Beyond Birthday Bound Security of CLRW1^4

Avijit Dutta

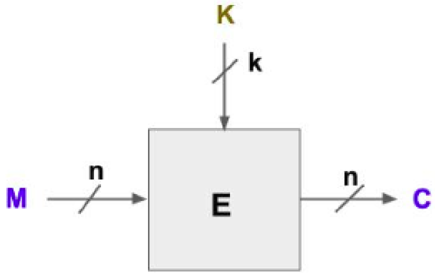
Institute for Advancing Intelligence, TCG CREST

Research Talk at ASK, 2023

tcg crest
Inventing Harmonious Future

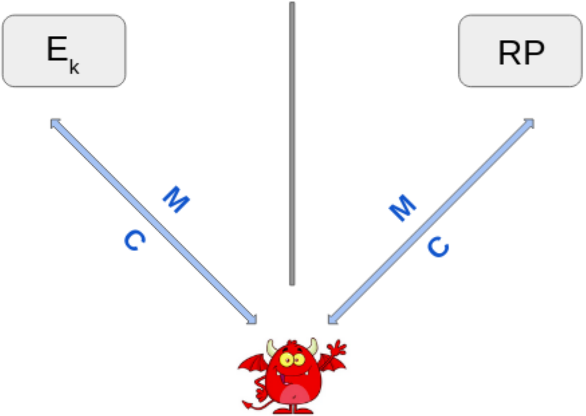
December 02, 2023

Block Cipher



- A family of permutations indexed by key
- Process fixed size data
- Key size and data size need not be equal
- For each key k, E_k is a permutation over $\{0,1\}^n$
- Popular examples of block ciphers are AES, PRESENT, GIFT etc.

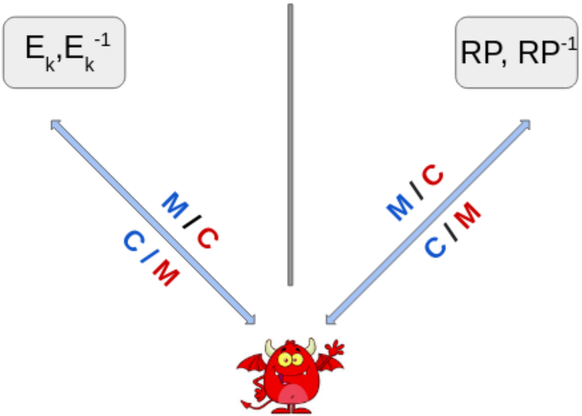
PRP Security :



$$\mathbf{Adv}_{\mathsf{E}}^{\mathrm{PRP}}(A) := |\Pr_{K \leftarrow \{0,1\}^k}[A^{\mathsf{E}_K} = 1] - \Pr_{\mathsf{RP} \leftarrow \mathsf{Perm}(n)}[A^{\mathsf{RP}} = 1]|$$

Formal Security Notion of BC

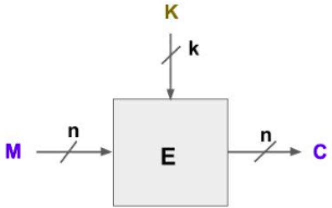
SPRP Security :



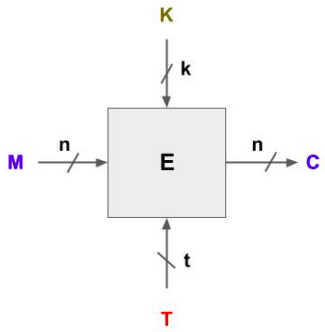
$$\mathbf{Adv}_{\mathsf{E}}^{\mathrm{SPRP}}(A) := \left| \Pr_{K \leftarrow \{0,1\}^k}[A^{\mathsf{E}_K, \mathsf{E}_K^{-1}} = 1] - \Pr_{\mathsf{RP} \leftarrow \mathsf{Perm}(n)}[A^{\mathsf{RP}, \mathsf{RP}^{-1}} = 1] \right|$$

Block Cipher in Modes of Operations

- Block Cipher processes fixed size data
- To process arbitrary size data, block ciphers are invoked as primitive in certain way that defines the modes of operations
- Although it provides security, but does not bring variability into the cipher
- To introduce variability, one needs to change the block cipher key
- Frequnt changes of key is a costly business



