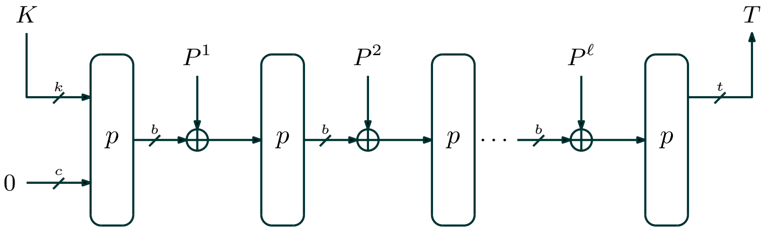
# Tightness of the Suffix Keyed Sponge Bound

**Christoph Dobraunig and Bart Mennink**

FSE 2022

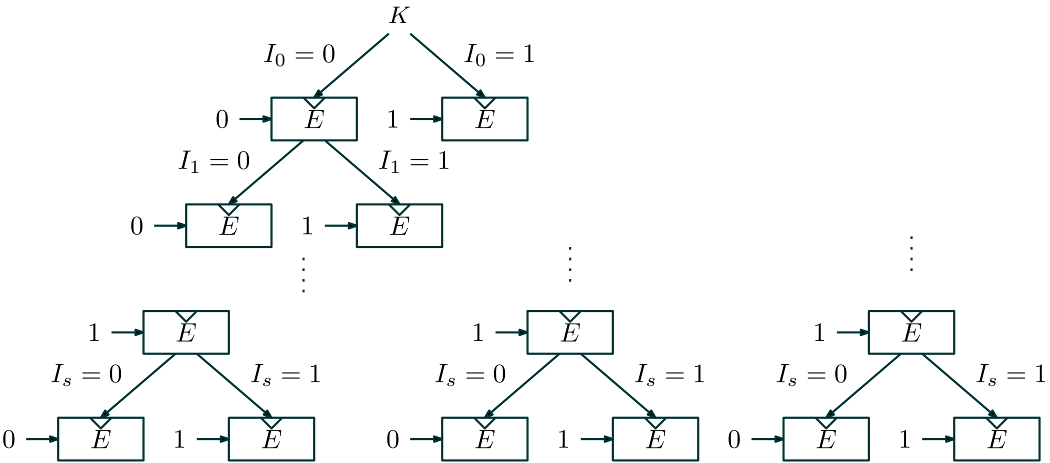
March 2022

# How to Build a MAC?



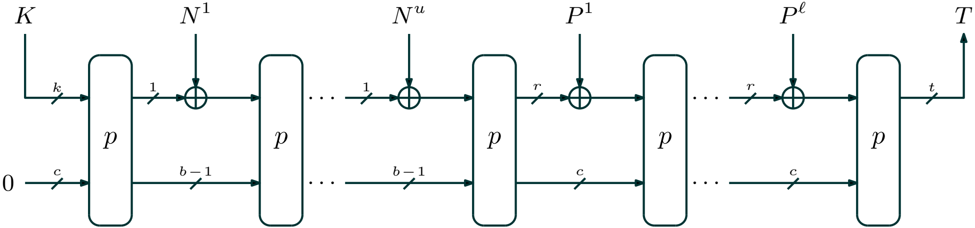

- Full-state keyed sponge [BDP+12; MRV15; DMV17]
- Very efficient
- No mode-level protection against side-channel attacks
- Mixing of changing input with static secret enables, e.g., DPA [KJJ99]

# Limit the Data Complexity



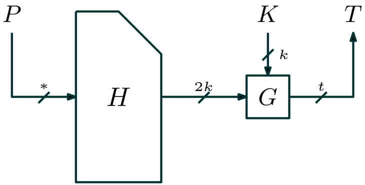

- Single bit per static secret using GGM-like [GGM86] construction, e.g., [SPY+09]

