Tight Security of TNT and Beyond

Attacks, Proofs and Possibilities for the Cascaded LRW Paradigm

Ashwin Jha[1,2] **Mustafa Khairallah**[3,4] Mridul Nandi[5]
Abishanka Saha[5]

[1]Ruhr-Universtät Bochum, Bochum, Germany
[2]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
[3]Seagate Research Group, Singapore, Singapore
[4]Lund University, Lund, Sweden
[5]Indian Statistical Institute, Kolkata, India

Eurocrypt 2024

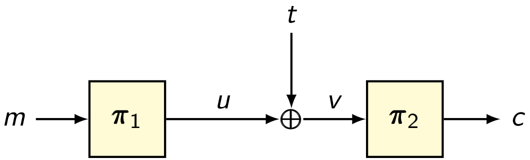
Tweakable Block Ciphers

"Many modes of operation and other applications using block ciphers have nonetheless a requirement for "essentially different" instances of the block cipher in order to prevent attacks that operate by, say, permuting blocks of the input." - Liskov, Rivest and Wagner 2002

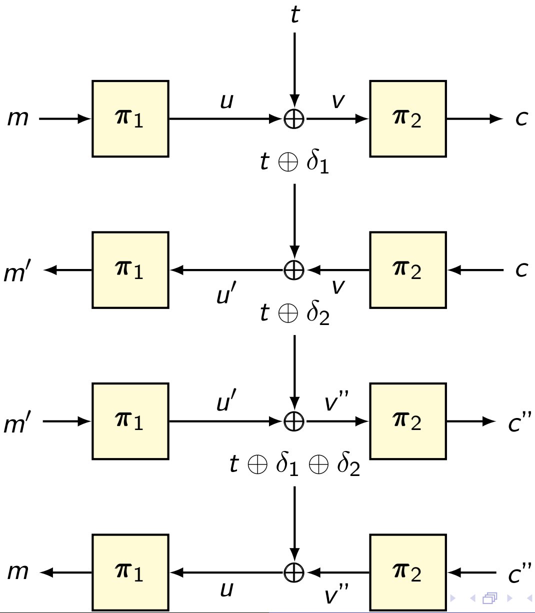
	T_1	T_2	T_3	T_4
K_4	P_4	P_4	P_4	P_4
K_3	P_3	P_3	P_3	P_3
K_2	P_2	P_2	P_2	P_2
K_1	P_1	P_1	P_1	P_1

	T_1	T_2	T_3	T_4
K_4	P_m	P_n	P_o	P_p
K_3	P_i	P_j	P_k	P_k
K_2	P_e	P_f	P_g	P_h
K_1	P_a	P_b	P_c	P_d

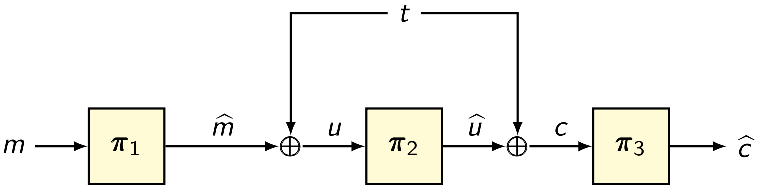
LRW1



LRW1: Folklore 4-point CCA.



The TNT construction [Bao+20]



TNT state of the art

1. In Eurocrypt 2020, [Bao+20] presented TNT as a 3-round generalization of LRW1. The claimed security is $2n/3$ bits.

2. In Asiacrypt 2020 [Guo+20], the authors presented a $O(2^{3n/4})$-query CPA attack and a similar CPA security bound.

3. In [ZQG23], the authors presented a bound for r-round LRW1 using compositional techniques, yet it gives only birthday bound in the case of TNT.

4. [Guo+20] and [ZQG23] conjectured that the security of TNT maybe even higher than $2n/3$ bits.

Why study TNT?