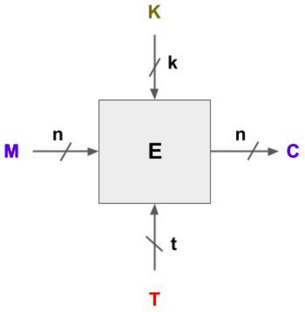
Tweakable Block Cipher



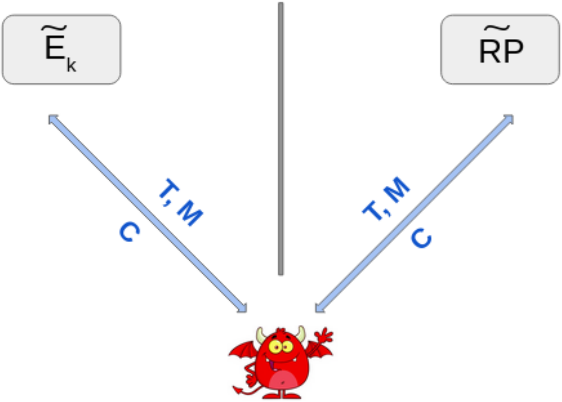
- An additional public value tweak T (controlled by adversary)
- Like Block Cipher, it process fixed size data
- For each (k, t), $M \mapsto \mathsf{E}_k^t(M)$ is a permutation over $\{0,1\}^n$

Tweakable Block Cipher

- Each fixed setting of the tweak gives rise to a independent family of BC
- Fixing the input and varying tweaks yields a random function.
- Fixing the tweak and varying input yields a random permutation
- Key provides uncertainity
- Tweak Provides variability

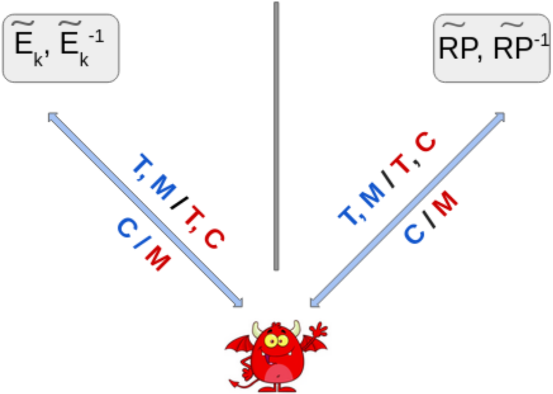


TPRP Security :



$$\mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{\mathsf{E}}}(A) := |\Pr_{K \leftarrow \{0,1\}^k}[A^{\widetilde{\mathsf{E}}_K} = 1] - \Pr_{\widetilde{\mathsf{RP}} \leftarrow \widetilde{\mathsf{Perm}}(n)}[A^{\widetilde{\mathsf{RP}}} = 1]|$$

STPRP Security :



$$\mathbf{Adv}_{\widetilde{\mathsf{E}}}^{\mathrm{STPRP}}(A) := \left| \Pr_{K \leftarrow \{0,1\}^k}\left[A^{\widetilde{\mathsf{E}}_K, \widetilde{\mathsf{E}}_K^{-1}} = 1\right] - \Pr_{\widetilde{\mathsf{RP}} \leftarrow \widetilde{\mathsf{Perm}}(n)}\left[A^{\widetilde{\mathsf{RP}}, \widetilde{\mathsf{RP}}^{-1}} = 1\right] \right|$$

Designing Tweakable Block Ciphers

- There are two ways to design a tweakable block cipher:
  1. Design from classical block ciphers in a black box fashion
  2. Design tweakable block ciphers from scratch

- In the black box setting, there are two design approaches:
  1. Tweakable block ciphers are designed from classical block ciphers by assuming that the underlying block ciphers are pseudorandom permutations.
  2. This design strategy was introduced by Liskov et al.

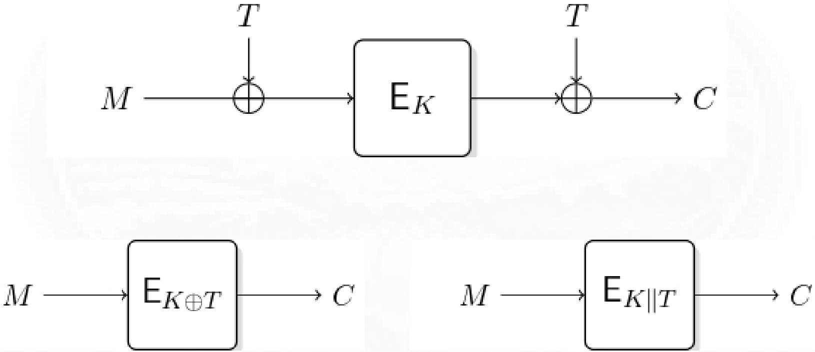
  1. Tweakable block ciphers are designed from classical block ciphers by assuming that the underlying block ciphers function as ideal ciphers.
  2. This design strategy was introduced by Mennink.

- These two design approaches not only differ in their security assumptions but also in their design principles.

