Cascading Four Round LRW1 is Beyond Birthday Bound Secure

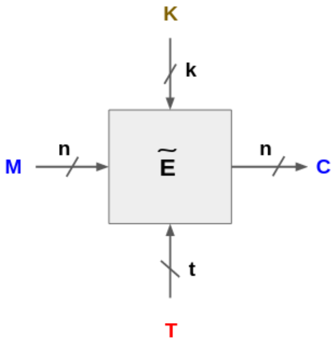
Nilanjan Datta [1], **Shreya Dey** [1, 2], Avijit Dutta [1] and Sougata Mandal [1, 2]

[1]Institute for Advancing Intelligence, TCG Crest
[2]Ramakrishna Mission Vivekananda Educational and Research Institute.

FSE, 2024

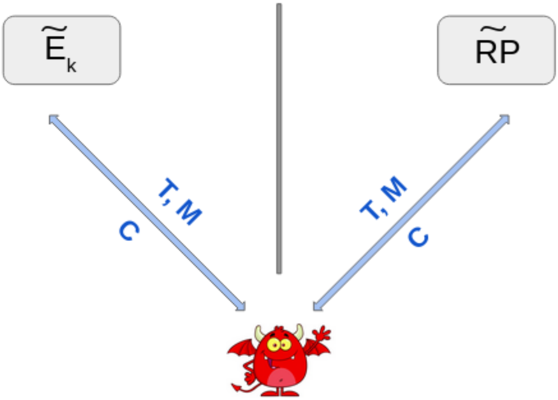
March 27, 2024

Tweakable Block Cipher



- Tweak T is a public value (controlled by adversary)
- Like Block Cipher, it process fixed size data
- For each (K, T), $M \mapsto \widetilde{\mathsf{E}}_K^T(M)$ is a permutation over $\{0,1\}^n$
- For each K, $\widetilde{\mathsf{E}}_K$ is a family of permutations over $\{0,1\}^n$

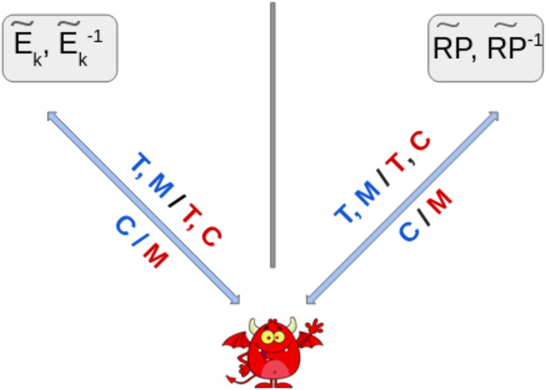
TPRP Security :



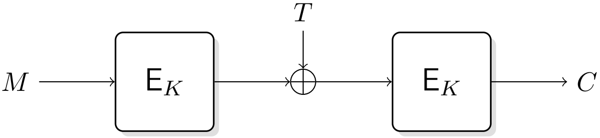
Adversary should not be able to distinguish!

Formal Security Notion of TBC

STPRP Security :



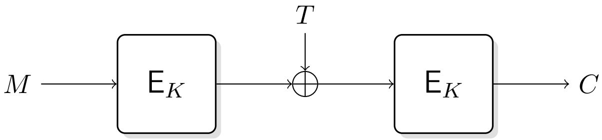
Adversary should not be able to distinguish!



LRW1 Construction, [Liskov et al., CRYPTO'02]

- Achieves tight CPA security upto $2^{n/2}$ queries

Designing TBC from BC

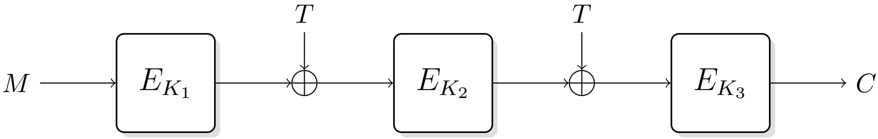


LRW1 Construction, [Liskov et al., CRYPTO'02]

- Achieves tight CPA security upto $2^{n/2}$ queries

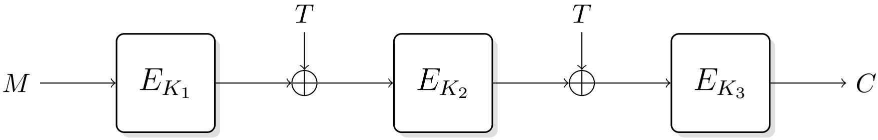
LRW1 is NOT CCA secure!

