# Forking Sums of Permutations for Optimally Secure and Highly Efficient PRFs


Avijit Dutta[1] **Eik List**[3]

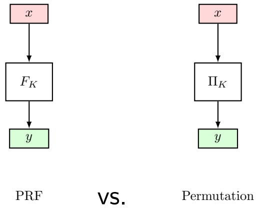
[1]Institute for Advancing Intelligence, TCG CREST, Kolkata, India

[2]Independent researcher visiting at Nanyang Technological University, Singapore


Asian Symmetric Key Workshop
December 2024

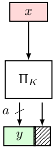
# Motivation

# PRFs

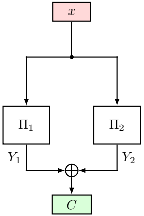



- PRFs are highly important primitives for e.g. encryption and authentication
- Designing a dedicated pseudorandom function from scratch is hard
- Collision probabilities accumulate with every iteration
- Easier: Design a PRP and build a PRF from it
- Simply using a PRP as a PRF reduces its security to the birthday bound ($O(2^{n/2})$-bit for $n$-bit permutation) [BKR94, BR06, CN08]
- Better: Use simple provably secure constructions
  $\Longrightarrow$ Many closely related developments. . .

# Fixed-output-length PRFs with Beyond-birthday-bound Security (I)



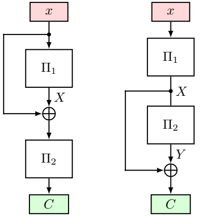

Truncation




SoP [BKR98]

- Hall et al. [HWKS98]: Truncating permutations
  Output $a$ out of $n$ bits $\Longrightarrow$ $O(n - a/2)$-bit PRF security
- Bellare et al. [BKR98]: Sum of independent permutations
- Various cryptanalysis [Luc00, DHT17, DNS22]: sum is almost optimally ($O(n)$-bit) secure

# Fixed-output-length PRFs with Beyond-birthday-bound Security (II)

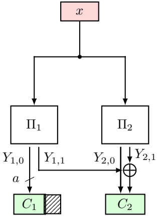



EDM [CS16] EDMD [MN17a]

- Cogliati and Seurin [CS16]: Encrypted Davies-Meyer (EDM) $O(2n/3)$-bit PRF security
- Mennink and Neves [MN17a]:
  Improved security result to $O(n)$-bit
  Proposed its dual EDMD
- Results based on assumptions on Mirror Theory for general block size [NPV17, Pat10]

Cogliati et al. [CDN$^+$23] recently proved the Mirror-Theory result for general $\xi_{\max}$

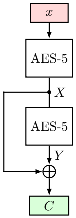
# Fixed-output-length PRFs with Beyond-birthday-bound Security (III)




STH [GM20]

- Gunsing and Mennink [GM20]: Summation-Truncation Hybrid
- Trade-off between PRF security and output length
- Outputs $a$ bits from the first permutation call
- $O(n - a/2)$-bit security

# More Efficient Primitives (I)




FastPRF [MN17b]

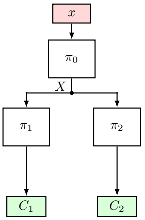
Hoang et al. [HKR15]:

- Proposed AEZ
- Proved security when instantiated with ideal permutations
- Then, instantiated with four-round AES

Mennink and Neves [MN17b]:

- Proposed FastPRF
- Reduced the permutations in EDMD
- Claimed full PRF security though
- Instantiation AES-PRF with $5 + 5$-rd. AES

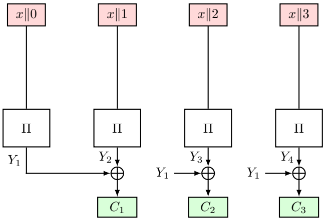
# More Efficient Primitives (II)




ForkPRP2 [ALP+19]

- Andreeva et al. [ALP+19]:
  ForkCipher as new primitive
- Fork secret middle state and branch for multiple independent permutations
- Iterate-Fork-Iterate paradigm
- Goal: higher efficiency than 2 full PRPs

# From Fixed- to Variable-output-length PRFs



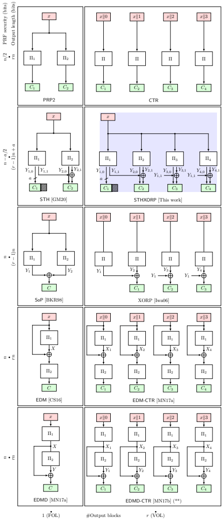

XORP [Iwa06]

- Iwata [Iwa06]: extended SoP to variable-output-length PRF called XORP
- Iwata et al. [IMV16]: XORP[$r$] (with $r$ branches) is $O(n - \log_2(r))$-bit PRF-secure
- Andreeva et al. [ALP$^+$19]: Proposed MultiForkCiphers

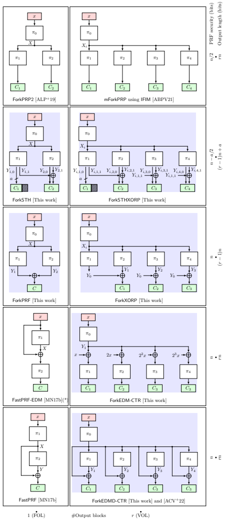
# Core Observation

- Many closely related developments, but they seem not organized yet
- We propose an organization in a spectrum spanned by the dimensions of
  1. PRF security
  2. output length
  3. forking

# Organization




(a) Full-round primitives.



