On Large Tweaks in Tweakable Even-Mansour with Linear Tweak and Key Mixing

Benoît Cogliati [1] Jordan Ethan [2] Ashwin Jha [2] Soumya Kanti Saha [3]

[1]Thales DIS France SAS, Meudon, France

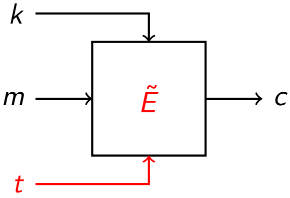
[2]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

[3]Indian Institute of Science, Bengaluru, India

March 26, 2024

Table of Contents

Tweakable Block Cipher (TBC)

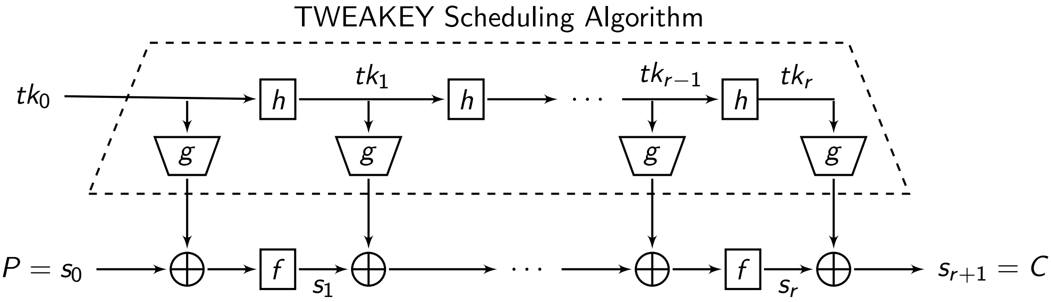


- Tweak t bring variability to BC & publicly controlled.
- For each (k, t), $m \mapsto \tilde{E}(k, t, m)$ is a permutation.
- Wide range of applications:
  - AEs [LRW11; Rog04; PS16],
  - MACs [Nai15; Iwa+17; CLS17; GLN19; CLL22],
  - Other security goals [Min09; RZ11; JN18; BLN18].

Designing TBC

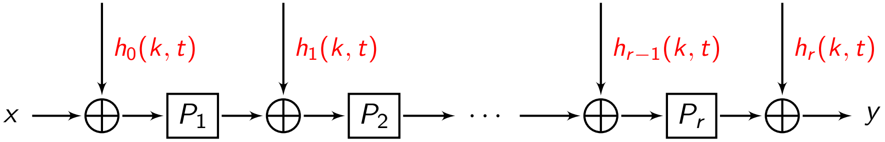
- Two ways of designing TBCs:
  - From a block cipher (in black box) $\rightarrow$ could be non efficient or BB secure.
  - From lower level primitive - permutations
- In our work we concentrate on designing it from permutations.

TWEAKEY Framework - Jean et al. [JNP14]



- Tweak and key is seen as unified (tweakey) and the schedule is linear.
- High level design follows Tweakable Even-Mansour.
- No provable security analysis.

Tweakable Even Mansour



TEM: $P_1, \ldots, P_r$ and k are random and independent.

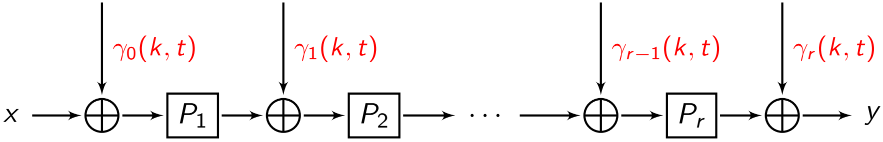
- r even & h XOR universal $\rightarrow$ TEM construction [CLS15] (secure up to $2^{(r/(r+2))n}$ queries).
- $r = 4$ & h linear $\rightarrow$ TEML construction [CS15] (secure up to $2^{2n/3}$ queries).
- Drawbacks: deviates from TWEAKEY framework ($r > 4$) & no support for large tweaks.

Our Contributions

1. TEM with $2r$ rounds ($2r$-TEML) αn-bit tweak where the schedule follows a property (α-bijective) is IND-CCA secure up to $2^{((r-\alpha)/r)n}$ queries (using the coupling technique).
2. TEM with rn-bit key (tweakey) and r-bijective key schedule in the chosen key model:
   - for $r+2$ rounds $\rightarrow$ there is an attack,
   - for $r+3$ rounds we prove the security.

Table of Contents

r-TEML with Tweak and Key Mixing



TEM^{γ}: $P_1, \ldots, P_r$ and k are random and independent.

