Efficient Variants of TNT with BBB Security

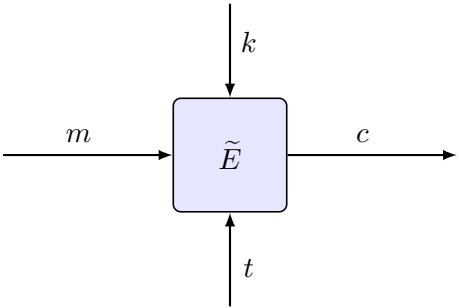
Ritam Bhaumik[1] **Wonseok Choi**[2] **Avijit Dutta**[3] **Cuauhtemoc Mancillas López**[4]
Hrithik Nandi[3,5] **Yaobin Shen**[6]

[1]CRC, TII
[2]Purdue University
[3]IAI, TCG CREST
[4]CINVESTAV-IPN
[5]RKMVERI, Belur
[6]Xiamen University

ProvSec 2024

September 26, 2024

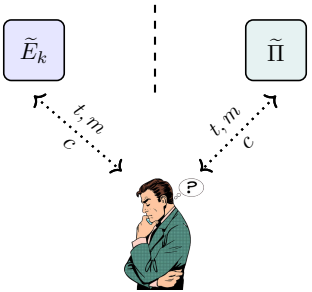
Tweakable Block Cipher



- A family of permutations indexed by secret key and public tweak
- $\widetilde{E}\colon \mathcal{M} \times \mathcal{K} \times \mathcal{T} \to \mathcal{C}$, where $\mathcal{M} \coloneqq \{0,1\}^n, \mathcal{K} \coloneqq \{0,1\}^k$, $\mathcal{T} \coloneqq \{0,1\}^t$ and $\mathcal{C} \coloneqq \{0,1\}^n$
- For a fixed key, tweak pair (k,t), $\widetilde{E}_{k,t}$ is a permutation over $\{0,1\}^n$
- TBCs have found diverse applications in designing of AE schemes, MACs, PRFs, Wide block encryption modes

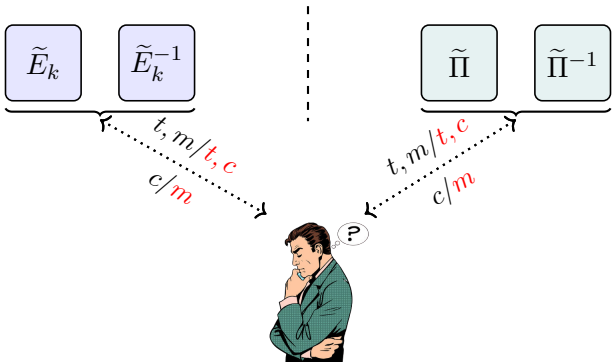
Security Notions of Tweakable Block Cipher: TPRP

- $\widetilde{E}\colon \mathcal{M} \times \mathcal{K} \times \mathcal{T} \to \mathcal{C}$ is a tweakable block cipher
- $\widetilde{\Pi}$ is a tweakable random permutation, a family of independent random permutations parameterized by tweak t



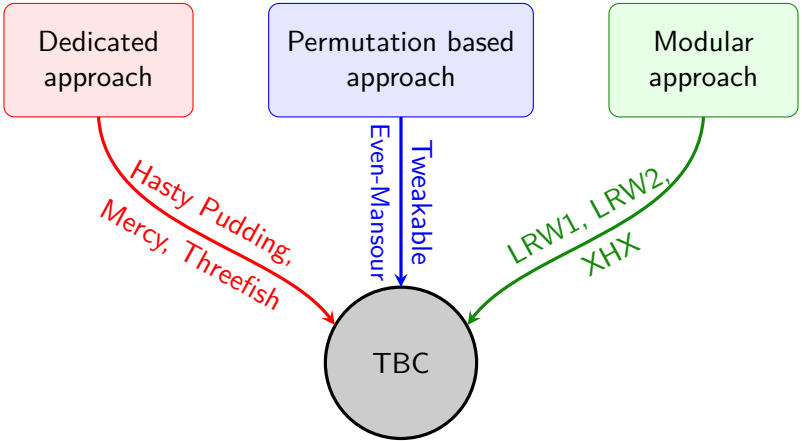
$$\mathsf{Adv}^{\mathsf{TPRP}}_{\mathcal{A},\widetilde{E}}(q) \coloneqq |\Pr[k \xleftarrow{\$} \mathcal{K}\colon \mathcal{A}^{\widetilde{E}_k(\cdot,\cdot)} \to 1] - \Pr[\widetilde{\Pi} \xleftarrow{\$} \mathsf{TPerm}(n)\colon \mathcal{A}^{\widetilde{\Pi}(\cdot,\cdot)} \to 1]|$$