# Speed-Up I



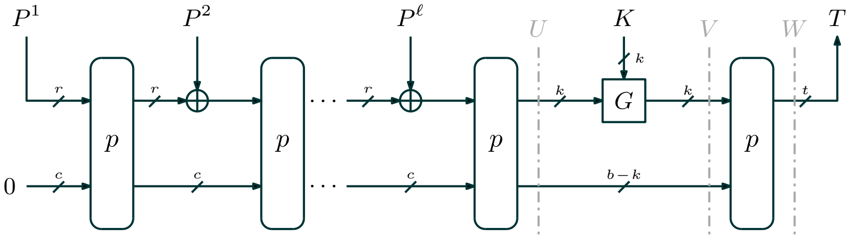

- Use a nonce as proposed in, e.g., [TS14]
- Leakage resilience analysis in [DM19a]
- SCA resistance depends on uniqueness of nonce $N$

# Speed-Up II



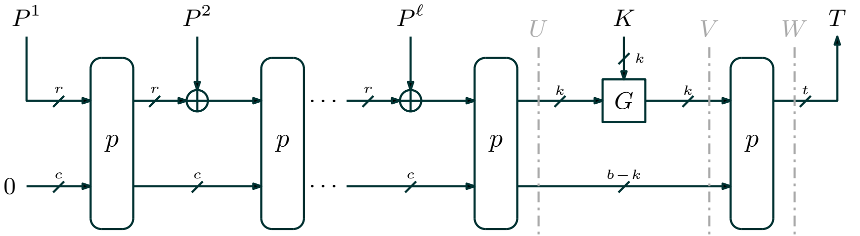

- Hash-then-PRF as proposed in, e.g., [USS+20]
- Leakage-resilient-PRF $G$ processes $2k$-bit input for $k$-bit security

# Speed-Up III

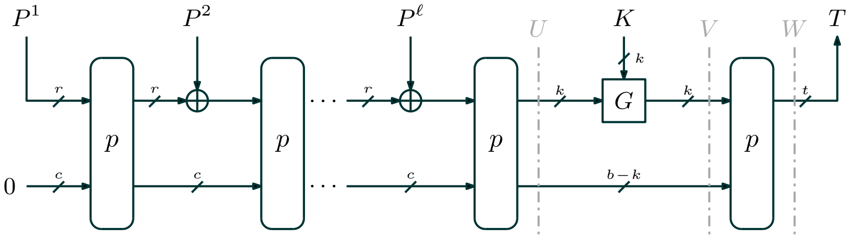



- Use SuKS as proposed in [DEM+17]
- Leakage-resilient-PRF $G$ processes $k$-bit input for $k$-bit security
- Leakage resilience analysis in [DM19b]

# Security of SuKS




- If $G$ is an XOR and $k \leq r$:
  - Construction well-known [BDP+11]
  - indifferentiability results applies [BDP+08]
- What if $G$ is a PRF or if $k > r$?




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- $G$ is $2^{-\delta}$-uniform and $2^{-\varepsilon}$-universal
- $\mu_{b-c,c}^q$ smallest natural number $x$ that $\Pr(\mu > x) \leq \frac{x}{2^c}$ [DMV17]

# Example Values

- Assume $\textsc{Ascon}$-like instance with $c = 256$, $r = 64$, $k = t = 128$
- XOR as $G$: $2^{-k}$-uniform and 0-universal

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

# Example Values

- Assume Ascon-like instance with $c = 256$, $r = 64$, $k = t = 128$
- XOR as $G$: $2^{-k}$-uniform and 0-universal

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \le \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

- PRF as $G$: $2^{-k}$-uniform and $2^{-k}$-universal

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \le \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

# Example Values

- Assume Ascon-like instance with $c = 256$, $r = 64$, $k = t = 128$
- XOR as $G$: $2^{-k}$-uniform and 0-universal

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

- PRF as $G$: $2^{-k}$-uniform and $2^{-k}$-universal

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

Can we find attacks in both cases?

Or can we improve the bound of [DM19b]?