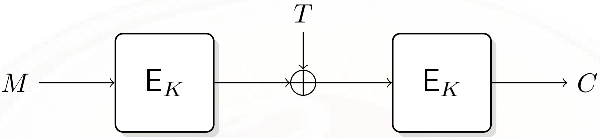
Our study is on designing TBC from BC where BC is a PRP

Designing Tweakable Block Ciphers from Block Ciphers

Some Insecure Constructions:



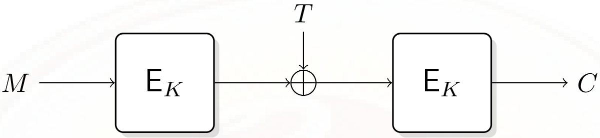
Designing Tweakable Block Ciphers from Block Ciphers



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

Tight CPA security upto $2^{n/2}$ queries, assuming E_k is secure PRP

Designing Tweakable Block Ciphers from Block Ciphers

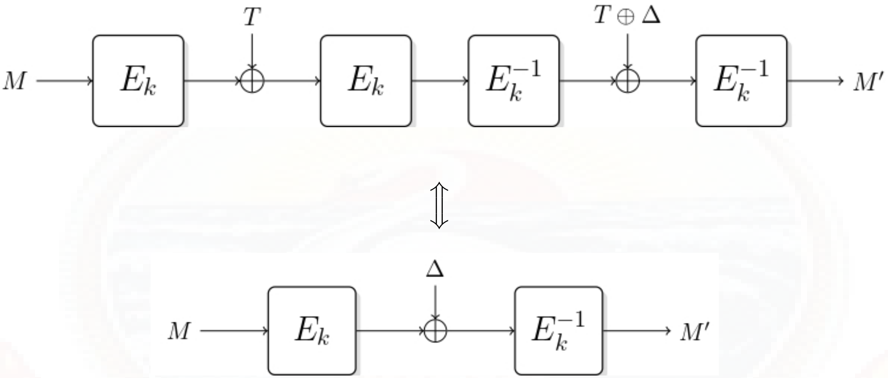


LRW1 Construction, [Liskov et al., CRYPTO'02]

Tight CPA security upto $2^{n/2}$ queries, assuming E_k is secure PRP

LRW1 is not CCA secure

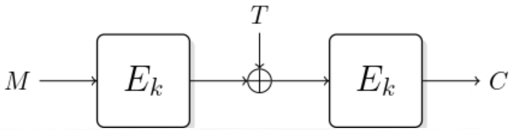
CCA Insecurity of LRW1 Construction



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

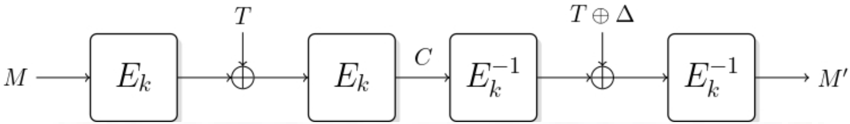
CCA Insecurity of LRW1 Construction

Attack Algorithm



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

Attack Algorithm

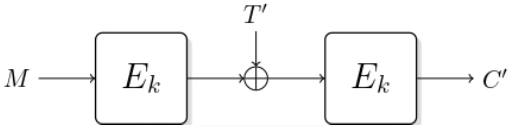


Adversary $\mathcal{A}$ makes a decryption query $(C, T \oplus \Delta)$ and obtains the plaintext M'

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

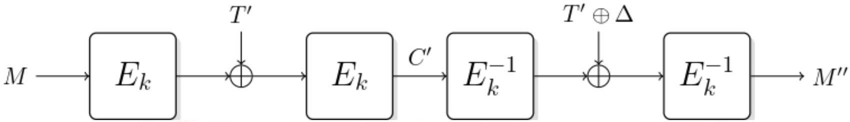
CCA Insecurity of LRW1 Construction

Attack Algorithm



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

Attack Algorithm

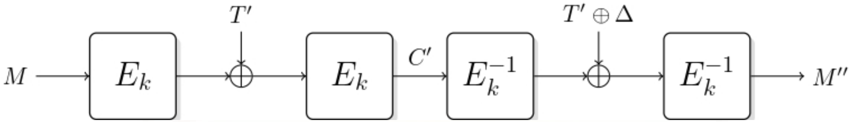


Adversary $\mathcal{A}$ makes a decryption query $(C', T' \oplus \Delta)$ and obtains the plaintext M''

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

CCA Insecurity of LRW1 Construction

Attack Algorithm



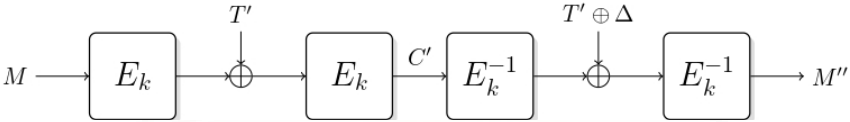
Adversary $\mathcal{A}$ makes a decryption query $(C', T' \oplus \Delta)$ and obtains the plaintext M''

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

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

CCA Insecurity of LRW1 Construction

Attack Algorithm



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

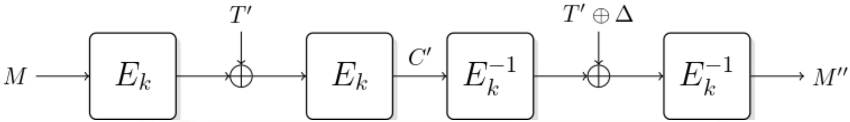
(II) It yields the characteristic equation: $E_K(M) \oplus E_K(M'') = \Delta$

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

- Can we have a STPRP secure TBC with a single BC call ?