Security Notions of Tweakable Block Cipher: STPRP



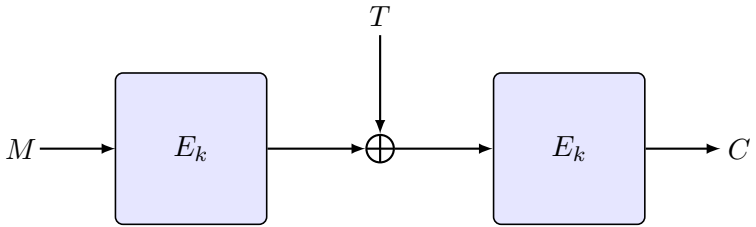
$$\mathsf{Adv}^{\mathsf{STPRP}}_{\mathcal{A},\widetilde{E}}(q) \coloneqq |\Pr[k \xleftarrow{\$} \mathcal{K} \colon \mathcal{A}^{\widetilde{E}_k(\cdot,\cdot),\widetilde{E}_k^{-1}(\cdot,\cdot)} \to 1] - \Pr[\widetilde{\Pi} \xleftarrow{\$} \mathsf{TPerm}(n) \colon \mathcal{A}^{\widetilde{\Pi}(\cdot,\cdot),\widetilde{\Pi}^{-1}(\cdot,\cdot)} \to 1]|$$

Design Approaches of TBC



In this work, we are focusing on Modular approach

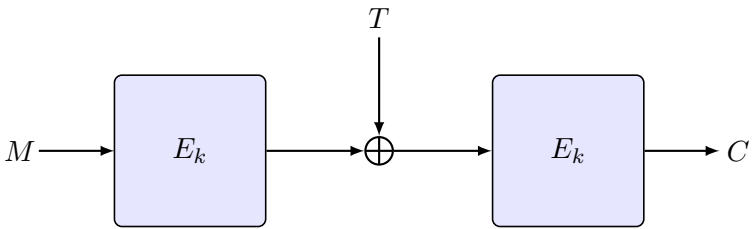
Modular Approach: Designing TBC from BC



LRW1 Construction

- LRW1 construction was proposed by Liskov et al. at CRYPTO'02
- It achieves Tight CPA security upto $2^{n/2}$ queries, assuming E_k is n-bit secure PRP

Modular Approach: Designing TBC from BC

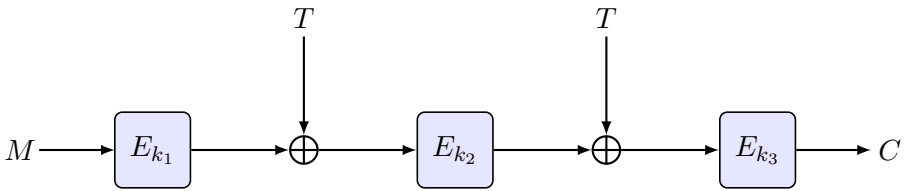


LRW1 Construction

- LRW1 construction was proposed by Liskov et al. at CRYPTO'02
- It achieves Tight CPA security upto $2^{n/2}$ queries, assuming E_k is n-bit secure PRP

