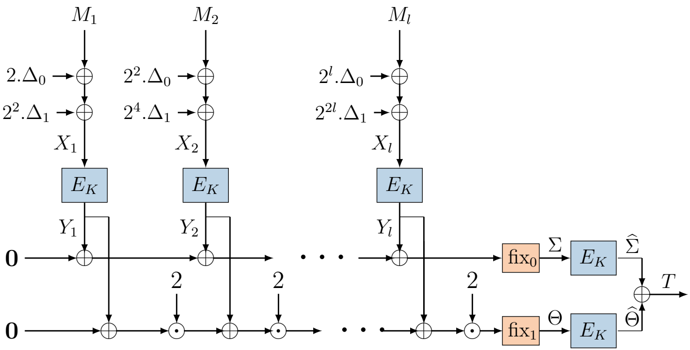


ECF : $\Sigma_i \in \{\Sigma_j, X_\alpha^j\}, \Theta_i \in \{\Theta_k, X_\alpha^k\}$

Proof Idea of 1k-PMAC_Plus: Bad Events

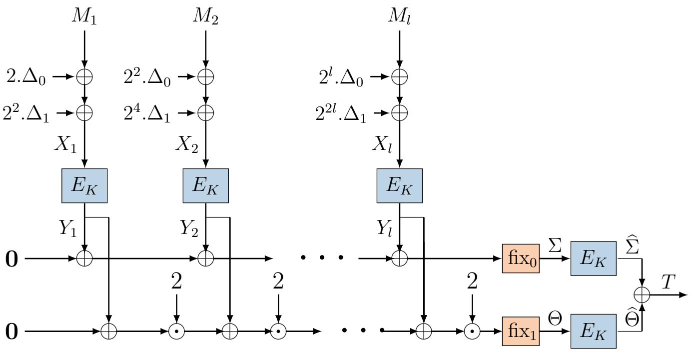


- RCOLL_1: $\Sigma_i = \Sigma_j$ and Θ_i is fresh but $\widehat{\Theta}_i \in \mathrm{Ran}(E_K)$
- RCOLL_2: $\Theta_i = \Theta_j$ and Σ_i is fresh but $\widehat{\Sigma}_i \in \mathrm{Ran}(E_K)$



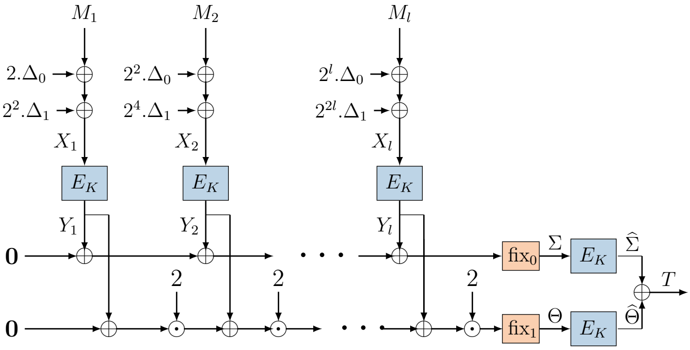
- $\mathrm{PCF1}_1$: $\Sigma_i = X^\star_\alpha$ and Θ_i is fresh but $Y^\star_\alpha \oplus T_i = Y^k_\beta$
- $\mathrm{PCF1}_2$: $\Theta_i = X^\star_\alpha$ and Σ_i is fresh but $Y^\star_\alpha \oplus T_i = Y^k_\beta$

Proof Idea of 1k-PMAC_Plus: Bad Events



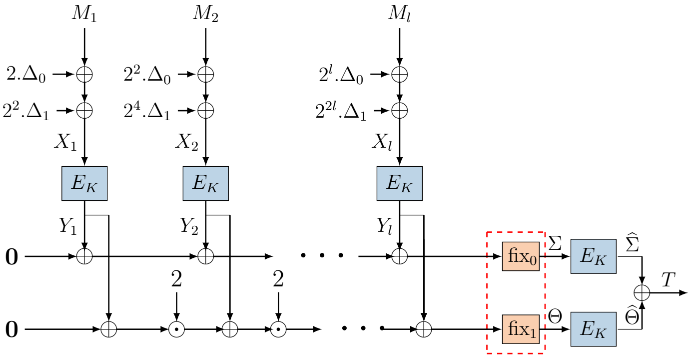
- $\mathrm{PCF2}_1$: $\Sigma_i = X_\alpha^j$ and Θ_i is fresh but $\Sigma_k = X_\beta^l$ and $Y_\alpha^j \oplus T_i = Y_\beta^l \oplus T_k$

Proof Idea of 1k-PMAC_Plus: Bad Events



- PCF2$_2$: $\Sigma_i = X_\alpha^j$ and Θ_i is fresh but $\Theta_k = X_\beta^l$ and $Y_\alpha^j \oplus T_i = Y_\beta^l \oplus T_k$

Proof Idea of 1k-PMAC_Plus: Bad Events



- PCF2$_3$: $\Theta_i = X_\alpha^j$ and Σ_i is fresh but $\Theta_k = X_\beta^l$ and $Y_\alpha^j \oplus T_i = Y_\beta^l \oplus T_k$

