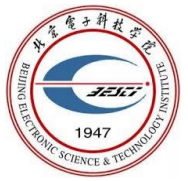
How to Recover the Full Plaintext of XCB

Peng Wang, Shuping Mao, Ruozhou Xu, Jiwu Jing, Yuewu Wang

August 18

Crypto 2025

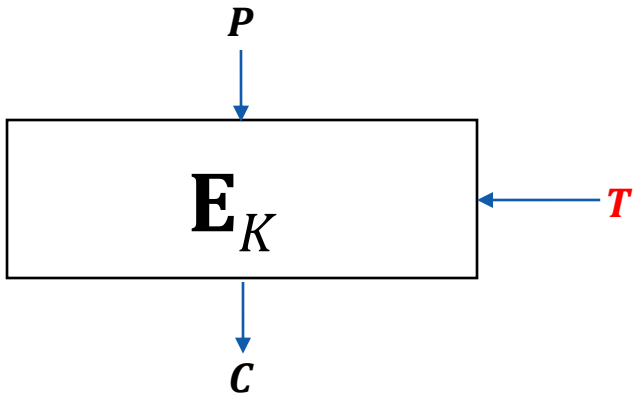


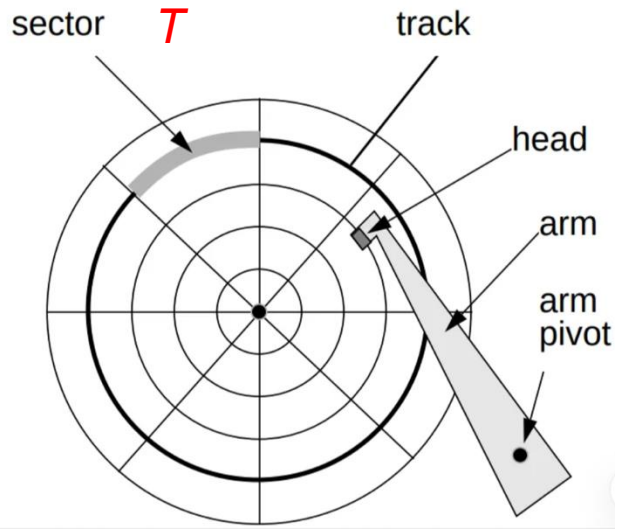
Overview

1. TEM and XCB
2. Full plaintext recovery attacks on XCB
3. How to fix XCB?
4. Conclusions

1. TEM and XCB

Tweakable enciphering mode (TEM)





- length-preserving encryption scheme
- strong tweakable pseudorandom permutation (**STPRP**) security

$$\mathbf{E}_K^{T_1} \quad \mathbf{E}_K^{T_2} \quad \cdots\cdots \quad \mathbf{E}_K^{T_i} \quad \cdots\cdots$$

$$\approx$$

$$\pi_{T_1} \quad \pi_{T_2} \quad \cdots\cdots \quad \pi_{T_i} \quad \cdots\cdots$$

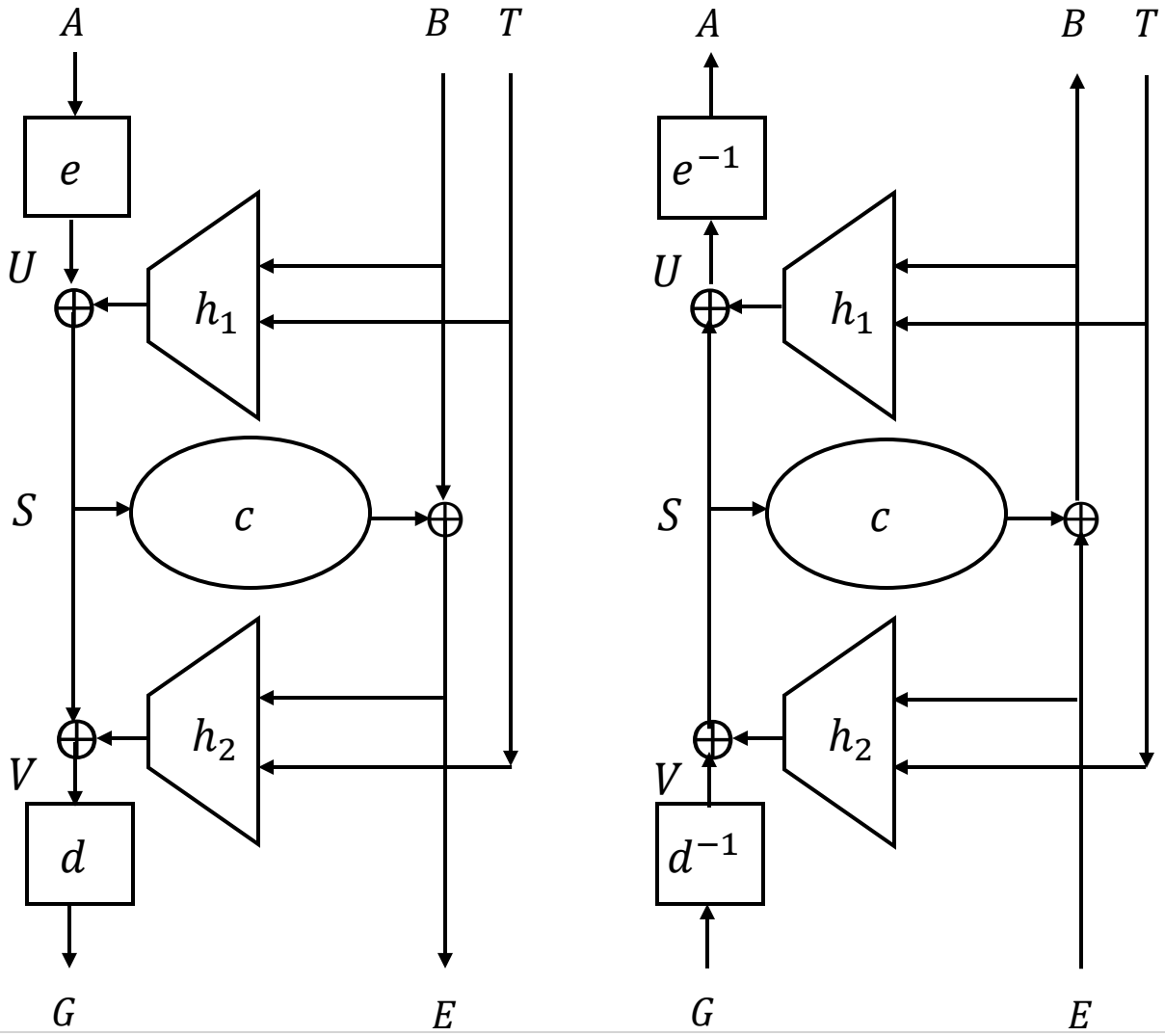
Versions of XCB

Initial version [MF04]
without security proof

Standard version [MF04]
with security proof

IEEE 1619.2: IEEE standard for wide-block encryption for shared storage media (2011, 2021)

The XCB structure



- XCBv1 and XCBv2 follow the same structure.
- e and d: encryption and decryption of block cipher.
- h_1 and h_2: universal hash function.
- c: a stream cipher.

XCB=(**E**,**D**)

Universal hash functions in XCB are separable

$$h_H(X,Y) = X_1 H^{u+v+1} \oplus X_2 H^{u+v} \oplus \cdots \oplus X_{u-1} H^{v+3} \oplus X_u H^{v+2} \oplus Y_1 H^{v+1} \oplus Y_2 H^v \oplus \cdots \oplus Y_{v-1} H^3 \oplus Y_v H^2 \oplus (\mathrm{bin}_{\frac{n}{2}}(|X|) \parallel \mathrm{bin}_{\frac{n}{2}}(|Y|))H$$

In XCBv1, h_1 and h_2 are defined as:

$$h_i(X,T) = h_{H_i}(X,T), i = 1,2$$

In XCBv2, h_1 and h_2 are defined as:

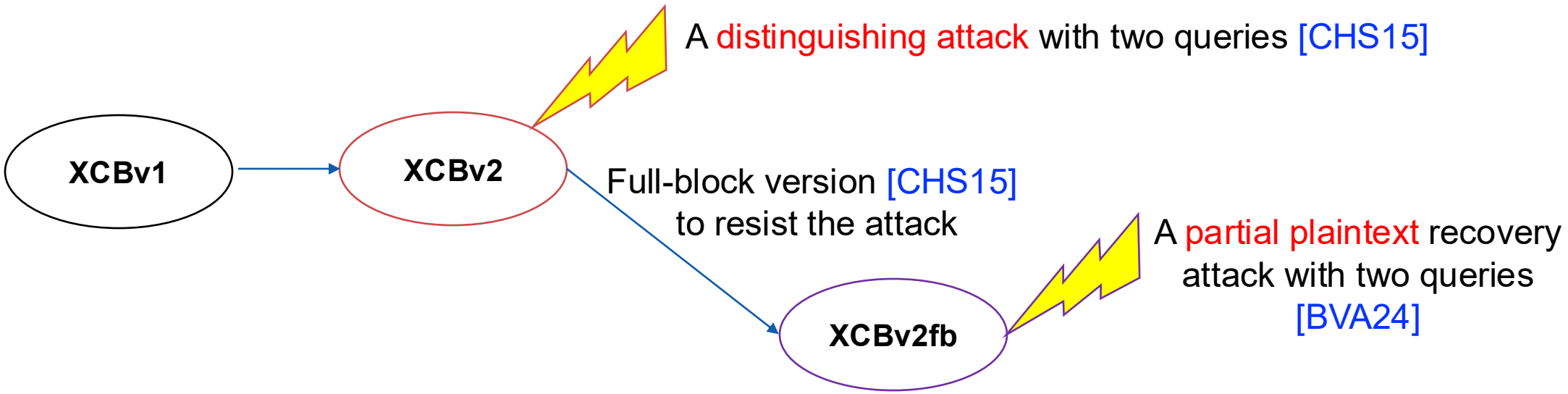
$$h_1(X,T) = h_H(0^n \| T, \mathrm{pad}(X) \| 0^n),$$

$$h_2(X,T) = h_H(T \| 0^n, \mathrm{pad}(X) \| \mathrm{bin}_{\frac{n}{2}}(|(T \| 0^n)|) \parallel \mathrm{bin}_{\frac{n}{2}}(|X|))$$

h_1 and h_2 are separable:

$$h_1(X \oplus \Delta_1, T \oplus \Delta_2) = h_1(X,T) \oplus g_1(\Delta_1, \Delta_2),$$
$$h_2(X \oplus \Delta_1, T \oplus \Delta_2) = h_2(X,T) \oplus g_2(\Delta_1, \Delta_2).$$