LRW1 is Birthday Bound secure

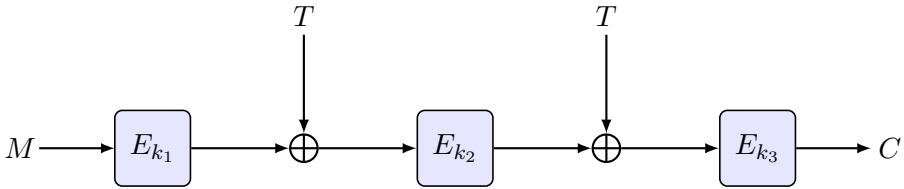
Seeking BBB secure TBC (Cascaded LRW1)



CLRW1^3 (TNT) Construction

- Proposed by Bao et al. at EUROCRYPT'20
- [Bao et al., EUROCRYPT'20]: CCA security upto $2^{2n/3}$ queries
- [Guo et al., ASIACRYPT'20]: Tight CPA security upto $2^{3n/4}$ queries
- [Jha et al., EUROCRYPT'24]: Tight CCA security upto $2^{n/2}$ queries

Seeking BBB secure TBC (Cascaded LRW1)

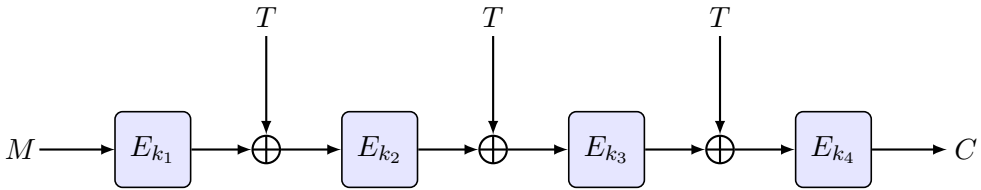


CLRW1^3 (TNT) Construction

- Proposed by Bao et al. at EUROCRYPT'20
- [Bao et al., EUROCRYPT'20]: CCA security upto $2^{2n/3}$ queries
- [Guo et al., ASIACRYPT'20]: Tight CPA security upto $2^{3n/4}$ queries
- [Jha et al., EUROCRYPT'24]: Tight CCA security upto $2^{n/2}$ queries

TNT now achieves tight Bithday-Bound security

The search begins anew



CLRW1^4 Construction

- Proposed by Datta et al. at ToSC Volume 2023, Issue 4
- [Datta et al., ToSC'23(4)]: CCA security upto $2^{3n/4}$ queries

Efficient Variants of TNT with BBB Security

Can we fix TNT efficiently with BBB security?

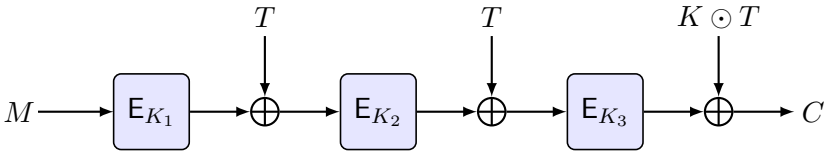
Efficient Variants of TNT with BBB Security

Can we fix TNT efficiently with BBB security?

Our Contributions :

- We have proposed two efficient (compared to CLRW1[4]) variants of TNT construction
  - b-TNT1
  - b-TNT2
- We have shown that both constructions achieve CCA security upto $2^{3n/4}$ queries
- We have experimentally verified that both b-TNT1 and b-TNT2 perform better than CLRW1[4] in terms of throughput

b-TNT1 Construction

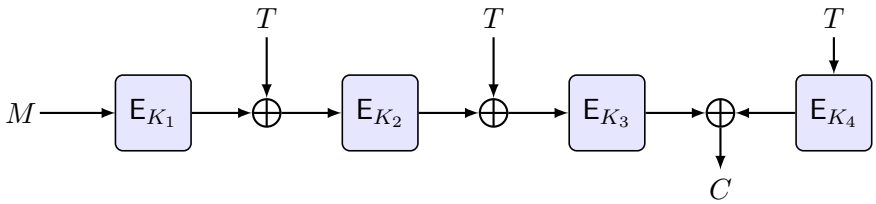


b-TNT1 construction (3 BC calls and 1 field multiplication)