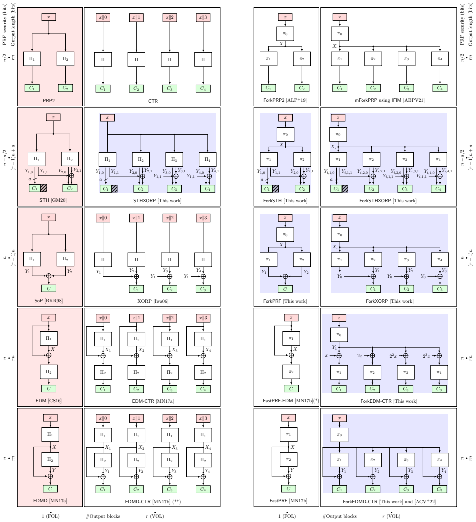

(b) Reduced-round primitives.

# Outline

- Overview of our organization
- Identify and fill the gaps that previous works left
- Give formal security arguments for all constructions
- Propose AES-based instantiation for most interesting constructions ForkEDMD-CTR and ForkXORP-CTR
- Report on software-implementation results

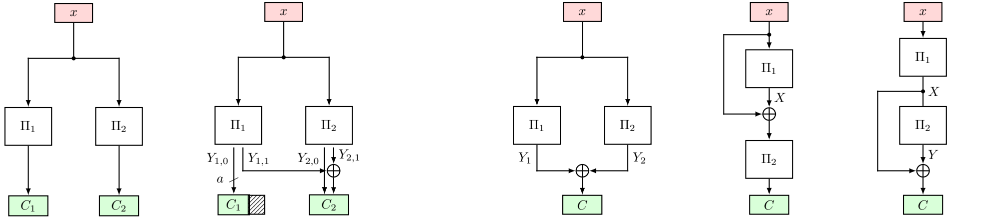
# Framework

# Organization (I)



(a) Full-round primitives. (b) Reduced-round primitives.

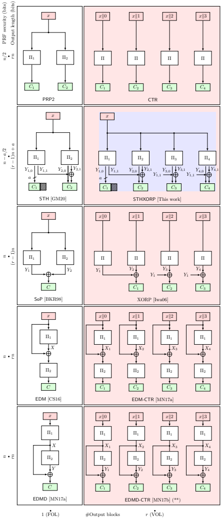
# (1) Fixed-output-length PRFs



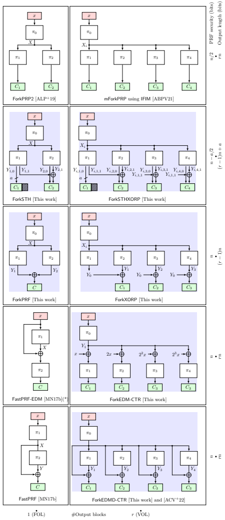

| PRP2 | STH [GM20] | SoP [BKR98] | EDM [CS16] | EDMD [MN17a] |
|---|---|---|---|---|
| $2n$ bits | $a + n$ bits | $n$ bits | $n$ bits | $n$ bits |
| $O(n/2)$ | $O(n - a/2)$ | $O(n)$ | $O(n)$ | $O(n)$ |

- Trade-off: Output length ($2n \rightarrow n$ bits) vs. PRF security ($n/2 \rightarrow n$ bits)

# Organization (II)

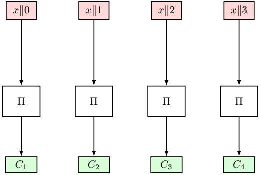



(a) Full-round primitives.



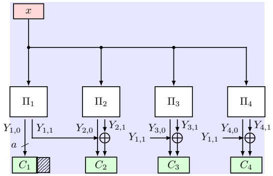

(b) Reduced-round primitives.

