Breaking the IEEE Encryption Standard XCB-AES in Two Queries

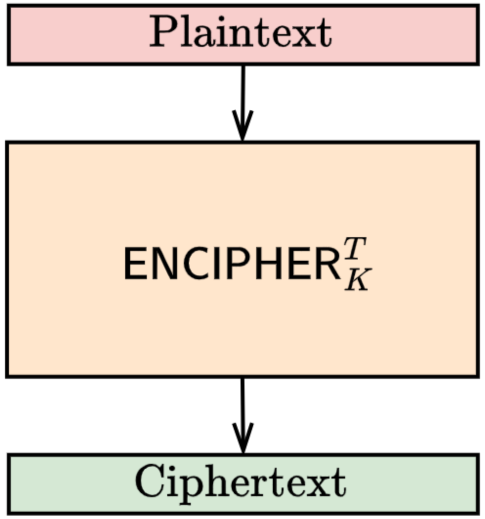
CRYPTO 2025

Amit Singh Bhati
COSIC, KU Leuven; 3MI Labs, Belgium

Elena Andreeva
TU Wien, Austria

Tweakable Enciphering Modes (TEMs)

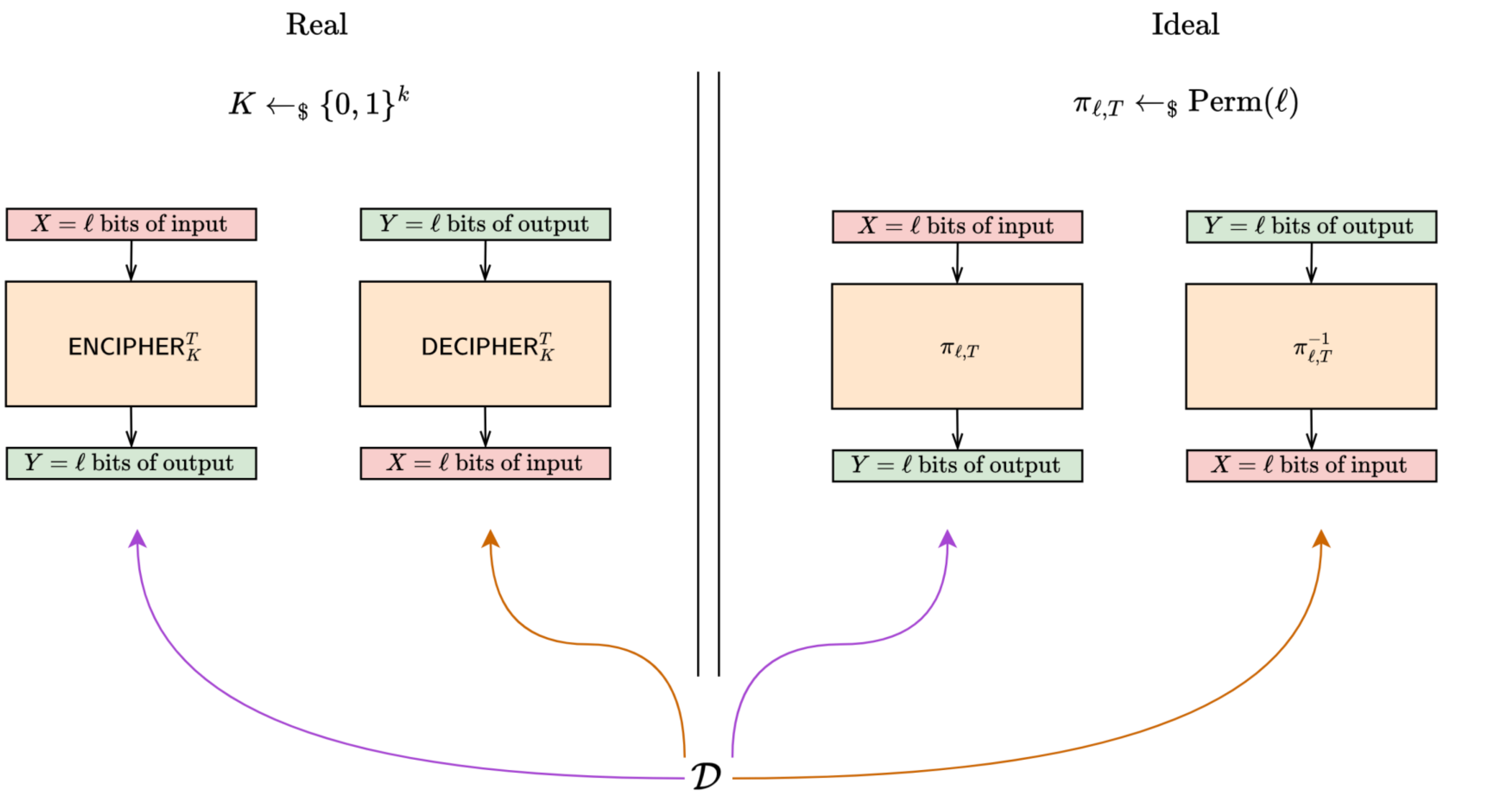
Tweakable Enciphering Mode (TEM) [HR03]



1. Length Preserving Encryption (LPE)
2. Generalization of (tweakable) block ciphers
   - Variable tweak and input size
3. NIST reintroduced it as accordion mode [CD+24]
4. Uses: disk-sector and full-disk encryption, key-wrapping, robust AEAD [HKR17]

What is a Secure TEM?

TEM Security [HR03]



- Variable-Input-Length Strong Tweakable Pseudo-Random Permutation (VIL-STPRP)
- Analogous to IND-CCA encryption notion

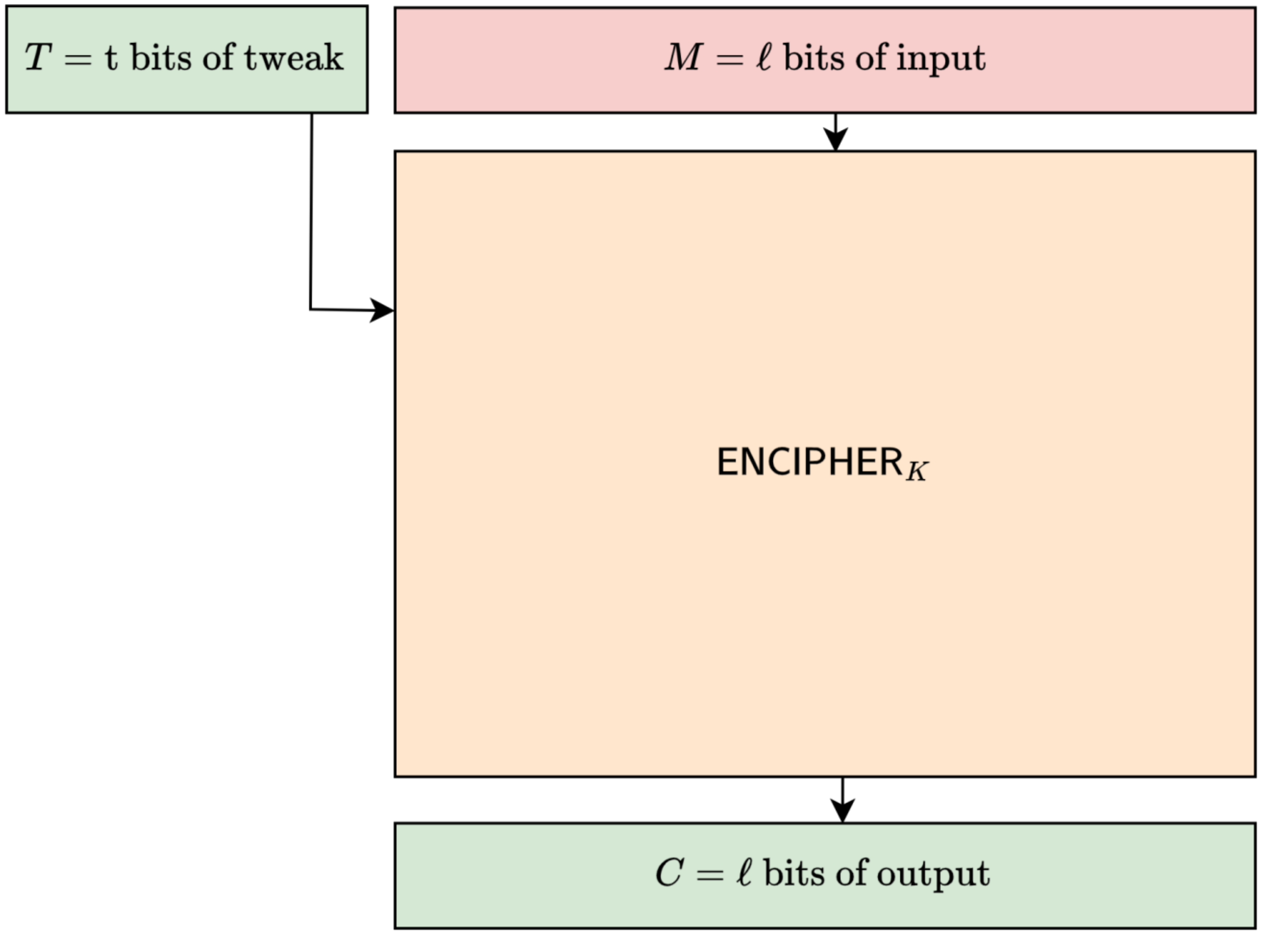
KU LEUVEN

XCB-AES: IEEE 1619.2 TEM Standard

XCB-AES: IEEE 1619.2 TEM Standard [MF07]

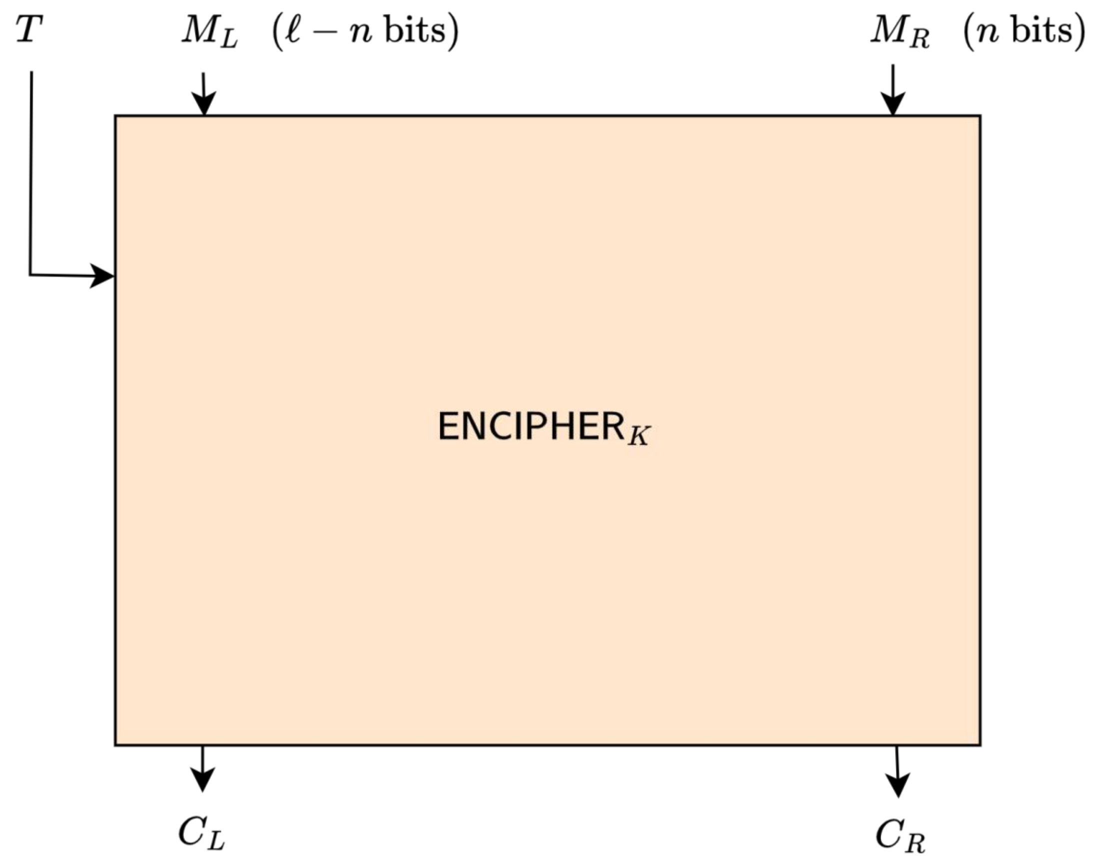
- A TEM standardized for storage media encryption (2010, 2021)
- An efficient Hash-CTR-Hash design
- Built on AES and polynomial hashing
- Alias XCBv2fb

XCB-AES: IEEE 1619.2 TEM Standard [MF07]