Security Result

$$\mathbf{Adv}^{\mathrm{STPRP}}_{\mathsf{b\text{-}TNT1}}(\mathsf{A}) \leq 3\mathbf{Adv}^{\mathrm{SPRP}}_{\mathsf{E}}(\mathsf{A}') + \frac{3q^2}{2^{2n}} + \frac{5q^{4/3}}{2^n} + \frac{45q^4}{2^{3n}} + \frac{1}{2^n}$$

b-TNT2 Construction

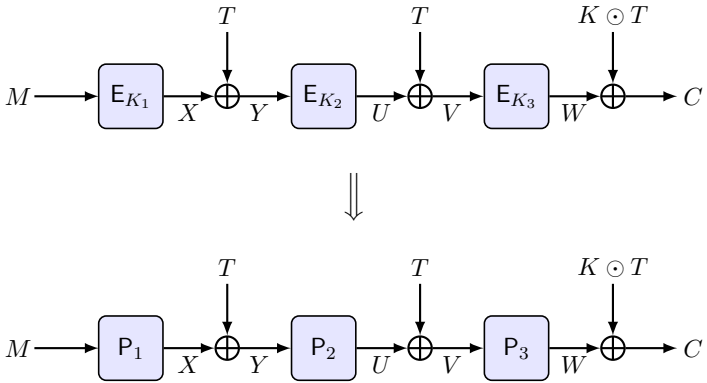


b-TNT2 construction (4 BC calls)

Security Result

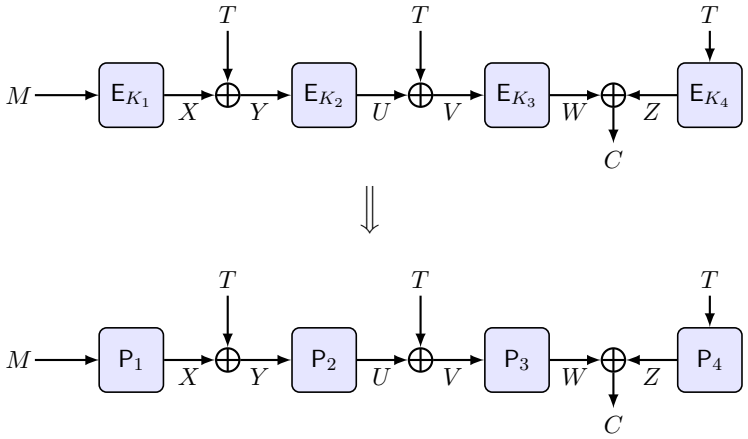
$$\mathbf{Adv}^{\mathrm{STPRP}}_{\mathsf{b\text{-}TNT2}}(\mathsf{A}) \leq 3\mathbf{Adv}^{\mathrm{SPRP}}_{\mathsf{E}}(\mathsf{A}') + \mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(\mathsf{B}) + \frac{4q^2}{2^{2n}} + \frac{6q^{4/3}}{2^n} + \frac{53q^4}{2^{3n}}.$$

Proof Sketch: Replacing BCs with random permutations (b-TNT1)



- At the cost of the strong pseudorandom permutation advantage of the underlying BC.

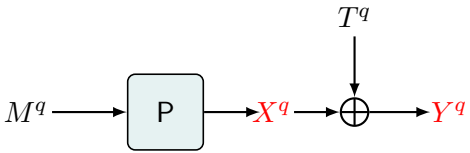
Proof Sketch: Replacing BCs with random permutations (b-TNT2)

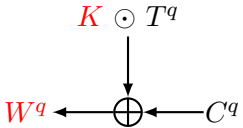


- At the cost of the sprp advantage and prp advantage (for E_{K_4}) of the underlying BC.