# (2) Extension to Variable-output-length PRFs



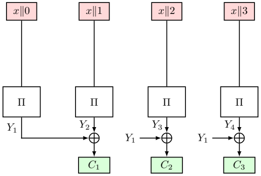

CTR

$rn$ bits
$O(n/2)$




STHXORP [This work]

$a + (r-1)n$ bits
$O(n - a/2 - \log_2(r))$



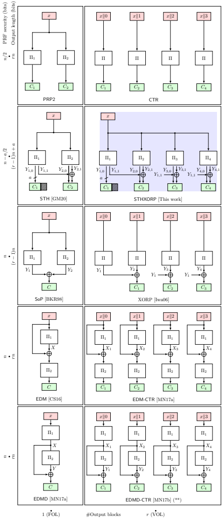

XORP [Iwa06]

$(r-1)n$ bits
$O(n - \log_2(r))$

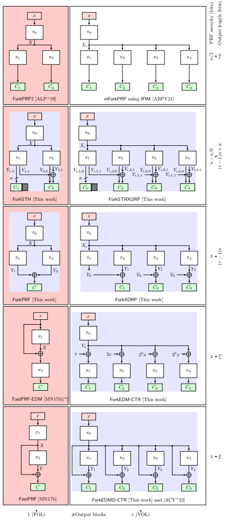
- Same trade-off between output length vs. PRF security
- Extension to VOL is trivial for PRP2, EDM, and EDMD

- Extension is not trivial for XORP and its STH variant
- We propose STH-XORP[r]

# Organization (III)

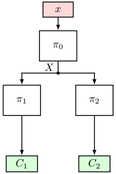



(a) Full-round primitives.




(b) Reduced-round primitives.

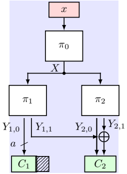
# (3) Forking Fixed-output-length PRFs (I)




ForkPRP2 [ALP+19]

$2n$ bits

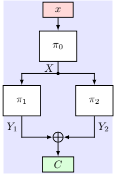
$O(n/2)$




ForkSTH [This work]

$a + n$ bits

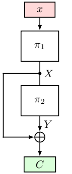
$O(n - a/2)$




ForkPRF [This work]

$n$ bits

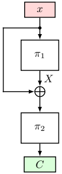
$O(n)$




FastPRF [MN17b]

$n$ bits

$O(n)$



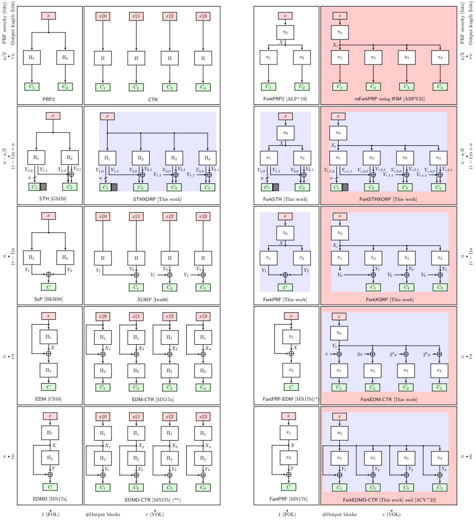

FastPRF-EDM [MN17b](*)

$n$ bits

$O(n)$

- Andreeva et al. introduced forking
- We propose ForkPRF as a forked version of SoP
- We propose ForkSTH as a generalization of ForkPRP2 and ForkPRF

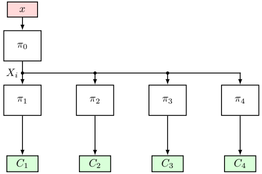
# Organization (IV)




(a) Full-round primitives.

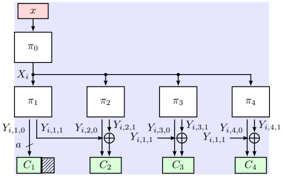
(b) Reduced-round primitives.

# (4) Multiple Forks for Forked Variable-output-length PRFs (I)



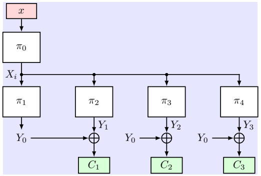

mForkPRP using IFIM [ABPV21]

$rn$ bits
$O(n/2)$




ForkSTHXORP [This work]

$a + (r-1)n$ bits
$O(n - a/2 - \log_2(r))$

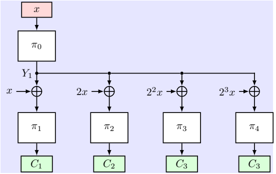



ForkXORP [This work]

$(r-1)n$ bits
$O(n - \log_2(r))$

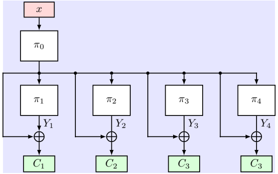
- Multi-ForkCipher by Andreeva et al. [ALP$^+$19, ABPV21] extends ForkCipher to forked VOL-PRFs
- We propose ForkXORP[r]: Extends ForkPRF similarly fork several blocks and add first output to each of the other bottom-permutation outputs
- We propose ForkSTHXORP[r] for the spectrum between mForkPRP[r] and ForkXORP[r]

