Multi-User Security of the Sum of Truncated Random Permutations

Wonseok Choi[1] Hwigyeom Kim[2]
Jooyoung Lee[2] Yeongmin Lee[2]

[1]KIAS, Seoul, Korea

[2]KAIST, Daejeon, Korea

2022 ASIACRYPT

December 7th, 2022

Outline

Outline

Motivation

- Block ciphers are one of the most common primitives in the world
  - AES, standardized by NIST, is commonly used in many ways, e.g., wireless security, processor security, file encryption, and SSL/TLS.
- Block cipher: n-bit inputs and n-bit outputs
  - for amounts of data larger than a block
    $\Rightarrow$ repeatedly apply the cipher

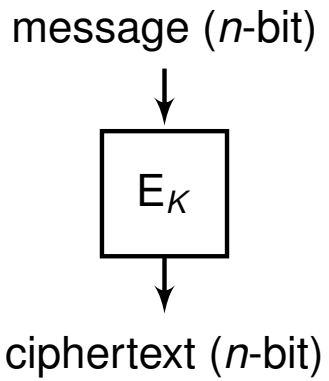

Figure 1: A block cipher

Motivation

- Block ciphers are one of the most common primitives in the world
  - AES, standardized by NIST, is commonly used in many ways, e.g., wireless security, processor security, file encryption, and SSL/TLS.
- Block cipher: n-bit inputs and n-bit outputs
  - for amounts of data larger than a block
    $\Rightarrow$ repeatedly apply the cipher

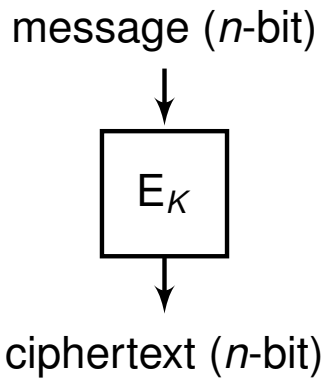

Figure 1: A block cipher

Motivation

- Naive constructions based on a block cipher
  - Counter mode: used in GCM (also standardized by NIST)
  - and other many legacy block-cipher-based MACs and AEs

  only guarantee the **birthday-bound security**

- Solution: replace E_K (block cipher) with pseudorandom functions (PRFs) - called “Luby-Rackoff backward”

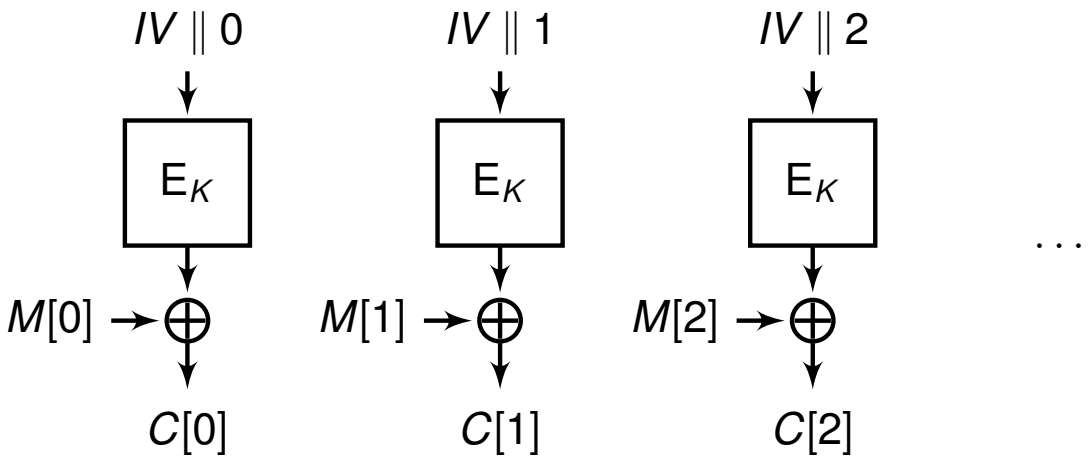

Figure 2: A counter mode

Motivation

- Naive constructions based on a block cipher
  - Counter mode: used in GCM (also standardized by NIST)
  - and other many legacy block-cipher-based MACs and AEs

  only guarantee the **birthday-bound security**

- Solution: replace E_K (block cipher) with pseudorandom functions (PRFs) - called “Luby-Rackoff backward”