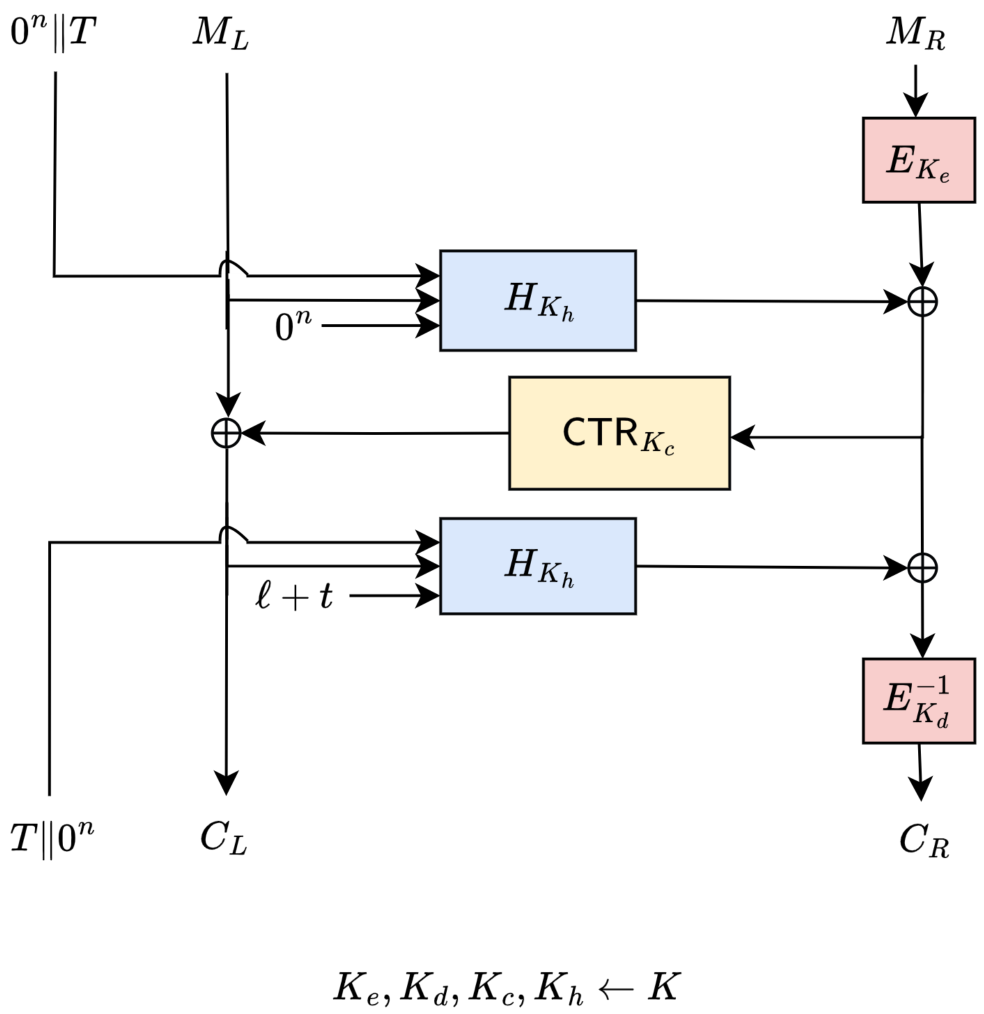
KU LEUVEN

XCB-AES: IEEE 1619.2 TEM Standard [MF07]



KU LEUVEN

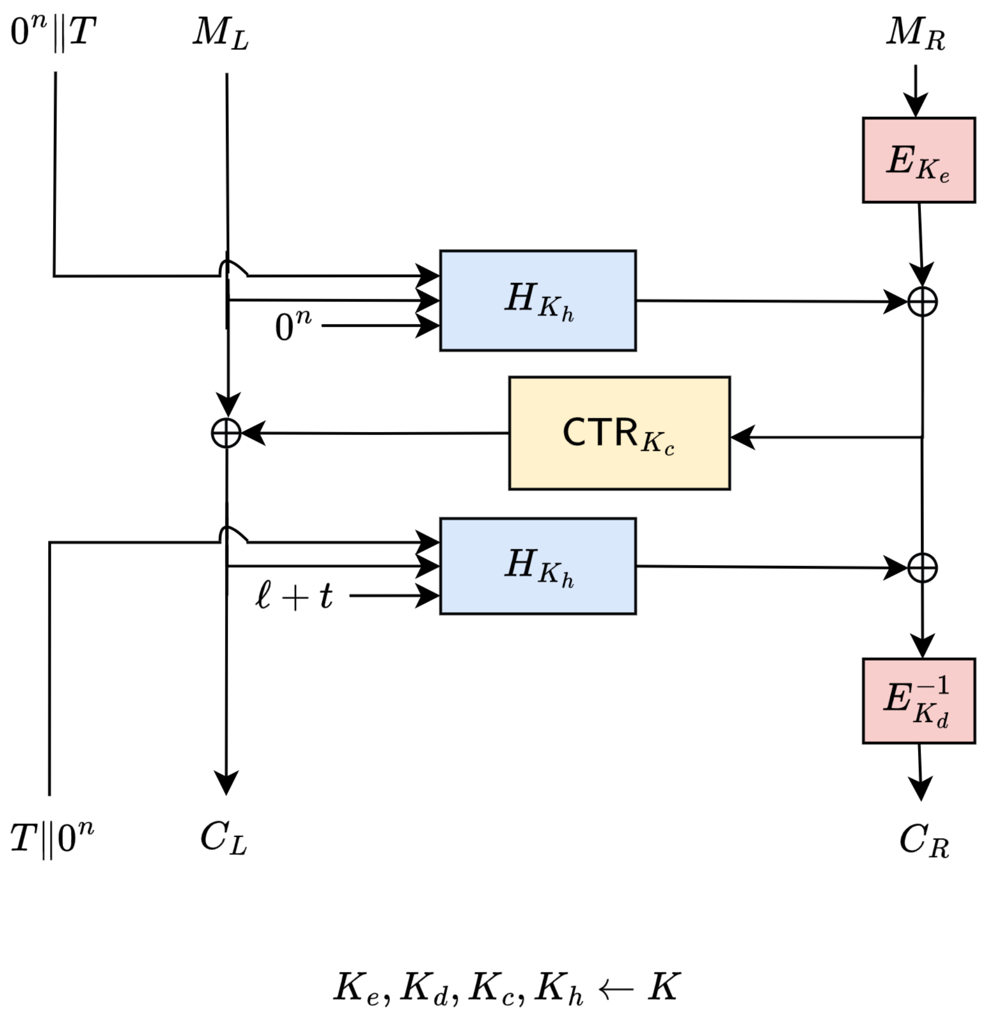
XCB-AES: IEEE 1619.2 TEM Standard [MF07]



- Internal components
  1. CTR = Counter mode
  2. E = AES blockcipher
  3. H = a polynomial/rolling hash
     e.g., Polyval, GHASH

KU LEUVEN

XCB-AES: IEEE 1619.2 TEM Standard [MF07]



- Internal components
  1. CTR = Counter mode
  2. E = AES blockcipher
  3. H = a polynomial/rolling hash
     e.g., Polyval, GHASH

$$\text{Poly}_K(A_1 \| A_2 \| \ldots) = A_1 K \oplus A_2 K^2 \oplus \ldots$$

KU LEUVEN

XCB-AES Results Timeline

XCB-AES Results Timeline

- **2010** IEEE standardized XCB-AES for storage media encryption
- **2013** Padding attack found on XCB-AES [CHS13]
- **2021** IEEE updated XCB-AES standard with its padding-free variant XCBv2fb

XCB-AES Results Timeline

2010 IEEE standardized XCB-AES for storage media encryption

2013 Padding attack found on XCB-AES [CHS13]

2021 IEEE updated XCB-AES standard with its padding-free variant XCBv2fb

- Proven VIL-STPRP up to birthday bound for block-aligned messages [CHS13]
- Translates to security up to $2^{52-\log\ell}$ queries

KU LEUVEN

XCB-AES Results Timeline

2010 IEEE standardized XCB-AES for storage media encryption

2013 Padding attack found on XCB-AES [CHS13]

2021 IEEE updated XCB-AES standard with its padding-free variant XCBv2fb

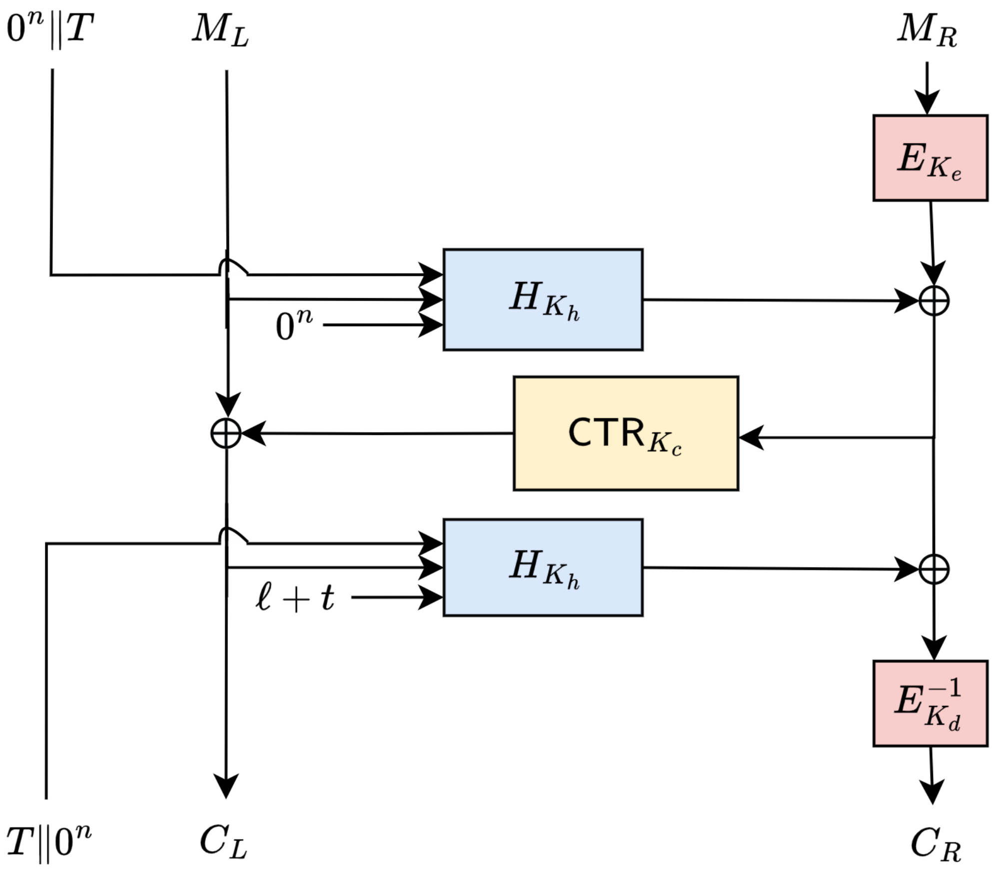
- Proven VIL-STPRP up to birthday bound for block-aligned messages [CHS13]
- Translates to security up to $2^{52-\log\ell}$ queries