Proof Sketch: Releasing intermediate variables (b-TNT1)

- In the real world the original intermediate values $(X^q, Y^q, U^q, V^q, W^q, K)$ will be released
- In the ideal world the intermediate values will be sampled accordingly:
  - K will be sampled as a dummy key from the key space

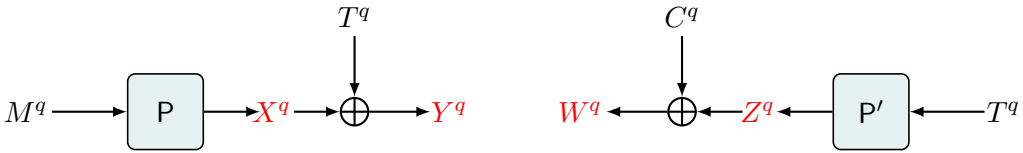




(U^q, V^q) is yet to be sampled

Proof Sketch: Releasing intermediate variables (b-TNT2)

- In the real world the original intermediate values $(X^q, Y^q, U^q, V^q, W^q, Z^q)$ will be released
- In the ideal world the intermediate values will be sampled accordingly:



(U^q, V^q) is yet to be sampled

Proof Sketch: Bad partial transcript

Partial transcript: $X^q, Y^q, W^q, K(\text{b-TNT1})/Z^q(\text{b-TNT2})$

- The partial transcript is called Bad if one of the following holds:
  1. Bad_K: $K = 0^n$ (This condition is only for b-TNT1).
  2. Bad_1 (cycle of length 2): $\exists i, j \in [q]$ such that the following holds: $Y_i = Y_j, W_i = W_j$.
  3. Bad_2: $|\{(i,j) \in [q]^2 : i \neq j, Y_i = Y_j\}| \geq q^{2/3}$.
  4. Bad_3: $|\{(i,j) \in [q]^2 : i \neq j, W_i = W_j\}| \geq q^{2/3}$.
  5. Bad_4 (Y-W-Y path of length 4): $\exists i, j, k, l \in [q]$ such that the following holds: $Y_i = Y_j, W_j = W_k, Y_k = Y_l$.
  6. Bad_5 (W-Y-W path of length 4): $\exists i, j, k, l \in [q]$ such that the following holds: $W_i = W_j, Y_j = Y_k, W_k = W_l$.

Proof Sketch: Constructing transcript graph

- For a bad partial transcript, (U^q, V^q) will be sampled degenerately i.e., $U_i = V_i = 0$ $\forall i \in [q]$.

- For a good partial transcript construct an edge labeled bipartite graph $\mathcal{G} := \mathcal{G}(Y^q, W^q)$:

  - **Vertices:** $Y^q = \{Y_1, \ldots, Y_q\} \bigsqcup W^q = \{W_1, \ldots, W_q\}$

  - **Labeled edges:** $\{Y_i, W_i\} \in E$ with label T_i

  - For two distinct indices $i \neq j$, if $Y_i = Y_j$, then we merge the corresponding vertices. Similarly, for two distinct indices, if $W_i = W_j$, then we merge the corresponding vertices.

Proof Sketch: Structures of a good transcript graph

Properties of a good transcript graph

- Simple, contains no cycle
- Has no even length path with label sum 0
- Every path has a maximum length of 3
- Maximum component size can be $2q^{2/3}$