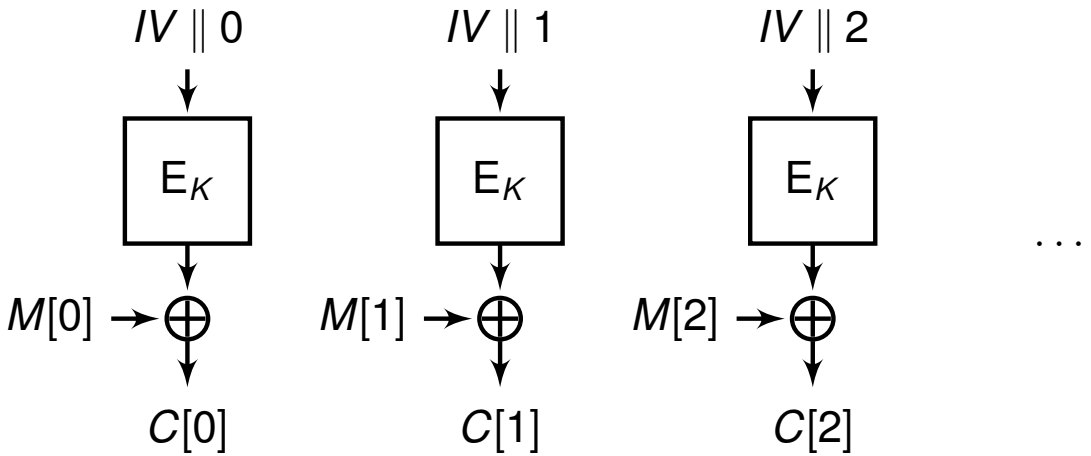

Figure 2: A counter mode

PRF Constructions

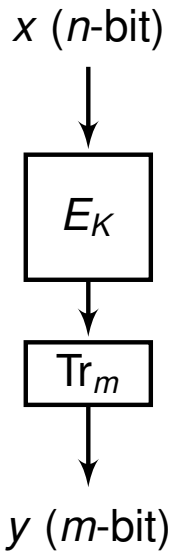

Figure 3: Truncation construction: TRP

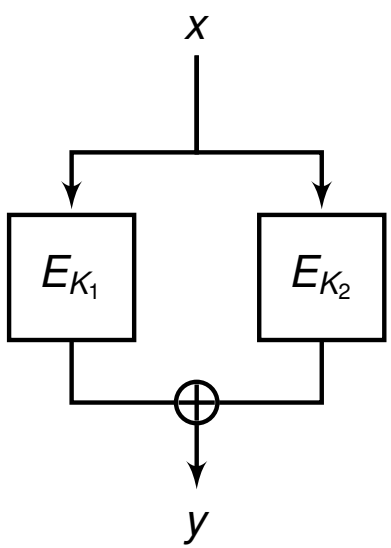

Figure 4: XOR construction: SoP

Indistinguishability of TRP

- Indistinguishability [12, 8, 1]
  - Gilboa et al. [8] (JoC '18): prove the tight security
  - follows from a result of [16] in 1978
- Gunsing and Mennink [11] (Crypto '20): introduce Summation-Truncation-Hybrid (STH) construction
  - concatenating outputs of two independent TRPs and sum of discarded bits from those TRPs

Indistinguishability of SoP

- Indistinguishability [1, 13, 5, 15, 14, 6]
  - Dai et al. [6] (Crypto '17): secure up to $O(2^n)$ queries
- Bhattacharya and Nandi [2] (Asiacrypt '21):
  - sum of three permutations
  - secure up to $O(2^n)$ queries for each of $O(2^n)$ users

Outline

Standard Model

- Cryptographic systems (e.g. PRFs) are
  - composed of secure cryptographic primitives (e.g. block ciphers)
  - supported by security proofs
- Standard model: a keyed block cipher $\Rightarrow$ a secure keyed pseudorandom permutation (PRP)
  - A secure keyed PRP $\Leftrightarrow$ a truly random permutation
- How to show the **security** of a given construction in the standard model?

Standard Model

- Cryptographic systems (e.g. PRFs) are
  - composed of secure cryptographic primitives (e.g. block ciphers)
  - supported by security proofs
- Standard model: a keyed block cipher $\Rightarrow$ a secure keyed pseudorandom permutation (PRP)
  - A secure keyed PRP $\Leftrightarrow$ a truly random permutation
- How to show the **security** of a given construction in the standard model?

Standard Model

- Cryptographic systems (e.g. PRFs) are
  - composed of secure cryptographic primitives (e.g. block ciphers)
  - supported by security proofs
- Standard model: a keyed block cipher $\Rightarrow$ a secure keyed pseudorandom permutation (PRP)
  - A secure keyed PRP $\Leftrightarrow$ a truly random permutation
- How to show the **security** of a given construction in the standard model?