# (4) Multiple Forks for Forked Variable-output-length PRFs (II)




ForkEDM-CTR [This work]

$rn$ bits
$O(n - \log_2(r))$




ForkEDMD-CTR [This work] and [ACV+22]

$rn$ bits
$O(n - \log_2(r))$

- We propose ForkEDM-CTR as a forked VOL-PRF extension of EDM
- Needs multiplications in $GF(2^n)$ to prevent trivial collisions
- Similarly: ForkEDMD-CTR as a forked VOL-PRF extension of EDMD
- Similar parallel work: ButterKnife [ACL+22]

# Are Those All Optimally Secure Constructions?

- Chen et al. [CMP21] analyzed PRFs with two permutation calls
- Only six constructions provided optimal PRF security:
  - SoP, EDM, and EDMD
  - And their variants with the input summed to the output
- Latter variants just add redundancy

$\implies$ We have covered all close-to-optimally secure variants

# Aspects on Provable Security

# Proof Strategy

- We consider a treatment with pairwise independent random permutations
- Can use existing results from Mirror Theory

# Conversion from VOL-PRF to Nonce-based Modes

Table: Comparison of the considered constructions. Security is given for $n$-bit tweaks $T$. (*) The dual variant of FastPRF, i.e., FastPRF-EDM was considered but not proposed by [MN17b].

| Construction | Calls/block $n_r$ | $n_{r_t}$ | $n_{r_b}$ | Output (bits) | PRF Sec. (bits) | Reference |
|---|---|---|---|---|---|---|
| Fixed-input length and fixed-output length | | | | | | |
| FastPRF | – | $1$ | $1$ | $n$ | $n$ | [MN17b] |
| FastPRF-EDM | – | $1$ | $1$ | $n$ | $n$ | [MN17b] (*) |
| ForkPRP2 | – | $1$ | $2$ | $2n$ | $n/2$ | [ALP+19] |
| ForkPRF | – | $1$ | $1$ | $n$ | $n$ | [**This work**] |
| ForkSTH | – | $1$ | $2$ | $n+a$ | $n-a/2$ | [**This work**] |
| Fixed-input length and variable-output length | | | | | | |
| mForkPRP$[r]$ | – | $1$ | $r$ | $rn$ | $n/2$ | [ABPV21] |
| $\widetilde{\text{MFC}}[r]$ | – | $1$ | $r$ | $rn$ | $n$ | [ABPV21] |
| mIFI/ButterKnife | – | $1$ | $r$ | $rn$ | $n-\log_2(r/2)$ | [ACL+22] |
| ForkSTHXORP$[r]$ | – | $1$ | $r$ | $(r-1)n+a$ | $n-a/2-\log_2(r)$ | [**This work**] |
| ForkXORP$[r]$ | – | $1$ | $r$ | $(r-1)n$ | $n$ | [**This work**] |
| ForkEDM-CTR$[r]$ | – | $1$ | $r$ | $rn$ | $n$ | [**This work**] |
| ForkEDMD-CTR$[r]$ | – | $1$ | $r$ | $rn$ | $n$ | [**This work**] |
| STHXORP$[r]$ | $r$ | – | – | $(r-1)n+a$ | $n-a/2-\log_2(r)$ | [**This work**] |

# Conversion from VOL-PRF to Nonce-based Modes

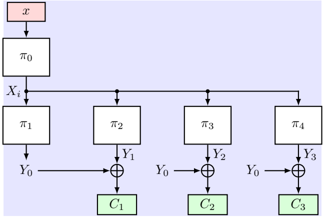
**Theorem 1**

Let $\mathcal{E}[\mathsf{C}[r]_{\boldsymbol{\pi}}]$ be a variable output length PRF instantiated with a function $\mathsf{C}[r]_{\boldsymbol{\pi}}$ set of pairwise independent secret permutations $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_{r+1})$, where $\pi_1, \ldots, \pi_{r+1} \twoheadleftarrow (\mathsf{Perm}(\{0,1\}^n))^{r+1}$. Let $D'$ be an adversary on the PRF security of $\mathsf{C}[r]_{\boldsymbol{\pi}}$. Then, for any distinguisher $D$ on the nE security of $\mathcal{E}[\mathsf{C}[r]_{\boldsymbol{\pi}}]$, it holds that

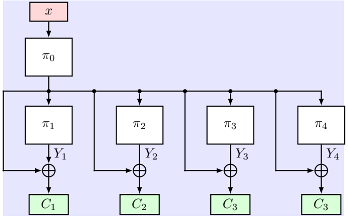
$$\mathbf{Adv}^{\mathsf{nE}}_{\mathcal{E}[\mathsf{C}[r]_{\boldsymbol{\pi}}]}(D) \leq \left\lceil \frac{q}{r} \right\rceil \cdot \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{C}[r]_{\boldsymbol{\pi}}}(D').$$