Summary of Probability of Bad Events

Events	Probability
ECF	$O(q\sigma^2/2^{2n})$
$\mathrm{RCOLL} = \mathrm{ROLL}_1 \vee \mathrm{RCOLL}_2$	$O(q^2\sigma/2^{2n})$
$\mathrm{PCF1} = \mathrm{PCF1}_1 \vee \mathrm{PCF1}_2$	$O(q\sigma^2/2^{2n})$
$\mathrm{PCF2} = \mathrm{PCF2}_1 \vee \mathrm{PCF2}_2 \vee \mathrm{PCF2}_3$	$O(q^2\sigma^2/2^{3n} + \sigma/2^n)$

Summary of Probability of Bad Events

Events	Probability
ECF	$O(q\sigma^2/2^{2n})$
$\mathrm{RCOLL} = \mathrm{ROLL}_1 \vee \mathrm{RCOLL}_2$	$O(q^2\sigma/2^{2n})$
$\mathrm{PCF1} = \mathrm{PCF1}_1 \vee \mathrm{PCF1}_2$	$O(q\sigma^2/2^{2n})$
$\mathrm{PCF2} = \mathrm{PCF2}_1 \vee \mathrm{PCF2}_2 \vee \mathrm{PCF2}_3$	$O(q^2\sigma^2/2^{3n} + \sigma/2^n)$

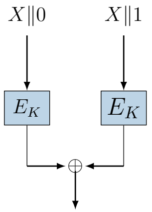
Bounding the Probability of Bad Transcript

$$\epsilon_{\mathrm{bad}} = O(q\sigma^2/2^{2n} + \sigma/2^n)$$

High Interpolation Probability of a good transcript for 1k-PMAC_Plus

- Sum of PRP under conditional distribution

Sum of Identical PRP under Conditional Distribution



$T = E_K(X\|0) \oplus E_K(X\|1)$

Sum of Identical PRP: Existing Results

Sum of Identical PRP: Secure upto $O(q/2^n)$ using Mirror Theory and χ^2 method.

Under Conditional Distribution

What happens when some i/p-o/p of permutations are fixed?

Our Result on Sum of Identical PRP Under Conditional Distribution

Theorem

Let $(u_1, \ldots, u_s)$ and $(v_1, \ldots, v_s)$ are all distinct. Then for all distinct $((X_1, Y_1) \ldots, (X_q, Y_q))$ and all non zero $(T_1, \ldots, T_q)$,

$$\Pr[\Pi(X_i \| 0) \oplus \Pi(Y_i \| 1) = T_i, i \in [q] \mid \Pi(u_1) = v_1, \ldots, \Pi(u_s) = v_s] \geq (1 - \epsilon)/2^{nq}, \text{ where } \epsilon \leq 4qs^2 + 8sq^2 + 6q^3/2^{2n}$$

Bounding the Probability for a Good Transcript

$$\epsilon_{\text{ratio}} = O(q\sigma^2/2^{2n})$$

Necessity of the Domain Separation of Two Lanes

Without $\mathsf{fix}_0, \mathsf{fix}_1$

$$\mathrm{ECF} := \Sigma_i \in \{\Sigma_j, X_\alpha^j\} \text{ and } \Theta_i \in \{\Theta_k, X_\alpha^k\}$$

Necessity of the Domain Separation of Two Lanes

Without $\mathsf{fix}_0, \mathsf{fix}_1$

$$\mathrm{ECF} := \Sigma_i \in \{\Sigma_j, X_\alpha^j\} \text{ and } \Theta_i \in \{\Theta_k, X_\alpha^k\}$$

With $\mathsf{fix}_0, \mathsf{fix}_1$

$$\mathrm{ECF} := \Sigma_i \in \{\Sigma_j, \Theta_j, X_\alpha^j\} \text{ and } \Theta_i \in \{\Sigma_k, \Theta_k, X_\alpha^k\}$$

Necessity of the Domain Separation of Two Lanes

Without $\mathsf{fix}_0, \mathsf{fix}_1$

$$\mathrm{ECF} := \Sigma_i \in \{\Sigma_j, X_\alpha^j\} \text{ and } \Theta_i \in \{\Theta_k, X_\alpha^k\}$$

With $\mathsf{fix}_0, \mathsf{fix}_1$

$$\mathrm{ECF} := \Sigma_i \in \{\Sigma_j, \Theta_j, X_\alpha^j\} \text{ and } \Theta_i \in \{\Sigma_k, \Theta_k, X_\alpha^k\}$$

To avoid analyzing extra bad events, we incorporate $\mathsf{fix}_0, \mathsf{fix}_1$;
Security is not hampered at all!

Main Contribution

- 1k-PMAC_Plus: First Single Key BBB Secure PRF.
- Improved Security bound: $O(q^3\ell^3/2^{2n}) \rightarrow O(q\sigma^2/2^{2n})$

Future Directions

- Tightness of this bound.
- How to increase the security to $3n/4$-bits?

Thank You For Your Kind Attention! Questions?