Indistinguishability

- Given two cryptosystems
  - S_0: Ideal world
  - S_1: Real world
- For example
  - S_0: a truly random function
  - S_1: a PRF algorithm
- An Adversary interacts with an oracle $\mathcal{O}$ in a black-box manner

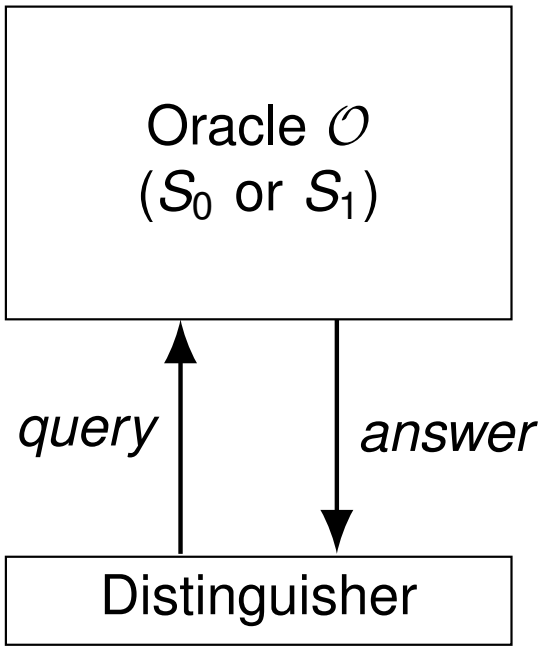

Figure 5: Indistinguishability game

