Multiforked Iterated Even-Mansour and a Note on the Tightness of IEM Proofs

Elena Andreeva [1] Amit Singh Bhati [2]
Andreas Weninger [1]

[1]TU Wien [2]3MI Labs, KU Leuven

Selected Areas in Cryptography 2025, Toronto, Canada,
13. Aug 2025

Der Wissenschaftsfonds.

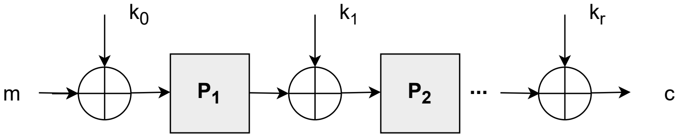
Iterated Even-Mansour (IEM)

many ciphers (e.g. AES):

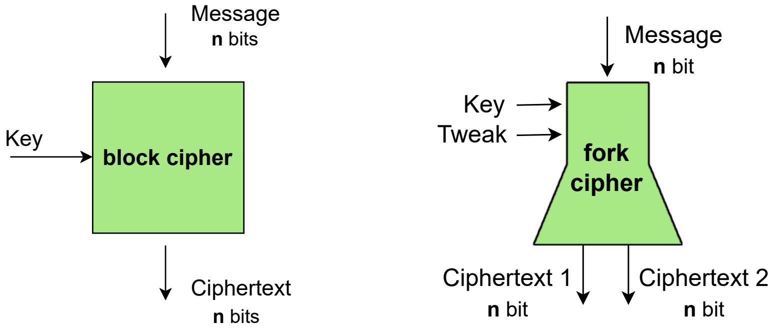
- repeated round function
- key expanded into round keys

IEM:

- public permutations $P_1, \ldots, P_r$
- $k_0, \ldots, k_r$ uniformly random (idealized key schedule)

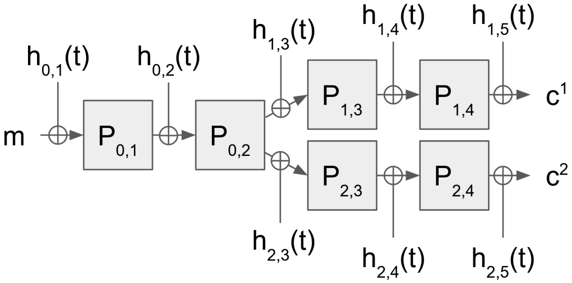


Forkcipher



forkcipher applications: encryption [ABPV21], AEAD [ALP$^+$19], PRG [AW23], KDF [BDA$^+$24], . . .

Forked IEM (Our work)

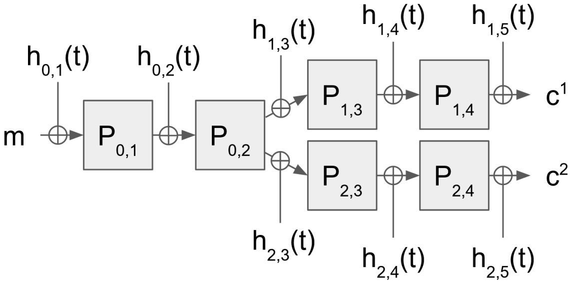


Forked IEM (4 rounds, 2 branches)

Variants

- no tweak: $h_i(\cdot)$ returns round key k_i
- idealized tweakey schedule: $h_i(\cdot) =$ random function

Forked IEM (Existing Variant)



Forked IEM (4 rounds, 2 branches)

Variants

- AXU tweakey schedule [KLL20]: $h_i(\cdot)$ based on AXU hash
  existing proof [KLL20]: only 2 rounds
  $\Rightarrow$ our proof: arbitrary rounds and branches

Security of IEM Variants

Tweakey schedule	IEM/TEM	Forked IEM
no tweaks	$2^{r\,n/(r+1)}$ [HT16]	$\mathbf{2^{r\,n/(r+1)}}$ [our work]
idealized	—	$\mathbf{2^{r\,n/(r+1)}}$ [our work]
AXU (2 rounds)	$2^{r\,n/(r+1)}$ [CLS15]	$2^{r\,n/(r+1)}$ [KLL20]
AXU (unrestricted)	$2^{r\,n/(r+2)}$ [CLS15]	$\mathbf{2^{r\,n/(r+2)}}$ [our work]

Security (in queries). r rounds construction.

Security of IEM Variants

Tweakey schedule	IEM/TEM	Forked IEM
no tweaks	$2^{r\,n/(r+1)}$ [HT16]	$\mathbf{2^{r\,n/(r+1)}}$ [our work]
idealized	—	$\mathbf{2^{r\,n/(r+1)}}$ [our work]
AXU (2 rounds)	$2^{r\,n/(r+1)}$ [CLS15]	$2^{r\,n/(r+1)}$ [KLL20]
AXU (unrestricted)	$2^{r\,n/(r+2)}$ [CLS15]	$\mathbf{2^{r\,n/(r+2)}}$ [our work]

Security (in queries). r rounds construction.