- We require $\gamma = (\gamma_0, \ldots, \gamma_r)$ to all be linear.
- For $r = 4$ rounds, n-bit tweak and $2n$-bit key $\rightarrow$ TEML construction [CS15].
- We want to minimize r for αn-bit tweak, can we have $r \leq \alpha$?
- Write $\gamma_i(k, t) = \lambda_i(k) \oplus \delta_i(t)$.
- If $r \leq \alpha$ & simple counting reasoning $\rightarrow$ collision attack.
- Is the condition $r > \alpha$ enough for security?

s-Bijective Tweakey Schedules

- For $2n$-bit tweak and any r, choose $\delta_i(t_1, t_2) = t_1, \delta_r(t_1, t_2) = t_2$ for $i \leq r - 1 \rightarrow$ similar attack.
- Jean et al. [JNP14] had similar observation $\rightarrow$ they require one-to-one relation between (k, t) to subsets of tweakey $(\gamma_i(k, t) : i \in I)$.

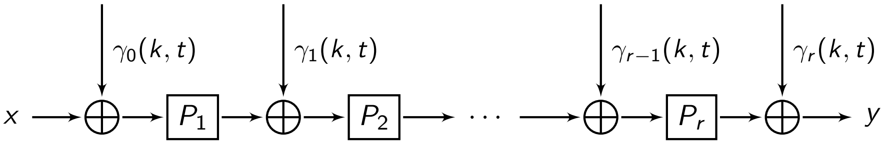
Definition (s-bijectivity)

A s-bijective schedule $\gamma := (\gamma_0, \ldots, \gamma_r)$ is a tuple of $r \geq s$ linear functions $\gamma_i : \{0, 1\}^{sn} \rightarrow \{0, 1\}^n$ such that for any contiguous s-subtuple, $\gamma' = (\gamma_i, \ldots, \gamma_{i+s-1})$ of γ, the mapping

$$(k, t) \mapsto (\gamma_i(k, t), \ldots, \gamma_{i+s-1}(k, t))$$

is a bijection.

r-$TEML$ Construction



r-$TEML$: $P_1, \ldots, P_r$ and k are random and independent.

- For random and independent $\mathbf{K} = (k_0, \ldots, k_r)$ - define $\gamma_i(t) = k_i \oplus \delta_i(t)$.
- We prove that for $r > \alpha$, any α-bijective tweak schedule δ, it achieves IND-CCA security up to $\mathcal{O}(N^{\frac{r-2\alpha}{r}})$, where $N = 2^n$.

Table of Contents

High-Level Proof

Following the proofs of [LS14; CLS15]:

- **Step 1:** Divide the computation to two parts,

$$2r\text{-TEML}_{\mathbf{k}}^{\delta,\mathbf{P}}(t,x) = \left(r\text{-TEML}_{\mathbf{k}_2}^{\delta^2 \mathbf{P}_2}\right)^{-1}\left(t, r\text{-TEML}_{\mathbf{k}_1}^{\delta^1,\mathbf{P}_1}(t,x) \oplus \delta_{r'}(t)\right).$$

- **Step 2:** Upper bound $||\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_P} - \mu_{\mathbf{t}}^*||$ where

$$\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_P} \sim TEML_{\mathbf{k}}^{\mathbf{P}}(\mathbf{t},\mathbf{x}) : \mathbf{P} \vdash \mathcal{Q}_P, \quad \mu_{\mathbf{t}}^* \sim U_{\mathbf{t}}.$$

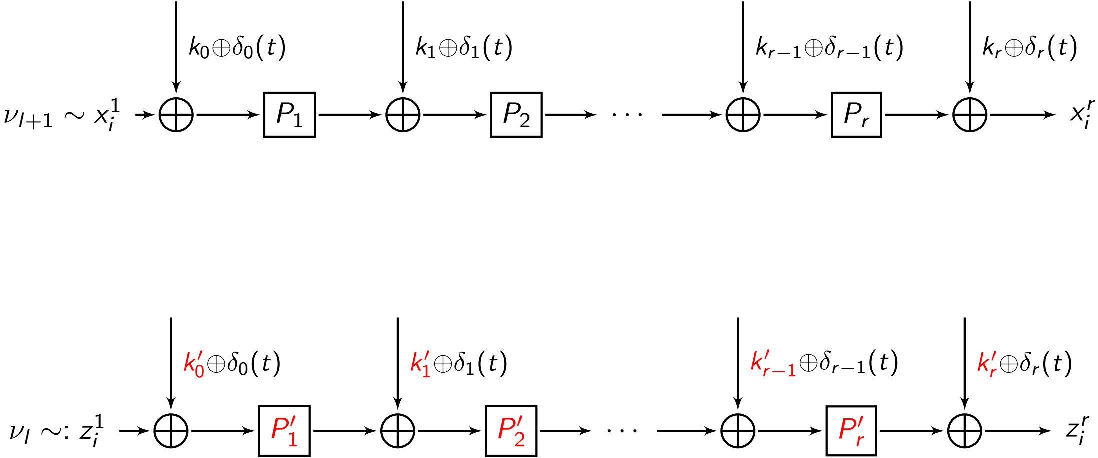
- **Step 3:** Simplify:

$$||\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_P} - \mu_{\mathbf{t}}^*|| \leq \sum_{l=0}^{q_c-1} ||\nu_{l+1} - \nu_l||$$

  where $\nu_l = (t_1, x_1), \ldots, (t_l, x_l), (t_{l+1}, {\color{red}z_{l+1}}), \ldots, (t_{q_c}, {\color{red}z_{q_c}})$

- **Main Goal:** for $l \in [0, q_c]$ upper bound $||\nu_{l+1} - \nu_l||$ - hybrid distances.

Proof Of Hybrid-Distances - Coupling



We want to couple: $P'_j\,(z_i^j \oplus k'_j \oplus \delta_j(t)) := P_j(x_i^j \oplus k_j \oplus \delta_j(t))$.

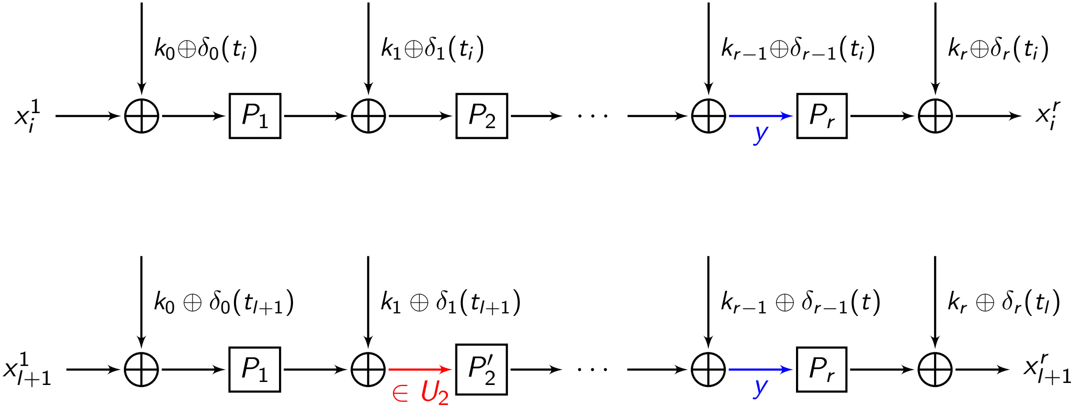
Proof Of Hybrid-Distances - Coupling

- It is enough to consider queries $i \leq l + 1$.
- From the coupling technique we get,

$$||\nu_{l+1} - \nu_l|| \leq \Pr(z_j^r \neq x_i^r : j \leq l + 1) \leq \Pr(z_{l+1}^r \neq x_{l+1}^r)$$

- The novelty of our approach lies in how to upper bound $\Pr(z_{l+1}^r \neq x_{l+1}^r)$ - coupling failure event.

Proof Of Hybrid-Distances - Coupling Failure



$YP_j = (y_{l+1}^j \in U_j)$ resp. WP_j (primitive collision with prob. $\leq q_p/N$),

$YY_j = \left(\exists i \in [1, r] : y_{l+1}^j = y_i^j\right)$ resp. WW_j (internal collision).

Proof Of Hybrid-Distances - Internal Collision

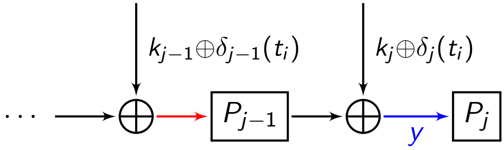
- There exists i: $y^j_{l+1} = y^j_i \to x^{j-1}_{l+1} \oplus x^{j-1}_i = h(t_i, t_{l+1}, k_j)$.
- In previous constructions,

