Towards Closing The Security Gap of Tweak-aNd-Tweak (TNT)

Chun Guo[1] Jian Guo[2] Eik List[3] Ling Song[4,5]

[1]Shandong University, Qingdao, China
[2]Nanyang Technological University, Singapore
[3]Bauhaus-Universität Weimar, Weimar, Germany
[4]Jinan University, Guangzhou, China
[5]IIE, CAS, Beijing, China

December 2020

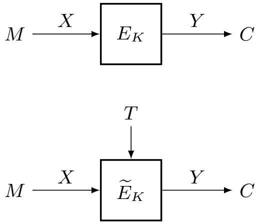
Section 1

Motivation

Tweakable Block Ciphers

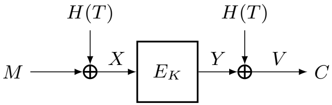
[LRW02]

- Add public tweak input to classical block ciphers
- Useful in encryption/authentication modes:
  - Security: Separate domains
  - Efficiency: Process more input material
- Many dedicated TBCs:
  - CRAFT [BLMR19]
  - Deoxys-BC [JNP14]
  - Skinny [BJK+16]
  - ...
- Generic constructions from classical block ciphers still relevant

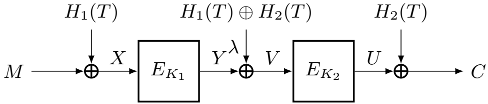


Generic Constructions

- LRW [LRW02], XEX [Rog04]
- Problem: $O(2^{n/2})$ security
- Cascades, e.g. CLRW2 [LST12]: $\geq O(2^{2n/3})$ security
- Generalized: $O(2^{rn/(r+1)})$ [LS13]
- Upper bound by Mennink [Men18] on CLRW2: $\leq O(\sqrt{n} \cdot 2^{3n/4})$ query security
- Lower bound by Jha and Nandi [JN20]: $\geq O(2^{3n/4})$ security



LRW [LRW02]

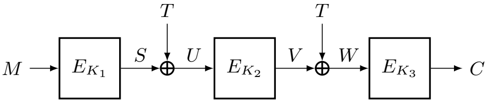


CLRW2 [LST12]

Tweak-aNd-Tweak (TNT)

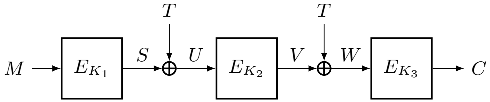
[BGGS20]

- Extension of CMT [LRW02]
- 3 independently keyed block ciphers E_{K_1}, E_{K_2}, E_{K_3}
- Secure up to $O(2^{2n/3})$ queries



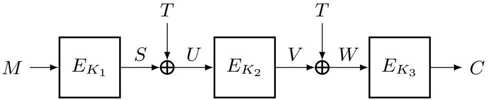
TNT-AES
[BGGS20]

- Instantiation with round-reduced AES for each block cipher
- Proposal: TNT-AES$[6, 6, 6]$
- Boomerang distinguisher on TNT-AES$[*, 5, *]$



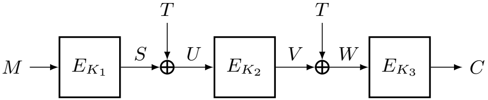
Open Questions

- Can we tighten the gap between attacks $O(2^n)$ and proof $O(2^{2n/3})$ queries?
- Adversary perspective: distinguishers?
- Constructive perspective: improve security



Contribution

- Adapt Mennink's information-theoretic distinguisher [Men18] and reducing the complexity
- Adapt Jha and Nandi's [JN20] STPRP proof of CLRW2 for TPRP security of TNT
- Towards closing the security gap around $O(\sqrt{n} \cdot 2^{3n/4})$ and $O(2^{3n/4})$ queries