Recent Developments on LRW1



CLRW1^3(TNT) Construction, [Bao et al., EC'20]

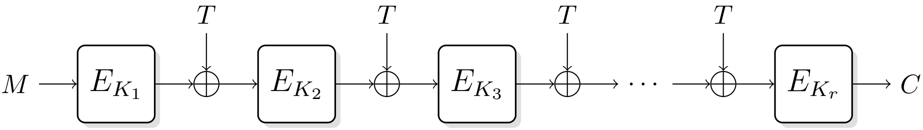
- Achieves CCA security upto $2^{2n/3}$ queries **[Bao et al., EC'20]**



CLRW1^3(TNT) Construction, [Bao et al., EC'20]

- Achieves CCA security upto $2^{2n/3}$ queries **[Bao et al., EC'20]**
- Achieves tight CPA security upto $2^{3n/4}$ queries **[Guo et al., AC'20]**

Recent Developments on LRW1



CLRW1^r Construction, [Zhang et al., DCC'22]

- Achieves CCA security upto $2^{(r-1)n/(r+1)}$ queries, when r is odd **[Zhang et al. DCC'22]**
- Achieves CCA security upto $2^{(r-2)n/r}$ queries, when r is even **[Zhang et al. DCC'22]**

Invalid Security Bound of TNT

- First, [**Khairallah, ePrint 2023/1212**] presented a birthday bound CCA distinguishing attack on TNT
  - Analyzed the distinguisher using statistics of random permutation
- Later, **[Jha et al., ePrint 2023/1272]** presented a CCA distinguishing attack on TNT
  - Provided rigorous analysis for the advantage of the distinguisher

TNT is broken with $2^{\frac{n}{2}}$ queries!

Invalid Security Bound of TNT

- First, [**Khairallah, ePrint 2023/1212**] presented a birthday bound CCA distinguishing attack on TNT
  - Analyzed the distinguisher using statistics of random permutation
- Later, **[Jha et al., ePrint 2023/1272]** presented a CCA distinguishing attack on TNT
  - Provided rigorous analysis for the advantage of the distinguisher

TNT is broken with $2^{\frac{n}{2}}$ queries!

Security claim of **Bao et al.** stands **INVALID**

Current Scenario

- 3 round CLRW1 achieves Tight BB CCA security
  - BB CCA security is due to **[Zhang et al., DCC'22]**
  - Tightness of the bound is due to **[Khairallah, ePrint 2023/1233]** and **[Jha et al., ePrint 2023/1272]**
- 4 round CLRW1 achieves BB CCA security
  - Due to **[Zhang et al., DCC'22]**
- 5 round CLRW1 achieves BBB CCA security
  - Due to **[Zhang et al., DCC'22]**

Security bound of **Zhang et al.** is **NOT TIGHT!**

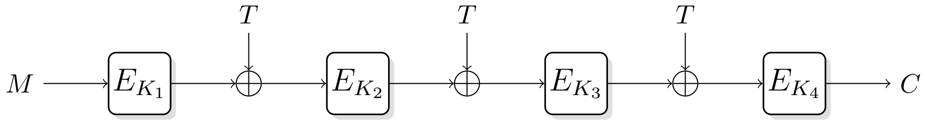
Current Scenario

- 3 round CLRW1 achieves Tight BB CCA security
  - BB CCA security is due to **[Zhang et al., DCC'22]**
  - Tightness of the bound is due to **[Khairallah, ePrint 2023/1233]** and **[Jha et al., ePrint 2023/1272]**
- 4 round CLRW1 achieves BB CCA security
  - Due to **[Zhang et al., DCC'22]**
- 5 round CLRW1 achieves BBB CCA security
  - Due to **[Zhang et al., DCC'22]**

Security bound of **Zhang et al.** is **NOT TIGHT!**

Can a BB CCA attack be found against CLRW1^4?
OR
Does CLRW1^4 achieve security beyond the BB?