2024 We break XCB-AES's VIL-STPRP, STPRP and SPRP security in 2 queries

Our attack applies to all other XCB-style modes as well

Our Result 1:
A 2-Query Plaintext Recovery Attack

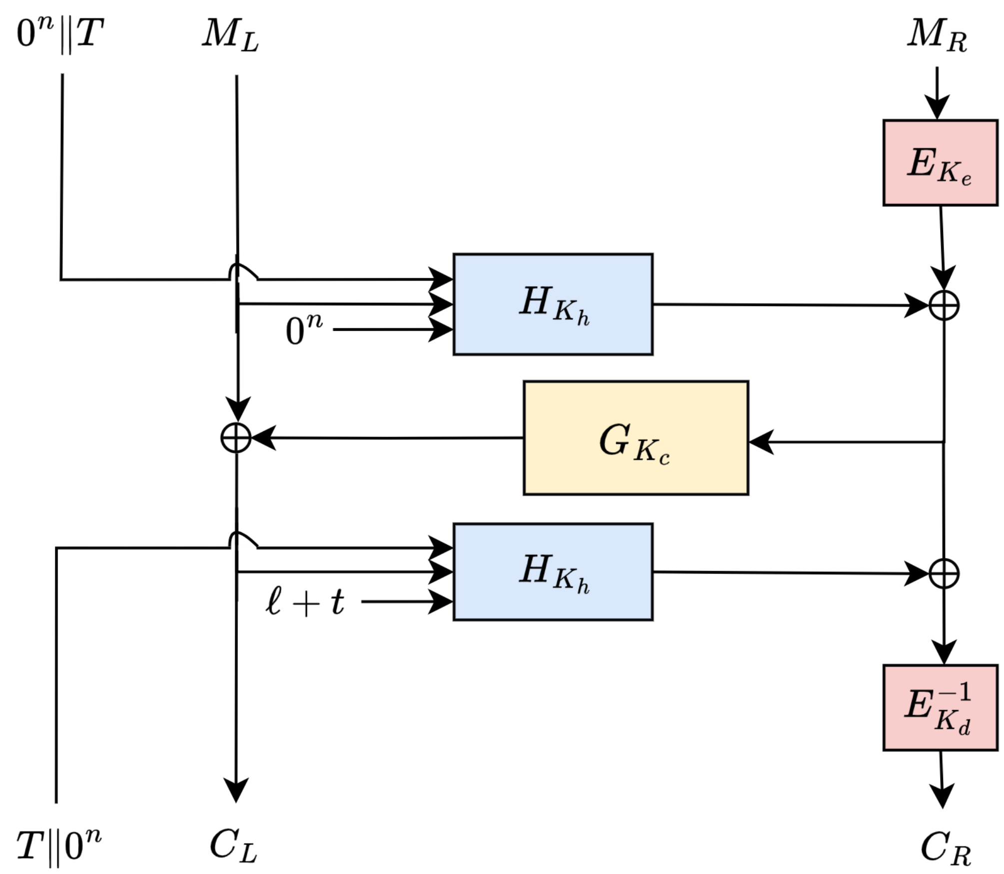
Our Shared Difference Attack



$K_e, K_d, K_c, K_h \leftarrow K$

KU LEUVEN

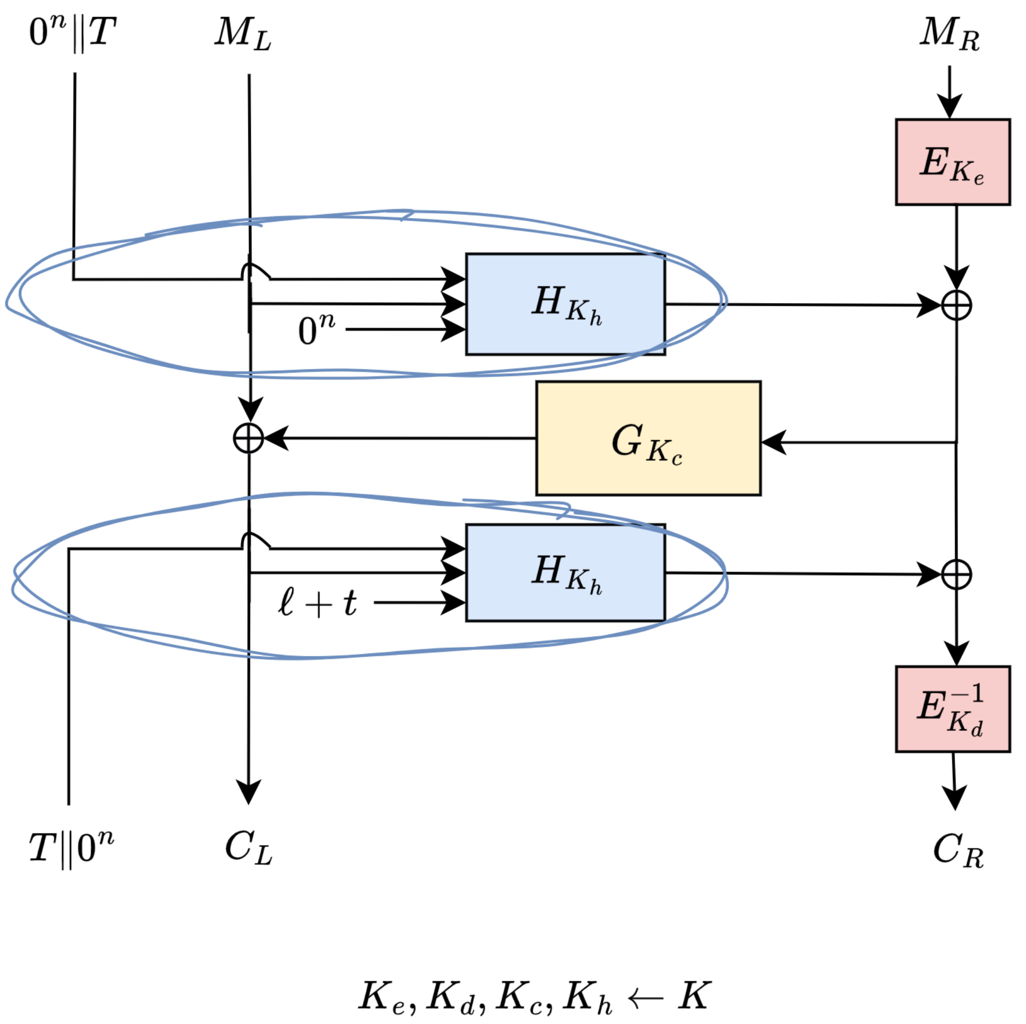
Our Shared Difference Attack



$K_e, K_d, K_c, K_h \leftarrow K$

KU LEUVEN

Our Shared Difference Attack



- $H_{K_h}(0^n\|T, M_L, 0^n)$

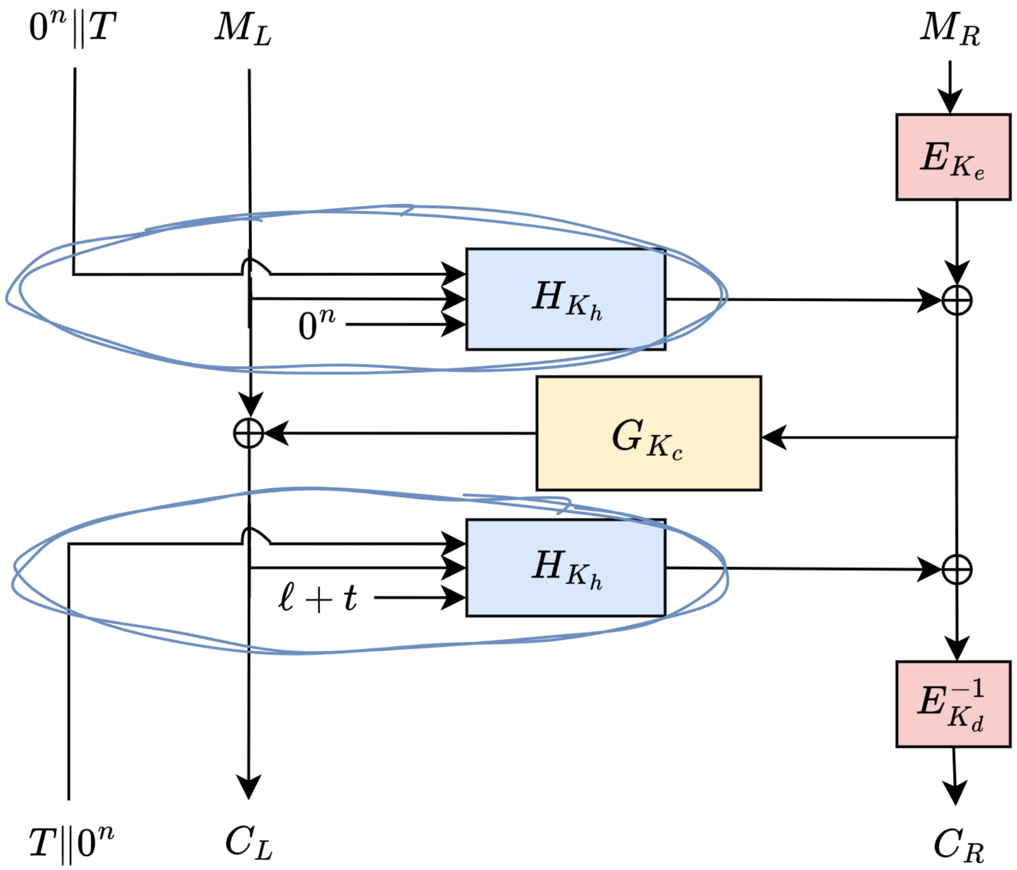
$$= \mathsf{Poly}_{K_h}(0^n\|\mathsf{pad}_n(T)\|\mathsf{pad}_n(M_L)\|0^n)$$

- $H_{K_h}(T\|0^n, C_L, \ell + t)$

$$= \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T)\|0^n\|\mathsf{pad}_n(C_L)\|\mathsf{bin}_n(\ell + t))$$

KU LEUVEN

Our Shared Difference Attack



$K_e, K_d, K_c, K_h \leftarrow K$

- $H_{K_h}(0^n \| T, M_L, 0^n)$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n)$$

$$= H_1(K_h, T, M_L)$$

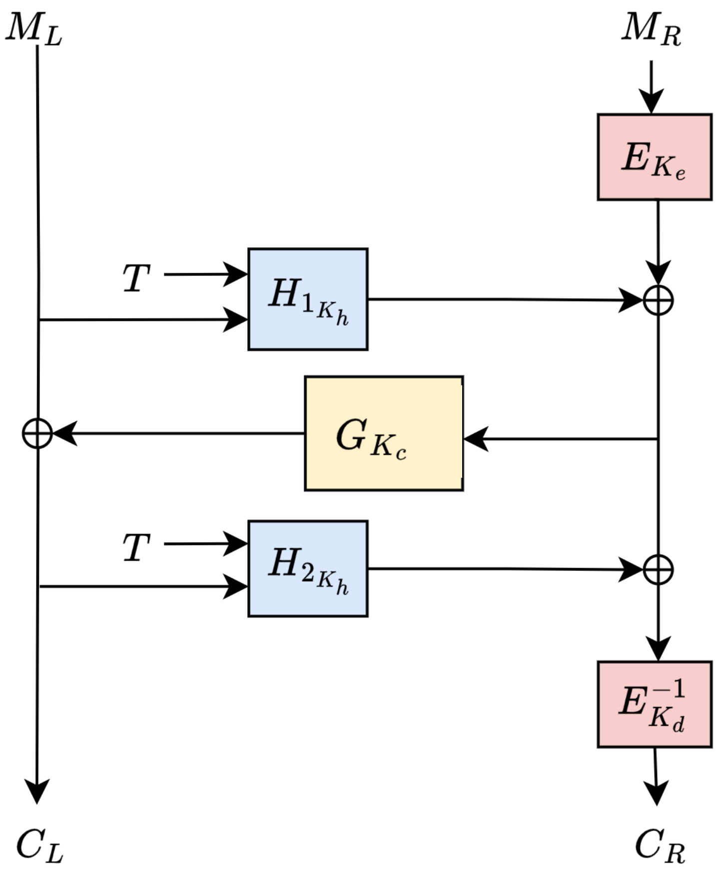
- $H_{K_h}(T \| 0^n, C_L, \ell + t)$

$$= \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L) \| \mathsf{bin}_n(\ell + t))$$

$$= H_2(K_h, T, C_L)$$

KU LEUVEN

Our Shared Difference Attack



$K_e, K_d, K_c, K_h \leftarrow K$

- $H_{K_h}(0^n \| T, M_L, 0^n)$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n)$$

$$= H_1(K_h, T, M_L)$$

- $H_{K_h}(T \| 0^n, C_L, \ell + t)$

$$= \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L) \| \mathsf{bin}_n(\ell + t))$$

$$= H_2(K_h, T, C_L)$$

KU LEUVEN

Polynomial Hash Separability

$$\mathsf{Poly}_K(A_1 \| A_2 \| (A_3 \oplus \Delta) \| A_4) = A_1 K \oplus A_2 K^2 \oplus (A_3 \oplus \Delta) K^3 \oplus A_4 K^4$$

$$= A_1 K \oplus A_2 K^2 \oplus A_3 K^3 \oplus A_4 K^4 \oplus \Delta K^3$$

$$= \mathsf{Poly}_K(A_1 \| A_2 \| A_3 \| A_4) \oplus \mathsf{Poly}_K(0^n \| 0^n \| \Delta \| 0^n)$$

Polynomial Hash Separability

$$H_1(K_h, T, M_L \oplus \Delta) = \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L \oplus \Delta) \| 0^n)$$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n) \oplus \mathsf{Poly}_{K_h}(0^n \| 0^{|\mathsf{pad}_n(T)|} \| 0^x \| \Delta \| 0^y \| 0^n)$$

KU LEUVEN

Polynomial Hash Separability

$$H_1(K_h, T, M_L \oplus \Delta) = \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L \oplus \Delta) \| 0^n)$$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n) \oplus \mathsf{Poly}_{K_h}(0^n \| 0^{|\mathsf{pad}_n(T)|} \| 0^x \| \Delta \| 0^y \| 0^n)$$

$$= H_1(K_h, T, M_L) \oplus f_\Delta$$

KU LEUVEN

Polynomial Hash Separability

$$H_1(K_h, T, M_L \oplus \Delta) = \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L \oplus \Delta) \| 0^n)$$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n) \oplus \mathsf{Poly}_{K_h}(0^n \| 0^{|\mathsf{pad}_n(T)|} \| 0^x \| \Delta \| 0^y \| 0^n)$$

$$= H_1(K_h, T, M_L) \oplus f_\Delta$$

$$H_2(K_h, T, C_L \oplus \Delta) = \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L \oplus \Delta) \| \mathsf{bin}_n(\ell + t))$$

$$= \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L) \| \mathsf{bin}_n(\ell + t)) \oplus \mathsf{Poly}_{K_h}(0^{|\mathsf{pad}_n(T)|} \| 0^n \| 0^x \| \Delta \| 0^y \| 0^n)$$