Section 2

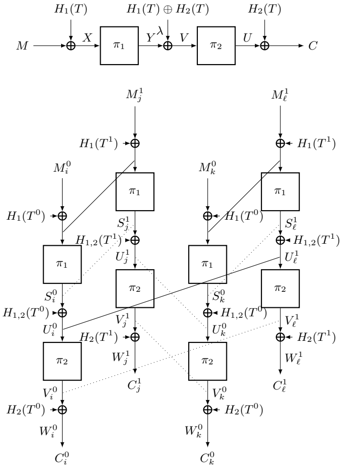
Distinguishers on TNT

Mennink's Distinguisher on CLRW2

[Men18]

- 2 tweaks, $2^{3n/4+x}$ messages each
- Fix threshold θ

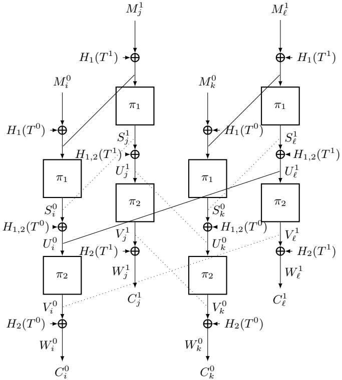
1. Fix tweaks T^0, $T^1 \in \mathbb{F}_2^t$
2. For $i \in 0..2^{3n/4+x}$, query T^0 and $M_i^0 = (0^{n/4-x} \| \langle i \rangle)$ for C_i^0
3. For $i \in 0..2^{3n/4+x}$, query T^1 and $M_i^1 = (0^{n/4-x} \| \langle i \rangle)$ for C_i^1
4. For $D \in \mathbb{F}_2^n$: $\mathcal{I}_D =^{\text{def}} \{(i,j) | M_i^0 \oplus M_j^1 = D\}$
5. For all $D \in \mathbb{F}_2^n$: Determine $N_D =^{\text{def}} \#(i,j) \neq (k,\ell) \in \mathcal{I}_D$: $C_i^0 \oplus C_\ell^1 = C_j^1 \oplus C_k^0$
6. If $\exists D \in \mathbb{F}_2^n$ such that $N_D \geq \theta$ return 1 return 0 otherwise.

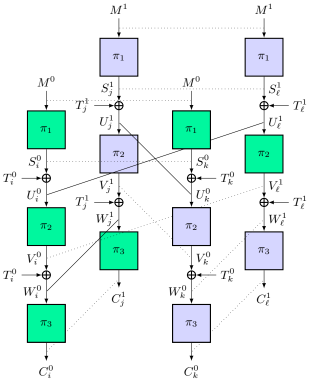


Mennink's Distinguisher on CLRW2

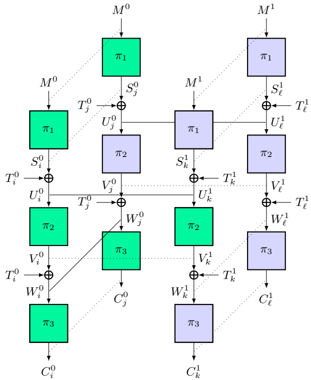
[Men18]

- Distinguisher quartets and random quartets: both probability 2^{-3n}
- $2\times$ #quartets for real construction as for ideal TPRP
- $O(\sqrt{n} \cdot 2^{3n/4})$ queries for detection
- $O(2^{3n/2})$ time
- Can it be adapted to TNT?
- Can it be improved?