4 Rounds Cascading of LRW1

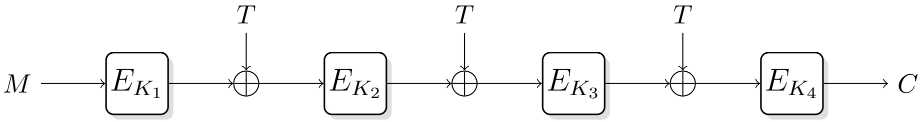


CLRW1^4 Construction

Our Contribution

- **We have shown CLRW1^4 is secure upto $2^{\frac{3n}{4}}$ CCA queries**
- **Confirms atleast 4 rounds are required for CLRW1 to achieve BBB security**

4 Rounds Cascading of LRW1



CLRW1^4 Construction

Our Contribution

- **We have shown CLRW1^4 is secure upto $2^{\frac{3n}{4}}$ CCA queries**
- **Confirms atleast 4 rounds are required for CLRW1 to achieve BBB security**

† Concurrent to this work, **[Jha et al., ePrint 2023/1272]** have also shown $3n/4$ bit security of CLRW1^4

Security Result

Suppose,

- Block cipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
- $\mathcal{A}$: An (q,t) adversary against the strong tweakable pseudo random permutation security of CLRW1^4 $(q \leq 2^{\frac{3n}{4}})$

Then,

- $\exists \mathcal{A}'$: An (q,t') adversary against the strong pseudo random permutation security of E $(t = t')$

such that

$$\mathbf{Adv}^{tsprp}_{CLRW1^4[E]}(\mathcal{A}) \leq 4\mathbf{Adv}^{sprp}_{E}(\mathcal{A}') + \frac{6q^2}{2^{2n}} + \frac{4q^{\frac{4}{3}}}{2^n} + \frac{38q^4}{2^{3n}}$$

Mirror Theory

System of Equations

- Equations : $\mathcal{L} = \{Y_1 \oplus W_1 = T_1, Y_2 \oplus W_2 = T_2, \cdots, Y_q \oplus W_q = T_q\}$
- Variable Set : $\{Y_1, Y_2, \cdots, Y_q\}$, $\{W_1, W_2, \cdots, W_q\}$
- Constants : $(T_1, T_2, \cdots, T_q)$

Graphical Representation

- Vertices : $\{Y_1, Y_2, \cdots, Y_q\}$, $\{W_1, W_2, \cdots, W_q\}$
- Edges : Labeled edge (Y_i, W_i) with label T_i
- Merge $Y_i(W_i)$ and $Y_j(W_j)$ $\iff$ $Y_i(W_i) = Y_j(W_j)$
- Distinct vertices : $\{Y'_1, Y'_2, \cdots, Y'_{q_Y}\}$ and $\{W'_1, W'_2, \cdots, W'_{q_W}\}$

Properties of the BAD graph

- ✓ Contains a path of length atleast 4
- ✓ Contains a cycle
- ✓ Contains an even length path with sum of labels is 0
- ✓ The size of a component is atleast $2q^{\frac{2}{3}}$

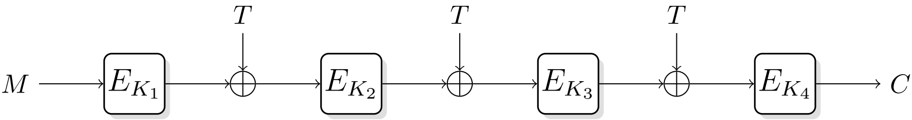
Mirror Theory **[JN, JoC'20]**

For a good graph, # of solutions to the associated system of equations is at least

$$\left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=\alpha+1}^{\beta+\gamma} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right) \times \frac{(2^n)_{q_1+\beta+q_3} \times (2^n)_{q_1+q_2+\gamma}}{\prod_{\lambda \in \lambda^q} (2^n)_{\mu_\lambda}}$$

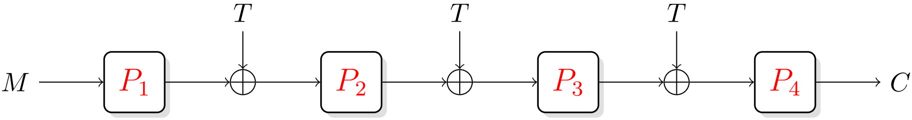
Proof Sketch: Using SPRP Security of E_k