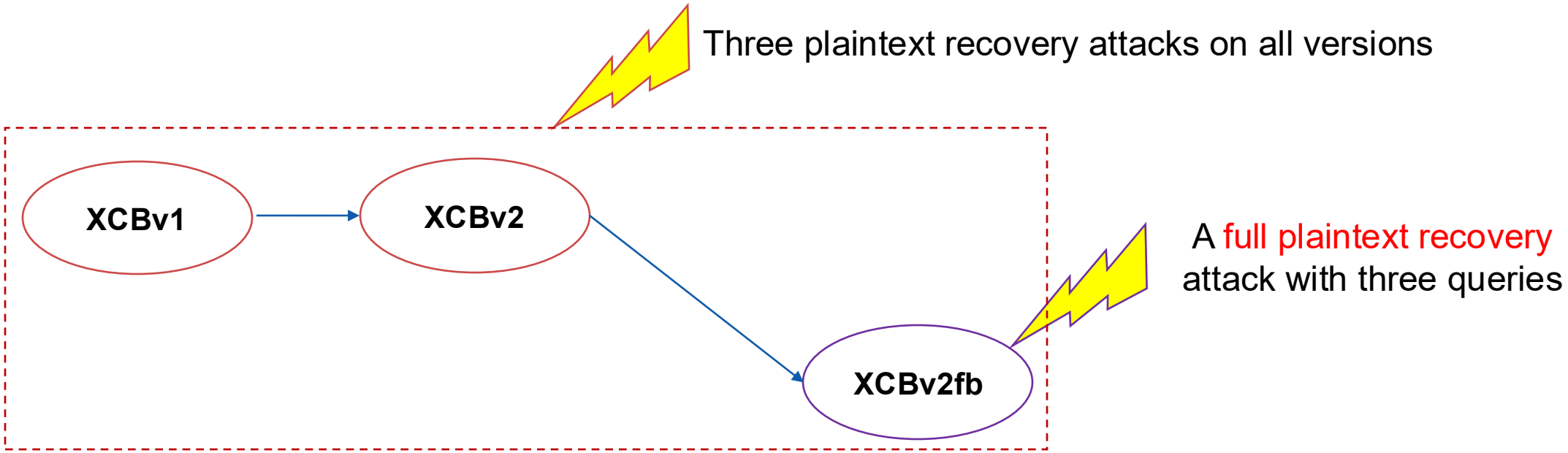
Previous attacks



- [CHS15] Debrup Chakraborty, Vicente Hernandez-Jimenez, and Palash Sarkar. Another look at XCB. Cryptogr. Commun., 7(4):439–468, 2015.
- [BVA24] Amit Singh Bhati, Michiel Verbauwhede, and Elena Andreeva. Breaking, repairing and enhancing XCBv2 into the tweakable enciphering mode GEM. Cryptology ePrint Archive, Paper 2024/1554, 2024.

Our attacks: how to recover the full plaintext

Inspired by the work of [BVA24].

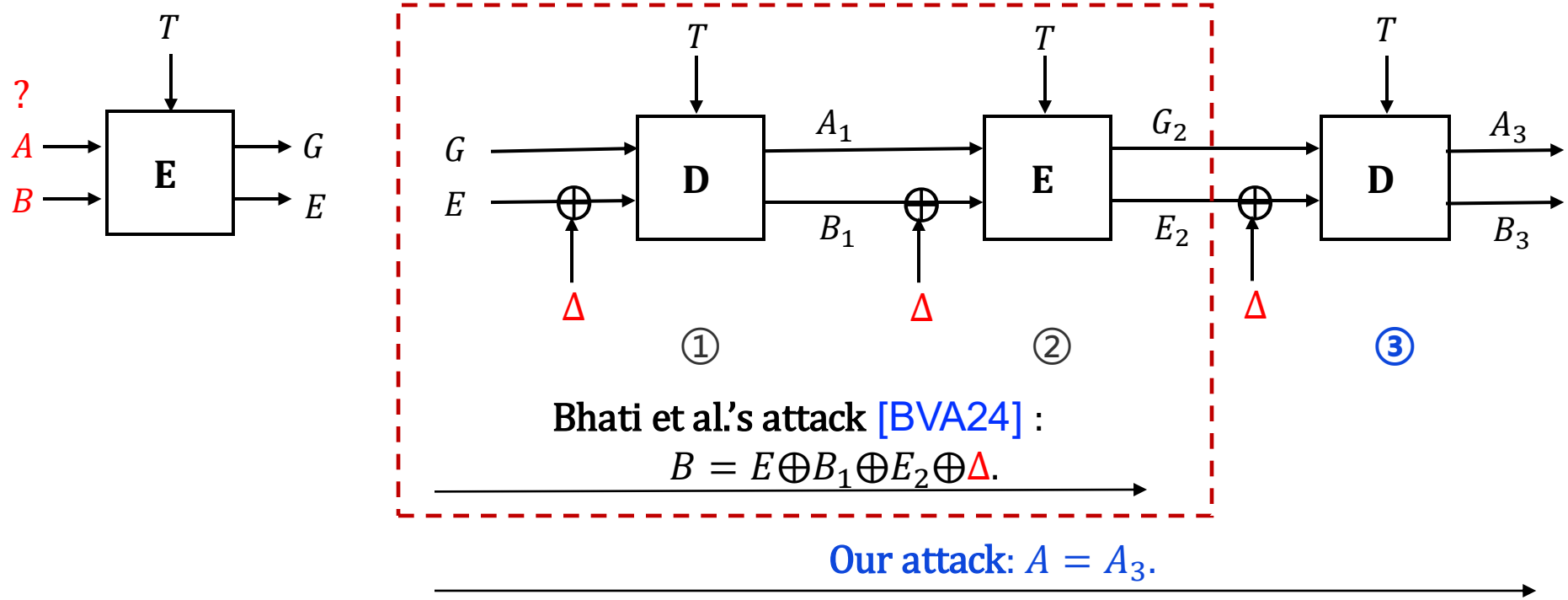


Summary of Attacks on XCB

	Message length	Number of queries	Recovered bits	Target schemes	Ref.
Attack in [CHS15]	$m > n$	2	N/A	XCBv2 [MF07]	[CHS15]
Attack in [BVA24]	$m > n$	2	$m - n$	XCBv2 [MF07], XCBv2fb [CHS15], HCI [Nan08], MXCB [Nan08]	[BVA24]
A warm-up attack	$m > n$	3	m		4.2
Attack 1	$m = n$	3	n	XCBv1 [MF04], XCBv2 [MF07], XCBv2fb [CHS15]	5.3
Attack 2	$m > n$	4	$m - n$	XCBv1 [MF04], XCBv2 [MF07], XCBv2fb [CHS15], HCI [Nan08], MXCB [Nan08]	5.4
Attack 3	$m > n$	7	m		5.5

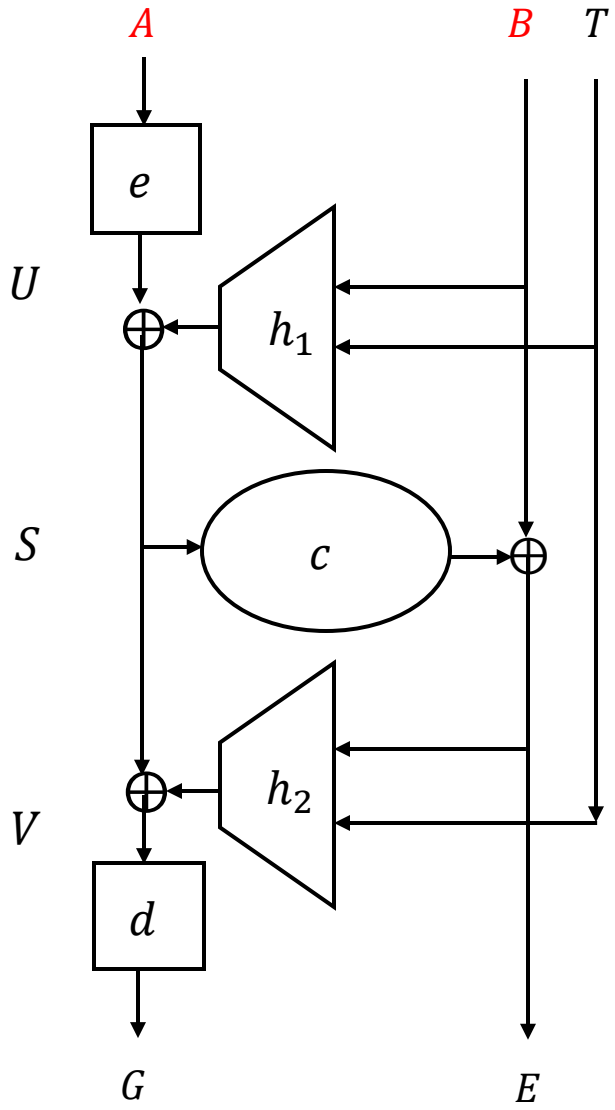
2. Full plaintext recovery attacks on XCB