CCA Insecurity of LRW1 Construction

Attack Algorithm



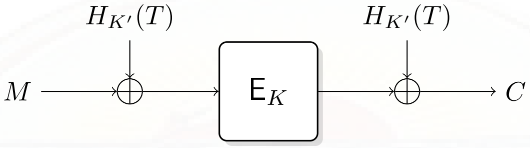
Adversary $\mathcal{A}$ makes a decryption query $(C', T' \oplus \Delta)$ and obtains the plaintext M''

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

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

- Can we have a STPRP secure TBC with a single BC call ?
- How many BC calls are required to yield STPRP security with linear tweak mixing ?

Designing Tweakable Block Ciphers from Block Ciphers



LRW2 Construction, [Liskov et al., CRYPTO'02]

Tight CCA security upto $2^{n/2}$ queries, assuming E_k is SPRP and H is AXU

Follow-ups on LRW2 Construction

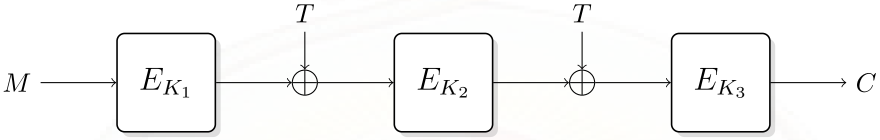
- Extended LRW2 to achieve BBB security [**Landecker et al., CRYPTO'12**]
  - Two-round cascading of LRW2 (CLRW2) is secure upto $2^{2n/3}$ queries
- Extended cascading LRW2 to r round [**Lampe and Seurin, FSE'13**]
  - CLRW2^r achieves CCA security upto $2^{(r-1)n/(r+1)}$ queries, when r is odd
  - CLRW2^r achieves CCA security upto $2^{rn/(r+2)}$ queries, when r is even
- Improved CLRW2 to a tight $3n/4$-bit CCA security bound [**Mennink, TCC'18 and Jha, Nandi, J. Cryptol.'20**]

Follow-ups on LRW2 Construction

- Extended LRW2 to achieve BBB security [**Landecker et al., CRYPTO'12**]
  - Two-round cascading of LRW2 (CLRW2) is secure upto $2^{2n/3}$ queries
- Extended cascading LRW2 to r round [**Lampe and Seurin, FSE'13**]
  - CLRW2^r achieves CCA security upto $2^{(r-1)n/(r+1)}$ queries, when r is odd
  - CLRW2^r achieves CCA security upto $2^{rn/(r+2)}$ queries, when r is even
- Improved CLRW2 to a tight $3n/4$-bit CCA security bound [**Mennink, TCC'18 and Jha, Nandi, J. Cryptol.'20**]

Such kind of follow up works is absent for LRW1 construction until the work of [Bao et al., EC'20]

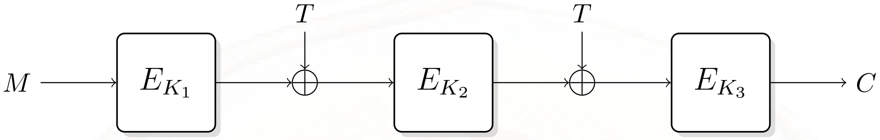
Recent Developments on LRW1



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

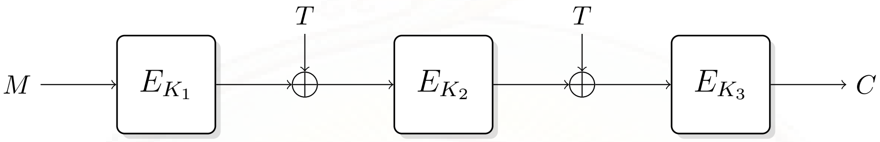
- CLRW1^3 achieves CCA security upto $2^{2n/3}$ many queries **[Bao et al., EC'20]**

Recent Developments on LRW1



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

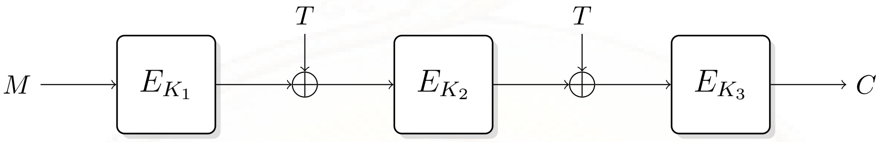
- CLRW1^3 achieves CCA security upto $2^{2n/3}$ many queries **[Bao et al., EC'20]**
- CLRW1^3 achieves tight CPA security upto $2^{3n/4}$ queries **[Guo et al., AC'20]**