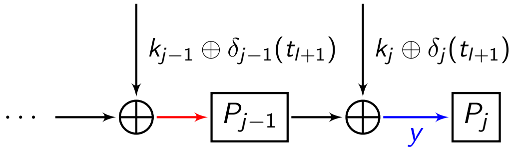
$$h(t_i, t_{l+1}, k_j) = \mathcal{H}_{k_j}(t_i) \oplus \mathcal{H}_{k_j}(t_{l+1})$$

  where $\mathcal{H}_{k_j}$ is $AXU \to h(t_i, t_{l+1}, k_j) \neq 0$ with very high probability.
- In our construction the key cancels out so,

$$h(t_i, t_{l+1}, k_j) = \delta_j(t_i \oplus t_{l+1}).$$

Proof Of Hybrid-Distances - Internal Collision





- $\delta_j(t_i \oplus t_{l+1}) = 0 \rightarrow$ cannot bound! (because of α-bijectivity happens $\leq \alpha - 1$).
- Otherwise, if inputs of P_{j-1} are not fresh $\rightarrow$ look at rounds $j' < j$.

Proof Of Hybrid-Distances - Activity Pattern

- Previous works consider the failure at each round independently.
- In our work, we can consider the full event of failing at some round together.
- The rest of the proof can be completed by analyzing each sub-event + probability chain rule.

Example: Partial Chain Probability Computation

$$
\begin{array}{c}
y^{j}_{l+1} \xleftarrow{\;q_p/N\;} {\color{blue}y^{j-1}_{l+1}} \xleftarrow{\;q_p/N\;} \cdots \xleftarrow{\;q_p/N\;} {\color{blue}y^{j'+1}_{l+1}} \longleftarrow y^{j'}_{l+1} \\
\Big| \\
y^{j}_{i} \xrightarrow{\;1\;} y^{j-1}_{i} \xrightarrow{\;1\;} \cdots \xrightarrow{\;1\;} y^{j'+1}_{i} \xrightarrow{\;2/N\;} {\color{red}y^{j'}_{i}}
\end{array}
$$

WLOG: $y^{j'}_{l+1} \in U_j$ and ${\color{red}y^{j'}_i \notin U_j}$.

- $y^{s}_{l+1} = x^{s-1}_{l+1} \oplus k_s \oplus \delta_s(t_{l+1}) \in U_j$ - randomness over the key k_s.
- $P_{j'}(y^{j'}_{l+1}) \oplus P_{j'}(y^{j'}_i) = x^{j'}_{l+1} \oplus x^{j'}_i = \delta_{j'+1}(t_{l+1} \oplus t_i)$. - randomness over permutation $P_{j'}$.
- Probability $\leq (2q_p/N)^s$ where s is the chain length.

Table of Contents

Conclusions

- For $2r$ rounds and αn-bit tweak we achieve IND-CCA security up to $2^{((r-\alpha)/r)n}$ queries.
- Coupling is not tight $\rightarrow$ We conjecture the same security can be achieved for less rounds.
- Activity pattern/Chains idea can maybe be deployed for other security proofs.
- In chosen key setting $\rightarrow$ $r+3$ rounds are sufficient and necessary for TEML with rn-bit key (tweakey) and r-bijective key (tweakey) schedule.

End

Thank You!

References I

[Bao+20] Zhenzhen Bao et al. "TNT: How to Tweak a Block Cipher". In: *Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part II*. Lecture Notes in Computer Science. 2020, pp. 641–673.

[BLN18] Ritam Bhaumik, Eik List, and Mridul Nandi. "ZCZ - Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls". In: *Advances in Cryptology - ASIACRYPT 2018, Proceedings, Part I*. 2018, pp. 336–366.

[CLL22] Wonseok Choi, Jooyoung Lee, and Yeongmin Lee. "Building PRFs from TPRPs: Beyond the Block and the Tweak Length Bounds". In: *IACR Cryptol. ePrint Arch.* (2022), p. 918.

[CLS15] Benoit Cogliati, Rodolphe Lampe, and Yannick Seurin. "Tweaking Even-Mansour Ciphers". In: *Advances in Cryptology - CRYPTO 2015, Proceedings, Part I*. 2015, pp. 189–208.

References II

[CLS17] Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. "New Constructions of MACs from (Tweakable) Block Ciphers". In: *IACR Trans. Symmetric Cryptol.* 2017.2 (2017), pp. 27–58.

[CS08] Debrup Chakraborty and Palash Sarkar. "A General Construction of Tweakable Block Ciphers and Different Modes of Operations". In: *IEEE Trans. Information Theory* 54.5 (2008), pp. 1991–2006.

[CS14] Shan Chen and John P. Steinberger. "Tight Security Bounds for Key-Alternating Ciphers". In: *Advances in Cryptology - EUROCRYPT 2014, Proceedings*. 2014, pp. 327–350.