A warm-up full plaintext recovery attack

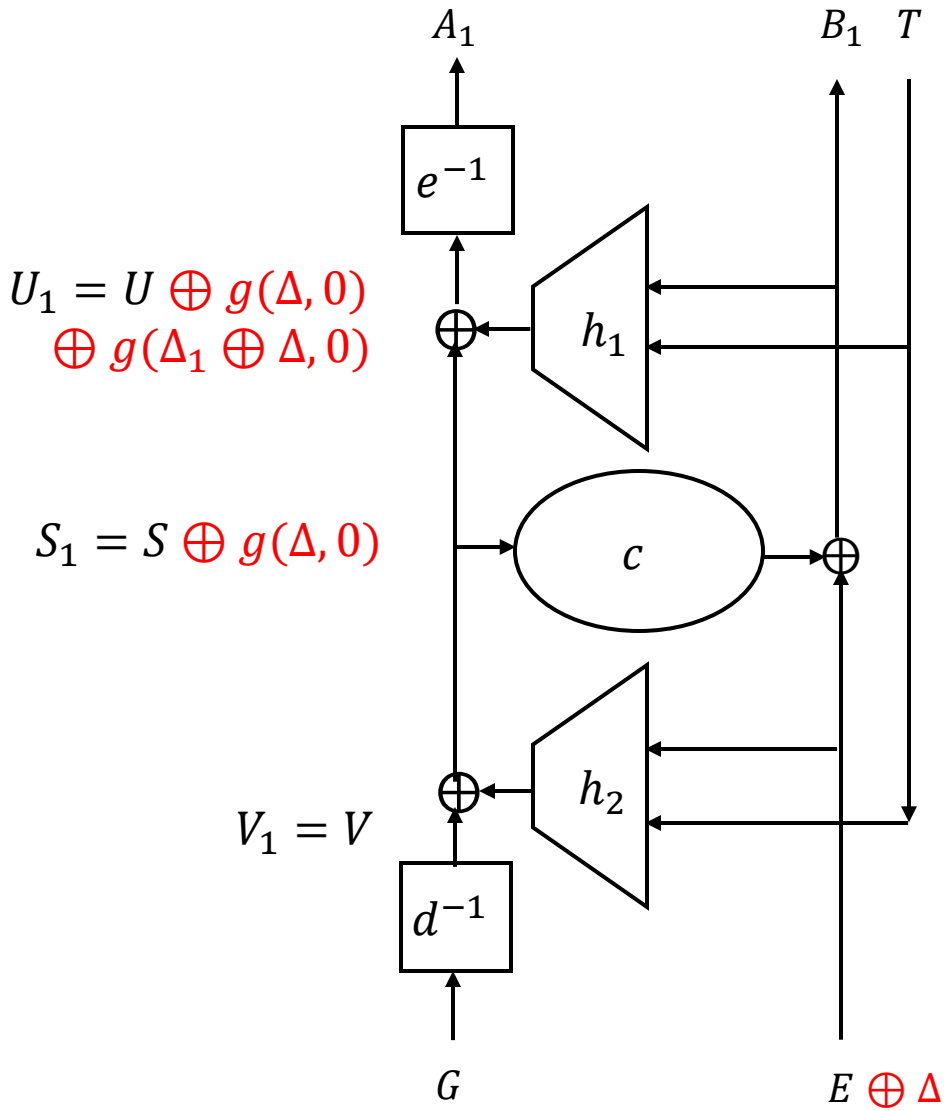


- The first two steps coincide with Bhati et al.'s attack.
- A full plaintext recovery attack with three queries.
- It is only applicable to XCBv2 (XCBv2fb) but not XCBv1. ☹

?