Multi-User Security

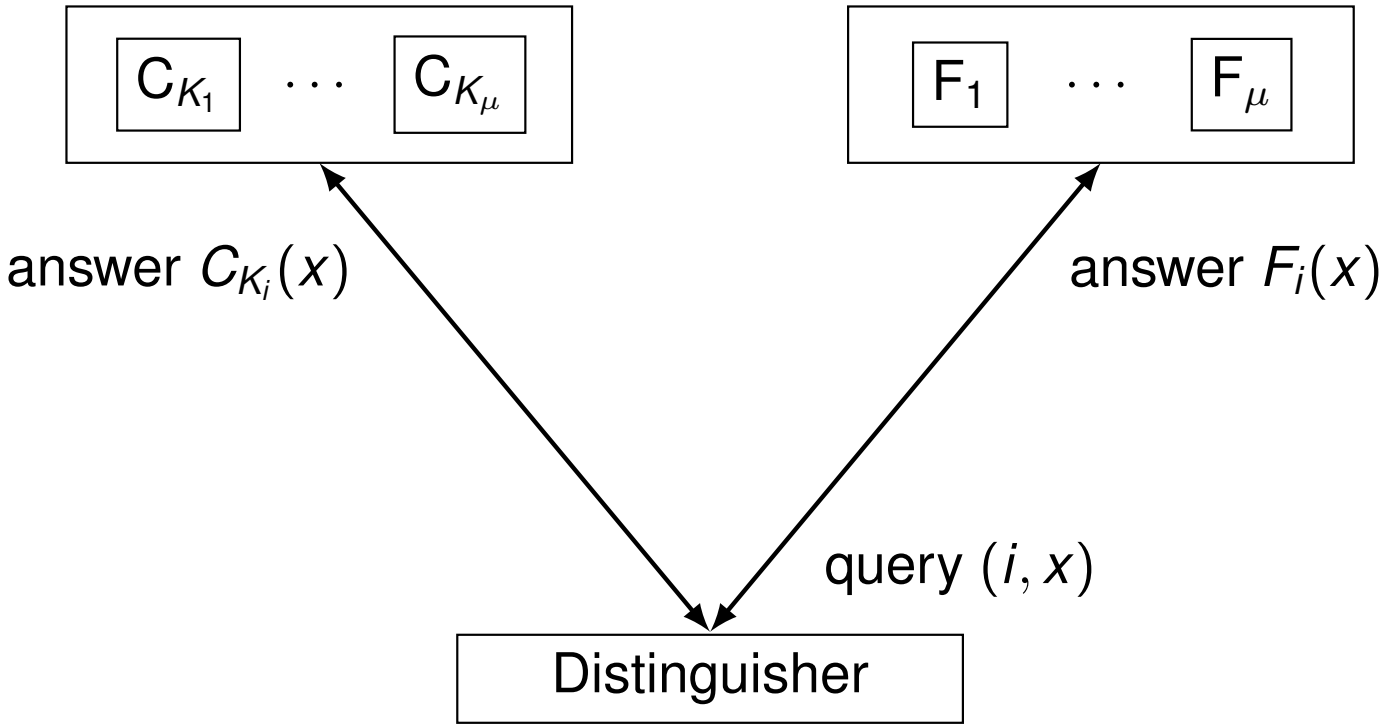

Figure 6: Multi-User Indistinguishability game

Outline

The Sum of Truncated Random Permutations

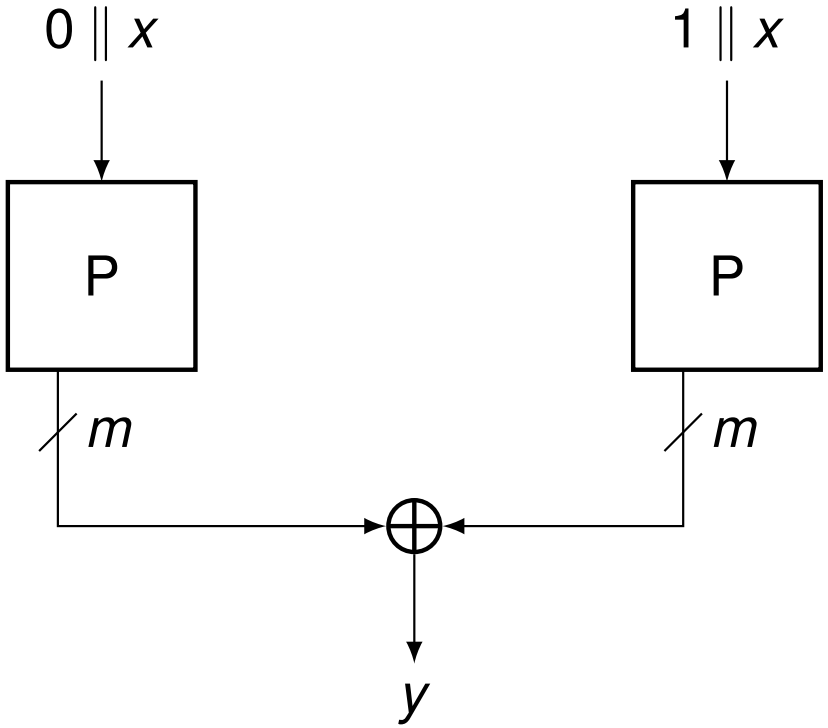

Figure 7: SaT1[P]

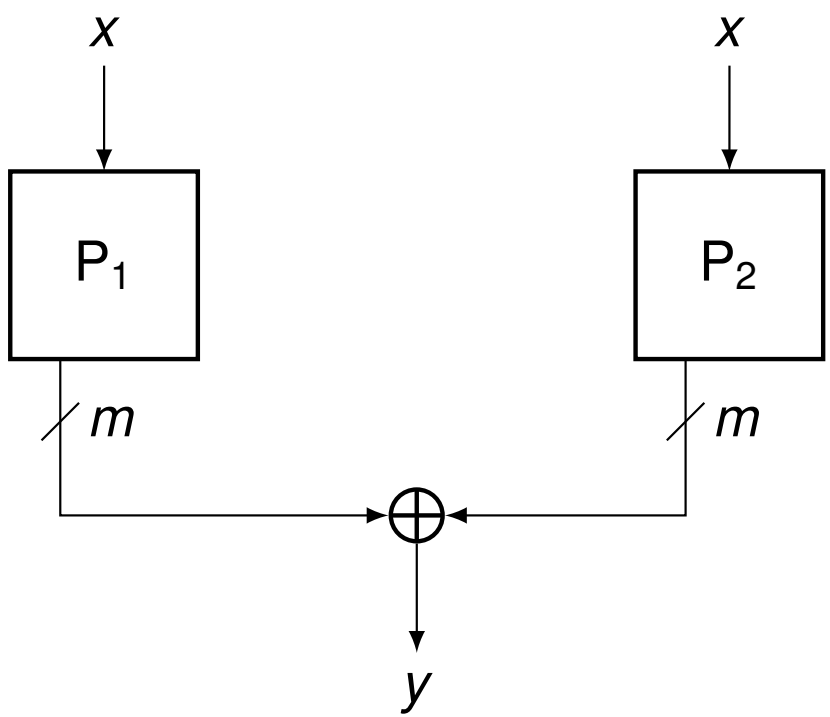

Figure 8: SaT2[P_1, P_2]

