# TNT: How to Tweak a Block Cipher

Zhenzhen Bao    Chun Guo    Jian Guo    Ling Song

EUROCRYPT 2020 – May 13, 2020

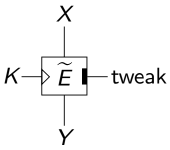
# Outline

Background: Tweakable Blockciphers (TBCs)

Our Contribution: Hybrid Approach – TNT Mode and TNT-AES

# Background - Tweakable Blockciphers (TBCs)

- Tweakable Blockcipher (TBC): a blockcipher with an additional input – the *tweak*.



- Why TBC? – Multiple independent blockciphers for modes of operation.

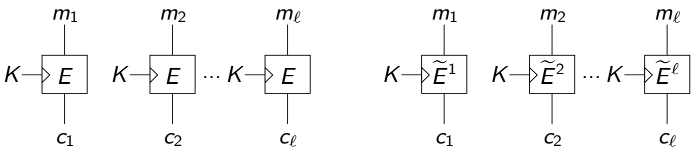


**Figure:** ECB using a TBC (the core of ΘCB3)

# Background - Beyond-Birthday-Bound (BBB) Security

Birthday-bound security $2^{n/2}$: consequences

- the mode (TBC mode, encryption mode, etc.) is secure only when the number of processed data blocks is less than $2^{n/2}$;
- 64-bit legacy blockciphers 3DES, $n = 64$: less than $2^{32}$ data blocks, practically vulnerable [BL16];
- 128-bit blockciphers AES: less data that can be securely processed, more frequent key update [GL17].

Hence, the needs of modes providing Beyond-Birthday-Bound (BBB) security are emerging.

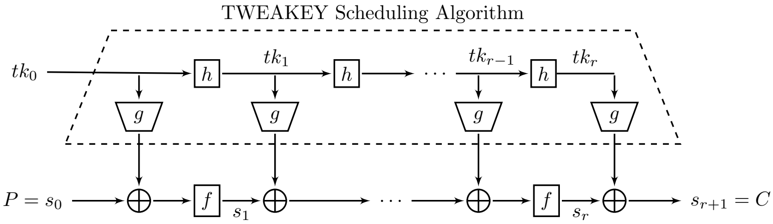
# Modular Approach: TBCs from Block Ciphers

TBCs from modes of operation

- Better understanding of the security: we know in clear that *when* it is insecure and *why* it is insecure.
- Usually less efficient than dedicated algorithms.
- Existing modes:
  - ⋆ Birthday-bound: LRW1, LRW2, XEX, $\widetilde{F}[1]$
  - ⋆ BBB: cascaded LRW2 (CLRW2), $\widetilde{F}[2]$, $\widetilde{E1}, \ldots, \widetilde{E32}$, XHX, XHX2

# Dedicated TBCs: Development

- Early design: Mercy [Cro00]
- Tweakey framework [JNP14b]: Deoxys-BC [Jea+14], SKINNY [Bei+16b], Kiasu [JNP14a]



- Security guarantees come from comprehensive cryptanalysis.
- Simpler retweaking?

# Outline

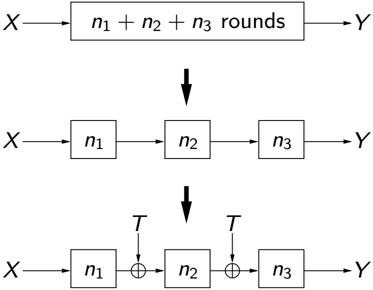
Background: Tweakable Blockciphers (TBCs)

Our Contribution: Hybrid Approach – TNT Mode and TNT-AES

# New Approach to Dedicated TBCs

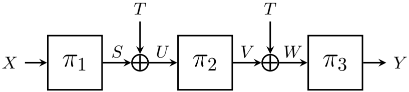
Tweak-aNd-Tweak: a new approach to reliable dedicated TBCs