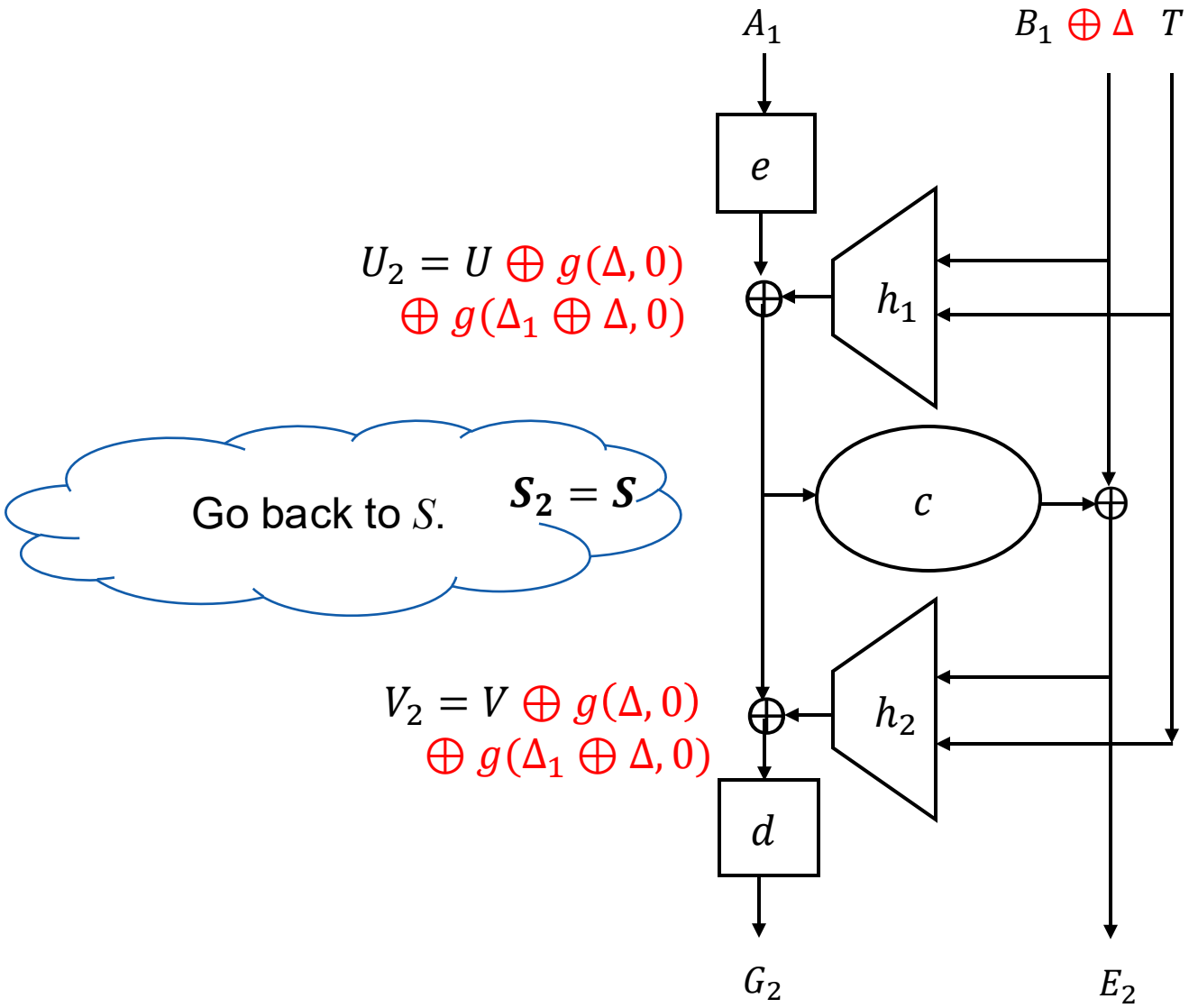
E



$\Delta_1 = c(S) \oplus c(S_1)$

①

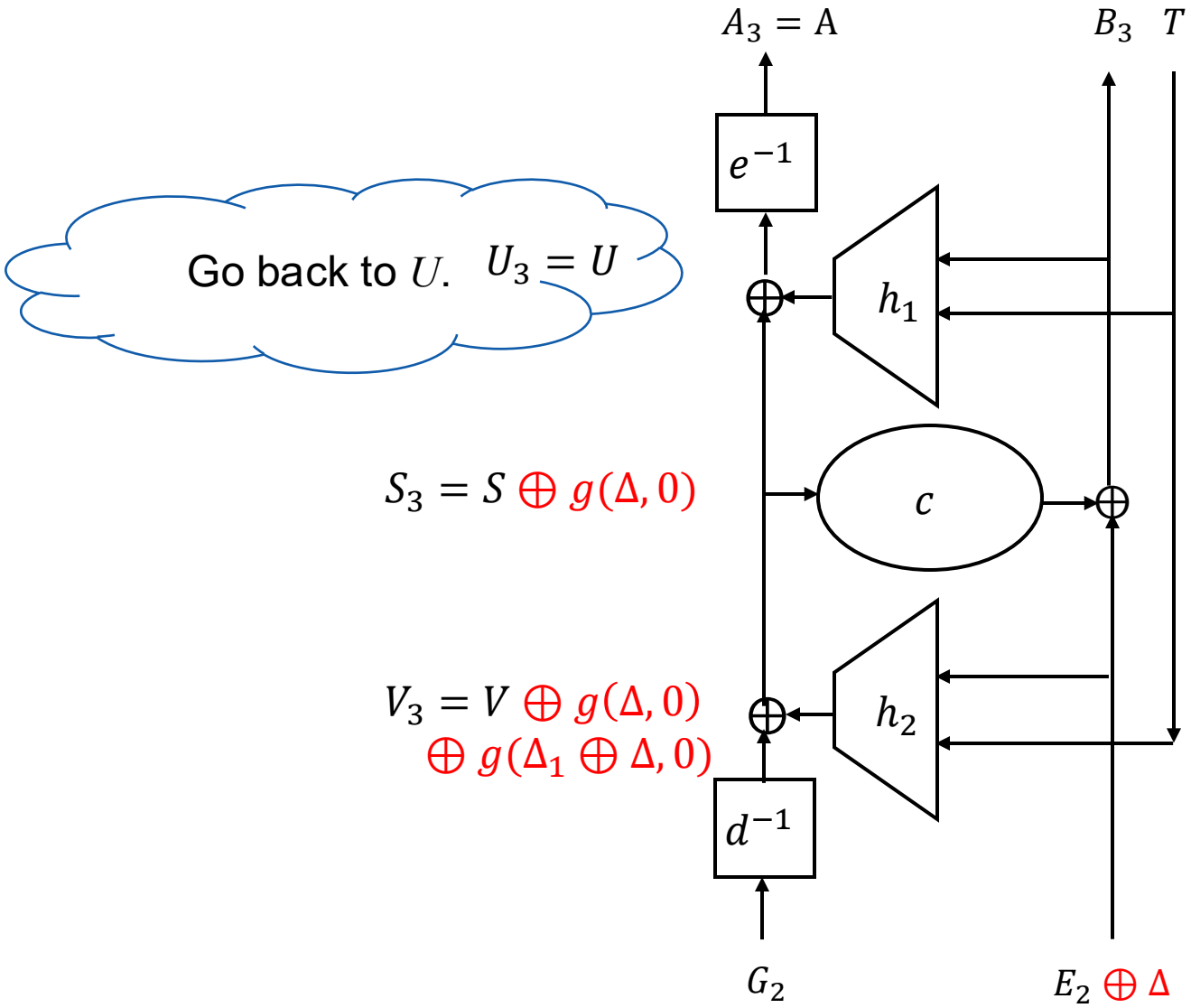
D



$$B = E \oplus B_1 \oplus E_2 \oplus \Delta.$$

②

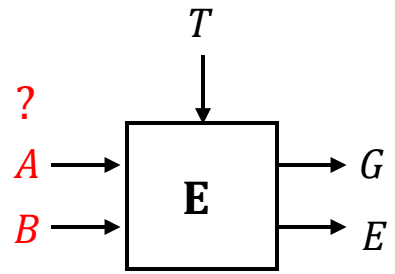
E

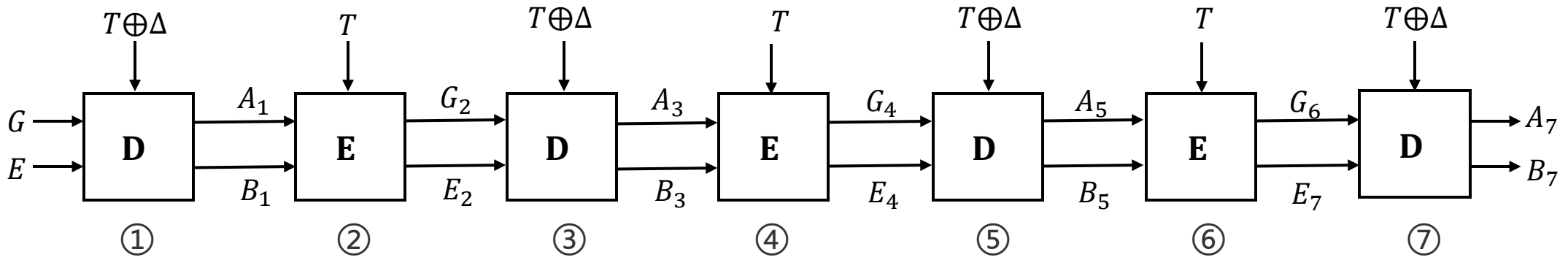

$A_3 = \mathrm{A}$
B_3
T
e^{-1}
Go back to U. $U_3 = U$
h_1
$S_3 = S \oplus g(\Delta, 0)$
c
$V_3 = V \oplus g(\Delta, 0)$
$\oplus\, g(\Delta_1 \oplus \Delta, 0)$
h_2
d^{-1}
G_2
$E_2 \oplus \Delta$

③

D

Our Three Attacks





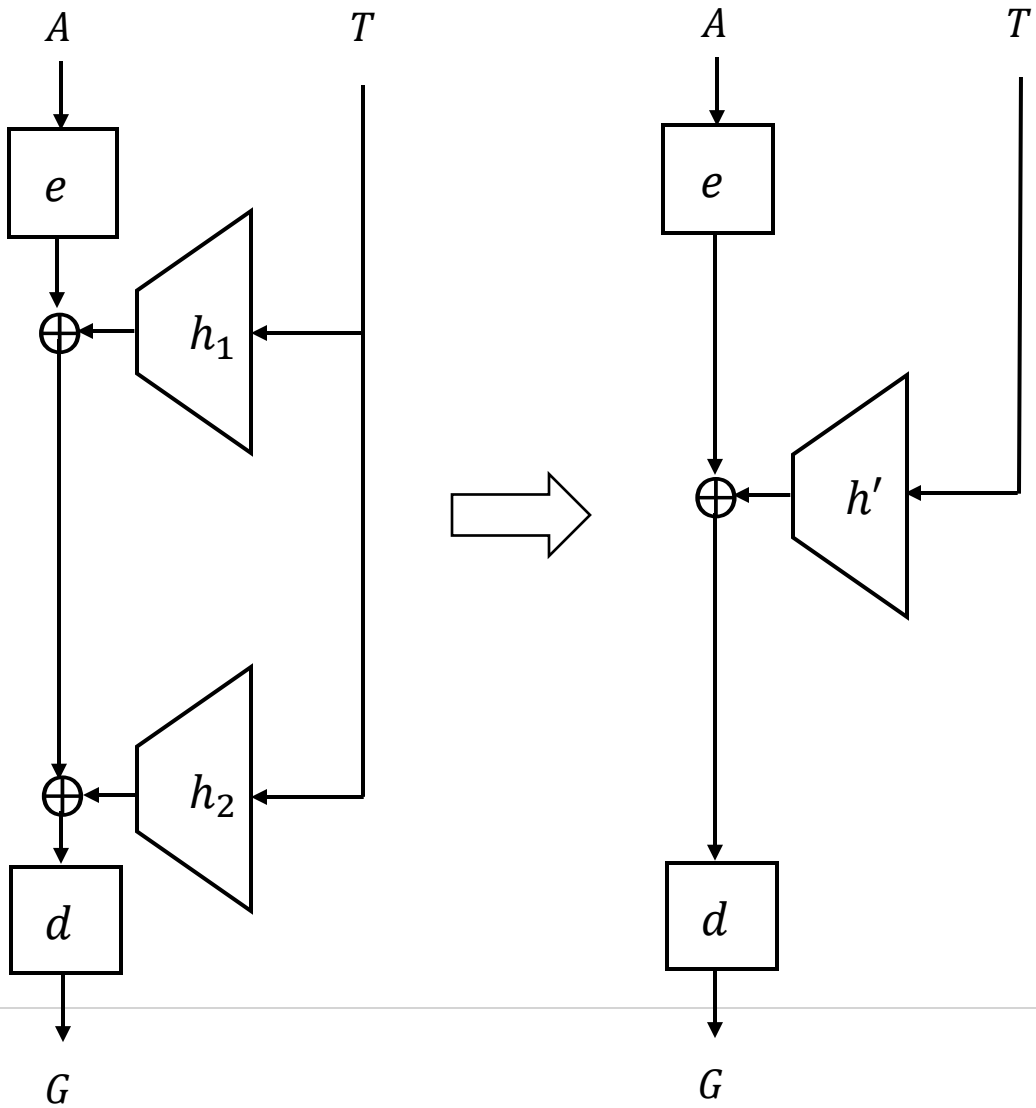
Attack 1: if $m = n$, then $A = A_3$.

Attack 2: $B = E \oplus B_3 \oplus E_4$.

Attack 3: $A = A_7, B = B_7$.

Three attacks are applicable to all versions of XCB.