1. TNT is a very efficient (BBB?) TBC from block ciphers.

2. The original security proof is based on the χ^2 method which was fairly recent in 2020 and most of its other applications are not in the CCA setting.

3. No CCA attack is known (except for the CPA attacks in [Guo+20] which use queries in one direction only).

Contributions

1. Birthday-bound CCA attack on TNT: Nullifying the bound of [Bao+20].

2. Birthday-bound CCA security of TNT and the single-key variant.

3. A Generalization of Cascaded LRW Paradigm.

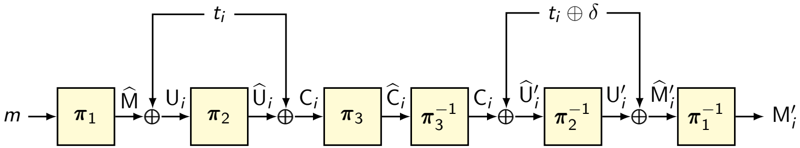
Summary of the results against the state of the art.

Construction	BC calls	Hash calls	Security bound	Tightness
LRW1 [LRW02]	1	0	$2^{n/2}$ (CPA) [LRW02]	✓
LRW2 [LRW02]	1	1	$2^{n/2}$ [LRW02]	✓
3-LRW1 (TNT [Guo+20])	3	0	$2^{2n/3}$ [Guo+20]	(flawed)
4-LRW1	4	0	$2^{3n/4}$ [Dat+23]	–
2-LRW2 (CLRW2 [LST12])	2	2	$2^{3n/4}$ [JN20]	✓ [Men18]
r-LRW1 [ZQG23]	r odd	0	$2^{\frac{r-1}{r+1}n}$ [ZQG23]	–
	r even		$2^{\frac{r-2}{r}n}$	–
r-LRW2 [LS13]	r odd	r	$2^{\frac{r-1}{r+1}n}$ [LS13]	–
	r even		$2^{\frac{r}{r+2}n}$	–
3-LRW1 (TNT)	3	0	$2^{n/2}$	✓
1k-TNT	3	0	$2^{n/2}$	✓
LRW+	2	2	$2^{3n/4}$	–
4-LRW1	4	0	$2^{3n/4}$	–

Best attacks on TNT-AES

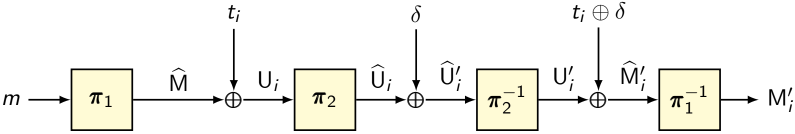
Ref.	Type	Data	Time	Adversary	Rounds
[Bao+20]	Boomerang	2^{126}	2^{126}	CCA	$\star - 5 - \star$
[Guo+20]	Impossible Differential	$2^{113.6}$	$2^{113.6}$	NCPA	$5 - \star - \star$
[Guo+20]	Generic	$2^{99.5}$	$2^{99.5}$	NCPA	$\star - \star - \star$
[BL23]	Truncated Boomerang	2^{76}	2^{76}	CCA	$\star - 5 - \star$
[BL23]	Truncated Boomerang	2^{87}	2^{87}	CCA	$5 - 5 - \star$
[BL23]	Truncated Boomerang	$2^{127.8}$	$2^{127.8}$	CCA	$\star - 6 - \star$
This paper	Generic	$\leq 2^{69}$	$\leq 2^{69}$	CCA	$\star - \star - \star$

Observation: π_3 does not contribute to CCA security



Observation: π_3 does not contribute to CCA security

The $\mathcal{O}_{\delta,m}$ oracle



Attack description

```
1: m ← 0^n                          ▷ m can be initialized to any constant
2: δ ← 1^n                 ▷ δ can be initialized to any non-zero constant
3: T ← {t_1, ..., t_q}                ▷ a set of q fixed but distinct tweaks
4: M ← ∅                                             ▷ an empty multiset
5: for i = 1 ... q do
6:     Ĉ_i ← O(t_i, m)
7:     M'_i ← O^{-1}(t_i ⊕ δ, Ĉ_i)  ▷ ln. 6 and 7 together give O_{δ,m}(t_i)
8:     M ← M ∪ {M'_i}
9: COLL(O_{δ,m}) ← collCount(M)
10: if COLL(O_{δ,m}) > θ(q, n) then
11:     return 1
12: else
13:     return 0
```