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

- CLRW1^r achieves CCA security upto $2^{(r-1)n/(r+1)}$ many queries, when r is odd **[Zhang et al. DCC'22]**

Recent Developments on LRW1



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

- CLRW1^r achieves CCA security upto $2^{(r-1)n/(r+1)}$ many queries, when r is odd **[Zhang et al. DCC'22]**
- CLRW1^r achieves CCA security upto $2^{(r-2)n/r}$ many queries, when r is even **[Zhang et al. DCC'22]**

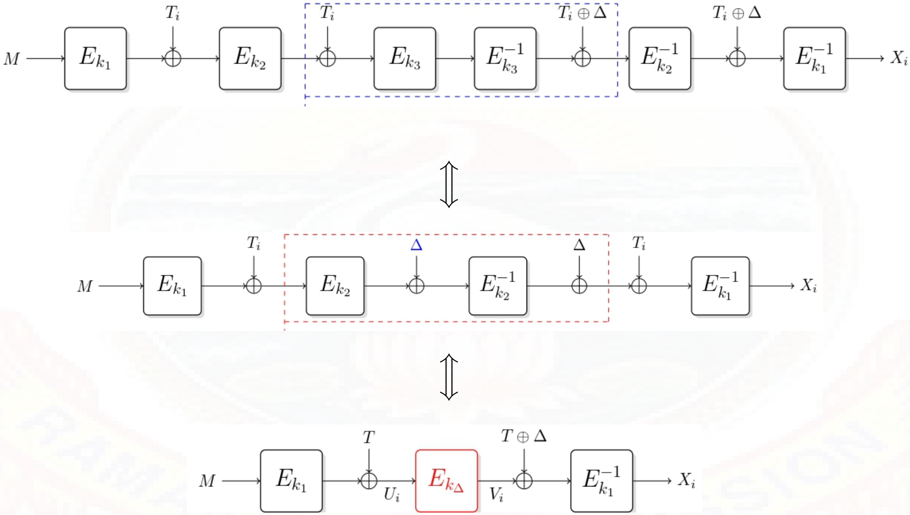
Invalid Security Bound of Bao et al. EUROCRYPT'20

- Extended cascading LRW1 to r round [**Zhang et al., DCC'22**]
  - $\mathsf{CLRW1}^r$ achieves CCA security upto $2^{\frac{(r-1)n}{r+1}}$ many queries, when r is odd
  - $\mathsf{CLRW1}^r$ achieves CCA security upto $2^{\frac{(r-2)n}{r}}$ many queries, when r is even

- Presented a birthday bound CCA distinguishing attack on $\mathsf{CLRW1}^3$ [**Khairallah, ePrint Arch., 2023/1233**]
  - Security claim of **Bao et al.** stands invalid

Birthday Bound Attack on CLRW1[3]

Extension of the CCA Attack on LRW1



Birthday Bound Attack on CLRW1^3

- The attack was first demonstrated by **[Khairallah et al., eprint 2023/1233]**.
- The attack was based on the statistics of random permutation
- Later, **[Jha et al., eprint 2023/1272]** presented a distinguishing attack and analyzed the its success probability in a more formal way

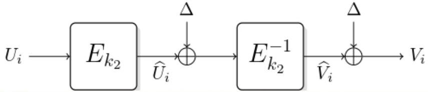
We describe the attack and analysis by [Jha et al., eprint 2023/1272]

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 $X_i = X_j$

Ideal World Collision Probability: $\Pr[\exists i \neq j : X_i = X_j] = 1 - \frac{(2^n)_q}{2^{nq}}$



Real World Collision Probability:

- $X_i = X_j \Leftrightarrow V_i \oplus V_j = t_i \oplus t_j$
- Since the same message m is used in the encryption, it implies $U_i \oplus U_j = t_i \oplus t_j$
- Therefore, $X_i = X_j \Leftrightarrow U_i \oplus V_i = U_j \oplus V_j$
- $X_i = X_j \Leftrightarrow U_i \oplus \widehat{U}_i = V_j \oplus \widehat{V}_j$

Birthday Bound Attack on CLRW1[3]

- $E_0 := \exists i \neq j : U_i \oplus V_i = U_j \oplus V_j$ holds if and only if
  1. $E_1 := \exists i \neq j : \widehat{U}_i \oplus \widehat{U}_j = \Delta$ or
  2. $E_2 := \exists i \neq j : (E_{k_2}^{-1}(\widehat{U}_i \oplus \Delta) \oplus U_i = E_{k_2}^{-1}(\widehat{U}_j \oplus \Delta) \oplus U_j)$
- Therefore, $E_0 \Leftrightarrow E_1 \vee E_2$

$$\Pr[E_0] = \Pr[E_1] + \Pr[E_1^c \wedge E_2]$$

- It is easy to calculate that $\Pr[E_1] \geq (2^n)_q / 2^{nq}$

$$\Pr_R[\exists i \neq j : X_i = X_j] = \Pr_I[\exists i \neq j : X_i = X_j] + \Pr[E_1^c \wedge E_2]$$