Replace Block Cipher with Random Permutation



CLRW1^4[E]

$$\Downarrow$$

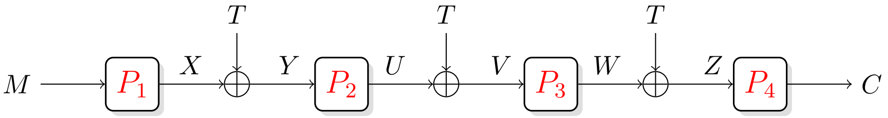


CLRW1^4[P]

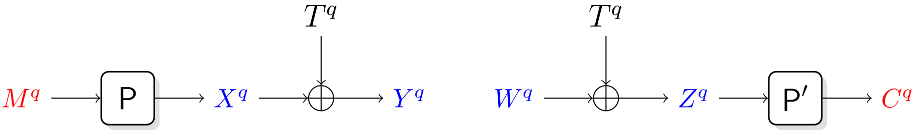
Proof Sketch: Releasing Intermediate Variables

It reveals the intermediate variables (X, Y, U, V, W, Z)

Releasing in Real World



Releasing in the Ideal World



$(\mathbf{U^q}, \mathbf{V^q})$ is yet to be sampled

Proof Sketch: Constructing Transcript Graph

Partial Trascript: $(M^q, X^q, Y^q, W^q, Z^q, C^q)$

Construct an edge labeled bipartite graph

- **Vertices:** $\mathcal{V}_1 = \{Y_1, Y_2, \cdots, Y_q\} \bigcup \mathcal{V}_2 = \{W_1, W_2, \cdots W_q\}$
- **Labeled Edges:** $\{Y_i, W_i\} \in E$ with label T_i

Merge Y_i and Y_j if $Y_i = Y_j$ and W_i and W_j if $W_i = W_j$

Proof Sketch: Graph Characteristics

Bad Partial Transcript

We call a partial transcript $(M^q, X^q, Y^q, W^q, Z^q, C^q)$ is **bad** if the graph $\mathcal{G}(Y^q, W^q)$ is a bad graph

Proof Sketch: Graph Characteristics

Bad Partial Transcript

We call a partial transcript $(M^q, X^q, Y^q, W^q, Z^q, C^q)$ is **bad** if the graph $\mathcal{G}(Y^q, W^q)$ is a bad graph

For a bad partial transcript, we sample (U^q, V^q) degenerately.

Proof Sketch: Graph Characteristics

Bad Partial Transcript

We call a partial transcript $(M^q, X^q, Y^q, W^q, Z^q, C^q)$ is **bad** if the graph $\mathcal{G}(Y^q, W^q)$ is a bad graph

For a bad partial transcript, we sample (U^q, V^q) degenerately.

Properties of the Good graph

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

Proof Sketch: Good Graph

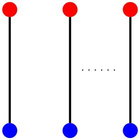


Figure: Type-I

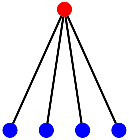


Figure: Type-II

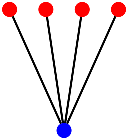


Figure: Type-III

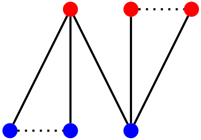


Figure: Type-IV

Proof Sketch: Sampling (U^q, V^q)

- Consider $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$, where $\mathcal{I}_b = \{i \in [q] : (Y_i, W_i) \in \text{Type}_b\}$
- Consider $\mathcal{E} := \left\{U_i \oplus V_i = T_i : i \in \mathcal{I}\right\}$
- Solution set, $\mathcal{S} = \left\{(U_i, V_i) : U^{\mathcal{I}} \leftrightsquigarrow Y^{\mathcal{I}}, V^{\mathcal{I}} \leftrightsquigarrow W^{\mathcal{I}}, U_{\mathcal{I}} \oplus V_{\mathcal{I}} = T_{\mathcal{I}}\right\}$
- Sample $(U^{\mathcal{I}}, V^{\mathcal{I}}) \xleftarrow{\$} \mathcal{S}$