Polynomial Hash Separability

$$H_1(K_h, T, M_L \oplus \Delta) = \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L \oplus \Delta) \| 0^n)$$

$$= \mathsf{Poly}_{K_h}(0^n \| \mathsf{pad}_n(T) \| \mathsf{pad}_n(M_L) \| 0^n) \ \oplus \ \mathsf{Poly}_{K_h}(0^n \| 0^{|\mathsf{pad}_n(T)|} \| 0^x \| \Delta \| 0^y \| 0^n)$$

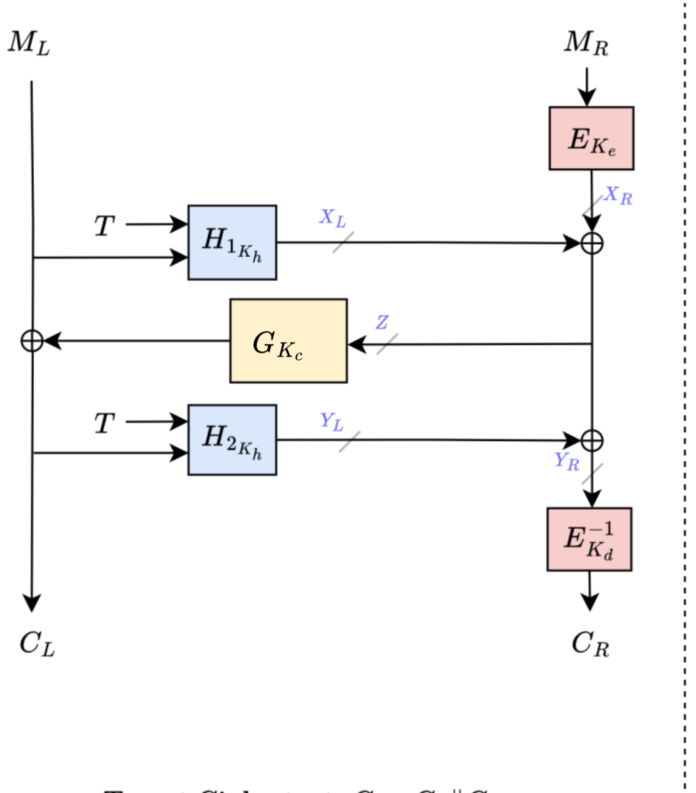
$$= H_1(K_h, T, M_L) \ \oplus \ f_\Delta$$

$$H_2(K_h, T, C_L \oplus \Delta) = \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L \oplus \Delta) \| \mathsf{bin}_n(\ell + t))$$

$$= \mathsf{Poly}_{K_h}(\mathsf{pad}_n(T) \| 0^n \| \mathsf{pad}_n(C_L) \| \mathsf{bin}_n(\ell + t)) \ \oplus \ \mathsf{Poly}_{K_h}(0^{|\mathsf{pad}_n(T)|} \| 0^n \| 0^x \| \Delta \| 0^y \| 0^n)$$

$$= H_2(K_h, T, C_L) \ \oplus \ f_\Delta$$

Our Shared Difference Attack

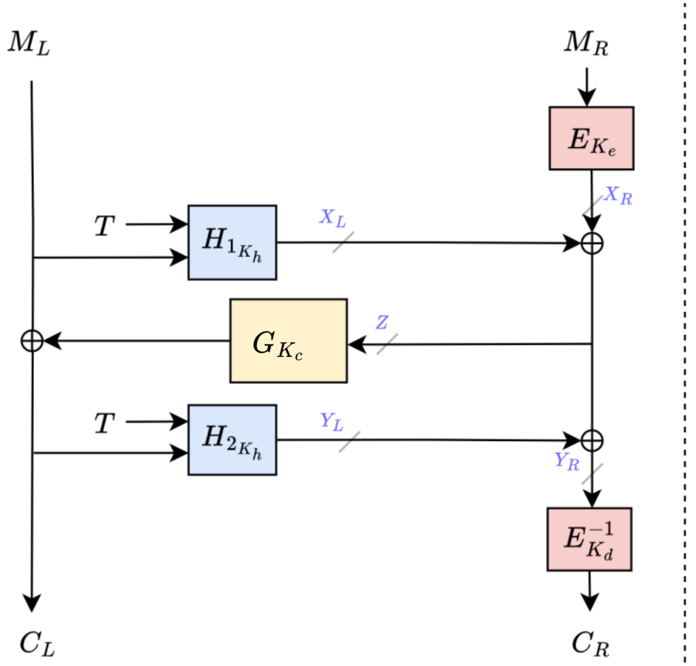


Target Ciphertext: $C = C_L \| C_R$

$\mathcal{A}$

KU LEUVEN

Our Shared Difference Attack



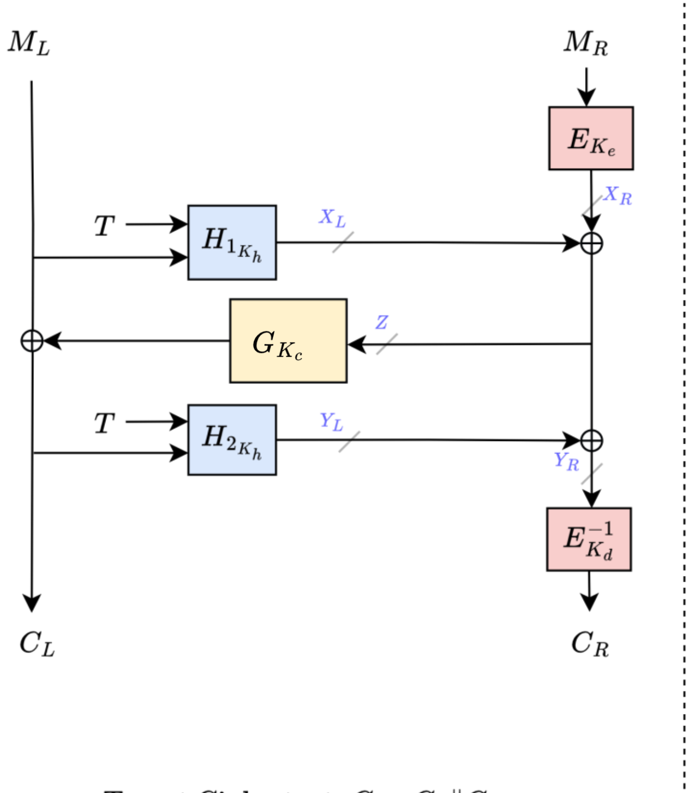
Target Ciphertext: $C = C_L \| C_R$

$\mathcal{A}$

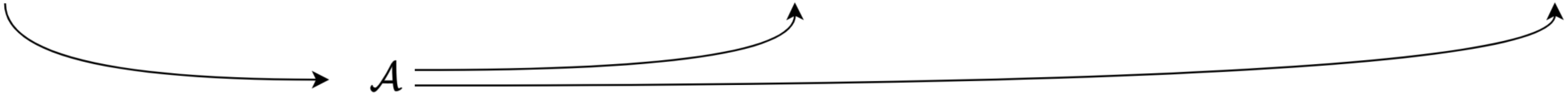
chooses a $\Delta \neq 0$,
targets the same T