The Sum of Three Random Permutations

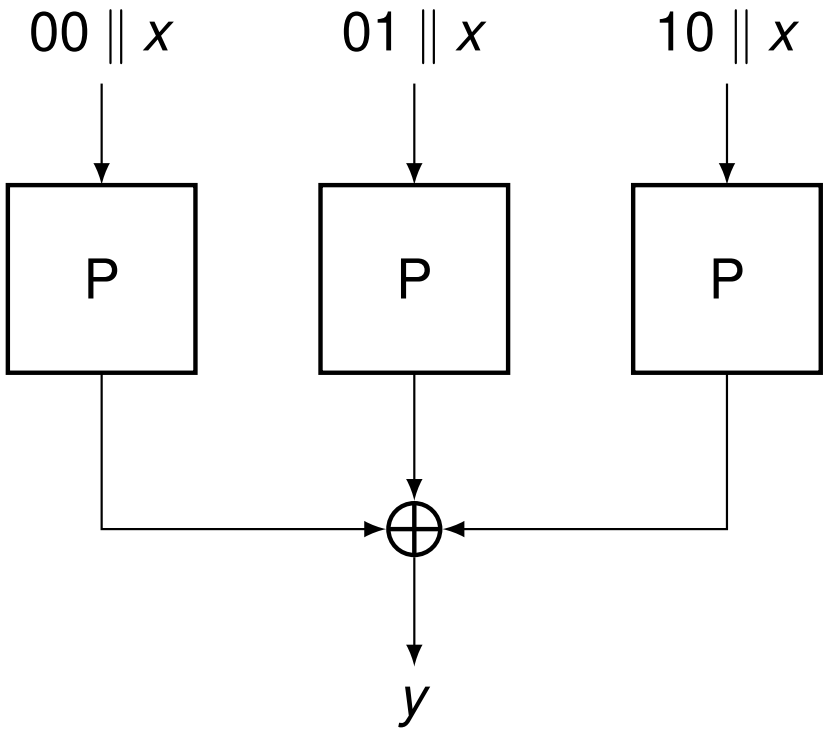

Figure 9: SoP3-1[P]

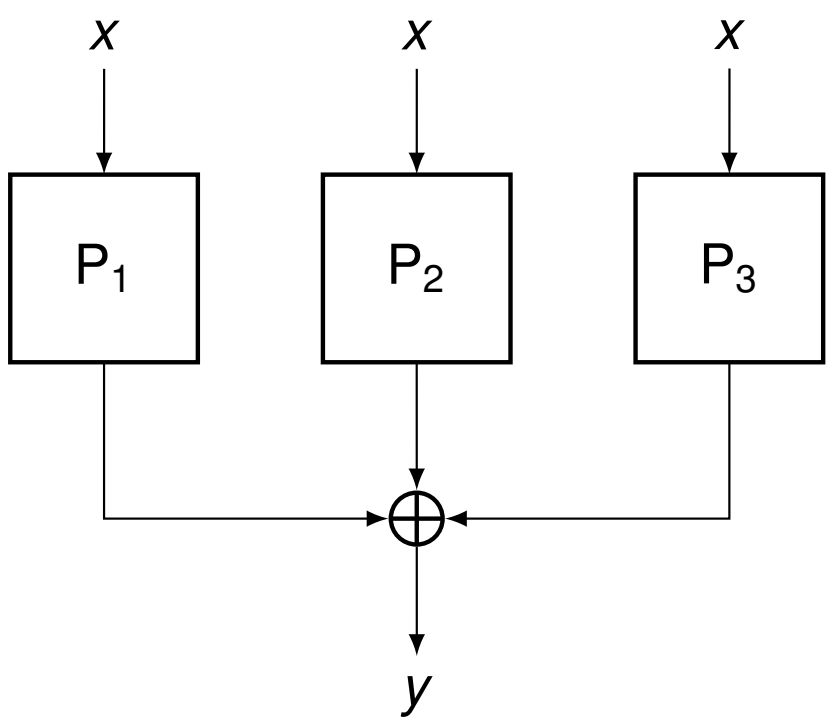

Figure 10: SoP3-2[P_1, P_2, P_3]

Multi-User Security of the Sum of Truncated Random Permutations

Construction	Security	Rate	Number of Keys	Reference
SaT1	$O(\sqrt{\mu q_{\max}}/2^{n-0.5m})$	$m/2$	1	Ours
SaT2	$O(\sqrt{\mu} q_{\max}^{1.5}/2^{2n-0.5m})$	$m/2$	2	Ours
SoP3-1	$O(\sqrt{\mu q_{\max}}/2^{n})$	$n/3$	1	[2]
SoP3-2	$O(\sqrt{\mu} q_{\max}^{2}/2^{2.5n})$	$n/3$	3	Ours

Table 1: Comparison of multi-user secure PRF constructions.