However, it remains to sample (U, V) for Type-IV component

- Select (Y_i, W_i) such that $\deg(Y_i) = \deg(W_i) \geq 2$
- Sample $U_i \xleftarrow{\$} \{0,1\}^n$
- Set $V_i = U_i \oplus T_i$

The sampling may lead to permutation incompatible transcript

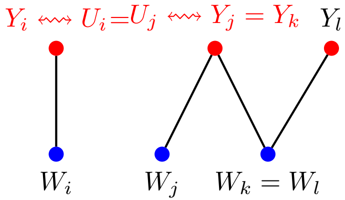


Figure: $\mathsf{Ucoll}_{1,4}$

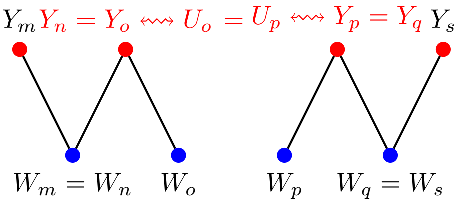


Figure: $\mathsf{Ucoll}_{4,4}$

Proof Sketch: Bad Sampling

Sampling Induced Bad Events

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

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

Proof Sketch: Analysis of Good Transcripts

Real World: Counted the number of times each permutation is invoked

Ideal World:

- **For Type-1, 2 and 3:** Used Mirror Theory results for the tweakable random permutations **[JN, JoC'20]**
- **For Type-4:** Counted the number of components

Conclusion

1. Is the proven security bound for CLRW1^4 tight or not?

Conclusion

1. Is the proven security bound for $\mathsf{CLRW1}^4$ tight or not?
2. Whether the bounds of $\mathsf{CLRW1}^r$ for general $r \geq 5$ can be improved.

Conclusion

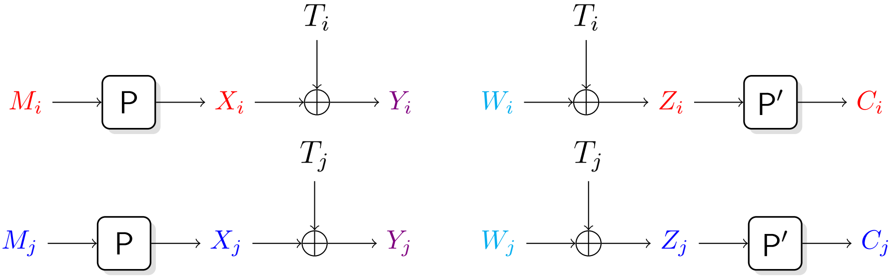
1. Is the proven security bound for CLRW1^4 tight or not?
2. Whether the bounds of CLRW1^r for general $r \geq 5$ can be improved.
3. What about the multi-user security of CLRW1^4?

Thank You!

Proof Sketch: Identifying Bad Events

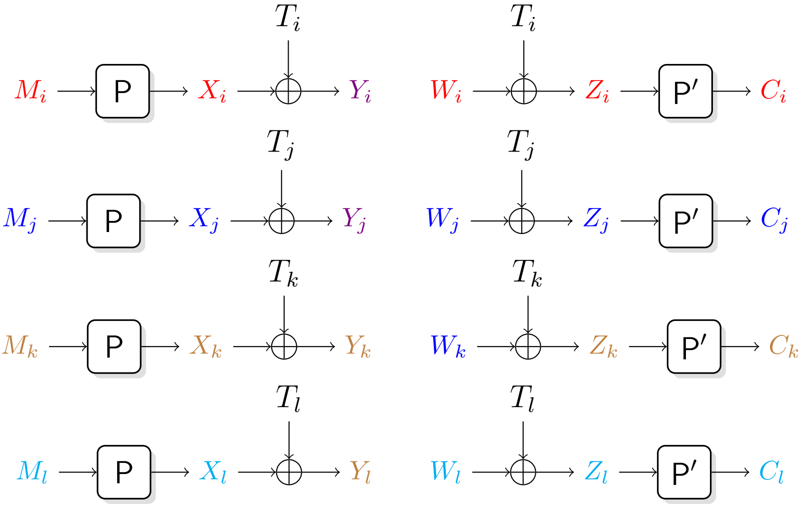
Bad 1: $\exists i, j \in [q]$ such that $Y_i = Y_j, W_i = W_j$