1. Cut an iterative blockcipher into 3 chunks
2. XOR the tweak at the two cutting points



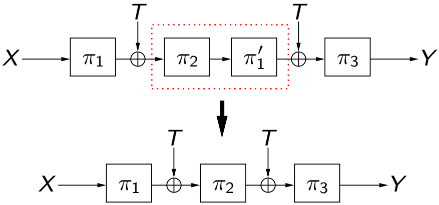
# New Approach to Dedicated TBCs

1. Cut a blockcipher into 3 chunks & add the tweak twice.
2. The underlying mode: Tweak-aNd-Tweak (TNT)



# New Approach to Dedicated TBCs

1. Cut a blockcipher into 3 chunks & add the tweak twice.
2. The underlying mode: Tweak-aNd-Tweak (TNT)
   Cascaded LRW1 or TNT:



- ⋆ LRW1 is only CPA secure up to birthday $2^{n/2}$ queries;
- ⋆ *Is* TNT *secure up to beyond-birthday* $2^{2n/3}$ *queries?*

# New Approach to Dedicated TBCs

1. Cut a blockcipher into 3 chunks & add the tweak twice.
2. The underlying mode: Tweak-aNd-Tweak (TNT)
   - ⋆ Security $2^{2n/3}$ goes beyond the birthday bound $2^{n/2}$
   - ⋆ Proved via the $\chi^2$ method [DHT17]:

# New Approach to Dedicated TBCs

1. Cut a blockcipher into 3 chunks & add the tweak twice.
2. The underlying mode: Tweak-aNd-Tweak (TNT)
   - ⋆ Security $2^{2n/3}$ goes beyond the birthday bound $2^{n/2}$
   - ⋆ Proved via the $\chi^2$ method [DHT17]:

Our main intermediate result: Given $\ell - 1$ tuples of queries and responses $Q_{\ell-1} = (T_1, X_1, Y_1), \ldots, (T_{\ell-1}, X_{\ell-1}, Y_{\ell-1})$, two conditional probabilities are sufficiently close:

$$\left| \Pr[\mathsf{TNT}(T_\ell, X_\ell) = Y_\ell \mid Q_{\ell-1}] - \Pr[\widetilde{\Pi}(T_\ell, X_\ell) = Y_\ell \mid Q_{\ell-1}] \right| \le O\Big(\frac{\ell}{2^{2n}}\Big).$$

*Then by the core lemma of $\chi^2$ method: get the final bound on the indistinguishability: When $D$ makes $q$ queries (including forward and backward ones) to $\mathsf{TNT}^{\pi_1,\pi_2,\pi_3}$ or $\widetilde{\Pi}$, it holds*

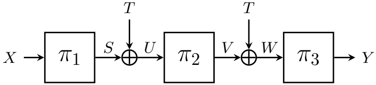
$$\left| \Pr[D^{\mathsf{TNT}^{\pi_1,\pi_2,\pi_3}} = 1] - \Pr[D^{\widetilde{\Pi}} = 1] \right| \le \sqrt{q \times O\Big(\frac{q^2}{2^{2n}}\Big)} = O\Big(\frac{q^{1.5}}{2^n}\Big)$$