KU LEUVEN

Our Shared Difference Attack

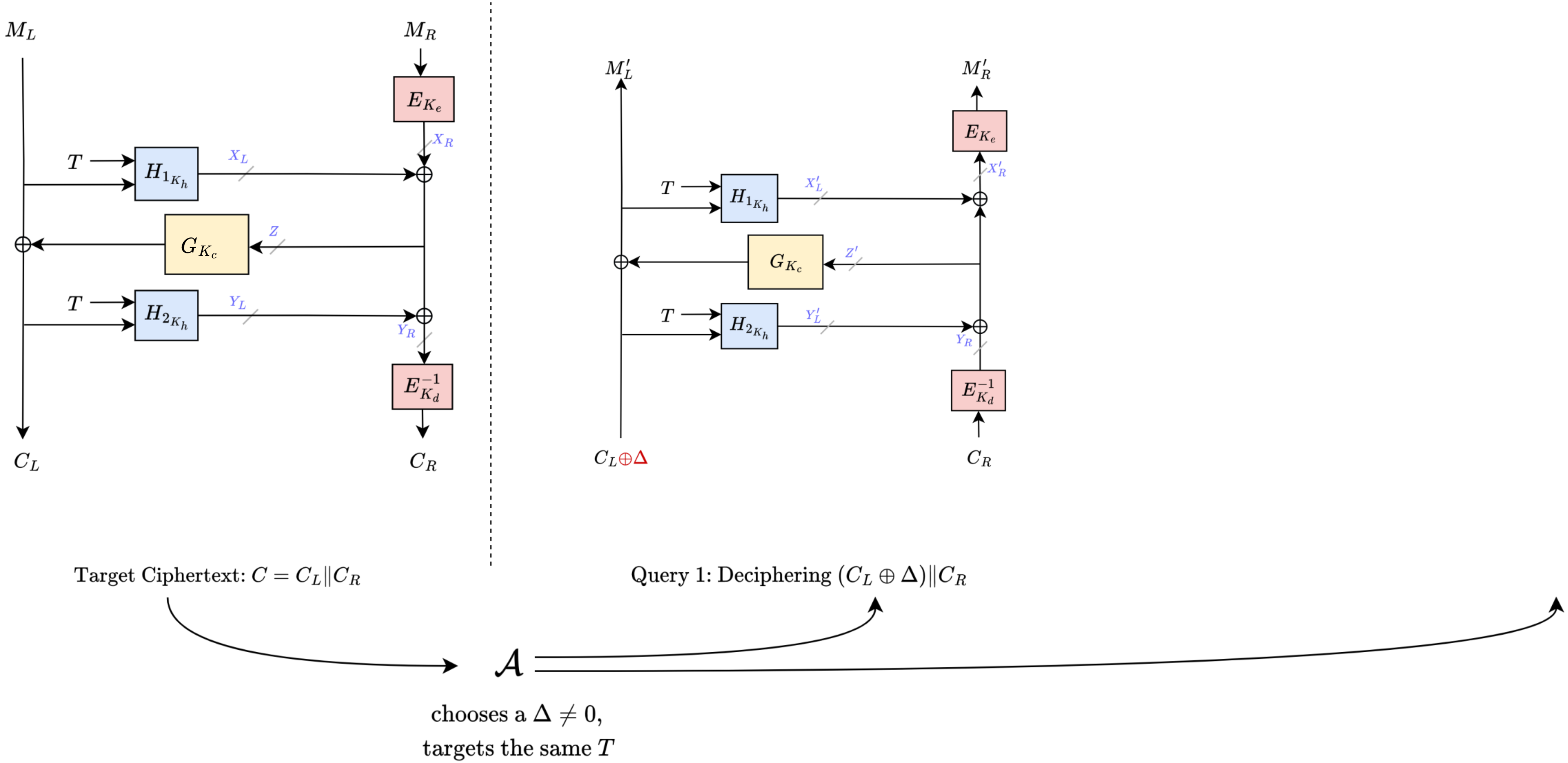


Target Ciphertext: $C = C_L \| C_R$



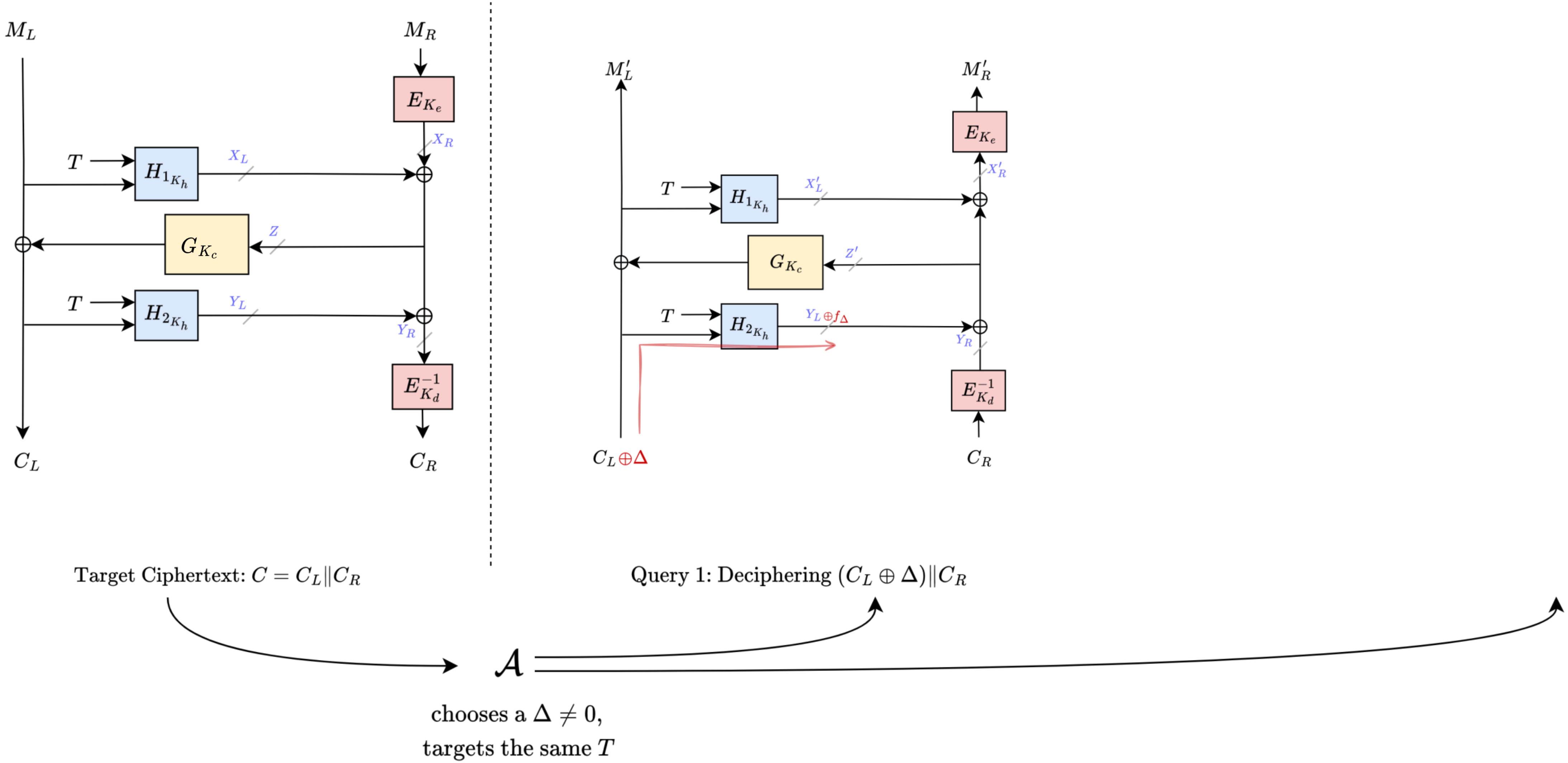
chooses a $\Delta \neq 0$,
targets the same T