- **Bad 2:** $\left|\{(i,j) \in [q]^2 : Y_i = Y_j\}\right| \geq q^{\frac{2}{3}}$
- **Bad 3:** $\left|\{(i,j) \in [q]^2 : W_i = W_j\}\right| \geq q^{\frac{2}{3}}$

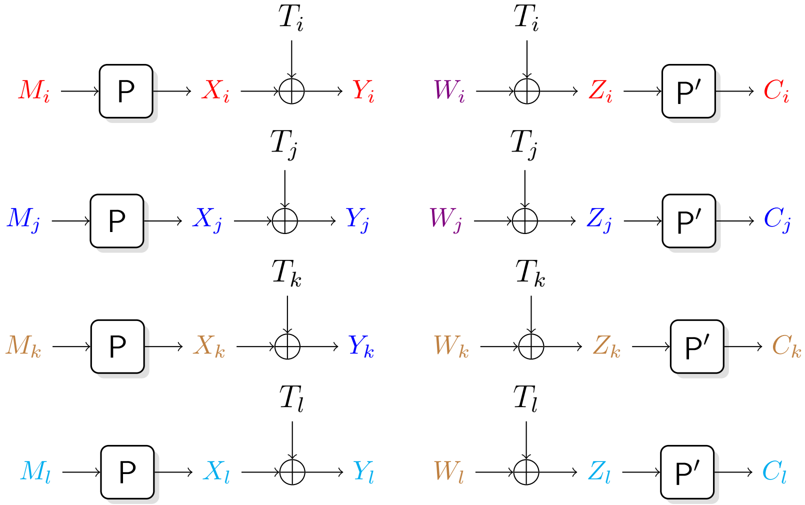
Proof Sketch: Identifying Bad Events

Bad 4: $\exists i, j, k, l \in [q]$ such that $Y_i = Y_j, W_j = W_k, Y_k = Y_l$

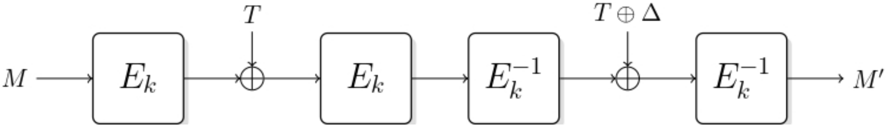


Proof Sketch: Identifying Bad Events

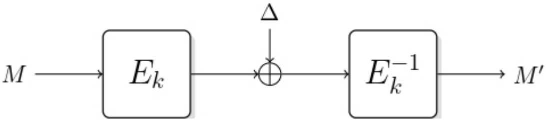
Bad 5: $\exists i, j, k, l \in [q]$ such that $W_i = W_j, Y_j = Y_k, W_k = W_l$



CCA Insecurity of LRW1 Construction



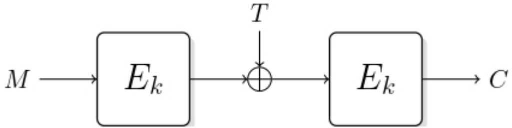
$$\Updownarrow$$



Characteristic Equation: $E_K(M) \oplus E_K(M') = \Delta$

CCA Insecurity of LRW1 Construction

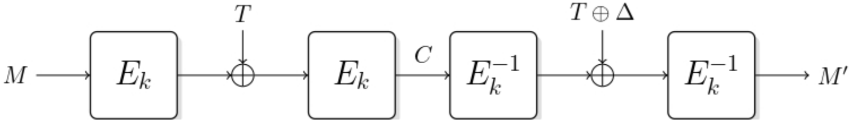
Attack Algorithm



Adversary $\mathcal{A}$ makes an encryption query (M, T) and obtains the ciphertext C

CCA Insecurity of LRW1 Construction

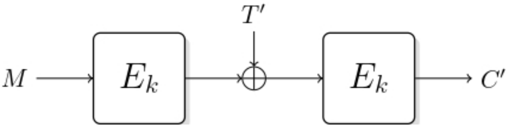
Attack Algorithm



Adversary $\mathcal{A}$ makes a decryption query $(C, T \oplus \Delta)$ and obtains the plaintext M'