A key observation

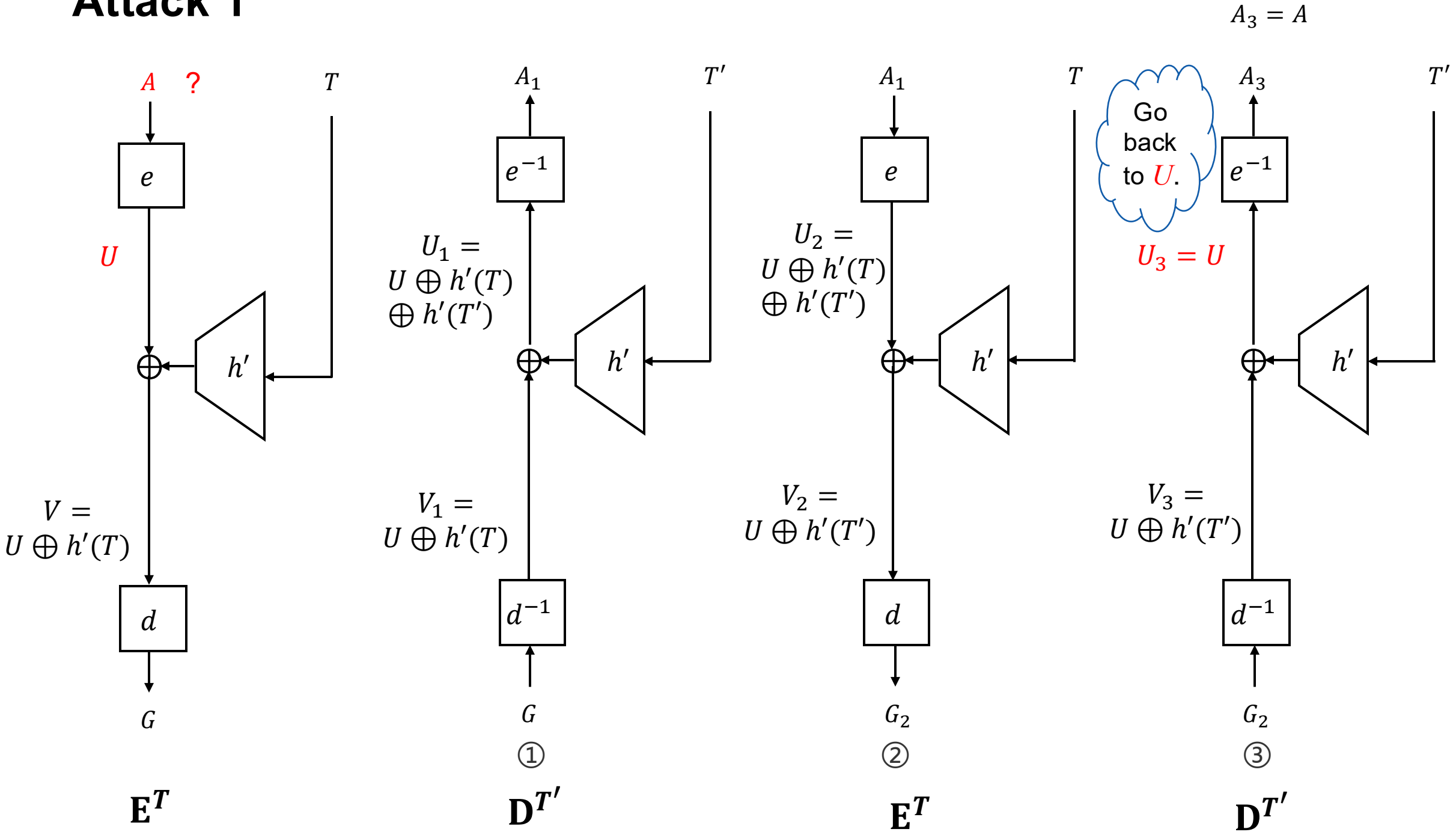


When $m = n$ $(P = A)$, XCB → LRW1

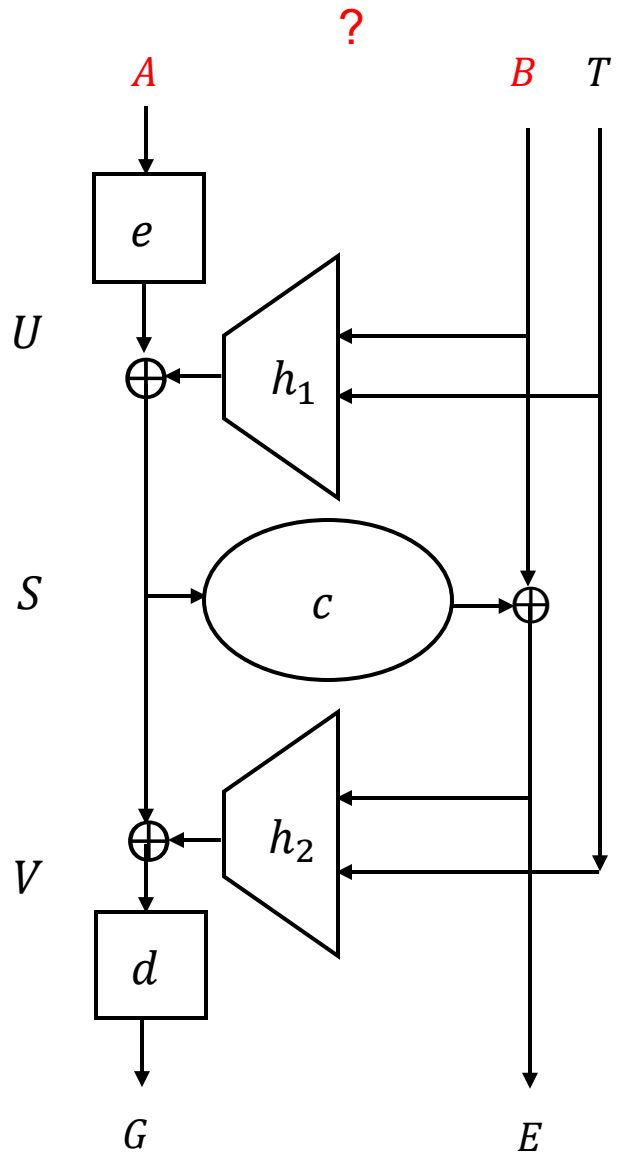
LRW1 is not CCA secure.

[LRW02, JKNS24]

Attack 1

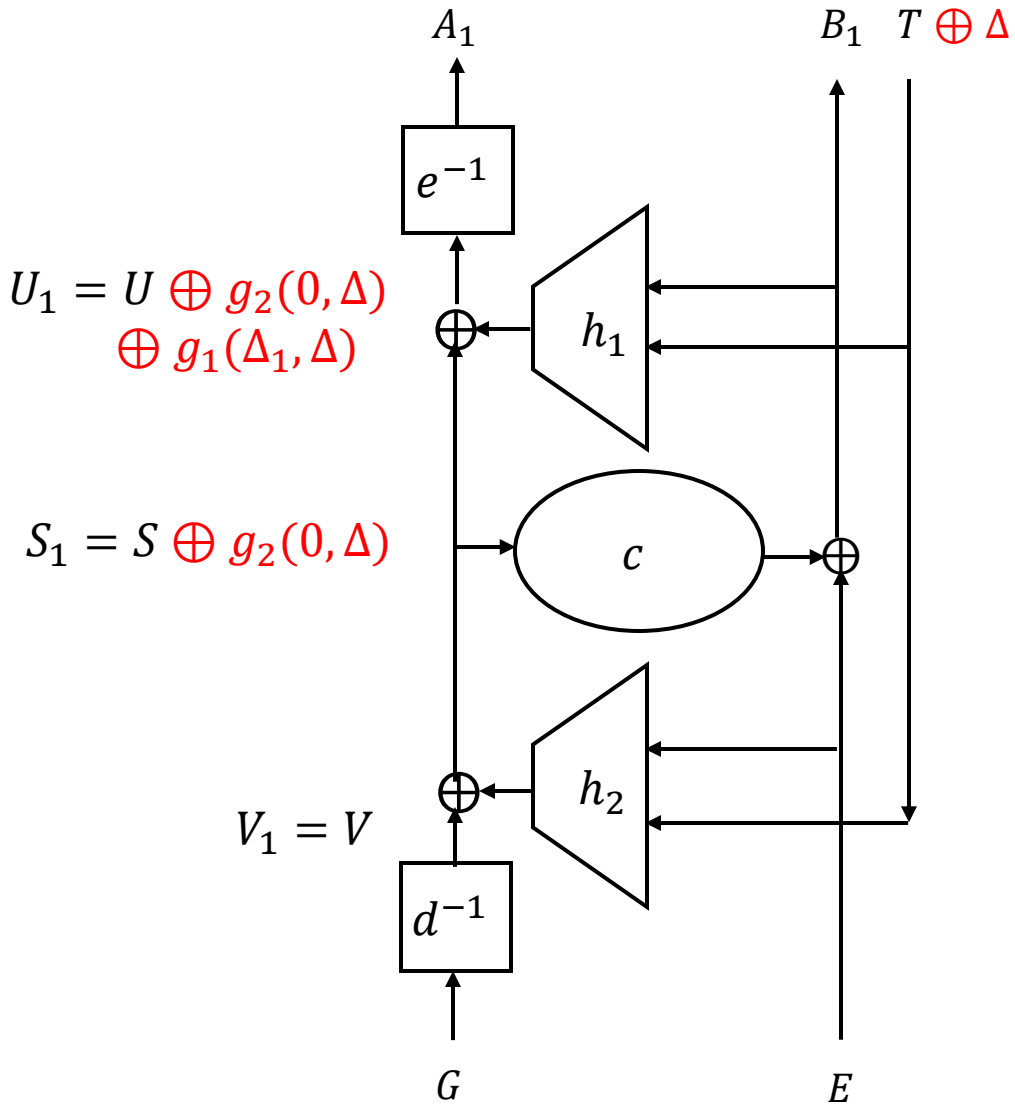

A ?
T
e
U
h′
V = U ⊕ h′(T)
d
G
E^T
A1
T′
e^−1
U1 = U ⊕ h′(T) ⊕ h′(T′)
h′
V1 = U ⊕ h′(T)
d^−1
G
①
D^T′
A1
T
e
U2 = U ⊕ h′(T) ⊕ h′(T′)
h′
V2 = U ⊕ h′(T′)
d
G2
②
E^T
A3 = A
Go back to U.
A3
T′
e^−1
U3 = U
h′
V3 = U ⊕ h′(T′)
d^−1
G2
③
D^T′

Attack 2 & 3



$\mathbf{E}^{T}$

Given $(T, G||E)$,
how to recover A and B?