# Instantiation

# Goal




ForkXORP [This work]




ForkEDMD-CTR [This work] and [ACV+22]

Goal:

- ForkXORP and ForkEDMD-CTR most promising for efficiency
- Find efficient instantiation using round-reduced standardized primitive

Requirements:

- Need pairwise independent permutations
- Can use tweaks
- Need only small tweaks for domains
- Need good tweak-difference diffusion

# ElasticTweak Framework (I)

[CDJ+19, CDJ+21]

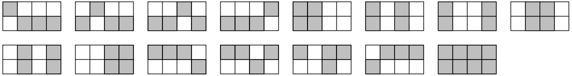
- Chakraborti et al. [CDJ+19, CDJ+21]: ElasticTweak framework
- Expands very small tweaks with code
- For AES: four-bit tweak $\mathbf{T} = (t_0, t_1, t_2, t_3)$ is expanded to eight bits as $(t_4, t_5, t_6, t_7) = \mathbf{J} \cdot \mathbf{T}^\top$:

$$\begin{bmatrix} t_4 \\ t_5 \\ t_6 \\ t_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix}.$$

# ElasticTweak Framework (II)

[CDJ$^+$19, CDJ$^+$21]

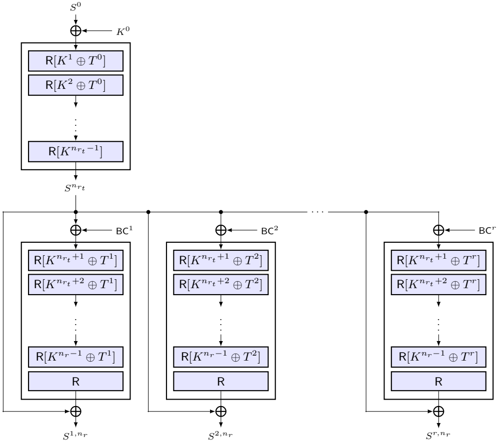
- For AES: 4-bit tweak, lsbs of bytes in top row
- Code is used to generate second row
- Branch number 4: four active bytes (gray)
- Possible tweak-difference patterns:



- $\implies$ at least three active diagonals
- Chakraborti et al. injected tweak only at every second round

# ForkTweAES

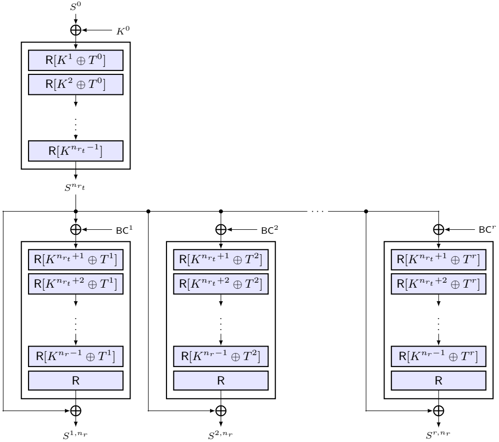
## Settings




Cryptanalysis must consider three settings

- **Setting (1):** Different bottom-permutation branches (distinct branch indices $i$ and $j$, with $i, j \in \{1..15\}$) of the same chunk.
- **Setting (2):** Equal branches $i$ from different chunks.
- **Setting (3):** Different branches $i$ and $j$ from different chunks.

# ForkTweAES




- AES rounds as primitive
- ElasticTweak code $4$-bit tweak expansion for up to $15$ branches
- Use $r_t = 5$ rounds at top (differentials)
- Use $r_b = 7$ rounds at bottom (rectangles, ID, differentials)
- Adopts $n$-bit branch constants $BC^i$ at forking point from ForkAES (inter-branch differentials)
- Tweaks are injected in every round except the final one (enough active S-boxes in rectangle differentials)
- Tweak injected at start of bottom
- More round keys: Iterate AES key schedule further (as in ForkAES)
- Top Tweak is $0$ to avoid tweak injections

# Implementation Results

Table: Performance in cycles per byte for our instantiations with selected number of branches $r$ and up to $16$ chunks with AES-NI, SSE4.1, and AVX2 on Intel i5-1240P.