(I) It yields the characteristic equation: $E_K(M) \oplus E_K(M') = \Delta$

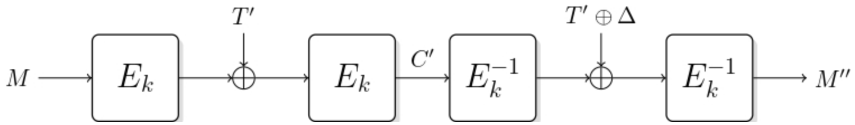
Attack Algorithm



Adversary $\mathcal{A}$ makes another encryption query (M, T') and obtains the ciphertext C'

CCA Insecurity of LRW1 Construction

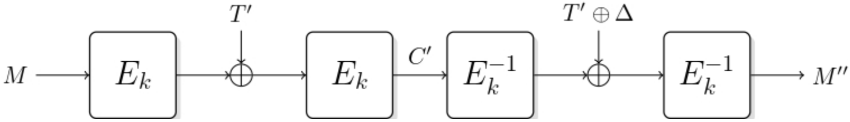
Attack Algorithm



Adversary $\mathcal{A}$ makes a decryption query $(C', T' \oplus \Delta)$ and obtains the plaintext M''

(II) It yields the characteristic equation: $E_K(M) \oplus E_K(M'') = \Delta$

Attack Algorithm



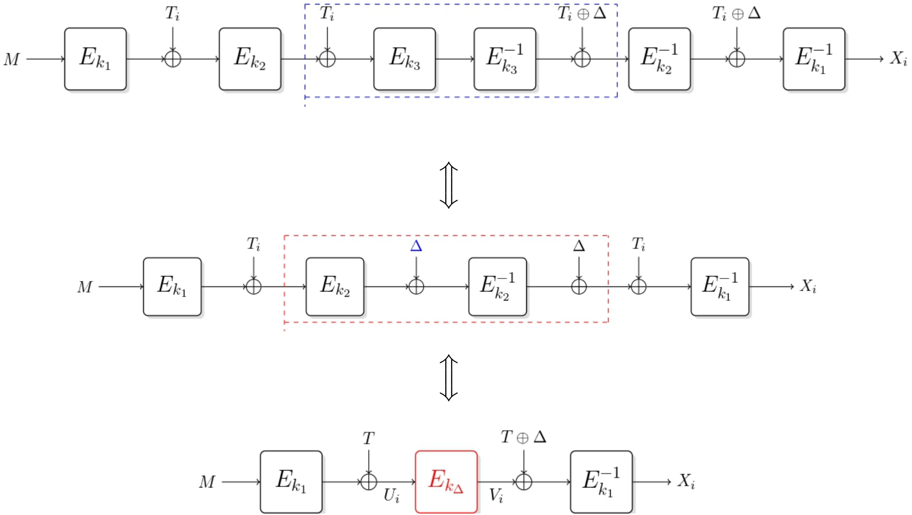
Adversary $\mathcal{A}$ makes a decryption query $(C', T' \oplus \Delta)$ and obtains the plaintext M''

(II) It yields the characteristic equation: $E_K(M) \oplus E_K(M'') = \Delta$

From (I) and (II), $E_k(M) \oplus E_K(M') = \Delta = E_K(M) \oplus E_K(M'') \Rightarrow M' = M''$

Birthday Bound Attack on CLRW1^3

Extension of the CCA Attack on LRW1



Birthday Bound Attack on CLRW1[3]

- Fix a message $m \in \{0,1\}^n$
- Fix a subspace $\mathcal{T} = \{t_1, t_2, \ldots, t_q\} \subseteq \{0,1\}^n$.
- Fix a $\Delta \notin \mathcal{T}$.
- For all $t_i \in \mathcal{T}$, do the following:

  - Make encryption query (m, t_i) and the response is C_i
  - Make the decryption query $(C_i, t_i \oplus \Delta)$ and the response is X_i
  - $\mathcal{A}$ outputs 1 if $\exists j < i$ such that $X_i = X_j$