Birthday Bound Attack on CLRW1^3

$$\mathbf{Adv}^{tsprp}_{\mathsf{CLRW1}^3} \geq \Pr[E_1^c \wedge E_2] = \Pr[E_1^c]\Pr[E_2|E_1^c]$$

- It can be shown that

$$\Pr[E_1^c] \geq \left(1 - \frac{(2^n)_q}{2^{nq}}\right) \cdot \left(1 - \frac{2q^3}{2^{2n}}\right).$$

- Using simple algebra, one can show that

$$\Pr[E_2|E_1^c] \geq \alpha(q)\left(1 - \frac{\alpha(q)}{2}\left(1 + \frac{2}{2^n - q - 3}\right)\right).$$

- where $\alpha(q) = \binom{q}{2}/(2^n - q - 1)$

$$\mathbf{Adv}^{tsprp}_{\mathsf{CLRW1}^3} \geq \alpha(q)(1 - \alpha(q))(1 - \tfrac{\alpha(q)}{2} - \tfrac{\alpha(q)}{2^n - q - 3})\left(1 - \tfrac{2q^3}{2^{2n}}\right)$$

Current Status

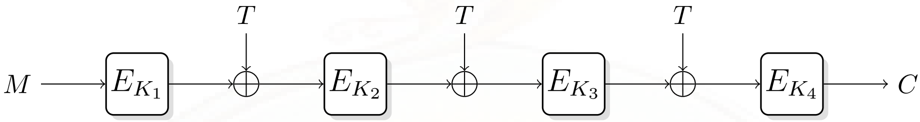
- CLRW1^3 achieves tight BB CCA security
  - Birthday bound CCA attack on CLRW1^3 due to **[Khairallah, eprint 2023/1233]** and **[Jha et al., eprint 2023/1272]**
  - Tightness of the bound is due to **[Zhang et al., DCC'22]**, and **[Jha et al., eprint 2023/1272]**
- CLRW1^4 achieves BB CCA security due to **[Zhang et al., DCC'22]**
- CLRW1^5 achieves BBB CCA security due to **[Zhang et al., DCC'22]**
- However, the bound of **[Zhang et al., DCC'22]** is loose due to the application of coupling lemma.

Current Status

- CLRW1^3 achieves tight BB CCA security
  - Birthday bound CCA attack on CLRW1^3 due to **[Khairallah, eprint 2023/1233]** and **[Jha et al., eprint 2023/1272]**
  - Tightness of the bound is due to **[Zhang et al., DCC'22]**, and **[Jha et al., eprint 2023/1272]**
- CLRW1^4 achieves BB CCA security due to **[Zhang et al., DCC'22]**
- CLRW1^5 achieves BBB CCA security due to **[Zhang et al., DCC'22]**
- However, the bound of **[Zhang et al., DCC'22]** is loose due to the application of coupling lemma.

> How many rounds are required for CLRW1 to achieve BBB security against all adaptive CCA adversaries?

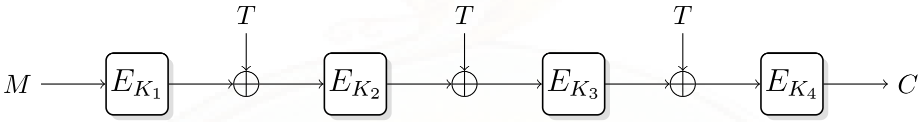
4 Rounds Cascading of LRW1



CLRW1^4 Construction

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

4 Rounds Cascading of LRW1



CLRW1^4 Construction

- **We have shown CLRW1^4 is secure upto $2^{\frac{3n}{4}}$ CCA queries**
- **Hence, four rounds are sufficient 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,

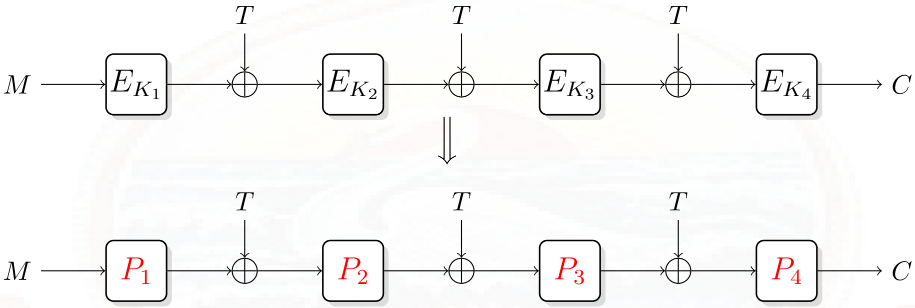
- $\exists \mathcal{A}'$: An (q,t') adversary against the strong pseudo random permutation security of E ($t = t'$)