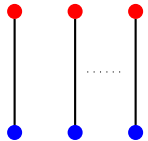


Figure: Type-1

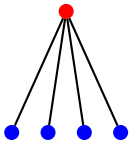


Figure: Type-2

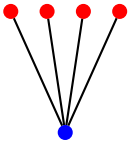


Figure: Type-3

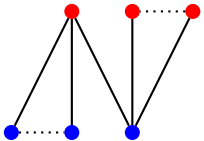


Figure: Type-4

Proof Sketch: Sampling (U^q, V^q) for good transcripts

- Consider $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$, where $\mathcal{I}_b = \{i \in [q] : (Y_i, W_i) \in \text{Type-}b\}$ for $b \in [4]$
- Consider $\mathcal{E} = \{U_i \oplus V_i = T_i : i \in \mathcal{I}\}$, where $U_i = U_j$ iff $Y_i = Y_j$ and $V_i = V_j$ iff $W_i = W_j$ for all $i \neq j \in [q]$
- Solution set of $\mathcal{E}$, $\mathcal{S} = \{(u^{\mathcal{I}}, v^{\mathcal{I}}) : u^{\mathcal{I}} \leftrightsquigarrow Y^{\mathcal{I}}, v^{\mathcal{I}} \leftrightsquigarrow W^{\mathcal{I}}, u^{\mathcal{I}} \oplus v^{\mathcal{I}} = T^{\mathcal{I}}\}$
- Now we sample (U^q, V^q) in the following way:
  - $(U^{\mathcal{I}}, V^{\mathcal{I}}) \xleftarrow{\$} \mathcal{S}$, i.e., it uniformly samples one valid solution from the set of all valid solutions
  - For Type-4 graph select (Y_i, W_i) such that the degree of both Y_i and W_i is at least 2. Then, we sample $U_i \xleftarrow{\$} \{0,1\}^n$ and set $V_i = U_i \oplus T_i$
  - Then for the other edges (Y_j, W_j) of Type-4 graph, either $Y_j = Y_i$, then $U_j = U_i$ and $V_j = U_j \oplus T_j$ or $W_j = W_i$, then $V_j = V_i$ and $U_j = V_j \oplus T_j$

Proof Sketch: Sampling induced bad events

- The sampling of the values (U^q, V^q) may lead to permutation incompatibility

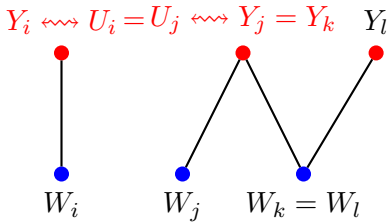


Figure: $\mathsf{Ucoll}_{1,4}$

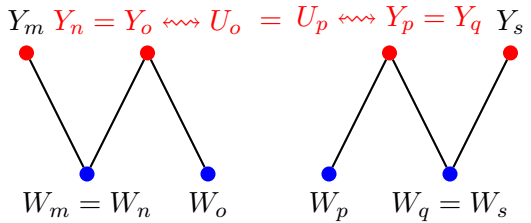


Figure: $\mathsf{Ucoll}_{4,4}$

- $\mathsf{Ucoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ such that $Y_i \neq Y_j$ and $U_i = U_j$, for $\alpha \in [4]$ and $\beta \in [\alpha, 4]$
- $\mathsf{Vcoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ such that $W_i \neq W_j$ and $V_i = V_j$, for $\alpha \in [4]$ and $\beta \in [\alpha, 4]$

$$\mathsf{Bad\text{-}samp} := \bigcup_{\substack{\alpha \in [4] \\ \beta \in [\alpha, 4]}} (\mathsf{Ucoll}_{\alpha,\beta} \cup \mathsf{Vcoll}_{\alpha,\beta})$$

Proof Sketch: Good transcript analysis

- Real World: Counted the number of calls of each permutations.
- Ideal World:
  - For graph of Type-1,2,3: Used Mirror Theory results for the tweakable random permutations developed by Jha and Nandi [JN, JoC'20]
  - For graph of Type-4: Counted the number of components
- Finally, using Expectation Method we derive the advantage bound of both the constructions.

Experimental Results

Cycles and cycles per byte for proposed constructions, constructions labeled with * also include the key schedule cost.

Construction	Cycles	Cycles per byte
CLRW1^4	184	11.5
b-TNT1	150	9.37
b-TNT2	164	10.25
CLRW1^{4*}	1719	107.44
b-TNT1$*$	1240	77.5
b-TNT2$*$	1645	102.81

- Unlike CLRW1^4, b-TNT1 requires three block cipher calls along with a field multiplication
- b-TNT2 requires four block cipher calls but its execution of block cipher calls can be pipelined which makes it efficient over CLRW1^4

Open Problems

- Is the proven security bound of b-TNT1 and b-TNT2 tight?
- Can we design any other efficient BBB secure TBC constructions?
- What about the multi user security of the constructions b-TNT1, b-TNT2 and CLRW1[4]?

Thank You!