# This Work

- Tightness of the suffix keyed sponge bound of [DM19b]

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

# This Work

- Tightness of the suffix keyed sponge bound of [DM19b]

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- First term non-surprising: inner collisions on hash part

# This Work

- Tightness of the suffix keyed sponge bound of [DM19b]

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- First term non-surprising: inner collisions on hash part
- Two attacks if XOR as $G$:
  - $\mu$-collision based attack that matches third term
  - $\mu$-collision based attack that matches second term

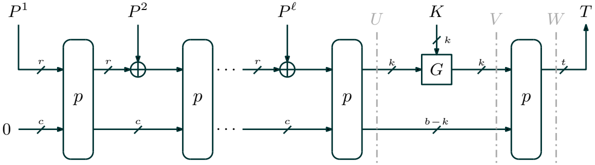
# This Work

- Tightness of the suffix keyed sponge bound of [DM19b]

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- First term non-surprising: inner collisions on hash part
- Two attacks if XOR as $G$:
  - $\mu$-collision based attack that matches third term
  - $\mu$-collision based attack that matches second term
- One attack if PRF as $G$:
  - $\mu$-collision based attack that matches second term

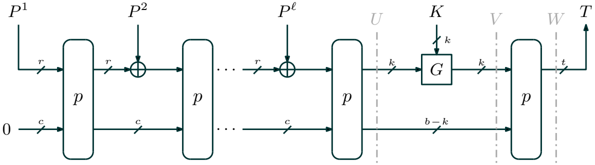
# XOR as $G$: $\mu$-Collision on Tag




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

# XOR as $G$: $\mu$-Collision on Tag




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

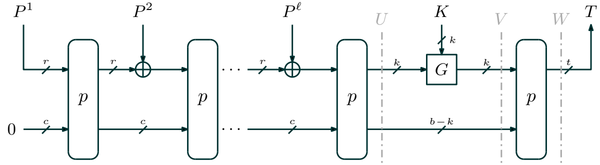
(1) $q$ construction queries gives tags $T_i$ and corresponding $U_i$

(2) Find a $\mu$-fold collision $T$ in the tags $T_i$

(3) Make $N$ primitive queries $p^{-1}(T \| Z_j)$ for varying $Z_j$

(4) For outcome $Y \| \mathrm{right}_{b-k}(U_i)$ compute the key $K = Y \oplus \mathrm{left}_k(U_i)$

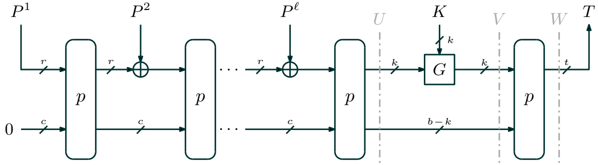
# XOR as $G$: $\mu$-Collision on Tag




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $T$ gives speed-up of $\mu$ in search for $\mathrm{right}_{b-t}(W_i)$

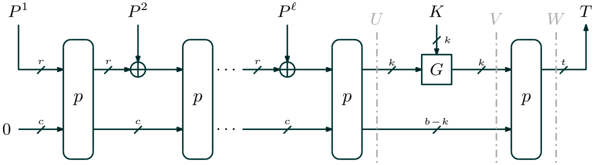
# XOR as $G$: $\mu$-Collision on Tag




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $T$ gives speed-up of $\mu$ in search for $\mathrm{right}_{b-t}(W_i)$
- Parameters $b = 256$ and $k = 128$:
  - Complexity $(q, N) \approx (2^{124.1}, 2^{125.8})$
  - Huge online complexity