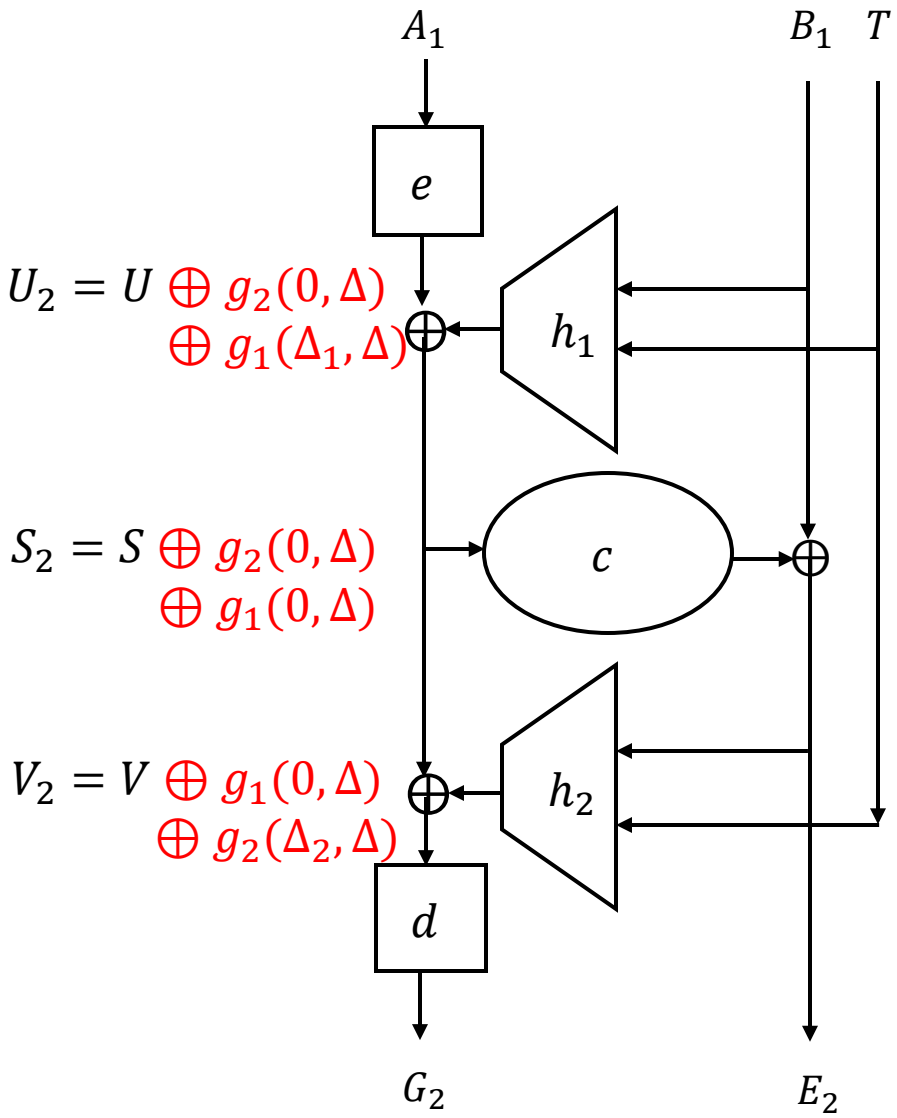


$T' = T \oplus \Delta$

$\Delta_1 = c(S) \oplus c(S_1)$

①

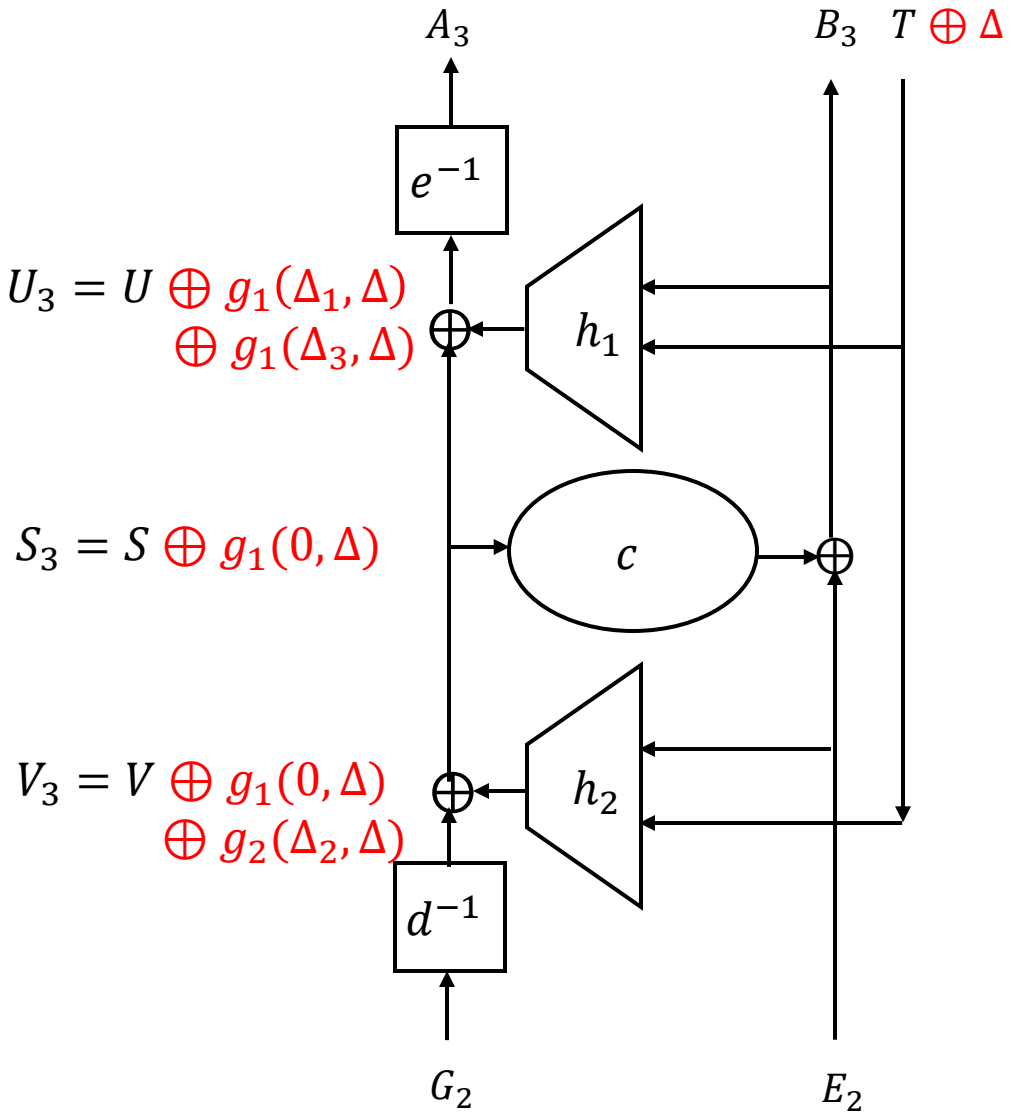
$\mathbf{D}^{T'}$



$\Delta_2 = c(S_1) \oplus c(S_2))$

②

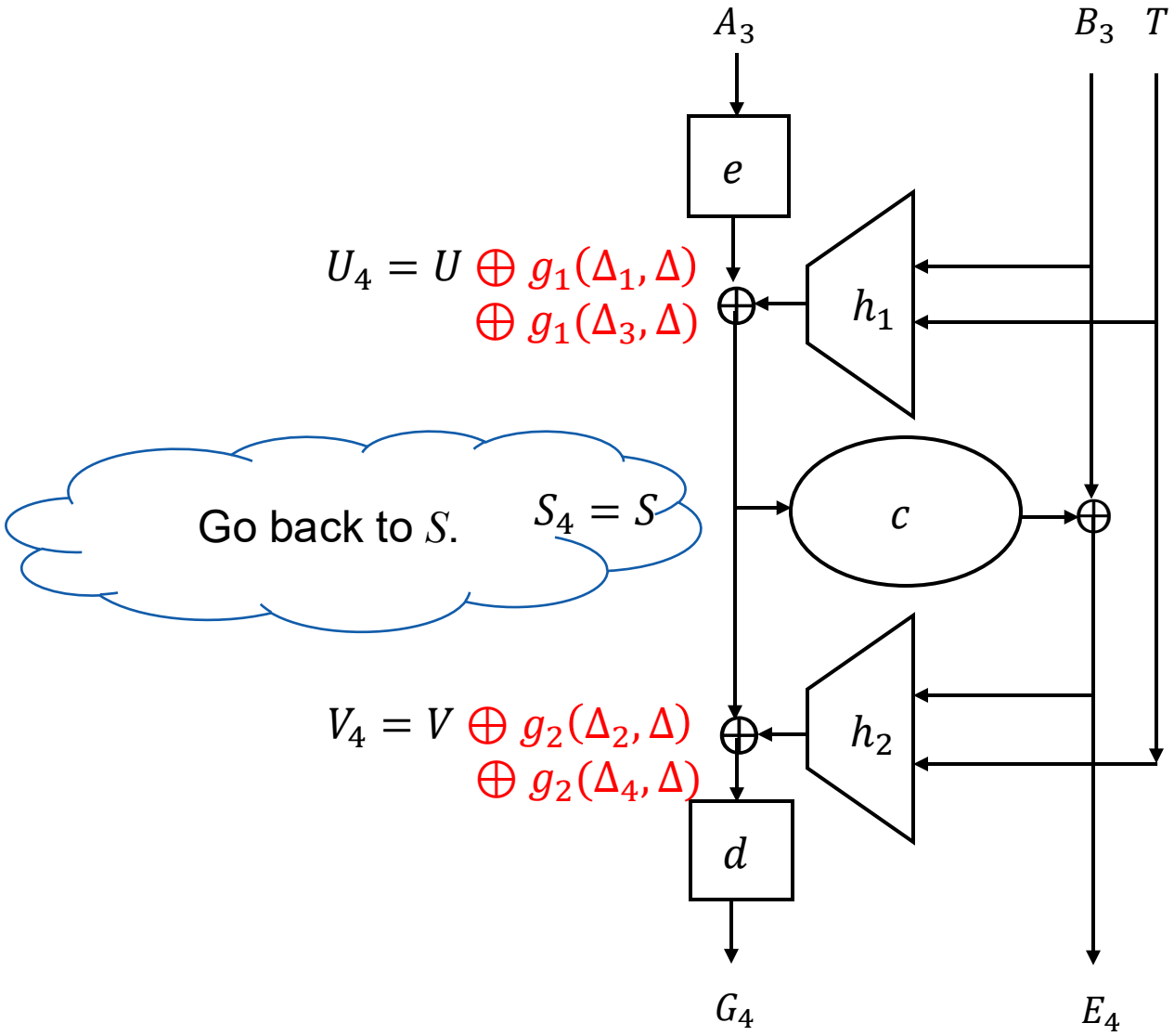
$\mathbf{E}^{\boldsymbol{T}}$



$\Delta_3 = c(S_2) \oplus c(S_3)$

③

$\mathbf{D}^{T'}$

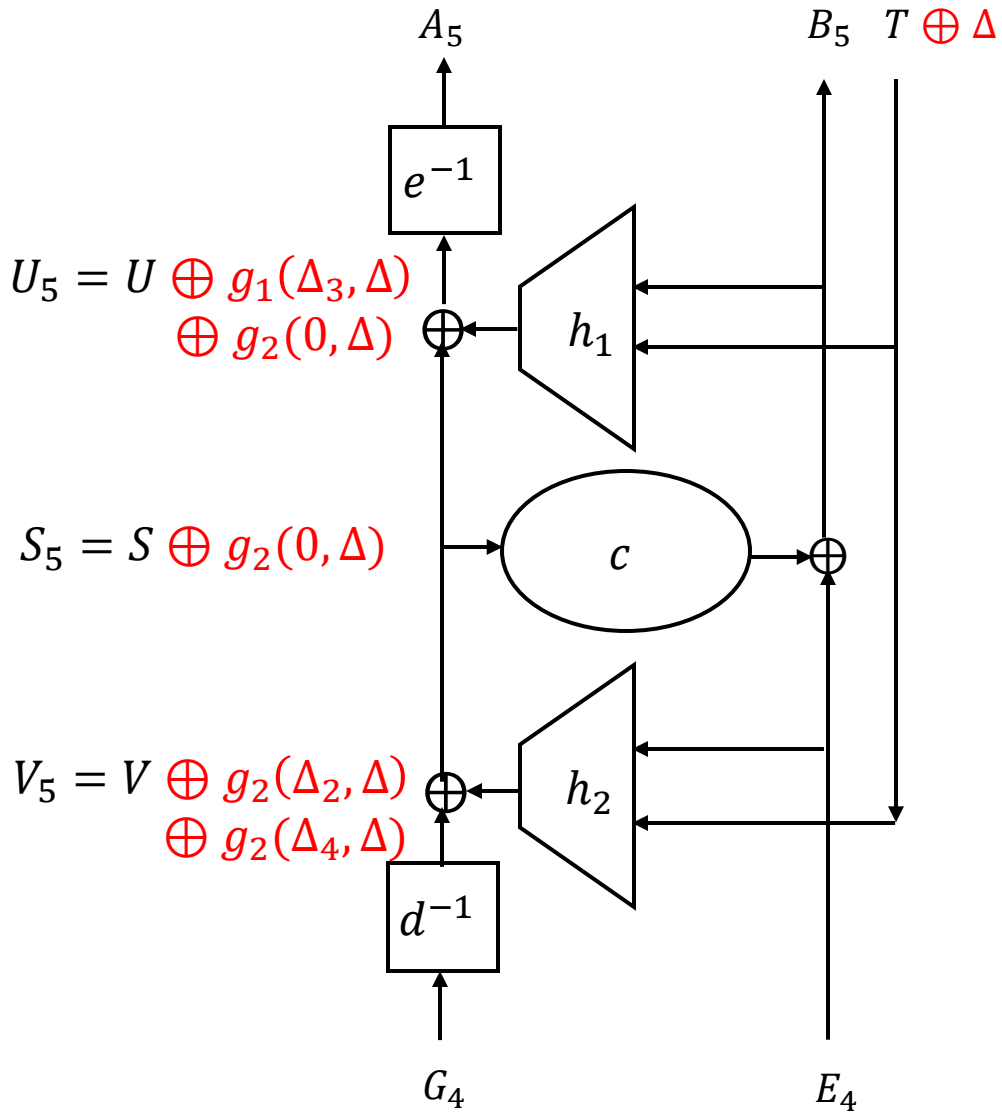