Our Shared Difference Attack



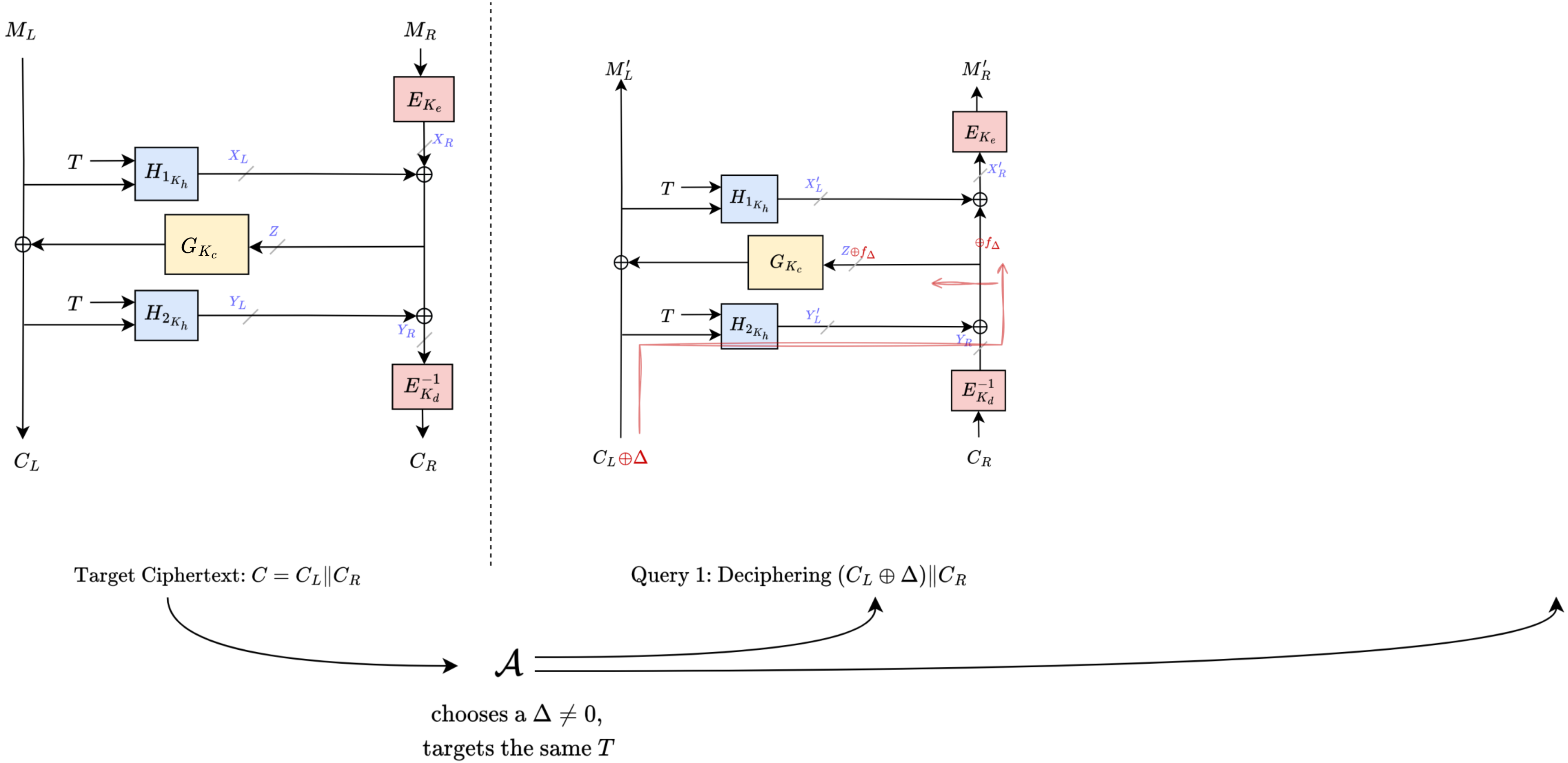
KU LEUVEN

Our Shared Difference Attack

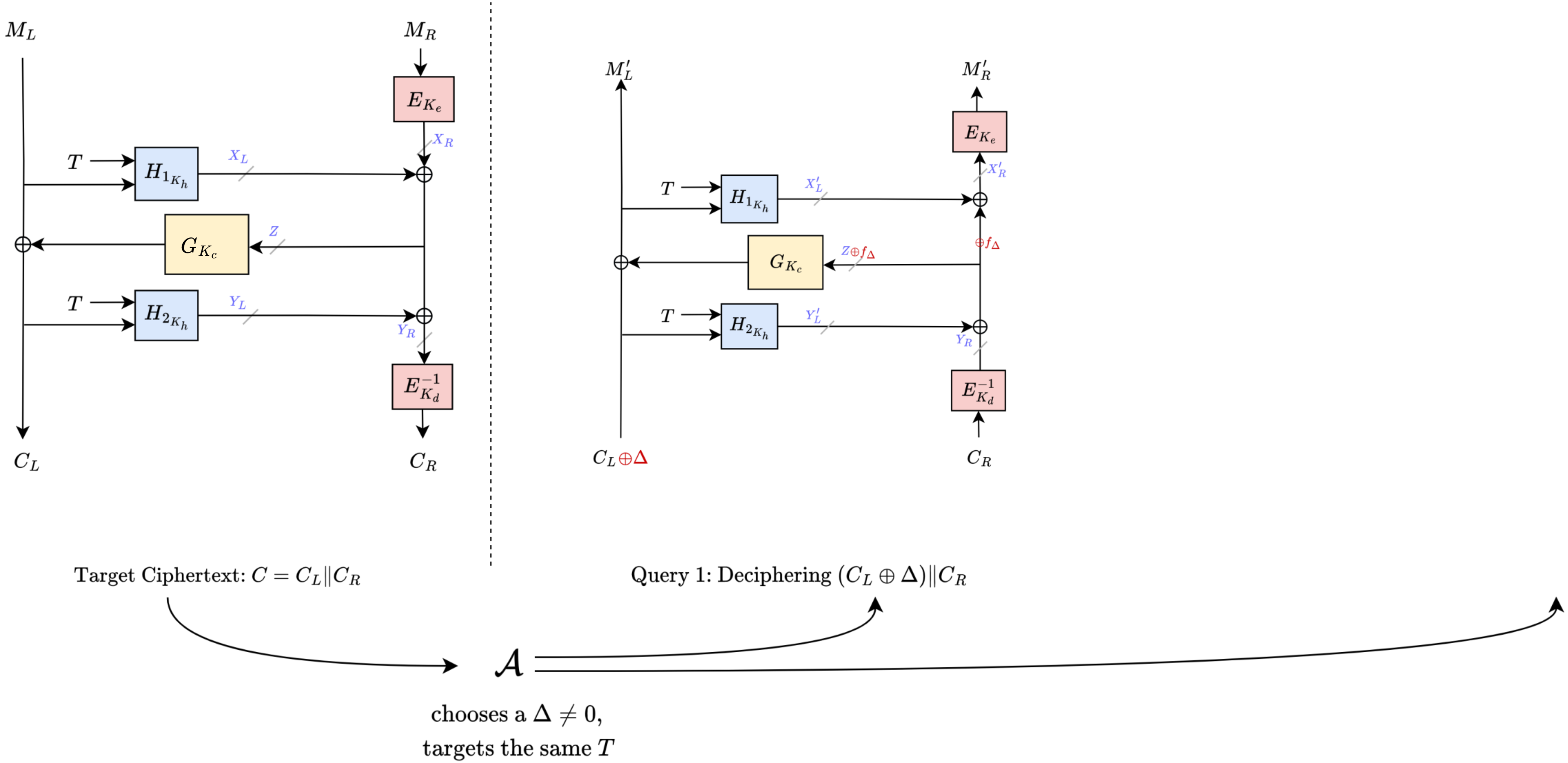


KU LEUVEN

Our Shared Difference Attack

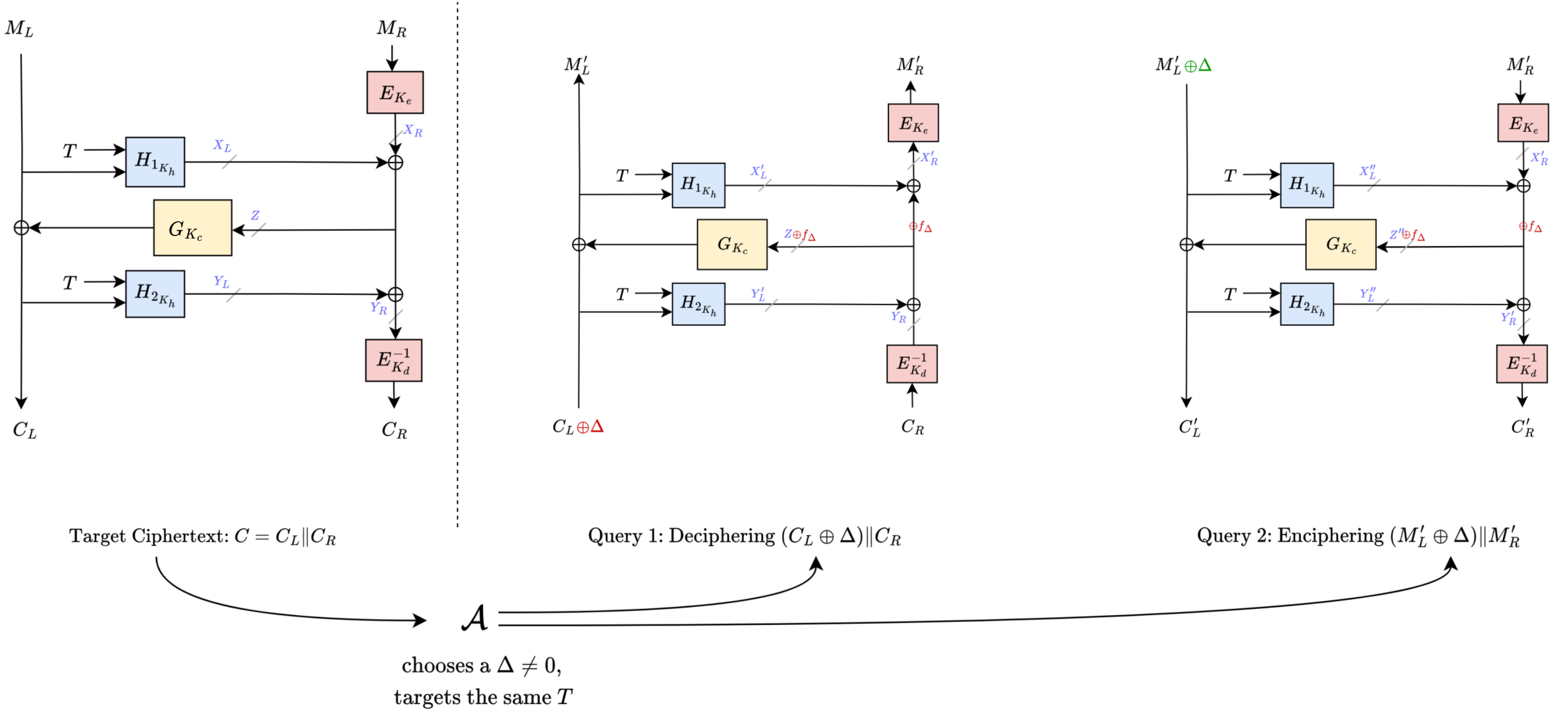


Our Shared Difference Attack

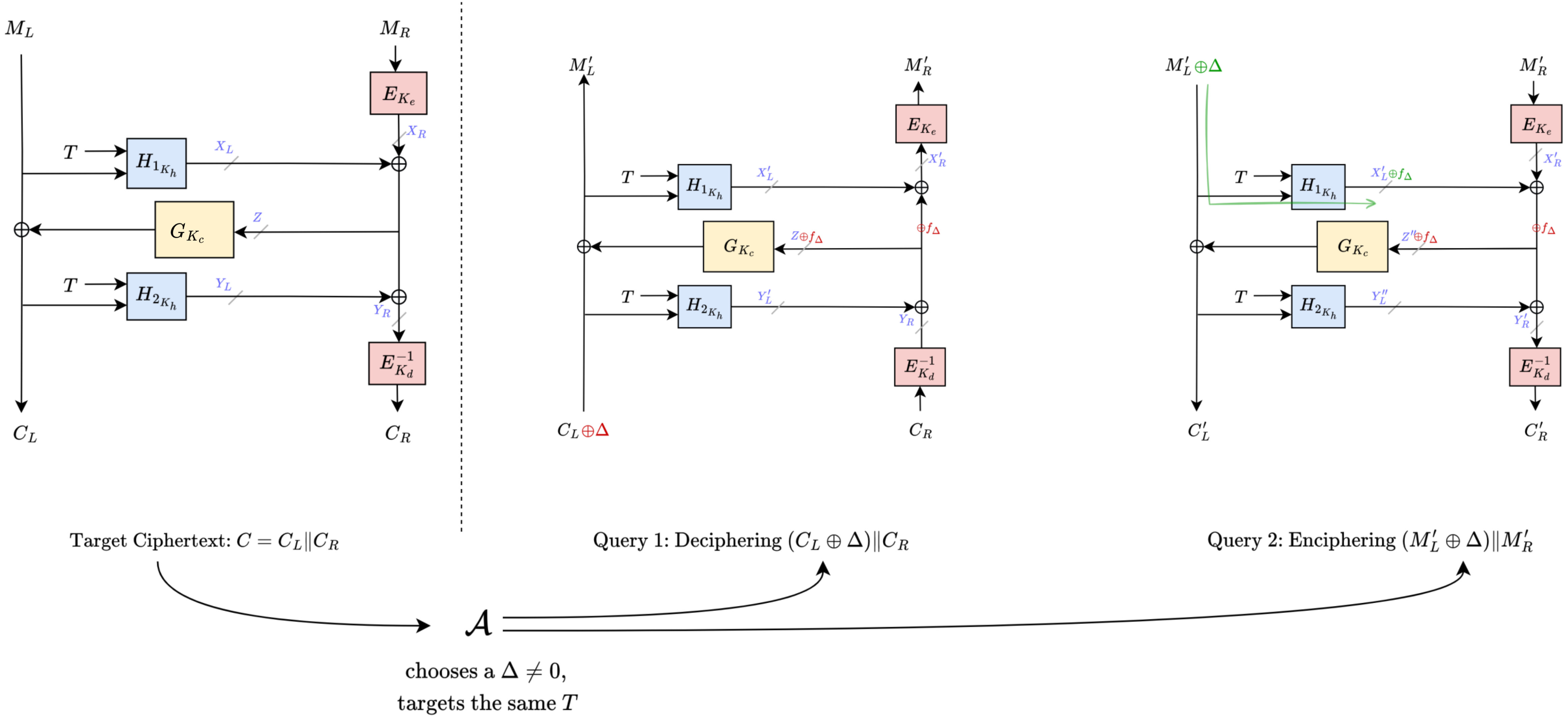


KU LEUVEN

Our Shared Difference Attack

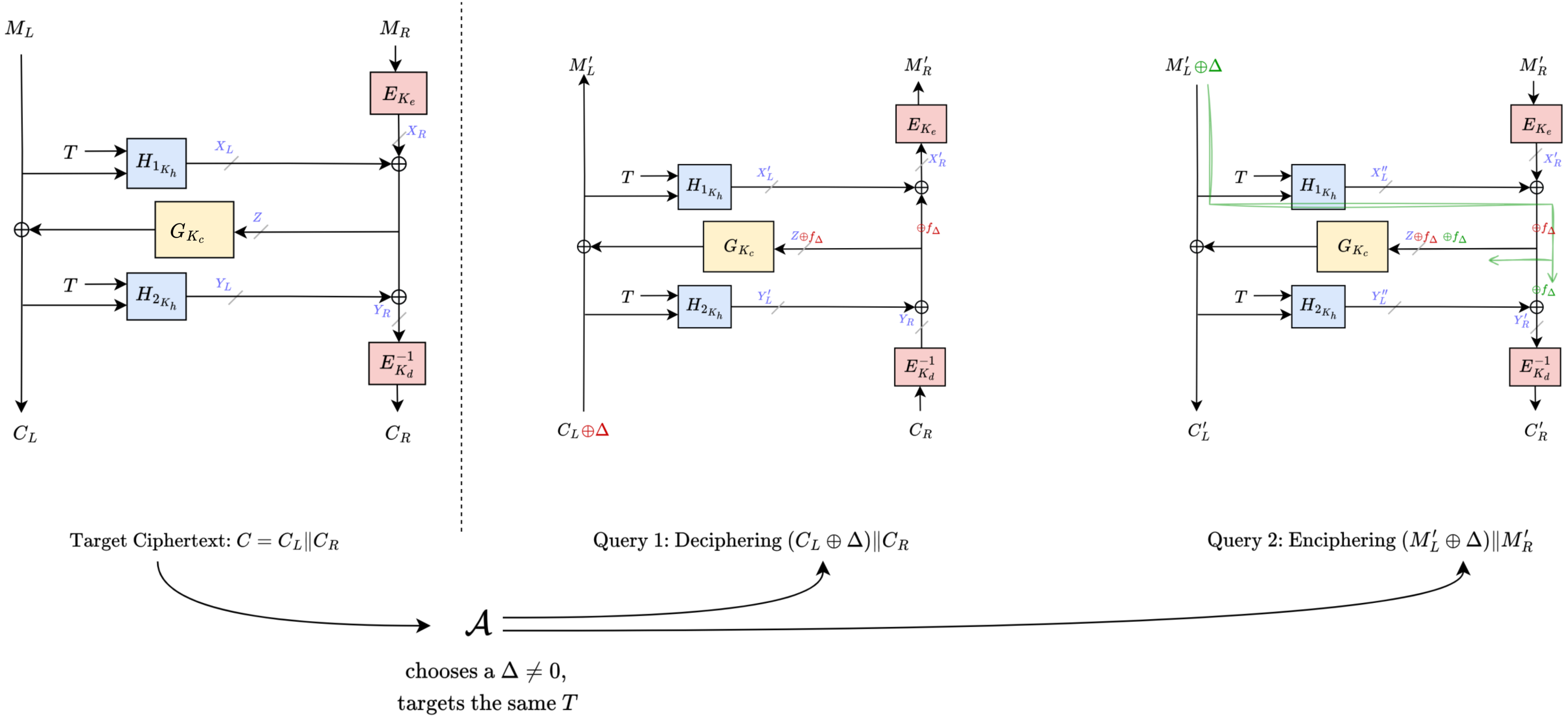


Our Shared Difference Attack



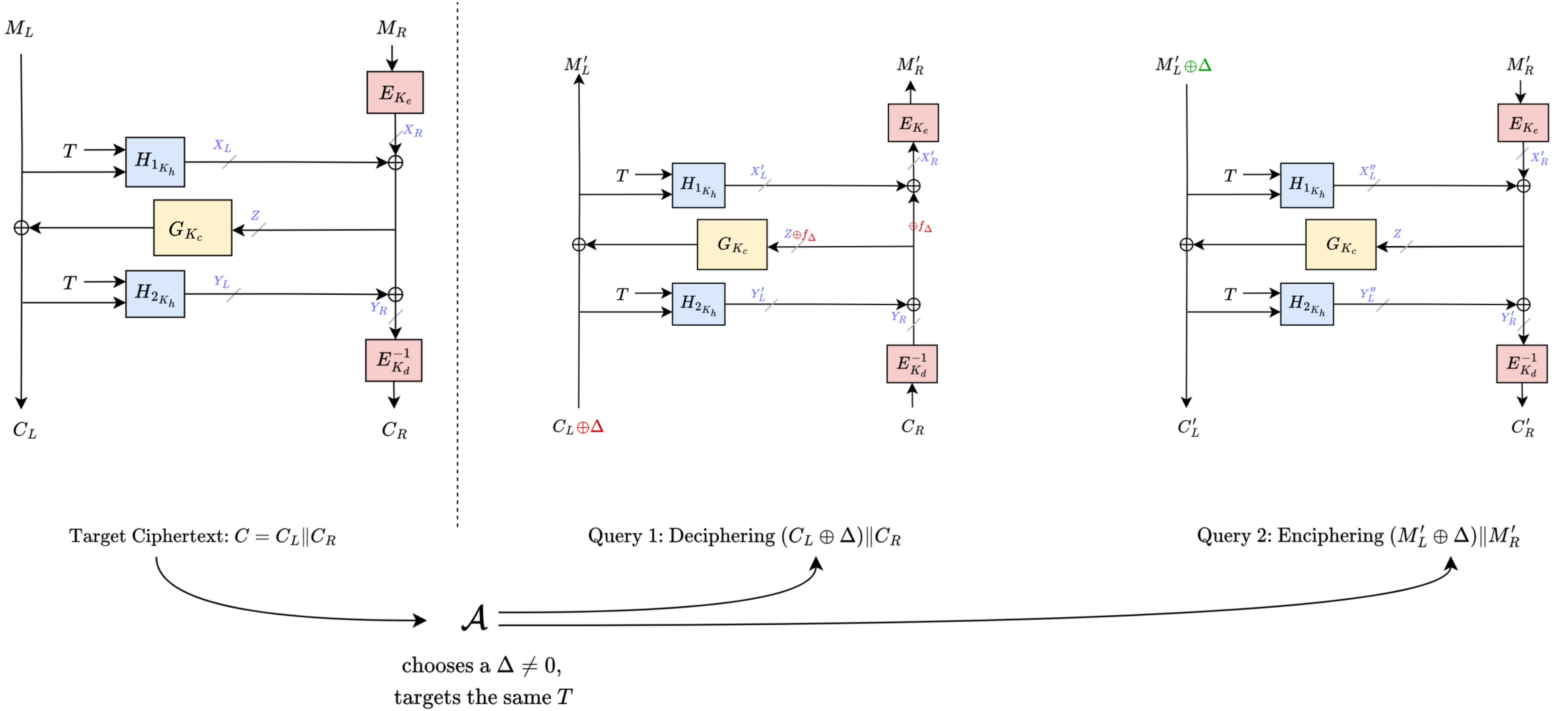
KU LEUVEN

Our Shared Difference Attack

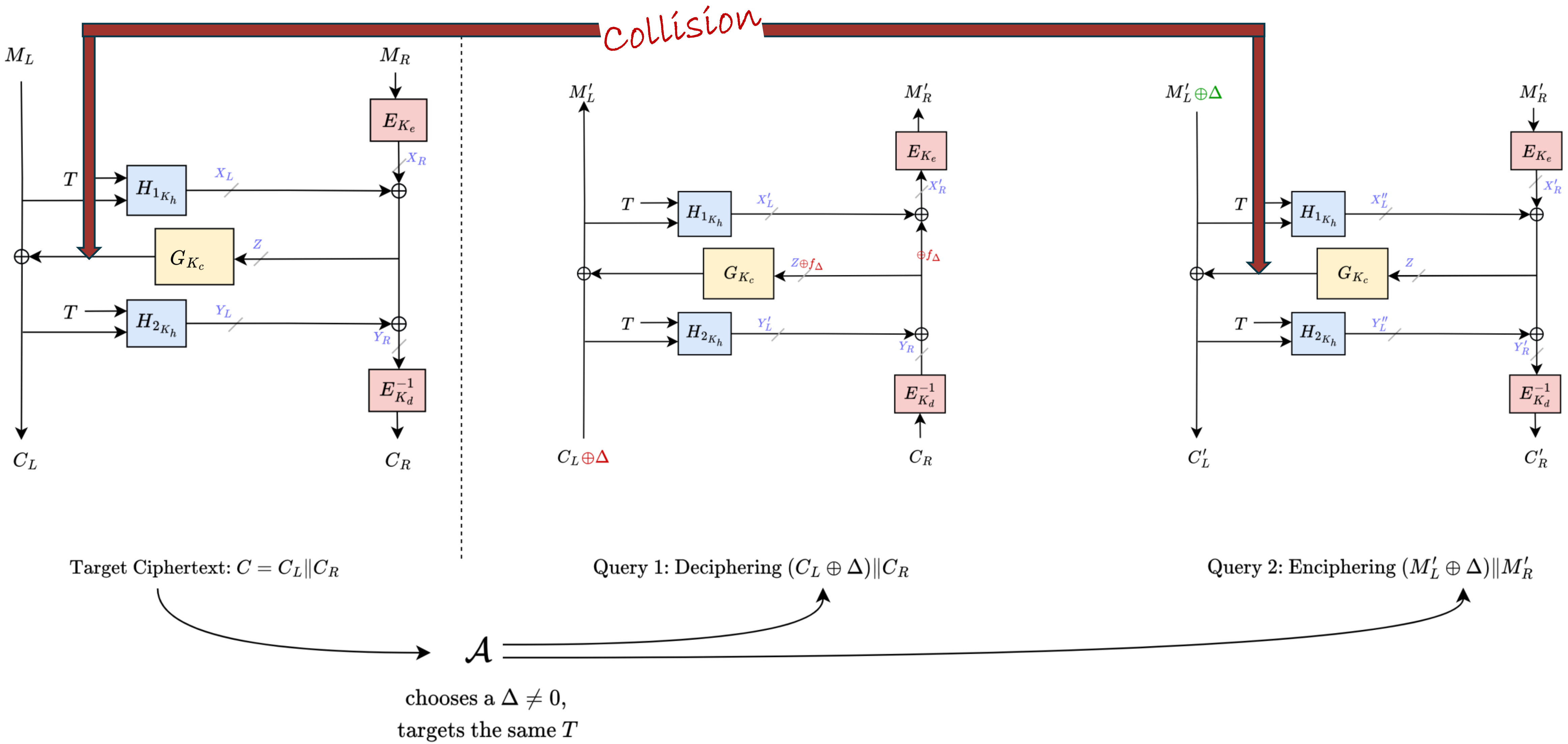


KU LEUVEN

Our Shared Difference Attack

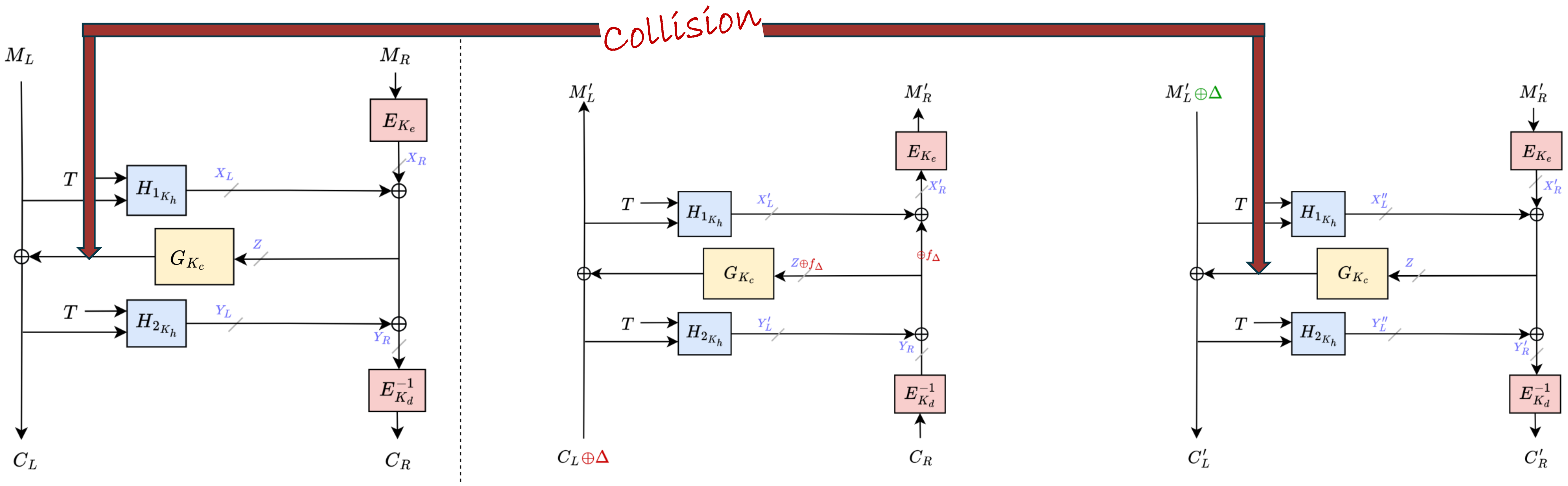


Our Shared Difference Attack



KU LEUVEN

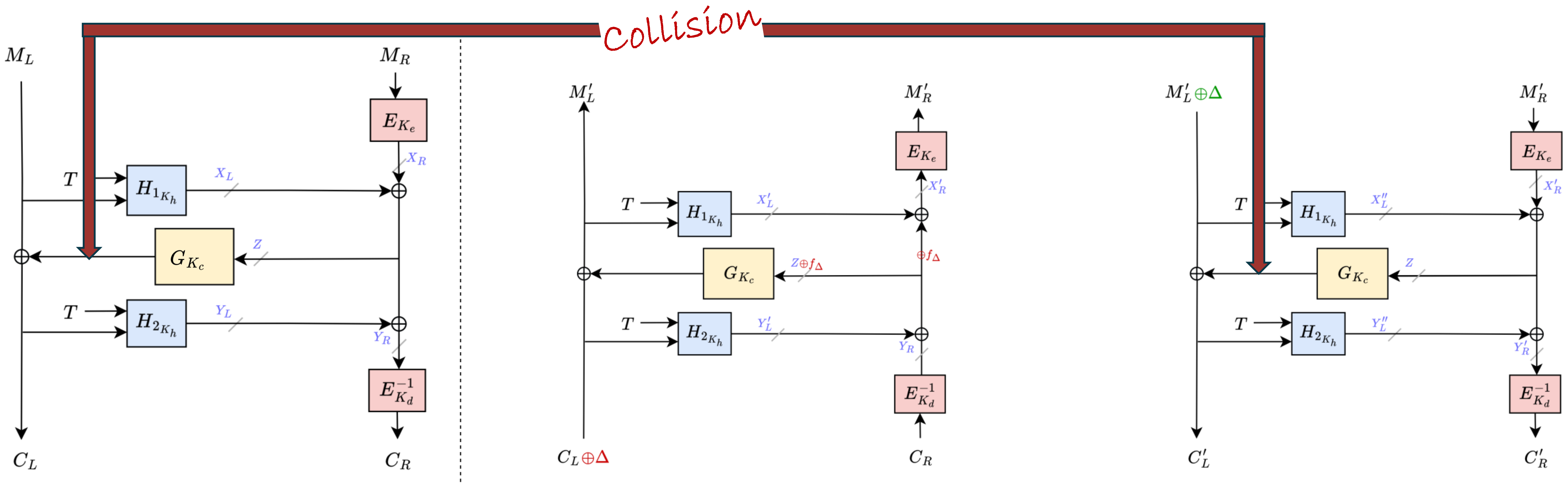
Our Shared Difference Attack



$$M_L \oplus C_L = (M'_L \oplus \Delta) \oplus C'_L$$

KU LEUVEN

Our Shared Difference Attack



$$M_L \oplus C_L = (M'_L \oplus \Delta) \oplus C'_L$$

$$M_L = (M'_L \oplus \Delta) \oplus C'_L \oplus C_L$$

Message Recovered

KU LEUVEN

Why Does This Work?

Root Cause: A Shared Difference Property

Shared Difference Property of Polynomial Sum

- $H_{\text{sum}}(K, T, M, C) = H_1(K, T, M) \oplus H_2(K, T, C)$

Shared Difference Property of Polynomial Sum

- $H_{\text{sum}}(K, T, M, C) = H_1(K, T, M) \oplus H_2(K, T, C)$
- $H_{\text{sum}}(K, T, M \oplus \Delta, C \oplus \Delta) = H_1(K, T, M \oplus \Delta) \oplus H_2(K, T, C \oplus \Delta)$

Shared Difference Property of Polynomial Sum

- $H_{\text{sum}}(K, T, M, C) = H_1(K, T, M) \oplus H_2(K, T, C)$

- $H_{\text{sum}}(K, T, M \oplus \Delta, C \oplus \Delta) = H_1(K, T, M \oplus \Delta) \oplus H_2(K, T, C \oplus \Delta)$

$$= H_1(K, T, M) \oplus f_\Delta \oplus H_2(K, T, C) \oplus f_\Delta$$