More than 2 branches?

- b branches (AXU schedule, r rounds): $\mathbf{\frac{1}{b^2} 2^{r\,n/(r+2)}}$ queries

Proof Approach

- no tweaks: Expectation method [HT16]
  - represent attacker knowledge as graph & simplify graph
  - at the core: bound difference between 1 forked and 2 non-forked instances

Proof Approach

- no tweaks: Expectation method [HT16]
  - represent attacker knowledge as graph & simplify graph
  - at the core: bound difference between 1 forked and 2 non-forked instances
- idealized tweakey schedule: Expectation method [HT16]
  - expectation method also gives multi-user security (independent keys per user)
  - multi-user no tweak $\approx$ single-user ideal tweakey schedule

Proof Approach

- no tweaks: Expectation method [HT16]
  - represent attacker knowledge as graph & simplify graph
  - at the core: bound difference between 1 forked and 2 non-forked instances
- idealized tweakey schedule: Expectation method [HT16]
  - expectation method also gives multi-user security (independent keys per user)
  - multi-user no tweak $\approx$ single-user ideal tweakey schedule
- AXU tweak: Coupling [CLS15]
  - extending existing proof for non-forked to arbitrary many branches

Tightness of IEM Proofs

- tightness: security proof + attack (practical efficiency!)
- unproven attack [BKL+12] used to argue tightness (directly or indirectly) [CLS15, BKL+12, LPS12, Ste12, CS14]

Tightness of IEM Proofs

- tightness: security proof + attack (practical efficiency!)
- unproven attack [BKL+12] used to argue tightness (directly or indirectly) [CLS15, BKL+12, LPS12, Ste12, CS14]
  - attack trivially correct? No!
  - **we prove:** success probability $\leq \frac{1}{2^{n-1}}$
- with more queries still no proof

Tightness of IEM Proofs

- tightness: security proof + attack (practical efficiency!)
- unproven attack [BKL+12] used to argue tightness (directly or indirectly) [CLS15, BKL+12, LPS12, Ste12, CS14]
  - attack trivially correct? No!
  - **we prove:** success probability $\leq \frac{1}{2^{n-1}}$
- with more queries still no proof

We show: attack by Gaži [Gaž13] applies to IEM
$\Rightarrow$ tightness results remain

Conclusion

Main result: Forked IEM security

- arbitrary number of rounds
- 3 variants for tweakey schedule (no tweak / idealized / AXU)
- security of forked IEM $\approx$ non-forked IEM (with similar tweakey schedule)
- generalization to arbitrary number of branches for AXU variant

Note on tightness

- instantiation of Gaži [Gaž13] attack

Thank you!

andreas.weninger@tuwien.ac.at

References I

[ABPV21] Elena Andreeva, Amit Singh Bhati, Bart Preneel, and Damian Vizár.
1, 2, 3, fork: Counter mode variants based on a generalized forkcipher.
IACR Trans. Symm. Cryptol., 2021(3):1–35, 2021.

[ALP+19] 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 2019, Part II*, volume 11922 of *LNCS*, pages 153–182, Kobe, Japan, December 8–12, 2019. Springer, Heidelberg, Germany.

References II

[AW23] Elena Andreeva and Andreas Weninger.
A forkcipher-based pseudo-random number generator.
In Mehdi Tibouchi and XiaoFeng Wang, editors, *Applied Cryptography and Network Security*, pages 3–31, Cham, 2023. Springer Nature Switzerland.

[BDA+24] Amit Singh Bhati, Antonín Dufka, Elena Andreeva, Arnab Roy, and Bart Preneel.
Skye: An Expanding PRF based Fast KDF and its Applications.
In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 1082–1098, 2024.

References III

[BKL$^+$12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser.
Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract).
In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 45–62, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany.

References IV

[CLS15] Benoit Cogliati, Rodolphe Lampe, and Yannick Seurin.
Tweaking Even-Mansour ciphers.
In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 189–208, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[CS14] Shan Chen and John P. Steinberger.
Tight security bounds for key-alternating ciphers.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

References V

[Gaž13] Peter Gaži.
Plain versus randomized cascading-based key-length extension for block ciphers.
In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 551–570, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[HT16] Viet Tung Hoang and Stefano Tessaro.
Key-alternating ciphers and key-length extension: Exact bounds and multi-user security.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 3–32, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

References VI

[KLL20] Hwigyeom Kim, Yeongmin Lee, and Jooyoung Lee.
Forking tweakable Even-Mansour ciphers.
IACR Trans. Symm. Cryptol., 2020(4):71–87, 2020.

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin.
An asymptotically tight security analysis of the iterated Even-Mansour cipher.
In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 278–295, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

[Ste12] John Steinberger.
Improved security bounds for key-alternating ciphers via hellinger distance.
Cryptology ePrint Archive, Report 2012/481, 2012.
`https://eprint.iacr.org/2012/481`.