$\Delta_4 = c(S_3) \oplus c(S)$

$B = E \oplus B_3 \oplus E_4$

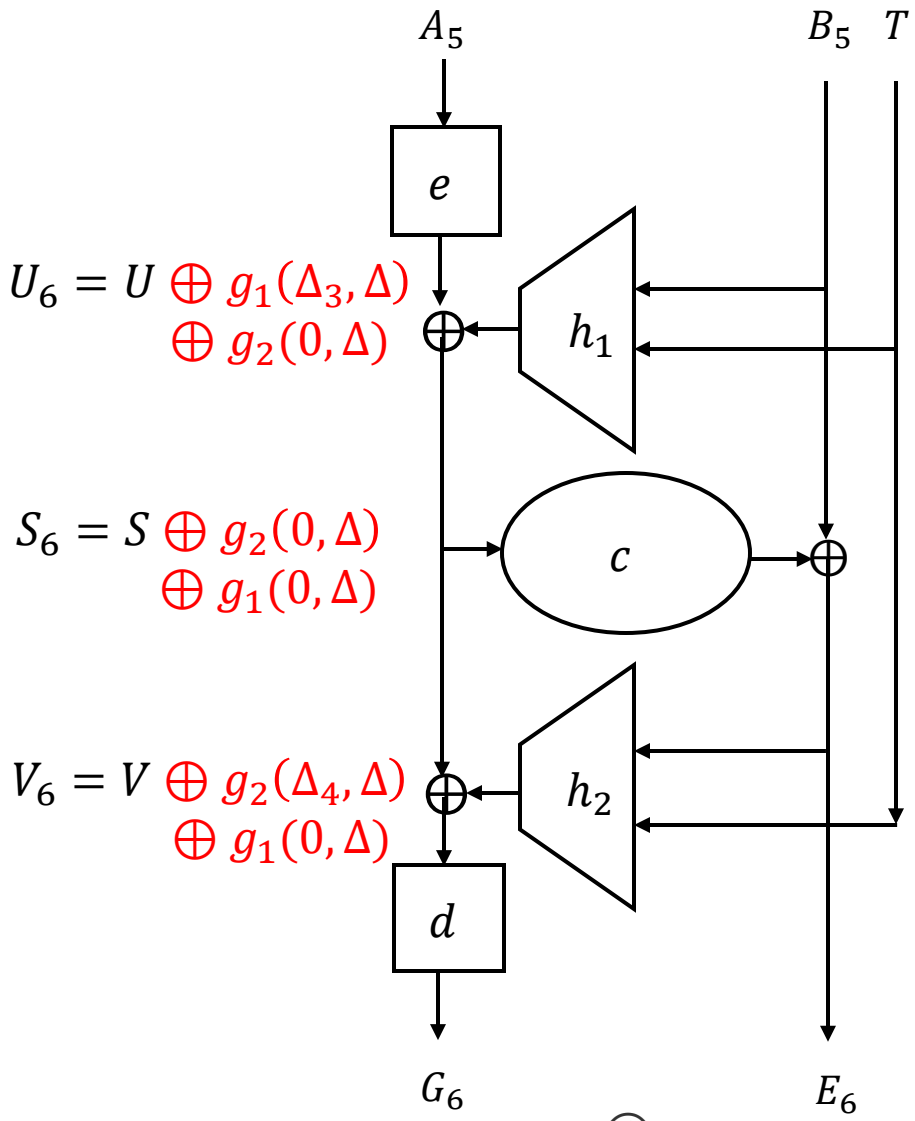
④

$\mathbf{E}^{\boldsymbol{T}}$


A_5
B_5
$T \oplus \Delta$
e^{-1}
$U_5 = U \oplus g_1(\Delta_3, \Delta)$
$\oplus g_2(0, \Delta)$
h_1
$S_5 = S \oplus g_2(0, \Delta)$
c
$V_5 = V \oplus g_2(\Delta_2, \Delta)$
$\oplus g_2(\Delta_4, \Delta)$
h_2
d^{-1}
G_4
E_4