such that

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

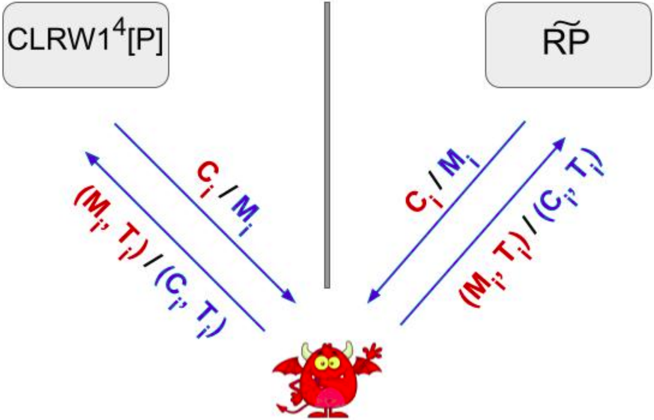
Sketch of the proof

Step 1: Replace Block Cipher with Random Permutation



$$\mathbf{Adv}^{\text{tsprp}}_{\mathsf{CLRW1}^4[E]}(\mathcal{A}) \leq 4\mathbf{Adv}^{\text{sprp}}_{E}(\mathcal{A}') + \mathbf{Adv}^{\text{tsprp}}_{\mathsf{CLRW1}^4[P]}(\mathcal{A})$$

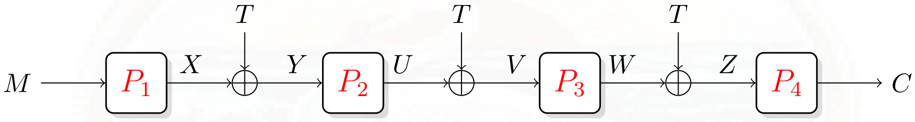
Online Phase of the Interaction:



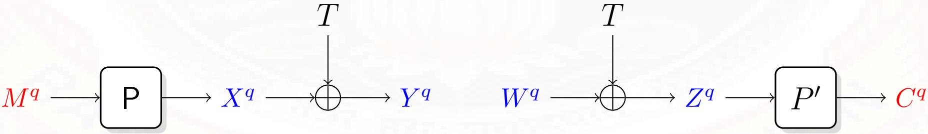
Sketch of the proof: Releasing Intermediate Variables

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

Releasing in Real World



Releasing in the Ideal World

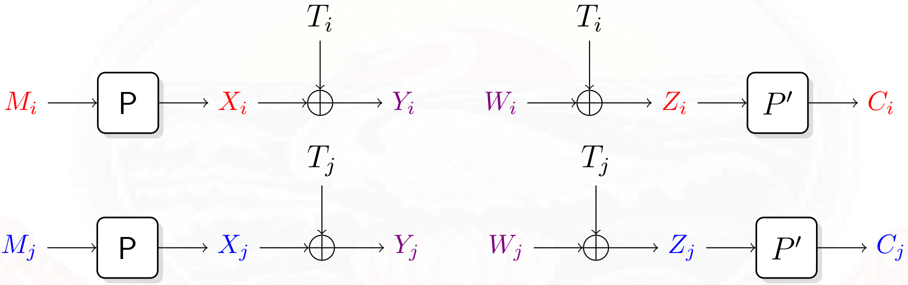


$(\mathbf{U^q}, \mathbf{V^q})$ is yet to be released in the ideal world.

Sketch of the proof: Identifying Bad Events

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

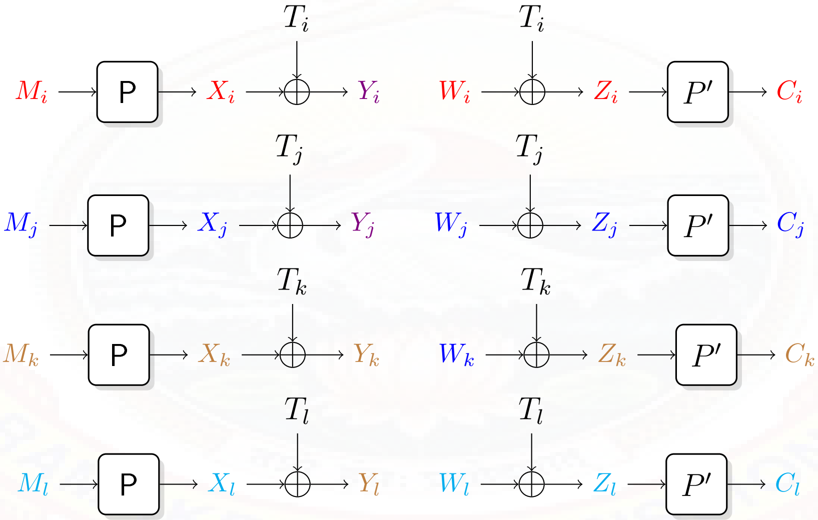
Bad 1: $\exists i, j \in [q]$ such that $Y_i = Y_j, W_i = W_j$