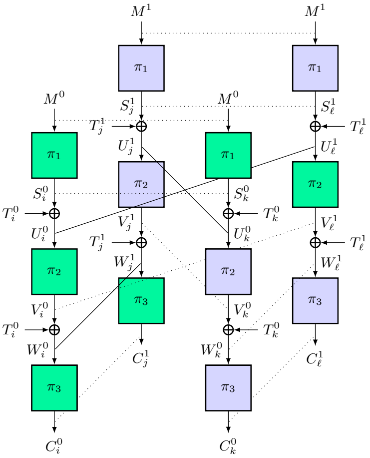
Cross-road distinguisher



Parallel-road distinguisher

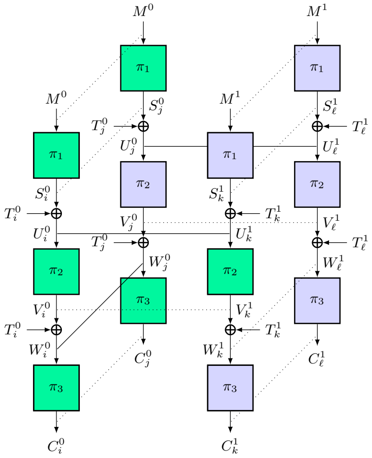
Cross-road Distinguisher

function CROSSROAD
  $K \twoheadleftarrow \mathbb{F}_2^k$
  $M^0 \twoheadleftarrow \mathbb{F}_2^n$
  $M^1 \twoheadleftarrow \mathbb{F}_2^n$
  coll $\leftarrow 0$
  $\mathcal{L} \leftarrow [] \times [0..2^n - 1]$ ▷ 2^n elements
  $\mathcal{D} \leftarrow 0 \times [0..2^n - 1]$ ▷ 2^n elements
  for $i \leftarrow 0..q-1$ **do** ▷ q iterations
    $T_i^0 \leftarrow \tau_0(i)$
    $C_i^0 \leftarrow \mathcal{E}_K(T_i^0, M^0)$
    $\mathcal{L}[C_i^0] \overset{\cup}{\leftarrow} \{T_i^0\}$
  for $j \leftarrow 0..q-1$ **do** ▷ q iterations
    $T_j^1 \leftarrow \tau_1(j)$
    $C_j^1 \leftarrow \mathcal{E}_K(T_j^1, M^1)$
    coll $\leftarrow$ coll + findNumColls($\mathcal{L}, \mathcal{D}, T_j^1, C_j^1$)
  return coll $\geq \theta$



Parallel-road Distinguisher

function PARALLELROAD
- $K \twoheadleftarrow \mathbb{F}_2^k$
- $M^0 \twoheadleftarrow \mathbb{F}_2^n$
- $M^1 \twoheadleftarrow \mathbb{F}_2^n$
- coll $\leftarrow 0$
- $\mathcal{L} \leftarrow [] \times [0..2^n - 1]$ ▷ 2^n elements
- $\mathcal{D} \leftarrow 0 \times [0..2^n - 1]$ ▷ 2^n elements
- **for** $i \leftarrow 0..q-1$ **do** ▷ q iterations
  - $T_i^0 \leftarrow \tau_0(i)$
  - $C_i^0 \leftarrow \mathcal{E}_K(T_i^0, M^0)$
  - **for all** T_j^0 **in** $\mathcal{L}[C_i^0]$ **do**
    - $\Delta T_{i,j}^0 \leftarrow T_i^0 \oplus T_j^0$
    - $\mathcal{D}[\Delta T_{i,j}^0] \leftarrow \mathcal{D}[\Delta T_{i,j}^0] + 1$
  - $\mathcal{L}[C_i^0] \xleftarrow{\cup} \{T_i^0\}$
- $\mathcal{L} \leftarrow [] \times [0..2^n - 1]$ ▷ 2^n elements
- **for** $k \leftarrow 0..q-1$ **do** ▷ q iterations
  - $T_k^1 \leftarrow \tau_1(k)$
  - $C_k^1 \leftarrow \mathcal{E}_K(T_k^1, M^1)$
  - **for all** T_ℓ^1 **in** $\mathcal{L}[C_k^1]$ **do**
    - ▷ $2^{n/2}$ calls over all executions
    - $\Delta T_{k,\ell}^1 \leftarrow T_k^1 \oplus T_\ell^1$
    - coll $\leftarrow$ coll $+ \mathcal{D}[\Delta T_{k,\ell}^1]$
  - $\mathcal{L}[C_k^1] \xleftarrow{\cup} \{T_k^1\}$
- **return** coll $\geq \theta$