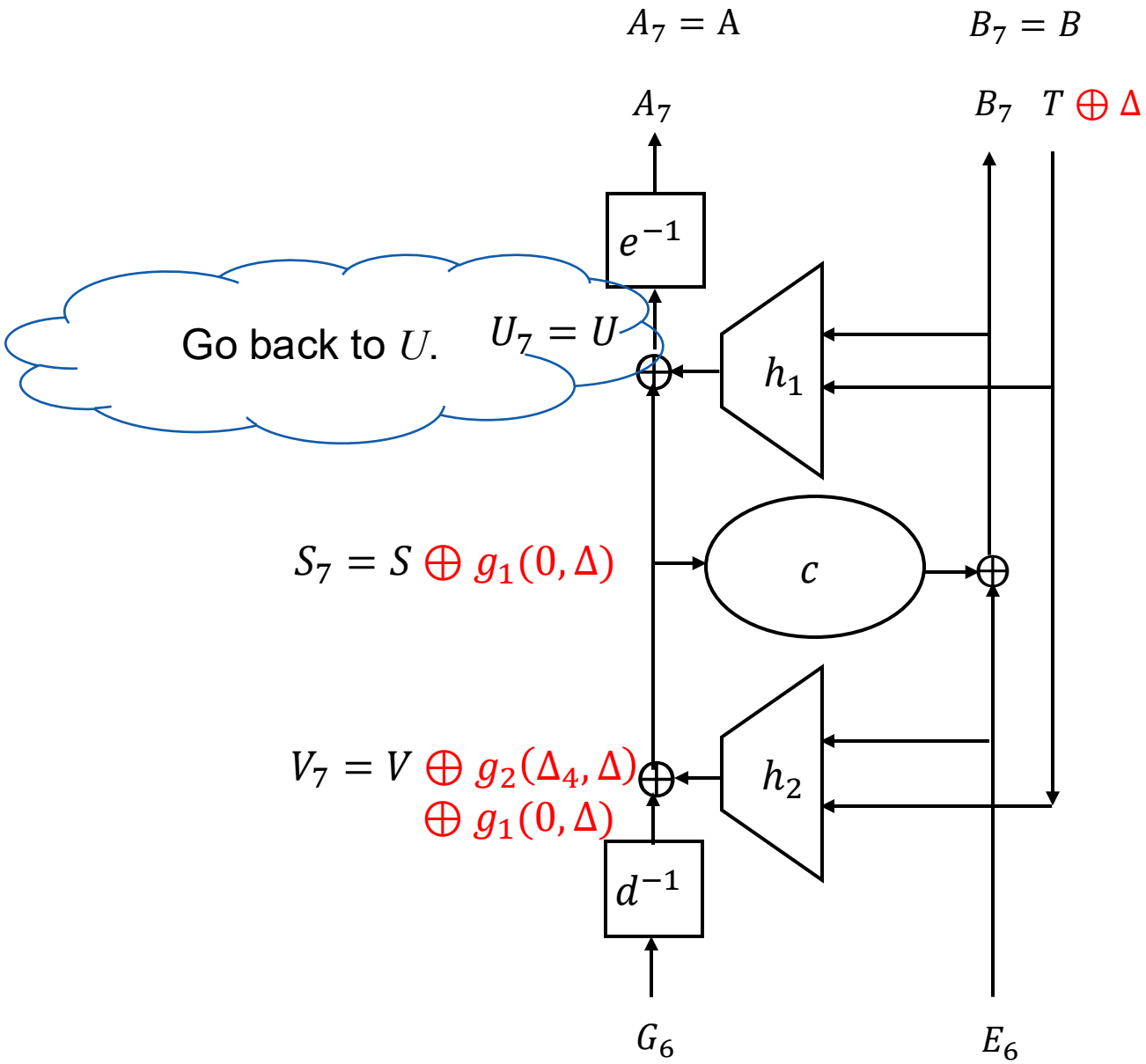
⑤

$\mathbf{D}^{T'}$



⑥

$\mathbf{E}^{\boldsymbol{T}}$

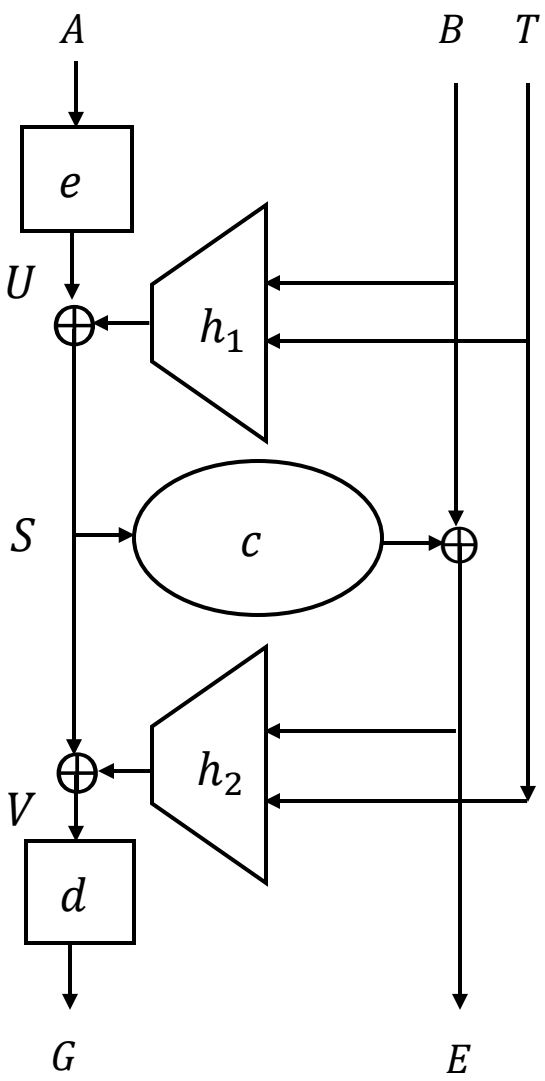


$A_7 = \mathrm{A}$

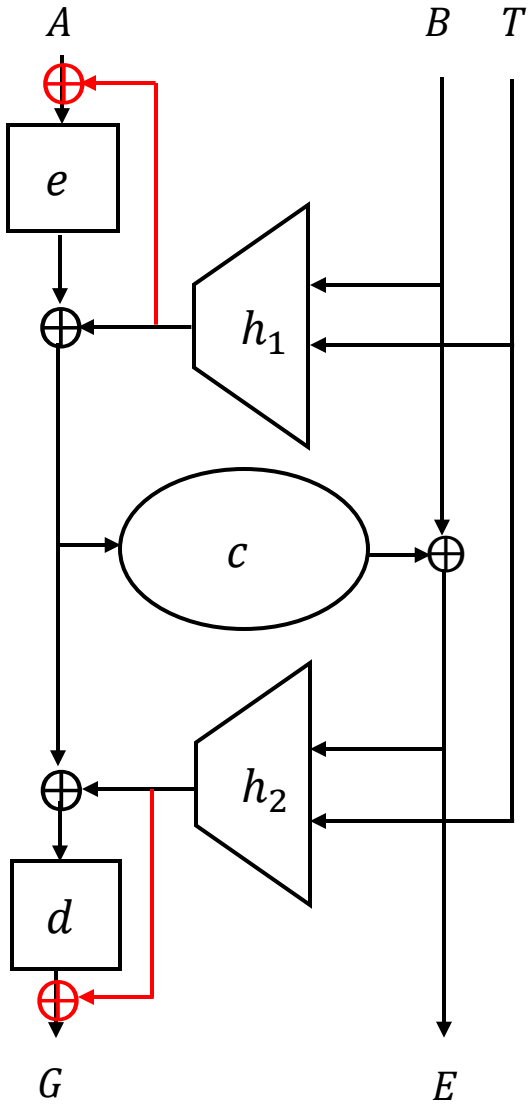
⑦

$\mathbf{D}^{T'}$

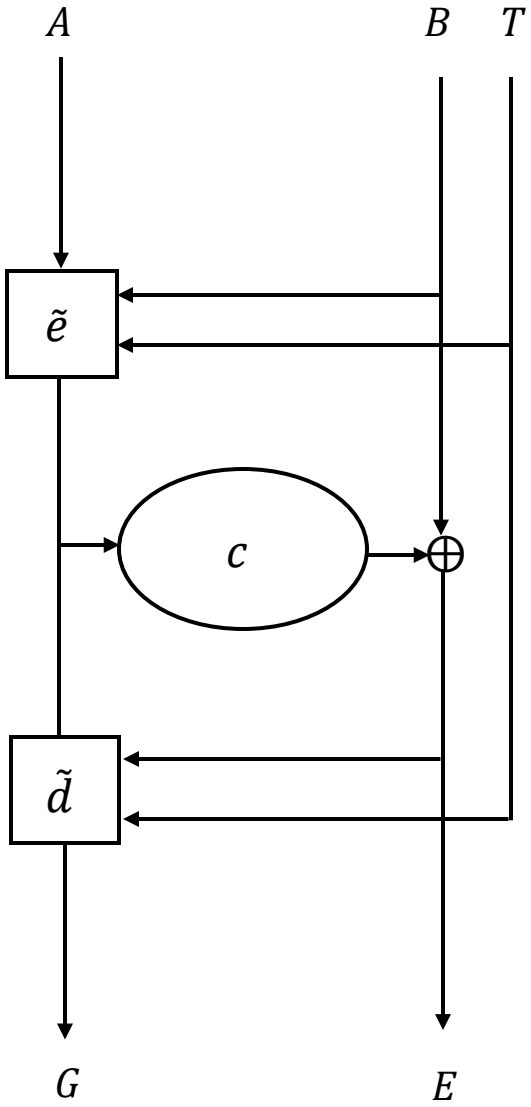
3. How to fixe XCB?



XCB



XCB*



PIV [ST13]

$$\mathbf{Adv}^{\mathrm{stprp}}_{\mathrm{XCB}^*[e,d,h_1,h_2,c]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{sprp}}_{e}(\mathcal{B}) + \mathbf{Adv}^{\mathrm{sprp}}_{d}(\mathcal{C}) + \mathbf{Adv}^{\mathrm{ivrnd}}_{c}(\mathcal{D}) + \frac{3q^2}{2^{n+1}} + 6\epsilon q^2$$

4. Conclusions

Conclusions

- All versions of XCB are not secure.
- All attacks can be applied to the standard version XCBv2.
- Our full plaintext recovery attack on XCBv2fb only needs three queries.
- Attack 1 shows the structure weakness of XCB.
- Attack 2 & 3 are applicable to the XCB structure with separable UHFs .
- We suggest reconsidering the continued use of XCB and its structure.

References

- [MF04] David A. McGrew and Scott R. Fluhrer. The extended codebook (XCB) mode of operation. IACR Cryptol. ePrint Arch., page 278, 2004.
- [MF07] David A. McGrew and Scott R. Fluhrer. The security of the extended codebook (XCB) mode of operation. In Selected Areas in Cryptography, 14th International Workshop, SAC 2007.
- [IEEE 1619.2] IEEE 1619.2: IEEE standard for wide-block encryption for shared storage media (2011, 2021).
- [CHS15] Debrup Chakraborty, Vicente Hernandez-Jimenez, and Palash Sarkar. Another look at XCB. Cryptogr. Commun., 7(4):439–468, 2015.
- [BVA24] Amit Singh Bhati, Michiel Verbauwhede, and Elena Andreeva. Breaking, repairing and enhancing XCBv2 into the tweakable enciphering mode GEM. Cryptology ePrint Archive, Paper 2024/1554, 2024.
- [LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. CRYPTO 2002.
- [JKNS24] Ashwin Jha, Mustafa Khairallah, Mridul Nandi, and Abishanka Saha. Tight security of TNT and beyond - attacks, proofs and possibilities for the cascaded LRW paradigm. EUROCRYPT 2024.
- [ST13] Thomas Shrimpton and R. Seth Terashima. A modular framework for building variable-input-length tweakable ciphers. ASIACRYPT 2013.

Thanks