- Security: the upper-bound of distinguishing advantage of each construction
- μ: the number of users
- $q_{\max}$: the maximum number of queries per user
- Rate: output bits per permutation call

The Previous Result

- Multi-user security of the sum of two random permutations
- Previous Result: naive approach - multiply μ for the previous single-user bound

$$O\left(\frac{\mu q_{\max}^2}{2^{2n}}\right)$$

- when $\mu = 2^n$, $q_{\max} \ll 2^{\frac{n}{2}}$ (birthday bound)

Improvement upon Past Knowledge

- Our Result: obtain by letting $m = 0$ for SaT2

$$O\left(\frac{\sqrt{\mu}q_{\max}^{1.5}}{2^{1.5n}}\right) = O\left(\sqrt{\frac{\mu q_{\max}^{3}}{2^{3n}}}\right)$$

- when $\mu = 2^n$, $q_{\max} \ll 2^{\frac{2n}{3}}$ (beyond-birthday bound)

- $m > 0$ cases: the **first** results

Technical Contribution

- Proof technique based on Chi-squared method
- Modifying the domain over which the expectation is taken
  - compute the expectation of the χ^2-divergence for truncated values
- Using involved counting

Application

- SaT1 and SaT2 can replace the key-generation algorithm in
  - AES-GCM-SIV [3, 9, 10] or
  - authenticated encryptions such as CWC+ [7] and SCM [4]

- Synthetic IVs derived from secure PRFs

Outline

Distinguish Games

- Define each world as an experiment:
  - Random function ($\mathcal{S}_0$) and SaT2 ($\mathcal{S}_1$)

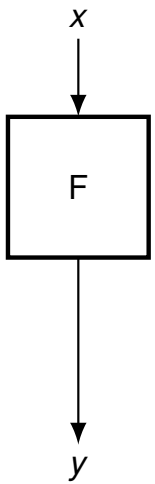

Figure 11: Experiment $\mathcal{S}_0$

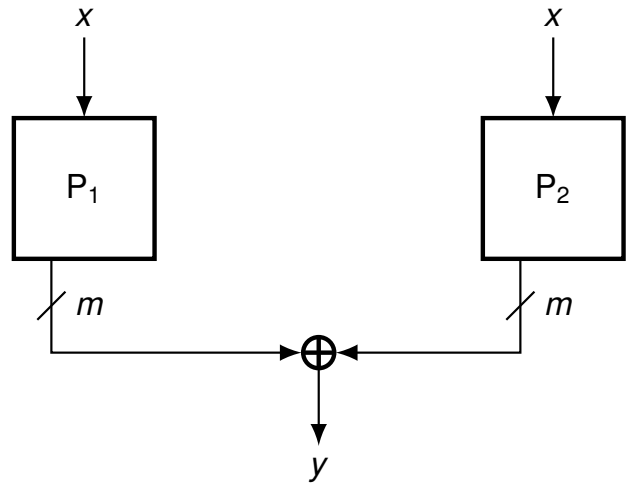

Figure 12: Experiment $\mathcal{S}_1$

- $\mathrm{p}^q_{\mathcal{S}}(\cdot)$: Probability distribution of q samplings from $\mathcal{S}$

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SaT2}}(\mathcal{A}) \leq \|\mathrm{p}^q_{\mathcal{S}_0}(\cdot) - \mathrm{p}^q_{\mathcal{S}_1}(\cdot)\|$$

Input-Independent Experiments

- $\mathcal{B}_0$ and $\mathcal{B}_1$ choose their outputs independently from given inputs
- This setting is NOT necessary but eases our understanding
- $\|\mathsf{p}^q_{\mathcal{S}_0}(\cdot) - \mathsf{p}^q_{\mathcal{S}_1}(\cdot)\| = \|\mathsf{p}^q_{\mathcal{B}_0}(\cdot) - \mathsf{p}^q_{\mathcal{B}_1}(\cdot)\|$

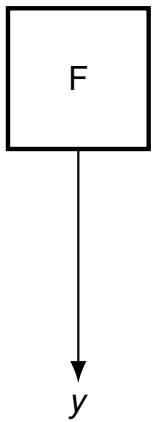

Figure 13: Experiment $\mathcal{B}_0$

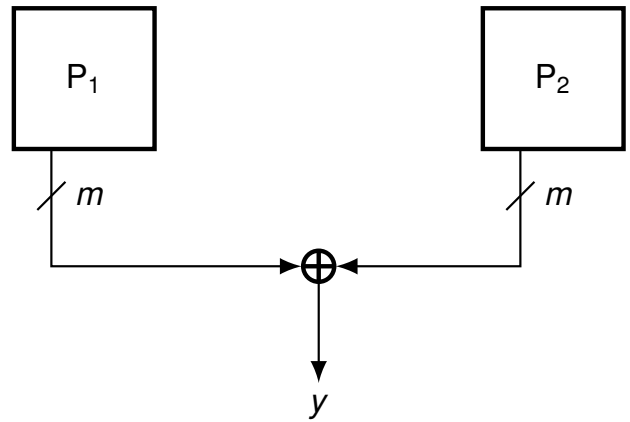

Figure 14: Experiment $\mathcal{B}_1$

Extra Information

- $\mathcal{C}_0$ and $\mathcal{C}_1$ return extra outputs, namely r
- r in $\mathcal{C}_1$ is the truncated output of P_1
- r in $\mathcal{C}_0$ mimics that of $\mathcal{C}_1$
- $\|\mathsf{p}^q_{\mathcal{B}_0}(\cdot) - \mathsf{p}^q_{\mathcal{B}_1}(\cdot)\| \leq \|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\|$