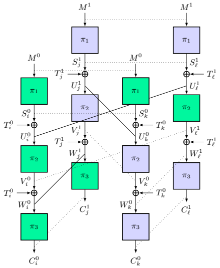


Parallel-road Distinguisher: More Efficient Algorithm

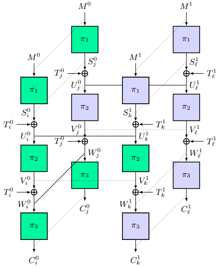
function PARALLELROAD
  $K \twoheadleftarrow \mathbb{F}_2^k$
  $M^0 \twoheadleftarrow \mathbb{F}_2^n$
  $M^1 \twoheadleftarrow \mathbb{F}_2^n$
  coll $\leftarrow 0$
  $\mathcal{L} \leftarrow [] \times [0..q-1]$ ▷ q elements
  $\mathcal{D} \leftarrow [] \times [0..q-1]$ ▷ q elements
  for $i \leftarrow 0..q-1$ **do** ▷ q iterations
    $T_i^0 \leftarrow \tau_0(i)$
    $C_i^0 \leftarrow \mathcal{E}_K(T_i^0, M^0)$
    $(b_i^0, c_i^0) \xleftarrow{n/4,3n/4} C_i^0$
    for all (T_j^0, b_j^0) **in** $\mathcal{L}[c_i^0]$ **do**
      if $b_i^0 = b_j^0$ **then** ▷ $C_i^0 = C_j^0$
        $\Delta T_{i,j}^0 \leftarrow T_i^0 \oplus T_j^0$
        $(s_{i,j}^0, t_{i,j}^0) \xleftarrow{n/4,3n/4} \Delta T_{i,j}^0$
        $\mathcal{D}[t_{i,j}^0] \xleftarrow{\cup} \{s_{i,j}^0\}$
    $\mathcal{L}[c_i^0] \xleftarrow{\cup} \{(T_i^0, b_i^0)\}$
$\mathcal{L} \leftarrow [] \times [0..q-1]$ ▷ q elements
for $k \leftarrow 0..q-1$ **do** ▷ q iterations
  $T_k^1 \leftarrow \tau_1(k)$
  $C_k^1 \leftarrow \mathcal{E}_K(T_k^1, M^1)$
  $(b_k^1, c_k^1) \xleftarrow{n/4,3n/4} C_k^1$
  for all (T_ℓ^1, b_ℓ^1) **in** $\mathcal{L}[c_k^1]$ **do**
    if $b_k^1 = b_\ell^1$ **then** ▷ $C_k^1 = C_\ell^1$
      $\Delta T_{k,\ell}^1 \leftarrow T_k^1 \oplus T_\ell^1$
      $(s_{k,\ell}^1, t_{k,\ell}^1) \xleftarrow{n/4,3n/4} \Delta T_{k,\ell}^1$
      for all $s_{i,j}^0$ **in** $\mathcal{D}[t_{k,\ell}^1]$ **do** ▷ $\Delta T_{i,j}^0 = \Delta T_{k,\ell}^1$
        if $s_{i,j}^0 = s_{k,\ell}^1$ **then**
          coll $\leftarrow$ coll $+ 1$
  $\mathcal{L}[c_k^1] \xleftarrow{\cup} \{(T_k^1, b_k^1)\}$
return coll $\geq \theta$

- $q \in O(\sqrt{n} 2^{3n/4})$ queries
- Bottleneck were the lists
- Used list of q sublists

Distinguishers on TNT



Cross-road distinguisher



Parallel-road distinguisher

- Ca. $(2^t)^2 \cdot 2^{-n}$ pairs collide in U
- $\binom{2^{2t-n}}{2} \cdot 2^{-n} \simeq 2^{4t-3n-1}$ correct quartets
- $(2^t)^2 \cdot 2^{-n}$ random pairs (C_i^0, C_j^1)
- $\binom{2^{2t-n}}{2} \cdot 2^{-n} \simeq 2^{4t-3n-1}$ random quartets
- $\implies 2\times$ quartets for real construction

- Ca. $(2^t)^2 \cdot 2^{-n}$ pairs collide in U
- $\binom{2^{2t-n}}{2} \cdot 2^{-n} \simeq 2^{4t-3n-1}$ correct quartets
- $\binom{2^t}{2} \cdot 2^{-n} \simeq 2^{2t-n-1}$ random pairs (C_i^0, C_j^0)
- $(2^{2t-n-1})^2 \cdot 2^{-n} \simeq 2^{4t-3n-2}$ random quartets
- $\implies 3\times$ quartets for real construction