Theoretical Advantage

Theorem

For $n \geq 4$, $10 \leq q \leq 2^n$, and $\theta(q, n) = (\mu_{\mathrm{re}} + \mu_{\mathrm{id}})/2$, we have

$$\mathbf{Adv}^{\text{ind-cca}}_{TNT}(\mathbf{A}^*) \geq 1 - 371\frac{2^n}{q^2}.$$

Specifically, for $q \geq 28 \times 2^{\frac{n}{2}}$, $\mathbf{Adv}^{\text{ind-cca}}_{TNT}(\mathbf{A}^*) \geq 0.5$.

$$\begin{aligned}
\mathbf{Adv}^{\text{ind-cca}}_{\mathrm{TNT}}(\mathbf{A}^*) &= \left|\Pr\left(\mathbf{A}^*(\mathrm{TNT}_{\delta,m}) = 1\right) - \Pr\left(\mathbf{A}^*(\widetilde{\boldsymbol{\pi}}_{\delta,m}) = 1\right)\right| \\
&= \left|\Pr\left(\mathrm{coll}_{\mathrm{re}} > \theta(q,n)\right) - \Pr\left(\mathrm{coll}_{\mathrm{id}} > \theta(q,n)\right)\right| \\
&\geq 1 - \frac{4(\sigma^2_{\mathrm{re}} + \sigma^2_{\mathrm{id}})}{(\mu_{\mathrm{re}} - \mu_{\mathrm{id}})^2}. \qquad (1)
\end{aligned}$$

Estimated Parameters

$$\mu_{\mathrm{re}} := \binom{q}{2}\frac{2}{2^n} \qquad \mu_{\mathrm{id}} := \binom{q}{2}\frac{1}{2^n} + \frac{q}{2^n}.$$

$$\sigma^2_{\mathrm{id}} \leq \frac{4q^2}{2^n} \qquad \sigma^2_{\mathrm{re}} \leq \frac{11q^2}{2^n}$$

1. These parameters and the theoretical advantage favour scalability over tightness.

2. We will see that the empirical advantage is significantly higher.

3. Our bound reaches 1 as q approaches 2^n.

4. See the paper for full calculations, see also 2023/1212 and 2023/1233 for alternate analyses.

Experimental Verification: Average number of collisions using random permutations

n	16					
$\log_2(q)$	6	7	8	9	10	11
real	0.06	0.27	0.96	3.72	15.62	63.59
ideal	0.023	0.12	0.48	1.98	7.91	31.17
n	20					
$\log_2(q)$	8	9	10	11	12	13
real	0.073	0.203	1.02	4.01	15.69	63.63
ideal	0.023	0.11	0.47	1.94	7.92	32.57

Experimental Verification: Success Rate

n	q	$\theta(q,n)$	**Success Rate**	q	$\theta(q,n)$	**Success Rate**
16	10	12	87.2%	11	48	99%
20	12	12	86.6%	13	48	99%
24	14	12	90%	15	48	99%
28	16	12	85%	17	48	99%
32	18	12	87.5%	19	48	99%

Emperical Advantage:

$$1 - 2\frac{2^n}{q^2}$$

TNT in practice:TNT-GIFT-64.

n	64			
$\log_2(q)$	32	33	34	35
Average Number of Collisions	1	4	16	61
Time	3 hrs	3 hrs 40 mins	12 hrs 15 mins	20 hrs
CPU Time	5 hrs	10 hrs	28 hr 15 mins	72 hrs
Number of Cores	2	4	8	16
RAM	96 GB	192 GB	128 GB	192 GB
Disk Space	73 GB	146 GB	292 GB	583 GB