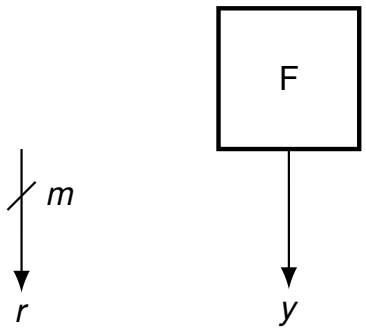

Figure 15: Experiment $\mathcal{C}_0$

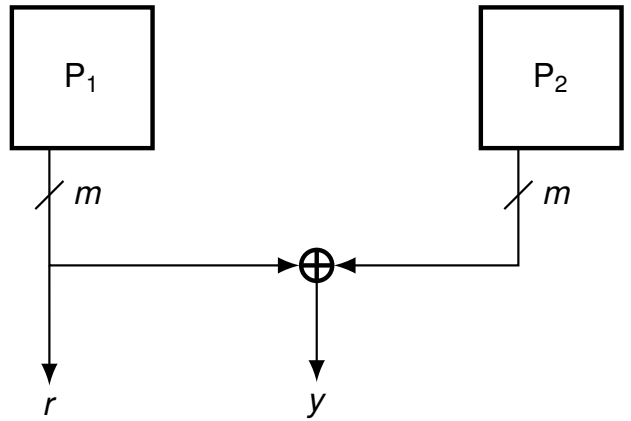

Figure 16: Experiment $\mathcal{C}_1$

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SaT2}}(\mathcal{A}) \leq \|\mathsf{p}^q_{\mathcal{S}_0}(\cdot) - \mathsf{p}^q_{\mathcal{S}_1}(\cdot)\| \leq \|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\|$$

Chi-squared Method

- $Z_{\mathcal{C},i}$: a random variable over Ω that follows
  - the distribution of the i-th answer obtained by $\mathcal{A}$ interacting with $\mathcal{C}$

$$\mathrm{p}^{\mathbf{z}}_{\mathcal{C},i}(z) \stackrel{\text{def}}{=} \Pr\left[Z_{\mathcal{C},i} = z \mid (Z_{\mathcal{C},1}, \ldots, Z_{\mathcal{C},i-1}) = \mathbf{z}\right]$$

- Chi-squared method:

$$\|\mathrm{p}^{q}_{\mathcal{C}_0}(\cdot) - \mathrm{p}^{q}_{\mathcal{C}_1}(\cdot)\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{E}_{\mathbf{z}}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}}$$

where

$$\chi^2(\mathbf{z}) \stackrel{\text{def}}{=} \sum_{z\in\Omega} \frac{\left(\mathrm{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z) - \mathrm{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\right)^2}{\mathrm{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)}$$

Probabilities Obtaining the i-th Answer

- Let $(r, y) \in \{0,1\}^m \times \{0,1\}^m$ be the i-the answer from the oracle
- $S_i(r, y)$: the number of possible output pairs $(r, r \oplus y)$ from P_1 and P_2 (consist with the previous answers)
- $T_i(y)$: the number of possible output pairs $(x, x \oplus y)$ from P_1 and P_2 for any $x \in \{0,1\}^m$

$$\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r, y) = \frac{S_i(r, y)}{2^m T_i(y)}, \qquad \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(r, y) = \frac{S_i(r, y)}{(2^n - i + 1)^2}$$

Computing the Expectation and the Variance

- We should compute $\underset{\mathbf{z}}{\mathbf{Ex}}[T_i(y)]$ and $\underset{\mathbf{z}}{\mathbf{Var}}[T_i(y)]$, but how?
- Let $\hat{\Omega} = \{0,1\}^n \times \{0,1\}^n$ and $\mathbf{h} \in \hat{\Omega}^{i-1}$ such that $\mathbf{h}$ is consistent with $\mathbf{z}$
  - $\mathbf{h}$ contains $i-1$ outputs of P_1 and P_2 before truncating

$$\underset{\mathbf{z}}{\mathbf{Ex}}[T_i(y)] = \underset{\mathbf{h}}{\mathbf{Ex}}[T_i(y)], \qquad \underset{\mathbf{z}}{\mathbf{Var}}[T_i(y)] = \underset{\mathbf{h}}{\mathbf{Var}}[T_i(y)]$$