Experiments on TNT with Small-PRESENT

n	t	Ideal	Real
16	11	0.026	0.061
16	12	0.485	1.009
16	13	7.967	15.970
16	14	127.458	255.133

n	t	Ideal	Real
20	14	0.032	0.055
20	15	0.494	0.960
20	16	8.087	16.162
20	17	128.057	255.739

n	t	Ideal	Real
24	17	0.034	0.066
24	18	0.482	1.009
24	19	7.979	16.174
24	20	127.941	255.661

Cross-road distinguisher

n	t	Ideal	Real
16	11	0.015	0.050
16	12	0.232	0.787
16	13	4.076	12.127
16	14	64.274	192.275

n	t	Ideal	Real
20	14	0.024	0.057
20	15	0.274	0.749
20	16	3.892	11.952
20	17	64.405	191.398

n	t	Ideal	Real
24	17	0.016	0.063
24	18	0.233	0.726
24	19	4.016	12.170
24	20	63.686	191.599

Parallel-road distinguisher

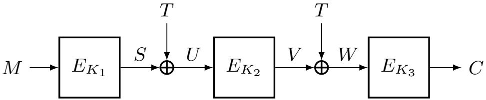
- Small-PRESENT-$[n]$ [Lea10] with $n \in \{16, 20, 24\}$
- Ideal $=$ random function
- 1000 random keys, 2 messages, 2^t tweaks
- $2x$ quartets for cross-road distinguisher
- $3x$ quartets for parallel-road distinguisher

Section 3

Distinguishers on TNT-AES

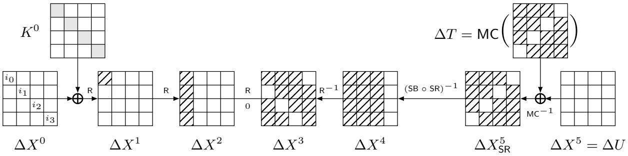
TNT-AES

- TNT-AES$[6, 6, 6]$
- Instantiation with 6-round AES



Impossible-differential Attack on TNT-AES$[5, *, *]$

Core Idea



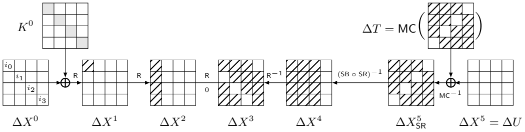
- Impossible differential
- Tweak-difference space $\mathcal{T} = \{\Delta T \mid \Delta T \in \mathcal{M}_{\{0,1,2\}}\}$
- "Correct" message pairs M, M' with $\Delta M \in \mathcal{D}_{\{0\}}$ with $\Delta X^5 \in \mathcal{T}$ will produce distinguisher $\implies$ more quartets
- Choose enough messages and enough tweaks for each message
- Correct message pairs cannot encrypt to ΔX^1
- Discard key candidates with correct message pairs

Impossible-differential Attack on TNT-AES$[5, *, *]$

Some Details

- Reduce $K^0[0, 5, 10, 15]$ to 2^{32-a}
- Assumption: each correct message pair filters about 2^{10} key candidates