(a) XORP-AES-$10[r]$.

| | #Chunks of $16(r-1)$ bytes | | | | | | |
|---|---|---|---|---|---|---|---|
| $r$ | 1 | 2 | 3 | 4 | 8 | 12 | 16 |
| 4 | 0.82 | 0.77 | 0.86 | 0.81 | 0.66 | 0.64 | 0.64 |
| 5 | 0.75 | 0.82 | 0.78 | 0.73 | 0.60 | 0.60 | 0.60 |
| 8 | 0.74 | 0.78 | 0.60 | 0.57 | 0.55 | 0.55 | 0.55 |
| 15 | 0.89 | 0.66 | 0.61 | 0.59 | 0.56 | 0.55 | 0.55 |

(b) ForkXORP-AES-5-$7[r]$.

| | #Chunks of $16(r-1)$ bytes | | | | | | |
|---|---|---|---|---|---|---|---|
| $r$ | 1 | 2 | 3 | 4 | 8 | 12 | 16 |
| 4 | 0.91 | 0.83 | 0.88 | 0.81 | 0.64 | 0.62 | 0.62 |
| 5 | 0.81 | 0.81 | 0.80 | 0.70 | 0.55 | 0.54 | 0.54 |
| 8 | 0.82 | 0.68 | 0.60 | 0.49 | 0.45 | 0.45 | 0.45 |
| 15 | 0.64 | 0.49 | 0.45 | 0.43 | 0.41 | 0.40 | 0.40 |

(c) EDMD-CTR-AES-$10$.

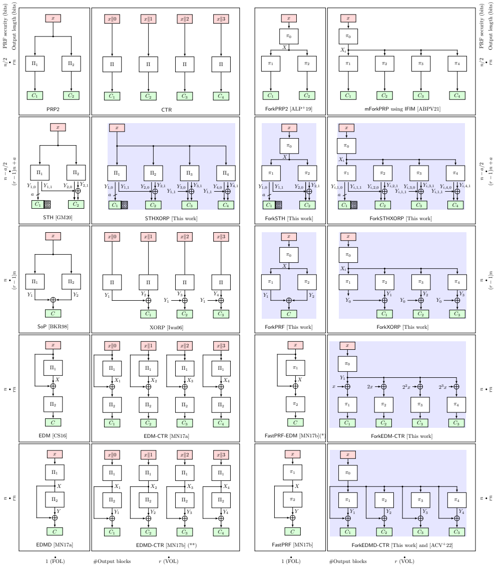
| | #Chunks of $16r$ bytes | | | | | | |
|---|---|---|---|---|---|---|---|
| $r$ | 1 | 2 | 3 | 4 | 8 | 12 | 16 |
| 4 | 1.17 | 1.22 | 1.10 | 0.97 | 0.95 | 0.95 | 0.95 |
| 5 | 1.13 | 1.22 | 1.09 | 1.00 | 0.95 | 0.96 | 0.95 |
| 8 | 1.22 | 0.97 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 |
| 16 | 0.97 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 | 0.95 |

(d) ForkEDMD-CTR-AES-5-$7[r]$.

| | #Chunks of $16r$ bytes | | | | | | |
|---|---|---|---|---|---|---|---|
| $r$ | 1 | 2 | 3 | 4 | 8 | 12 | 16 |
| 4 | 0.71 | 0.75 | 0.66 | 0.62 | 0.49 | 0.47 | 0.47 |
| 5 | 0.62 | 0.67 | 0.63 | 0.54 | 0.45 | 0.44 | 0.43 |
| 8 | 0.73 | 0.65 | 0.54 | 0.46 | 0.44 | 0.43 | 0.43 |
| 15 | 0.58 | 0.47 | 0.42 | 0.42 | 0.41 | 0.41 | 0.39 |

# Conclusion

# Summary




- Spectrum view of the close-to-optimal secure PRFs with at most sums of two permutations
- Organize by
  1. PRF security
  2. output length
  3. forking
- Identified and filled gaps
- Proposed instantiation based on round-reduced AES with tiny tweaks
- We acknowledge the parallel and independent work by Andreeva et al. [ACL+22] on ButterKnife

# Open Aspects

Future work can try to further…

- …increase understanding of our instantiation
- …increase the understanding of such settings
- …find lightweight instantiations from GIFT or SKINNY

Questions?

# References I


Elena Andreeva, Amit Singh Bhati, Bart Preneel, and Damian Vizár.
1, 2, 3, Fork: Counter Mode Variants based on a Generalized Forkcipher.
*IACR Trans. Symmetric Cryptol.*, 2021(3):1–35, 2021.

Elena Andreeva, Benoit Cogliati, Virginie Lallemand, Marine Minier, Antoon Purnal, and Arnab Roy.
Masked Iterate-Fork-Iterate: A new Design Paradigm for Tweakable Expanding Pseudorandom Function.
Cryptology ePrint Archive, Paper 2022/1534, 2022.

Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár.
Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT II*, volume 11922 of *LNCS*, pages 153–182. Springer, 2019.

Mihir Bellare, Joe Kilian, and Phillip Rogaway.
The Security of Cipher Block Chaining.
In Yvo Desmedt, editor, *CRYPTO*, volume 839 of *LNCS*, pages 341–358. Springer, 1994.

Mihir Bellare, Ted Krovetz, and Phillip Rogaway.
Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible.
In Kaisa Nyberg, editor, *EUROCRYPT*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.