Lemma

$$\underset{\mathbf{h}}{\mathbf{Ex}}[T_i(y)] = \frac{(2^n - i + 1)^2}{2^m}, \qquad \underset{\mathbf{h}}{\mathbf{Var}}[T_i(y)] \leq \frac{(i-1)^2}{2^m}.$$

Outline

Open Problems

- Reusing truncated bits [11]
- Application to AEADs
- Generalization of the method (ongoing work)
  - Obtaining (better) multi-user security bounds for various constructions

The End

- Thank you for listening!
- Any question?

Bibliography I

[1] Mihir Bellare and R. Impagliazzo. *A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion*. IACR Cryptology ePrint Archive, Report 1999/024. 1999.

[2] Srimanta Bhattacharya and Mridul Nandi. "Luby-Rackoff Backwards with More Users and More Security". In: *Advances in Cryptology – ASIACRYPT 2021*. Springer. 2021, pp. 345–375.

[3] Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. "Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2018, pp. 468–499.

Bibliography II

[4] Wonseok Choi et al. “Toward a Fully Secure Authenticated Encryption Scheme From a Pseudorandom Permutation”. In: *Advances in Cryptology – ASIACRYPT 2021*. Springer-Verlag, 2021.

[5] Benoît Cogliati, Rodolphe Lampe, and Jacques Patarin. “The Indistinguishability of the XOR of k Permutations”. In: *FSE*. Springer, 2014, pp. 285–302. DOI: 10.1007/978-3-662-46706-0_15. URL: https://www.iacr.org/archive/fse2014/85400174/85400174.pdf.

[6] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. “Information-Theoretic Indistinguishability via the Chi-Squared Method”. In: *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part III)*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10403. LNCS. Springer, 2017, pp. 497–523. DOI: 10.1007/978-3-319-63697-9_17.

Bibliography III

[7] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. “Beyond Birthday Bound Secure MAC in Faulty Nonce Model”. In: *Advances in Cryptology - EUROCRYPT 2019 (Proceedings, Part I)*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. LNCS. Springer, 2019, pp. 437–466. DOI: 10.1007/978-3-030-17653-2_15.

[8] Shoni Gilboa, Shay Gueron, and Ben Morris. “How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function?” In: *Journal of Cryptology* 31.1 (2018), pp. 162–171. DOI: 10.1007/s00145-017-9253-0.

[9] Shay Gueron, Adam Langley, and Yehuda Lindell. *AES-GCM-SIV: Specification and Analysis.* IACR Cryptology ePrint Archive, Report 2017/168. 2017.

Bibliography IV

[10] Shay Gueron and Yehuda Lindell. “GCM-SIV: Full nonce misuse-resistant authenticated encryption at under one cycle per byte”. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015, pp. 109–119.

[11] Aldo Gunsing and Bart Mennink. “The Summation-Truncation Hybrid: Reusing Discarded Bits for Free”. In: *Advances in Cryptology – CRYPTO 2020 (Proceedings, Part I)*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12170. LNCS. Springer, 2020, pp. 187–217. DOI: 10.1007/978-3-030-56784-2_7.

[12] Chris Hall et al. “Building PRFs from PRPs”. In: *Advances in Cryptology - CRYPTO ’98*. Ed. by Hugo Krawczyk. Vol. 1462. LNCS. Springer, 1998, pp. 370–389. DOI: 10.1007/BFb0055742.

Bibliography V

[13] Stefan Lucks. “The Sum of PRPs Is a Secure PRF”. In: *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*. Vol. 1807. Lecture Notes in Computer Science. Springer, 2000, pp. 470–484. DOI: 10.1007/3-540-45539-6_34. URL: https://www.iacr.org/archive/eurocrypt2000/1807/18070476-new.pdf.

[14] Bart Mennink and Bart Preneel. “On the XOR of Multiple Random Permutations”. In: *ACNS 2015*. Ed. by Tal Malkin et al. 2015, pp. 619–634. ISBN: 978-3-319-28166-7.

Bibliography VI

[15] Jacques Patarin. "A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations". In: *Information Theoretic Security*. Ed. by Reihaneh Safavi-Naini. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 232–248. ISBN: 978-3-540-85093-9.

[16] AJ Stam. "Distance Between Sampling with and without Replacement". In: *Statistica Neerlandica* 32.2 (1978), pp. 81–91.