$$\Pr[K \text{ filtered}] \simeq (1 - 2^{-22})^N \leq 2^{-a}$$

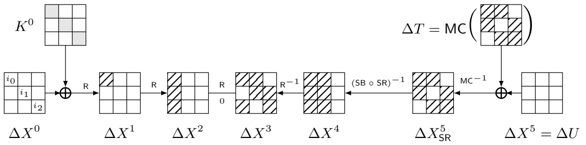


- $N \geq 2^{26.47}$ correct message pairs for $a \simeq 32$

- Structures of $2^{3n/4}$ tweaks from mixed space $\mathcal{T} = \mathcal{M}_{\{0,1,2\}}$
- $\Pr[\pi_1(M) \oplus \pi_1(M') \in \mathcal{T}] \simeq 2^{-32} \implies 2^{58.47}$ pairs needed $\implies$ 2 sets of $2^{29.24}$ messages
- $\Pr[\text{quartet} \mid \text{incorrect MP}] \simeq 2^{-354}$ vs. $\Pr[\text{quartet} \mid \text{correct MP}] \simeq 2^{-321}$
- Samajder and Sarkar [SS17]: $2^{83.3}$ tweaks/message suffice (normal-distr. assumption)
- $2^{30.3} \cdot 2^{83.3} \simeq 2^{113.6}$ message-tweak CPs
- Few key candidates left $\implies$ encryptions dominate time/memory complexity

MP = message pair $(M^0, T_i^0), (M^1, T_j^1), (M^0, T_k^0), (M^1, T_\ell^1)$

Implementation with (very) Small AES



- 36-bit variant of SMALL-AES [CMR05] (3×3 four-bit cells)
- Cross-road distinguisher
- Goal: Can we identify correct message pairs?
- Yes, huge distance
- #Quartets as expected

		With desired difference?			
		With		Without	
t	m	$\log_2(\mu)$	$\log_2(\sigma)$	$\log_2(\mu)$	$\log_2(\sigma)$
22	10 000	2.994	1.511	−10.480	−5.241
23	1 000	6.997	3.550	−6.158	−2.991
24	100	11.005	5.502	−1.837	−0.907
25	100	12.998	6.479	1.233	0.664
26	100	15.001	7.437	3.986	2.097
27	100	17.002	8.395	6.987	3.497

#Quartets for messages with and without correct difference after π_1.

Section 4

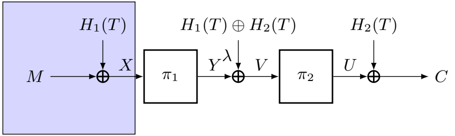
Security Analysis

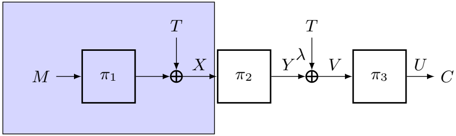
Transforming TNT to CLRW2

- Recent work by Jha and Nandi on CLRW2 [JN20]
- TPRP security (forward direction only)
- ϵ-almost-universal hash function
  $\widehat{H}_{\mathsf{CLRW2}}(M, T) \stackrel{\text{def}}{=} H_1(T) \oplus M$
  becomes
  $\widehat{H}_{\mathsf{TNT}}(M, T) \stackrel{\text{def}}{=} \pi_1(M) \oplus T$

$$\Pr[H_1(T) \oplus M = H_1(T') \oplus M'] \leq \epsilon$$
$$\Pr[\pi_1(M) \oplus T = \pi_1(M') \oplus T'] \leq \epsilon$$

- Ideal oracle samples $\pi_1 \twoheadleftarrow \mathsf{Perm}(\mathbb{F}_2^n)$
- Output is not masked, but we consider only TPRP



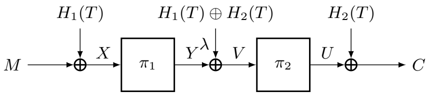


Jha and Nandi on CLRW2

[JN20]

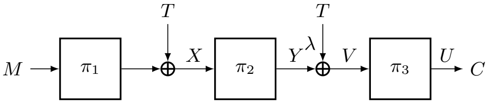
Sketch for $O(2^{3n/4})$ STPRP security:

- Smart sampling strategy of Y and V in the middle
- Two sets of bad events:
  - Bad hash keys
  - Bad sampling
- Analysis of good transcripts



Bad Events: 7 Bad Hash Equivalents

Core Difference to [JN20]



- bad$_1$: $\exists^* i, j \in [q]$ such that $X_i = X_j \wedge U_i = U_j$.

$$\Pr[\mathsf{bad}_1] = 0$$

- bad$_2$: $\exists^* i, j \in [q]$ such that $X_i = X_j \wedge T_i = T_j$.