$$= H_1(K, T, M) \oplus H_2(K, T, C)$$

Shared Difference Property of Polynomial Sum

- $H_{\text{sum}}(K, T, M, C) = H_1(K, T, M) \oplus H_2(K, T, C)$

- $H_{\text{sum}}(K, T, M \oplus \Delta, C \oplus \Delta) = H_1(K, T, M \oplus \Delta) \oplus H_2(K, T, C \oplus \Delta)$

$$= H_1(K, T, M) \oplus f_\Delta \oplus H_2(K, T, C) \oplus f_\Delta$$

$$= H_1(K, T, M) \oplus H_2(K, T, C)$$

$$H_{\text{sum}}(K, T, M \oplus \Delta, C \oplus \Delta) = H_{\text{sum}}(K, T, M, C)$$

due to separability of polynomial hash

Our attack was first disclosed on 13th Feb 2024 in our CRYPTO'24 submission. Had quite a rollercoaster with a case of established reviewer misconduct during submissions, before making it to CRYPTO'25.

Flaw in Existing Analysis

Flaw in Existing Analysis

- Existing proofs based on XOR-universal hash functions

Assumes H_1, H_2 are XOR-universal

↓

Implies H_{sum} is universal

↓

CTR IV unpredictable and hard to collide

↓

Independent and random CTR key streams up to birthday bound

Flaw in Existing Analysis

- Existing proofs based on XOR-universal hash functions

Assumes H_1, H_2 are XOR-universal

↓

Implies H_{sum} is universal

↓

CTR IV unpredictable and hard to collide

↓

Independent and random CTR key streams up to birthday bound

$$H_{\mathrm{sum}}(K, T, M \oplus \Delta, C \oplus \Delta) = H_{\mathrm{sum}}(K, T, M, C)$$

KU LEUVEN

Flaw in Existing Analysis

- Existing proofs based on XOR-universal hash functions

Assumes H_1, H_2 are XOR-universal

↓

$$H_{\text{sum}}(K,T,M\oplus\Delta,C\oplus\Delta) = H_{\text{sum}}(K,T,M,C)$$

~~Implies H_{sum} is universal~~

↓

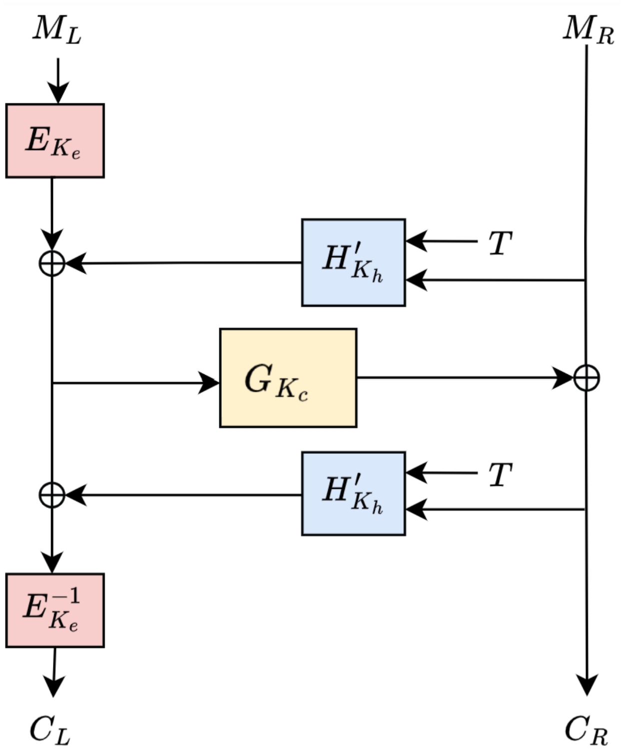
CTR IV unpredictable and hard to collide