[CS15] Benoît Cogliati and Yannick Seurin. "Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing". In: *Advances in Cryptology - ASIACRYPT 2015, Proceedings, Part II*. Ed. by Tetsu Iwata and Jung Hee Cheon. 2015, pp. 134–158.

References III

[GLN19] Tony Grochow, Eik List, and Mridul Nandi. "DoveMAC: A TBC-based PRF with Smaller State, Full Security, and High Rate". In: *IACR Trans. Symmetric Cryptol.* 2019.3 (2019), pp. 43–80.

[Gra+16] Robert Granger et al. "Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption". In: *Advances in Cryptology - EUROCRYPT 2016, Proceedings, Part I*. 2016, pp. 263–293.

[Iwa+17] Tetsu Iwata et al. "ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication". In: *Advances in Cryptology - CRYPTO 2017, Proceedings, Part III*. 2017, pp. 34–65.

[Jha+17] Ashwin Jha et al. "XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing". In: *Progress in Cryptology - LATINCRYPT 2017, Revised Selected Papers*. 2017, pp. 207–227.

References IV

[JN18] Ashwin Jha and Mridul Nandi. "On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers". In: *Cryptography and Communications* 10.5 (2018), pp. 731–753.

[JN20] Ashwin Jha and Mridul Nandi. "Tight Security of Cascaded LRW2". In: *J. Cryptol.* 33.3 (2020), pp. 1272–1317.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. "Tweaks and Keys for Block Ciphers: The TWEAKEY Framework". In: *Advances in Cryptology - ASIACRYPT 2014, Proceedings, Part II*. 2014, pp. 274–288.

[LL18] ByeongHak Lee and Jooyoung Lee. "Tweakable Block Ciphers Secure Beyond the Birthday Bound in the Ideal Cipher Model". In: *Advances in Cryptology - ASIACRYPT 2018, Proceedings, Part I*. 2018, pp. 305–335.

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. "An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher". In: *Advances in Cryptology - ASIACRYPT 2012, Proceedings*. 2012, pp. 278–295.

[LRW11] Moses Liskov, Ronald L. Rivest, and David A. Wagner. "Tweakable Block Ciphers". In: *J. Crypto.* 24.3 (2011), pp. 588–613.

[LS13] Rodolphe Lampe and Yannick Seurin. "Tweakable Blockciphers with Asymptotically Optimal Security". In: *Fast Software Encryption - FSE 2013, Revised Selected Papers*. 2013, pp. 133–151.

[LS14] Rodolphe Lampe and Yannick Seurin. "Security Analysis of Key-Alternating Feistel Ciphers". In: *Fast Software Encryption - FSE 2014, Revised Selected Papers*. 2014, pp. 243–264.

References VI

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. "Tweakable Blockciphers with Beyond Birthday-Bound Security". In: *Advances in Cryptology - CRYPTO 2012, Proceedings*. 2012, pp. 14–30.

[Men15a] Bart Mennink. "Optimally Secure Tweakable Blockciphers". In: *Fast Software Encryption - FSE 2015, Revised Selected Papers*. 2015, pp. 428–448.

[Men15b] Bart Mennink. "Optimally Secure Tweakable Blockciphers". In: *IACR Cryptology ePrint Archive* 2015 (2015), p. 363.

[Men18] Bart Mennink. "Towards Tight Security of Cascaded LRW2". In: *Theory of Cryptography - TCC 2018, Proceedings, Part II*. 2018, pp. 192–222.

[Min06] Kazuhiko Minematsu. "Improved Security Analysis of XEX and LRW Modes". In: *Selected Areas in Cryptography - SAC 2006, Revised Selected Papers*. 2006, pp. 96–113.

References VII

[Min09] Kazuhiko Minematsu. "Beyond-Birthday-Bound Security Based on Tweakable Block Cipher". In: *Fast Software Encryption - FSE 2009, Revised Selected Papers*. 2009, pp. 308–326.

[Nai15] Yusuke Naito. "Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher". In: *Provable Security - ProvSec 2015, Proceedings*. 2015, pp. 167–182.

[PS16] Thomas Peyrin and Yannick Seurin. "Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers". In: *Advances in Cryptology - CRYPTO 2016, Proceedings, Part I*. 2016, pp. 33–63.

[Rog04] Phillip Rogaway. "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC". In: *Advances in Cryptology - ASIACRYPT 2004, Proceedings*. 2004, pp. 16–31.

[RZ11] Phillip Rogaway and Haibin Zhang. "Online Ciphers from Tweakable Blockciphers". In: *Topics in Cryptology - CT-RSA 2011, Proceedings*. 2011, pp. 237–249.