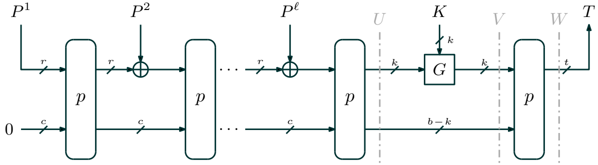
# XOR as $G$: $\mu$-Collision on Tag




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $T$ gives speed-up of $\mu$ in search for $\mathrm{right}_{b-t}(W_i)$
- Parameters $b = 256$ and $k = 128$:
  - Complexity $(q, N) \approx (2^{124.1}, 2^{125.8})$
  - Huge online complexity
- Usually $b > 2k$ due to first term of bound: third term not dominating

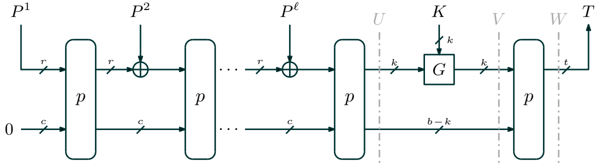
# XOR as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

# XOR as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

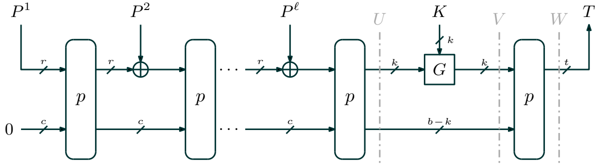
(1) Find a $\mu$-fold collision $U^\star$ in the $\mathrm{right}_{b-k}(U_i)$ (offline)

(2) Make $\mu$ construction queries to get the corresponding $T_i$

(3) Make primitive queries $p(Z_j \| U^\star)$ for varying $Z_j$

(4) For a match in $T_i$ compute $K = Z_j \oplus \mathrm{left}_k(U_i)$

# XOR as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$

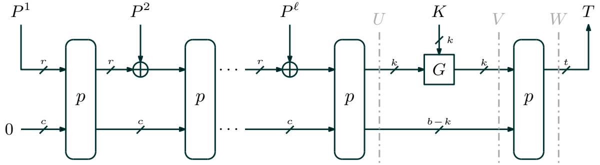



$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $\mathrm{right}_{b-k}(U_i)$ gives speed-up of $\mu$ in search for $\mathrm{left}_k(V_i)$

# XOR as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$

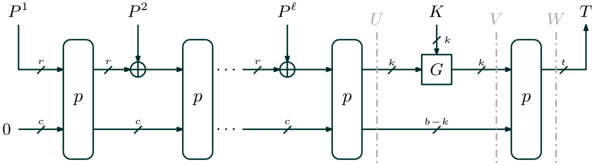



$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $\mathrm{right}_{b-k}(U_i)$ gives speed-up of $\mu$ in search for $\mathrm{left}_k(V_i)$
- Parameters $b = 272$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (6, 2^{125.9})$
  - Matching term in bound $\frac{16N}{2^{128}}$

# XOR as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$

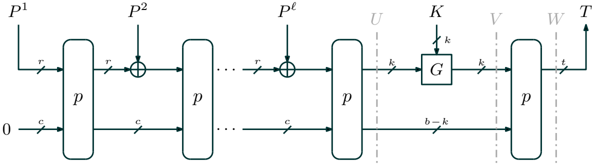



$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Idea: $\mu$-collision on $\mathrm{right}_{b-k}(U_i)$ gives speed-up of $\mu$ in search for $\mathrm{left}_k(V_i)$
- Parameters $b = 272$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (6, 2^{125.9})$
  - Matching term in bound $\frac{16N}{2^{128}}$
- Parameters $b = 320$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (2, 2^{127})$
  - Matching term in bound $\frac{5N}{2^{128}}$

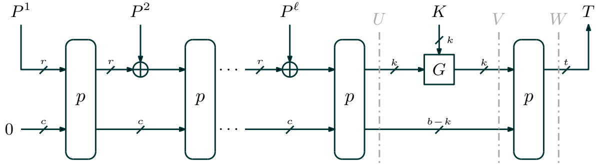
# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Previous attack corresponded to recovering the key

# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$

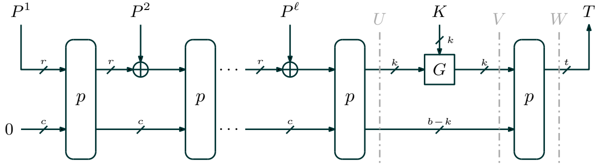



$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Previous attack corresponded to recovering the key
- With hard-to-invert $G$, this is not necessarily possible

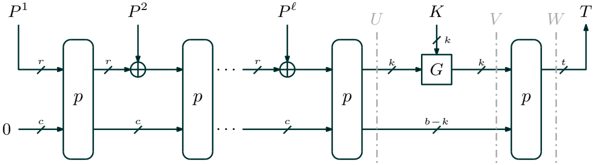
## PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Previous attack corresponded to recovering the key
- With hard-to-invert $G$, this is not necessarily possible
- Still, $\mu$-collisions can be used to mount a forgery against SuKS

# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

(1) Find a $\mu$-fold collision $U^\star$ in the $\mathrm{right}_{b-k}(U_i)$ (offline)

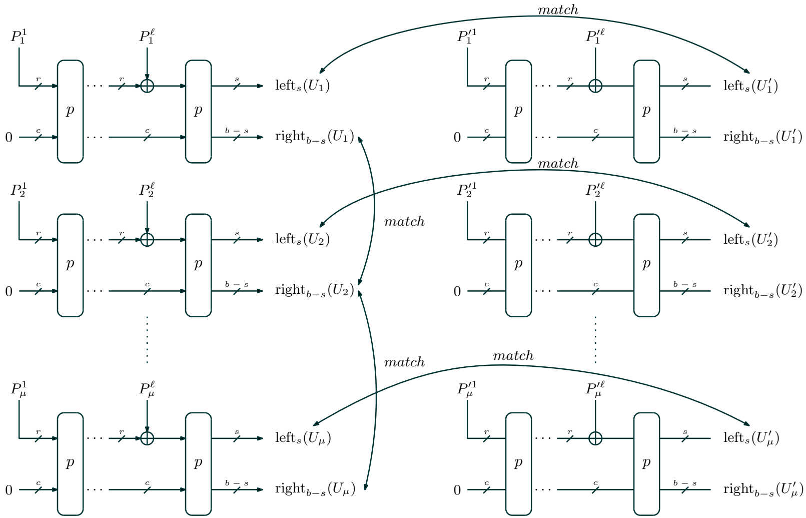
(2) For each of these $\mu$ plaintexts, find a collision in the $\mathrm{left}_k(U_i)$ (offline)

(3) Make $\mu$ construction queries (of the $\mu$-collision) to get the corresponding $T_i$

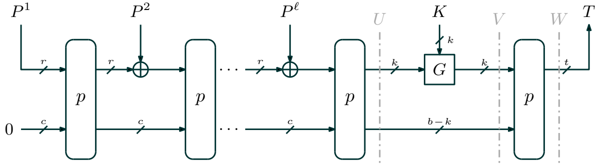
(4) Make primitive queries $p(Z_j \| U^\star)$ for varying $Z_j$

(5) For a match in $T_i$, use collision of step (2) to mount forgery

# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$



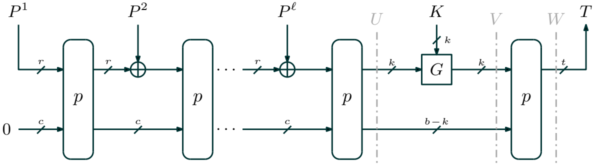
# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Parameters $b = 272$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (5, 2^{125.9})$
  - Matching term in bound $\frac{16N}{2^{128}}$

# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$

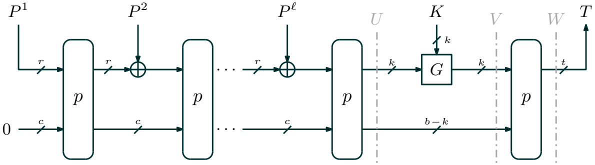



$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Parameters $b = 272$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (5, 2^{125.9})$
  - Matching term in bound $\frac{16N}{2^{128}}$
- Parameters $b = 320$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (2, 2^{127})$
  - Matching term in bound $\frac{5N}{2^{128}}$