What went wrong? A Snippet of the χ^2 method

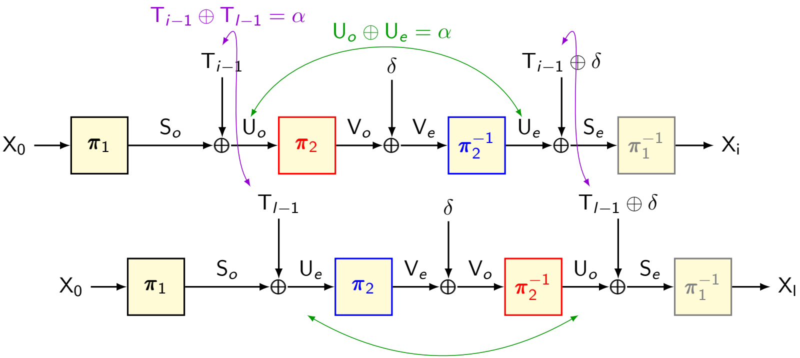
We observe the query-response transcript for the first $l-1$ queries.

1. We estimate the probability distribution of the possible corresponding internal values.

2. We estimate the probability distribution of the response to query l:

    2.1 For each possibility of the internal values, query l is completely determined.

Where do the extra collisions come from and why does it impact the proof?



Constructive results

Theorem

Let π_1, π_2, and π_3 be three independent random permutations of $\{0,1\}^n$. Then, for all $q \geq 1$, we have

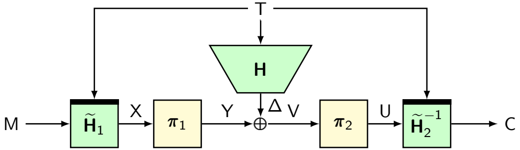
$$\mathbf{Adv}^{\text{ind-cca}}_{\text{TNT}}(q) \leq \frac{q^2}{2^n}.$$

Theorem

Let $\pi_1 = \pi_2 = \pi_3 = \pi$, where π is a uniform random permutation of $\{0,1\}^n$. Then, for all $q \geq 1$, we have

$$\mathbf{Adv}^{\text{ind-cca}}_{\text{1k-TNT}}(q) \leq \frac{8q^2}{2^n}.$$

LRW+



Theorem

Let $\tau, n \in \mathbb{N}$, and $\epsilon_1, \epsilon_2 \in [0,1]$. If $\widetilde{\mathcal{H}}$ and $\mathcal{H}$ are respectively ϵ_1-AUTPF and ϵ_2-AUHF, and KG $\left(\widehat{\mathcal{H}}\right)$ *is a PISM, then, for $q \leq 2^{n-2}$, we have*

$$\mathbf{Adv}^{\text{ind-cca}}_{\text{LRW+}}(q) \leq \epsilon(q,n),$$

where

$$\epsilon(q,n) = 2q^2\epsilon_1^{1.5} + \frac{4q^4\epsilon_1^2}{2^n} + \frac{32q^4\epsilon_1}{2^{2n}} + \frac{13q^4}{2^{3n}} + q^2\epsilon_1^2 + q^2\epsilon_1\epsilon_2 + \frac{2q^2}{2^{2n}}. \quad (2)$$

Conclusions

1. TNT is tightly secure up to birthday bound only (in the CCA setting).

2. Adding one more round reaches $3n/4$-bit security.

3. LRW+ provides a framework to encompass LRW1, LRW2 and any related construction.

Open Questions and Future Work

1. Optimal LRW construction for BBB security: is 4 permutation calls optimal?
2. Reduced-key version of 4-LRW1.
3. Exact security of 4-LRW1.
4. Security of short-tweak TNT.
5. Security of Longer Cascades of LRW.

Thank You