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

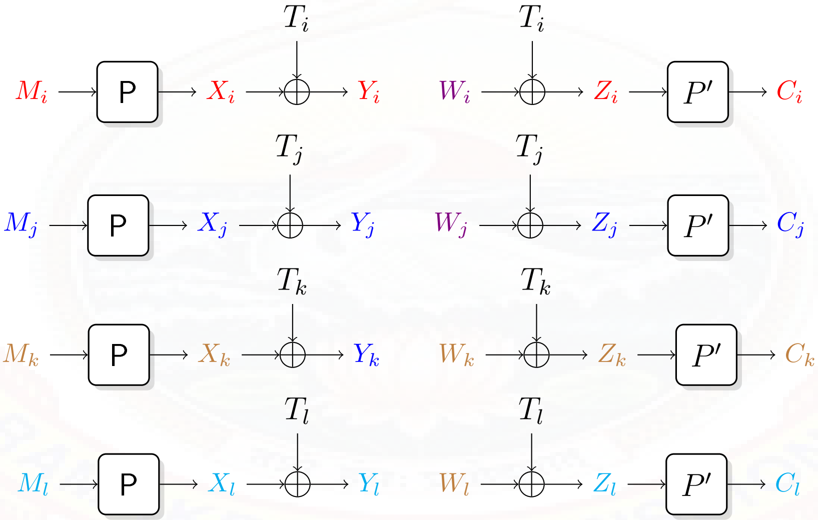
Sketch of the proof: Identifying Bad Events

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



Sketch of the proof: Identifying Bad Events

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



Sketch of the proof: Sampling (U^q, V^q) in the Ideal World

We construct an edge labeled bipartite graph given the partial transcript is **NOT BAD**

- **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 $W_i = W_j$

Sketch of the proof

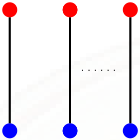


Figure: Type-I

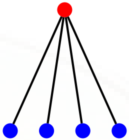


Figure: Type-II

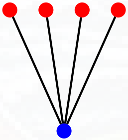


Figure: Type-III

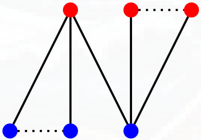


Figure: Type-IV

Sketch of the proof: 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 $\text{deg}(Y_i) = \text{deg}(W_i) \geq 2$
- Sample $U_i \xleftarrow{\$} \{0, 1\}^n$
- Set $V_i = U_i \oplus T_i$

Sketch of the proof: Sampling (U^q, V^q)

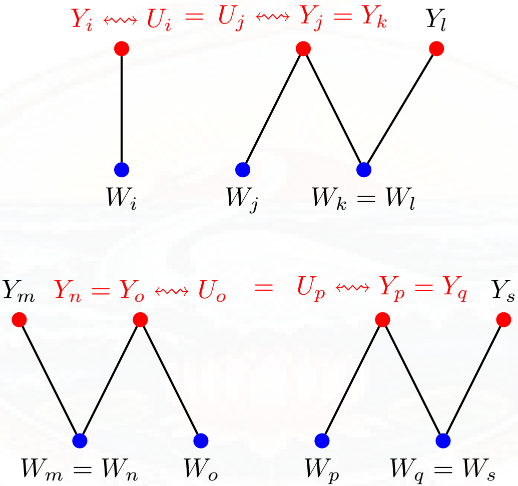
The sampling may lead to permutation incompatible transcript

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 $:= \bigcup_{\substack{\alpha \in [4] \\ \beta \in [\alpha,4]}} (\mathsf{UColl}_{\alpha,\beta} \cup \mathsf{VColl}_{\alpha,\beta})$

Sketch of the proof: Bad Sampling



Sketch of the proof: Analysis of Good Transcripts

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

Ideal World:

- **Type-1, type-2, type-3 Sampling:**
  - Non-degenerate
  - Does not contain any cycle
  - Maximum component size $\leq q^{\frac{2}{3}}$
- Used Mirror Theory results for the tweakable permutation for Type-I, Type-II, and Type-III
- We sample (U, V) in consistent way for Type-IV component and bound the ideal interpolation probability.

Open Problems

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. CPA bound of three-round CLRW1 is $3n/4$-bit secure. It is interesting to see whether we can prove the CPA bound of four round CLRW1 upto $4n/5$ bits.

Joint Work with Nilanjan Datta, Shreya Dey and Sougata Mandal.
Accepted at IACR ToSC, 2023 Issue 4

Thank You!