# PRF as $G$: $\mu$-Collision on $\mathrm{right}_{b-k}(U_i)$




$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq$$

$$\frac{2N^2}{2^c} + \frac{\mu_{b-k,k}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\mu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

- Parameters $b = 272$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (5, 2^{125.9})$
  - Matching term in bound $\frac{16N}{2^{128}}$
- Parameters $b = 320$ and $k = t = c/2 = 128$:
  - Complexity $(q, N) \approx (2, 2^{127})$
  - Matching term in bound $\frac{5N}{2^{128}}$
- Similar results as for XOR as $G$

# Conclusion

- Tightness attacks: similar complexity if $G$ is an XOR or a PRF
- Multicollisions can be used in attacks as indicated by the bound
- More in paper: detailed attack complexity computation

- Is there a better way to bound the multicollisions terms appearing in the bound?

Thank you for your attention!

# References


[BDP+08] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. On the Indifferentiability of the Sponge Construction. In: EUROCRYPT 2008. Ed. by N. P. Smart. Vol. 4965. LNCS. Springer, 2008, pp. 181–197.

[BDP+11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Cryptographic sponge functions (Version 0.1). `https://keccak.team/`. Jan. 2011.

[BDP+12] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Permutation-based encryption, authentication and authenticated encryption. Directions in Authenticated Ciphers. July 2012.

[DEM+17] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer. ISAP - Towards Side-Channel Secure Authenticated Encryption. In: IACR Trans. Symmetric Cryptol. 2017.1 (2017), pp. 80–105.

[DM19a] C. Dobraunig and B. Mennink. Leakage Resilience of the Duplex Construction. In: ASIACRYPT (3). Vol. 11923. LNCS. Springer, 2019, pp. 225–255.

[DM19b] C. Dobraunig and B. Mennink. Security of the Suffix Keyed Sponge. In: IACR Trans. Symmetric Cryptol. 2019.4 (2019), pp. 223–248.

# References

[DMV17] J. Daemen, B. Mennink, and G. Van Assche. Full-State Keyed Duplex with Built-In Multi-user Support. In: ASIACRYPT 2017. Ed. by T. Takagi and T. Peyrin. Vol. 10625. LNCS. Springer, 2017, pp. 606–637. DOI: 10.1007/978-3-319-70697-9_21. URL: https://doi.org/10.1007/978-3-319-70697-9%5C_21.

[GGM86] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. In: J. ACM 33.4 (1986), pp. 792–807.

[KJJ99] P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In: CRYPTO. Vol. 1666. LNCS. Springer, 1999, pp. 388–397.

[MRV15] B. Mennink, R. Reyhanitabar, and D. Vizár. Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption. In: ASIACRYPT 2015. 2015, pp. 465–489. DOI: 10.1007/978-3-662-48800-3_19. URL: https://doi.org/10.1007/978-3-662-48800-3_19.

[SPY+09] F.-X. Standaert, O. Pereira, Y. Yu, J.-J. Quisquater, M. Yung, and E. Oswald. Leakage Resilient Cryptography in Practice. Cryptology ePrint Archive, Report 2009/341. https://eprint.iacr.org/2009/341. 2009.

# References


[TS14] M. M. I. Taha and P. Schaumont. Side-channel countermeasure for SHA-3 at almost-zero area overhead. In: HOST 2014. IEEE Computer Society, 2014, pp. 93–96.

[USS+20] F. Unterstein, M. Schink, T. Schamberger, L. Tebelmann, M. Ilg, and J. Heyszl. Retrofitting Leakage Resilient Authenticated Encryption to Microcontrollers. In: IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020.4 (2020), pp. 365–388.