Mihir Bellare and Phillip Rogaway.
The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs.
In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *LNCS*, pages 409–426. Springer, 2006.

Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi, and Yu Sasaki.
Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher.
*IACR Cryptol. ePrint Arch.*, 2019:440, 2019.

# References II


Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi, and Yu Sasaki.
Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher.
In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *INDOCRYPT*, volume 13143 of *LNCS*, pages 114–137. Springer, 2021.

Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha.
Proof of mirror theory for a wide range of $\xi _{\max }$.
In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 470–501. Springer, 2023.

Yu Long Chen, Bart Mennink, and Bart Preneel.
Categorization of Faulty Nonce Misuse Resistant Message Authentication.
In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT III*, volume 13092 of *LNCS*, pages 520–550. Springer, 2021.

Donghoon Chang and Mridul Nandi.
A short proof of the PRP/PRF switching lemma.
*IACR Cryptol. ePrint Arch.*, page 78, 2008.

Benoît Cogliati and Yannick Seurin.
EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO I*, volume 9814 of *LNCS*, pages 121–149. Springer, 2016.

Wei Dai, Viet Tung Hoang, and Stefano Tessaro.
Information-Theoretic Indistinguishability via the Chi-Squared Method.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.
Full version at http://eprint.iacr.org/2017/537, version 20170616:190106.

Avijit Dutta, Mridul Nandi, and Abishanka Saha.
Proof of mirror theory for $\xi_{\max} = 2$.
*IEEE Trans. Inf. Theory*, 68(9):6218–6232, 2022.

# References III


Aldo Gunsing and Bart Mennink.
The Summation-Truncation Hybrid: Reusing Discarded Bits for Free.
In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO I*, volume 12170 of *LNCS*, pages 187–217. Springer, 2020.

Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway.
Robust Authenticated-Encryption AEZ and the Problem That It Solves.
In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT (1)*, volume 9056 of *LNCS*, pages 15–44. Springer, 2015.

Chris Hall, David A. Wagner, John Kelsey, and Bruce Schneier.
Building prfs from prps.
In *CRYPTO 1998, Proceedings*, pages 370–389, 1998.

Tetsu Iwata, Bart Mennink, and Damian Vizár.
CENC is Optimally Secure.
*IACR Cryptol. ePrint Arch.*, 2016:1087, 2016.

Tetsu Iwata.
New Blockcipher Modes of Operation with Beyond the Birthday Bound Security.
In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *LNCS*, pages 310–327. Springer, 2006.

Stefan Lucks.
The Sum of PRPs Is a Secure PRF.
In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *LNCS*, pages 470–484. Springer, 2000.

Bart Mennink and Samuel Neves.
Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO III*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.

# References IV

Bart Mennink and Samuel Neves.
Optimal PRFs from Blockcipher Designs.
*IACR Trans. Symmetric Cryptol.*, 2017(3):228–252, 2017.

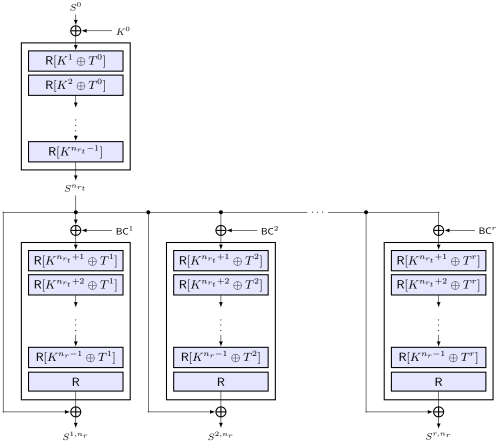
Valérie Nachef, Jacques Patarin, and Emmanuel Volte.
*Feistel Ciphers - Security Proofs and Cryptanalysis.*
Springer, 2017.

Jacques Patarin.
Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography.
*IACR Cryptology ePrint Archive*, 2010:287, 2010.

# Preliminary Cryptanalysis

# ForkTweAES

## Preliminary Cryptanalysis




Preliminary thoughts on

- Differential bounds
- Integrals
- IDs and ZCs
- MitM
- Differential-linear

# Differential bounds

Table: Lower bounds on the number of active S-boxes in small-tweak $\mathrm{AES}$-based TBCs with difference only in the tweak.