# Mode-level Comparison

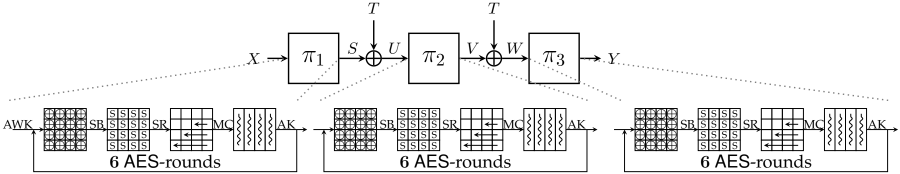
| | #T | #cost | AXU? | tdk | security ($\log_2$) | |
|---|---|---|---|---|---|---|
| LRW1 | $n$ | 2 SPRPs | no | no | $n/2$ | [LRW02] |
| XEX | $n$ | 1 SPRP | yes | no | $n/2$ | [Rog04] |
| LRW2 | * | 1 SPRP | yes | no | $n/2$ | [LRW02] |
| $\mathrm{CLRW2}_2$ | * | 2 SPRPs | yes | no | $3n/4$ | [Men18; JN19] |
| $\mathrm{CLRW2}_r$ | * | $r$ SPRPs | yes | no | $\frac{rn}{r+2}$ | [LS14] |
| Min | $t$ | 2 SPRPs | no | yes | $\max\{n/2, n-t\}$ | [Min09] |
| $\widetilde{F}[1]$ | $n$ | 1 IC | no | yes | $2n/3$ | [Men15] |
| $\widetilde{F}[2]$ | $n$ | 2 ICs | no | yes | $n$ | [Men15] |
| $\widetilde{E1}, \ldots, \widetilde{E32}$ | $n$ | 2 ICs | no | yes | $n$ | [Wan+16] |
| XHX | * | 1 IC | yes | yes | $n$ | [Jha+17] |
| XHX2 | * | 2 ICs | yes | yes | $4n/3$ | [LL18] |
| TNT | $n$ | 3 SPRPs | *no* | no | $2n/3$ | |

# New Approach to Dedicated TBCs

1. The framework TNT: TBC-mode has **BBB security** $2^{2n/3}$



2. AES-based instantiation TNT-AES:



Partially inherited from TNT – the most simple BBB-secure tweaking method & AES – both strong and efficient blockcipher, TNT-AES has

- ⋆ **security with provable and cryptanalysis support** ("prove-then-prune" [HKR15])
- ⋆ **competitive performance in the retweaking scenario**

Thanks for your attention!

# References I

[BL16] Karthikeyan Bhargavan and Gaëtan Leurent. “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. 2016, pp. 456–467. DOI: 10.1145/2976749.2978423. URL: https://doi.org/10.1145/2976749.2978423.

[GL17] Shay Gueron and Yehuda Lindell. “Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 1019–1036. ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3133992. URL: https://doi.org/10.1145/3133956.3133992.

[Cro00] Paul Crowley. “Mercy: A Fast Large Block Cipher for Disk Sector Encryption”. In: *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*. 2000, pp. 49–63. DOI: 10.1007/3-540-44706-7_4. URL: https://doi.org/10.1007/3-540-44706-7_4.

[JNP14b] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. “Tweaks and Keys for Block Ciphers: The TWEAKEY Framework”. In: *Advances in Cryptology – ASIACRYPT 2014, Part II*. Ed. by Palash Sarkar and Tetsu Iwata. Vol. 8874. LNCS. Kaoshiung, Taiwan, R.O.C.: Springer, Heidelberg, Germany, 2014, pp. 274–288. DOI: 10.1007/978-3-662-45608-8_15.

[Jea+14] Jérémy Jean et al. *Deoxys-II*. Finalist of CAESAR compeition, https://competitions.cr.yp.to/caesar-submissions.html. 2014.

[Bei+16b] Christof Beierle et al. “The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS”. In: *Advances in Cryptology – CRYPTO 2016, Part II*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9815. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2016, pp. 123–153. DOI: 10.1007/978-3-662-53008-5_5.

[JNP14a] Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. *KIASU v1*. Additional first-round candidates of CAESAR compeition, https://competitions.cr.yp.to/caesar-submissions.html. 2014.

# References II

[DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. “Information-Theoretic Indistinguishability via the Chi-Squared Method”. In: *Advances in Cryptology – CRYPTO 2017, Part III*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10403. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2017, pp. 497–523. DOI: 10.1007/978-3-319-63697-9_17.

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. “Tweakable Block Ciphers”. In: *Advances in Cryptology – CRYPTO 2002*. Ed. by Moti Yung. Vol. 2442. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2002, pp. 31–46. DOI: 10.1007/3-540-45708-9_3.