$$\Pr[\mathsf{bad}_2] = 0$$

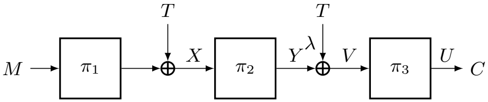
- bad$_3$: $\exists^* i, j \in [q]$ such that $U_i = U_j \wedge T_i = T_j$.

$$\Pr[\mathsf{bad}_3] = 0$$

- bad$_4$: $\exists^* i, j, k, \ell \in [q]$ such that $X_i = X_j \wedge U_j = U_k \wedge X_k = X_\ell$.

$$\Pr[\mathsf{bad}_4] \leq q^2 \epsilon^{1.5} \leq \frac{2q^2}{2^{1.5n}}$$

Bad Events: Bad Hash Equivalents (cont'd)



- bad$_5$: $\exists^* i, j, k, \ell \in [q]$ such that $U_i = U_j \wedge X_j = X_k \wedge U_k = U_\ell$.

$$\Pr[\mathsf{bad}_5] \leq \frac{2q^2}{2^{1.5n}}$$

- bad$_6$: $\exists k \geq 2^n/2q$, $\exists^* i_1, i_2, \ldots, i_k \in [q]$ such that $X_{i_1} = \cdots = X_{i_k}$.

$$\Pr[\mathsf{bad}_6] \leq \frac{16q^4}{2^{3n}}$$

- bad$_7$: $\exists k \geq 2^n/2q$, $\exists^* i_1, i_2, \ldots, i_k \in [q]$ such that $U_{i_1} = \cdots = U_{i_k}$.

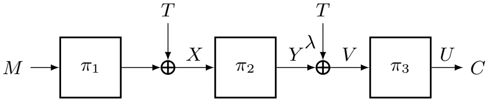
$$\Pr[\mathsf{bad}_7] \leq \frac{16q^4}{2^{3n}}$$

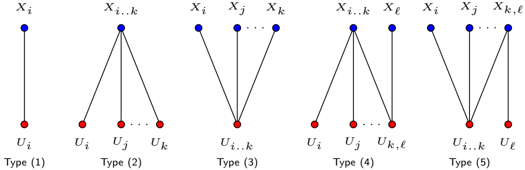
Lemma 1

For TNT, it holds in the ideal world that $\Pr[\mathsf{bad}] \leq \frac{4q^2}{2^{1.5n}} + \frac{32q^4}{2^{3n}}$.

Bad Events

[JN20]





Bad Sampling:

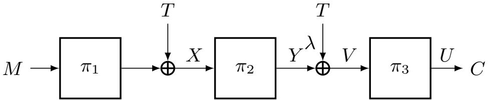
- Define transcript graph $\mathcal{G}(\mathcal{X}^q, \mathcal{U}^q)$ of relations X_i, U_i
- Consider the interesting components
- Group components of transcript into sets of components $\mathcal{I}_i$ for $i \in [1..5]$
- Ideal-world oracle tries to sample Y, V consistently
- If not possible: badsamp of components:
  - $\exists i \in \mathcal{I}_\alpha, j \in \mathcal{I}_\beta$: $X_i \neq X_j$ but $Y_i = Y_j$
  - $\exists i \in \mathcal{I}_\alpha, j \in \mathcal{I}_\beta$: $U_i \neq U_j$ but $V_i = V_j$

Lemma 2

For TNT, it holds in the ideal world that $\Pr[\text{badsamp}] \leq \frac{14q^4}{2^{3n}}$.