(a) Plaintext or tweak active.

| Construction | #Rounds 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Active plaintext or tweak | | | | | | | | | | |
| ForkTweAES | **0** | **4** | **8** | **14** | **18** | **22** | **26** | **30** | **34** | **38** |
| TweAES [CDJ+21] | 0 | 0 | 4 | 15 | 19 | 20 | 27 | 30 | 34 | 40 |
| Kiasu-BC [?] | 0 | 1 | 4 | 8 | 18 | 22 | 25 | 28 | 33 | 38 |
| Active tweak | | | | | | | | | | |
| ForkTweAES | **4** | **11** | **18** | **21** | **25** | **29** | **34** | **38** | **42** | **46** |
| TweAES [CDJ+21] | 4 | 15 | 20 | 20 | 27 | 30 | 34 | 40 | 44 | 50 |
| Kiasu-BC [?] | 1 | 4 | 17 | 23 | 25 | 26 | 29 | 37 | 44 | 50 |

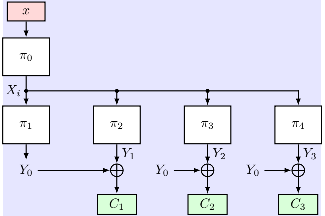
(b) Difference from branch constants.

| Construction | #Rounds 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| ForkTweAES | **14** | **15** | **19** | **23** | **28** | **32** | **36** | **40** | **44** | **48** |
| TweAES [CDJ+21] | 14 | 20 | 21 | 21 | 25 | 35 | 39 | 45 | 48 | 51 |
| Kiasu-BC [?] | 14 | 15 | 18 | 20 | 24 | 32 | 36 | 40 | 43 | 48 |

- We need diffusion in the first few rounds
- Against bommerangs/rectangles

# Proof Results

# ForkXORP



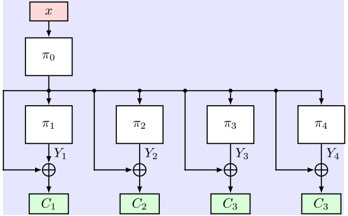

ForkXORP [This work]

**Theorem 2**

Let $r$, $n$, and $q$ be positive integers with $n \geq 30$ and $q \leq 2^n/12(r+1)^2$. Let $\pi_0, \pi_1, \ldots, \pi_r \twoheadleftarrow \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let $D$ be a PRF distinguisher on the construction $\mathsf{ForkXORP}_{\pi_0,\pi_1,\ldots,\pi_r}$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{ForkXORP}[r]}(D) \leq \frac{\binom{q}{r+1}}{2^{nr}}.$$

# ForkEDMD-CTR



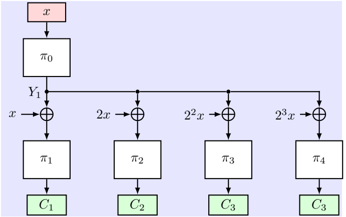

ForkEDMD-CTR [This work] and [ACV+22]

## Theorem 3

Let $r, n$, and $q$ be positive integers with $n \geq 7$ and $q \leq 2^n/12(r+1)^2$ and $\pi_0, \pi_1, \pi_2, \ldots, \pi_r \twoheadleftarrow \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let $D$ be a PRF distinguisher on the construction $\mathsf{ForkEDMD\text{-}CTR}_{\pi_0,\pi_1,\pi_2,\ldots,\pi_r}$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{ForkEDMD\text{-}CTR}[r]}(D) = 0\,.$$

# ForkEDM-CTR



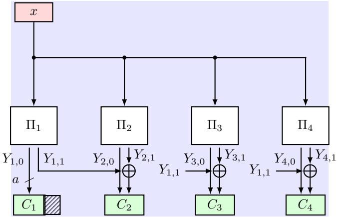

ForkEDM-CTR [This work]

## Theorem 4

Let $n$, $r$, and $q$ be positive integers with $n \geq 30$ and $q \leq 2^n/12(r+1)^2$. Let $\pi_0, \pi_1, \ldots, \pi_r \twoheadleftarrow \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let further $D$ be a PRF distinguisher on the construction $\mathsf{ForkEDM\text{-}CTR}_{\pi_0,\pi_1,\ldots,\pi_r}$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{ForkEDM\text{-}CTR}[r]}(D) \leq \frac{\binom{q}{r+1}}{2^{nr}} .$$

# STHXORP and ForkSTHXORP




STHXORP [This work]

## Theorem 5

Let $r$, $n$, $a$, $b$ and $q$ be positive integers with $r \geq 2$, $a + b = n$, and $q < 2^{b-2}$ and $q \leq 2^n/(2r)$. Let $\Pi_1, \ldots, \Pi_r \twoheadleftarrow \mathsf{Perm}(\{0,1\}^n)$ be independent random permutations. Let $D$ be a PRF distinguisher on the construction $\mathsf{STHXORP}_a[\Pi_1, \Pi_2, \ldots, \Pi_r]$. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{STHXORP}_a[r]}(D) \leq \left(\frac{4}{3}\right)^r \left(\frac{rq}{2^{n-a/3}}\right)^{3/2} + 2^{a-1} \cdot \left(\frac{16rq}{2^n}\right)^{2^{b-2}} + \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{trunc}_a}(rq)\,.$$