[Rog04] Phillip Rogaway. “Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC”. In: *Advances in Cryptology – ASIACRYPT 2004*. Ed. by Pil Joong Lee. Vol. 3329. LNCS. Jeju Island, Korea: Springer, Heidelberg, Germany, 2004, pp. 16–31. DOI: 10.1007/978-3-540-30539-2_2.

[Men18] Bart Mennink. “Towards Tight Security of Cascaded LRW2”. In: *TCC 2018: 16th Theory of Cryptography Conference, Part II*. Ed. by Amos Beimel and Stefan Dziembowski. Vol. 11240. LNCS. Panaji, India: Springer, Heidelberg, Germany, 2018, pp. 192–222. DOI: 10.1007/978-3-030-03810-6_8.

[JN19] Ashwin Jha and Mridul Nandi. *Tight Security of Cascaded LRW2*. Cryptology ePrint Archive, Report 2019/1495. https://eprint.iacr.org/2019/1495. 2019.

[LS14] Rodolphe Lampe and Yannick Seurin. “Tweakable Blockciphers with Asymptotically Optimal Security”. In: *Fast Software Encryption – FSE 2013*. Ed. by Shiho Moriai. Vol. 8424. LNCS. Singapore: Springer, Heidelberg, Germany, 2014, pp. 133–151. DOI: 10.1007/978-3-662-43933-3_8.

[Min09] Kazuhiko Minematsu. “Beyond-Birthday-Bound Security Based on Tweakable Block Cipher”. In: *Fast Software Encryption – FSE 2009*. Ed. by Orr Dunkelman. Vol. 5665. LNCS. Leuven, Belgium: Springer, Heidelberg, Germany, 2009, pp. 308–326. DOI: 10.1007/978-3-642-03317-9_19.

[Men15] Bart Mennink. *Optimally Secure Tweakable Blockciphers*. Cryptology ePrint Archive, Report 2015/363. http://eprint.iacr.org/2015/363. 2015.

# References III

[Wan+16] Lei Wang et al. "How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers". In: *Advances in Cryptology – ASIACRYPT 2016, Part I*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10031. LNCS. Hanoi, Vietnam: Springer, Heidelberg, Germany, 2016, pp. 455–483. DOI: 10.1007/978-3-662-53887-6_17.

[Jha+17] Ashwin Jha et al. *XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing*. Cryptology ePrint Archive, Report 2017/1075. https://eprint.iacr.org/2017/1075. 2017.

[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, Part I*. Ed. by Thomas Peyrin and Steven Galbraith. Vol. 11272. LNCS. Brisbane, Queensland, Australia: Springer, Heidelberg, Germany, 2018, pp. 305–335. DOI: 10.1007/978-3-030-03326-2_11.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. "Robust Authenticated-Encryption AEZ and the Problem That It Solves". In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. LNCS. Sofia, Bulgaria: Springer, Heidelberg, Germany, 2015, pp. 15–44. DOI: 10.1007/978-3-662-46800-5_2.

[PL18] Jin Hyung Park and Dong Hoon Lee. "FACE: Fast AES CTR mode Encryption Techniques based on the Reuse of Repetitive Data". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018.3 (2018). https://tches.iacr.org/index.php/TCHES/article/view/7283, pp. 469–499. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i3.469-499.

[Bei+16a] Christof Beierle et al. *The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS*. Cryptology ePrint Archive, Report 2016/660. http://eprint.iacr.org/2016/660. 2016.

[Jea+17] Jérémy Jean et al. "Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives - Applications to AES, PRESENT and SKINNY". In: *Cryptographic Hardware and Embedded Systems – CHES 2017*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. LNCS. Taipei, Taiwan: Springer, Heidelberg, Germany, 2017, pp. 687–707. DOI: 10.1007/978-3-319-66787-4_33.

# References IV

[Mor+11] Amir Moradi et al. “Pushing the Limits: A Very Compact and a Threshold Implementation of AES”. In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by Kenneth G. Paterson. Vol. 6632. LNCS. Tallinn, Estonia: Springer, Heidelberg, Germany, 2011, pp. 69–88. DOI: 10.1007/978-3-642-20465-4_6.