Good Transcripts

[JN20]

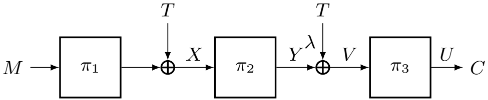


- Similar as for CLRW2 [JN20]

Lemma 3

For an arbitrary good transcript τ, it holds that

$$\frac{\Pr\left[\Theta_{\mathsf{real}} = \tau\right]}{\Pr\left[\Theta_{\mathsf{ideal}} = \tau\right]} \geq 1 - \frac{45q^4}{2^{3n}} - \frac{2q^2}{2^{2n}}\,.$$



Theorem 4 (TPRP Security of TNT)

Let $q \le 2^{n-2}$, and $E_{K_1}, E_{K_2}, E_{K_3} : \mathcal{K} \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ be block ciphers with $K_1, K_2, K_3 \twoheadleftarrow \mathcal{K}$. Then,

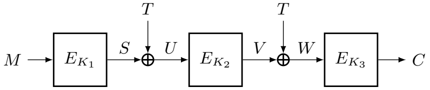
$$\mathbf{Adv}^{\mathsf{TPRP}}_{\mathsf{TNT}[E_{K_1}, E_{K_2}, E_{K_3}]}(q) \le \frac{91q^4}{2^{3n}} + \frac{2q^2}{2^{2n}} + \frac{4q^2}{2^{1.5n}} + 3 \cdot \mathbf{Adv}^{\mathsf{PRP}}_{E}(q)\,.$$

Section 5

Summary

Summary

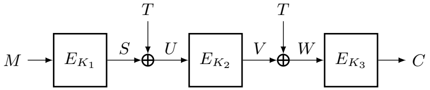
- Both constructive and adversarial perspective on TNT
- $O(2^{3n/4})$ TPRP security
  on the shoulders of [JN20]
- $O(\sqrt{n}2^{3n/4})$ distinguishers
  on the shoulders of [Men18]
- Impossible-differential attack on TNT-AES$[5, *, *]$
- Can be applied similarly to TNT-AES$[*, *, 5]$



Discussion and Future Work

Notes:

- Our work does not violate the security claims of TNT of at least $O(2^{2n/3})$ queries or security of TNT-AES$[6, 6, 6]$
- With their analysis of TNT-AES$[*, 5, *]$ $\implies$ 6 rounds are lower bound
- TNT is structurally very similar to CLRW2



Future work:

- STPRP analysis

Thank you for your attention

Bibliography I

Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song.
TNT: How to Tweak a Block Cipher.
In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT*, volume 12106 of *LNCS*, pages 1–31. Springer, 2020.

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO II*, volume 9815 of *LNCS*, pages 123–153. Springer, 2016.

Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh.
CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks.
IACR Trans. Symmetric Cryptol., 2019(1):5–45, 2019.

Carlos Cid, Sean Murphy, and Matthew J. B. Robshaw.
Small Scale Variants of the AES.
In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 145–162. Springer, 2005.

Ashwin Jha and Mridul Nandi.
Tight Security of Cascaded LRW2.
Journal of Cryptology, pages 1378–1432, 2020.

Jérémy Jean, Ivica Nikolic, and Thomas Peyrin.
Tweaks and Keys for Block Ciphers: The TWEAKEY Framework.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT II*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2014.

Gregor Leander.
Small Scale Variants Of The Block Cipher PRESENT.
IACR Cryptol. ePrint Arch., 2010:143, 2010.

Bibliography II

Moses Liskov, Ronald L. Rivest, and David Wagner.
Tweakable Block Ciphers.
In Moti Yung, editor, *CRYPTO*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

Rodolphe Lampe and Yannick Seurin.
Tweakable Blockciphers with Asymptotically Optimal Security.
In Shiho Moriai, editor, *FSE*, volume 8424 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2013.

Will Landecker, Thomas Shrimpton, and R. Seth Terashima.
Tweakable Blockciphers with Beyond Birthday-Bound Security.
In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.

Bart Mennink.
Towards Tight Security of Cascaded LRW2.
In Amos Beimel and Stefan Dziembowski, editors, *TCC II*, volume 11240 of *Lecture Notes in Computer Science*, pages 192–222. Springer, 2018.

Phillip Rogaway.
Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC.
In Pil Joong Lee, editor, *ASIACRYPT*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.

Subhabrata Samajder and Palash Sarkar.
Rigorous upper bounds on data complexities of block cipher cryptanalysis.
J. Mathematical Cryptology, 11(3):147–175, 2017.
https://doi.org/10.1515/jmc-2016-0026.