↓

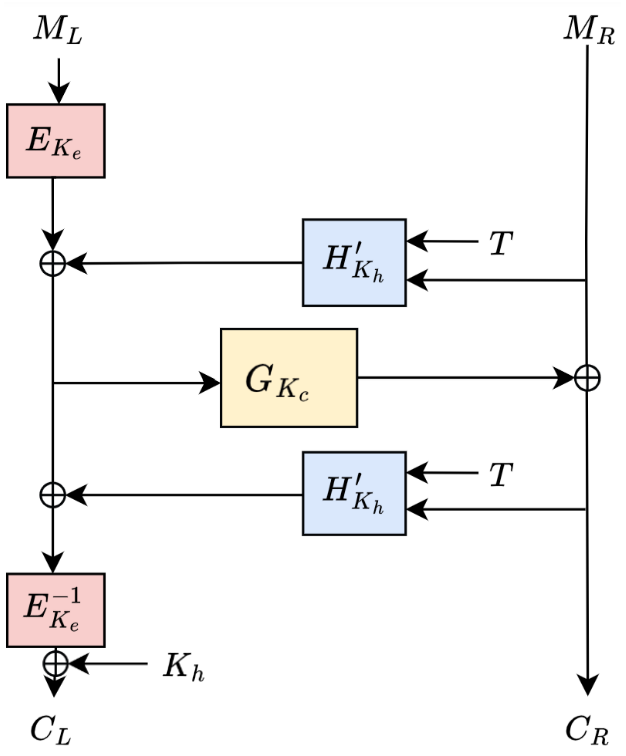
Independent and random CTR key streams up to birthday bound

Our Result 2:
Applications of Shared Difference Attack to Other XCB-style TEMs

Shared Difference Attack on Other XCB-style TEMs

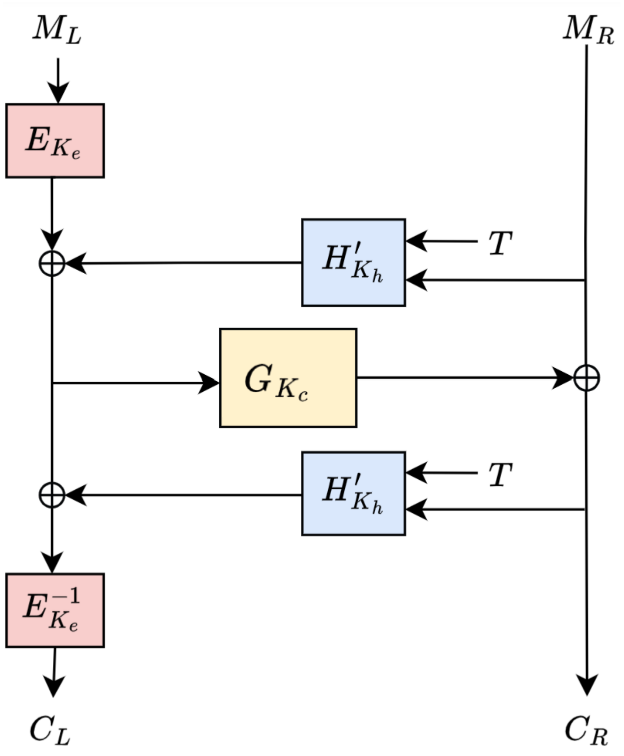


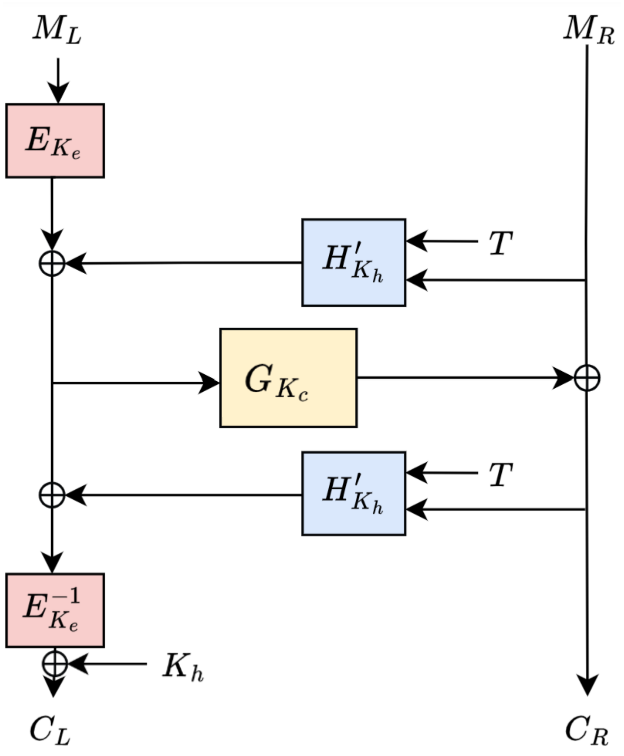
HCI [Nan08]



MXCB [Nan08]

Shared Difference Attack on Other XCB-style TEMs





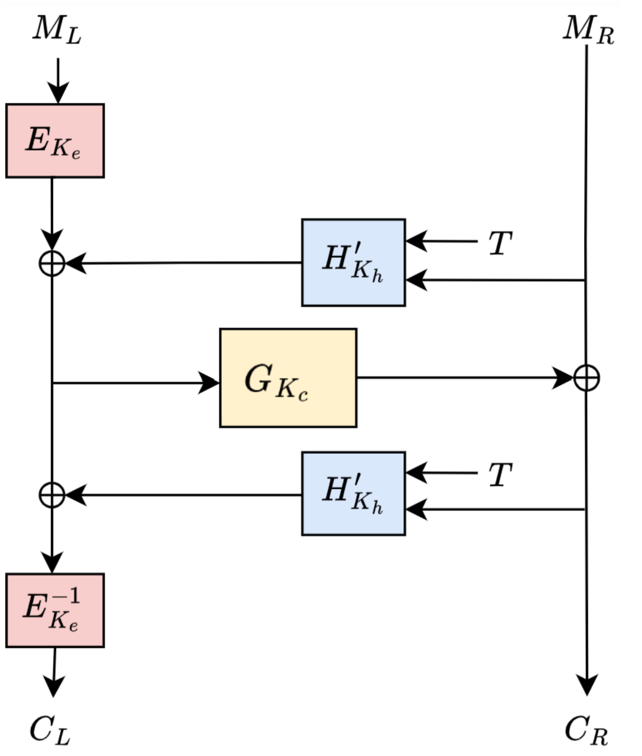
HCI [Nan08]

MXCB [Nan08]

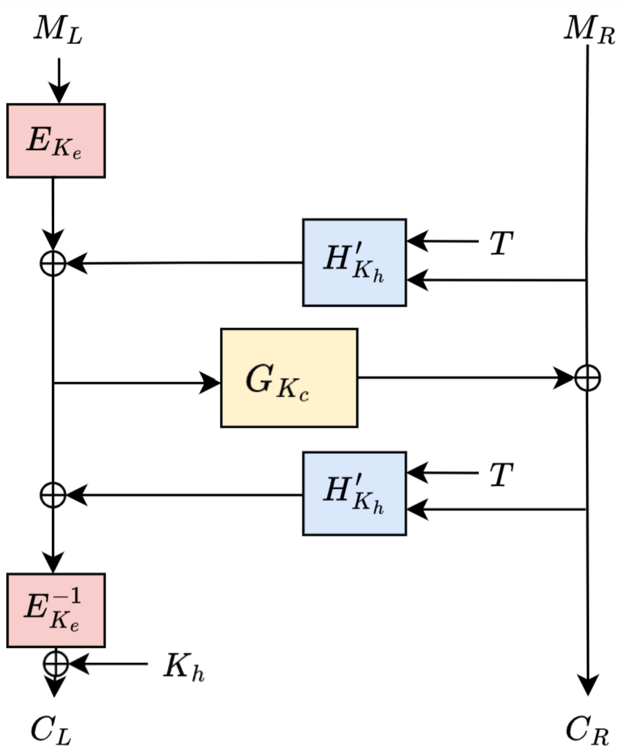
Mirrored XCB-AES,
Direct application of our attack

KU LEUVEN

Shared Difference Attack on Other XCB-style TEMs

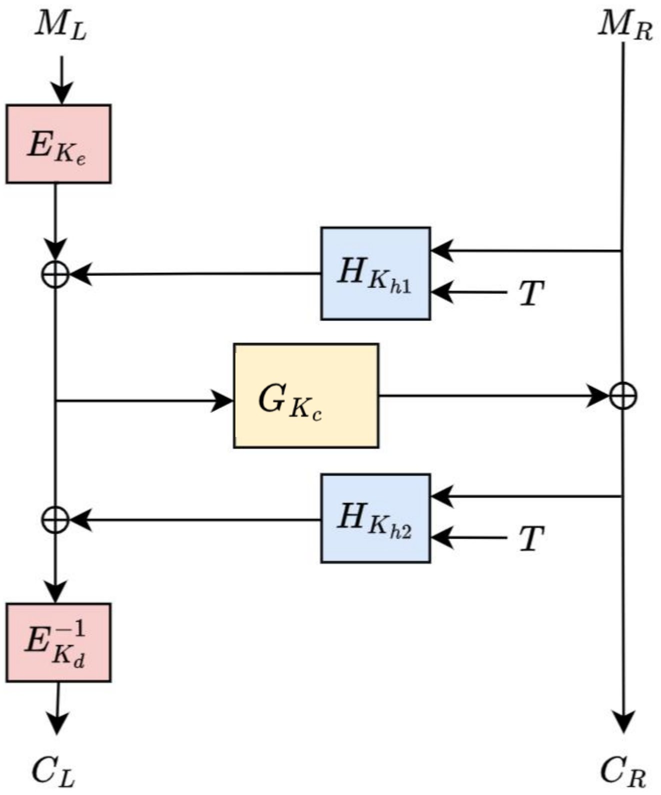


HCI [Nan08]



MXCB [Nan08]

Mirrored XCB-AES,
Direct application of our attack



XCBv1 [MF07]

Two-hash-key XCB-AES,
Attack by contradiction

KU LEUVEN

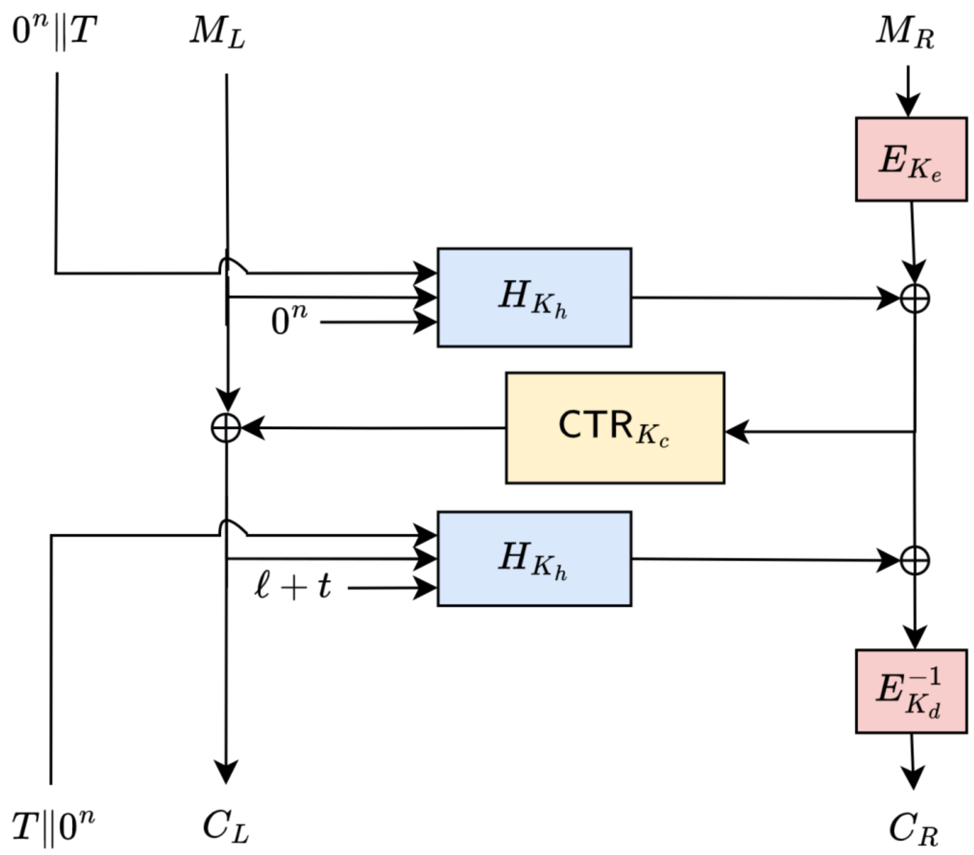
Summary of Results

Attack	Schemes	Message length	Attack type	# queries
LRW1 CCA attack by Khairallah [Kha23]	XCBv1, XCBv2, XCBv2fb	n bits	recovery of n bits	3
Shared difference attack [This work]	XCBv1	all $m > n$ bits	recovery of $m - n$ bits	4
	XCBv2, XCBv2fb, HCI, MXCB	all $m > n$ bits	recovery of $m - n$ bits	2
Flipped parts attack [This work]	HCI	all $m > n$ bits	distinguishing attack	3

m can be arbitrarily large

Countermeasures for XCB

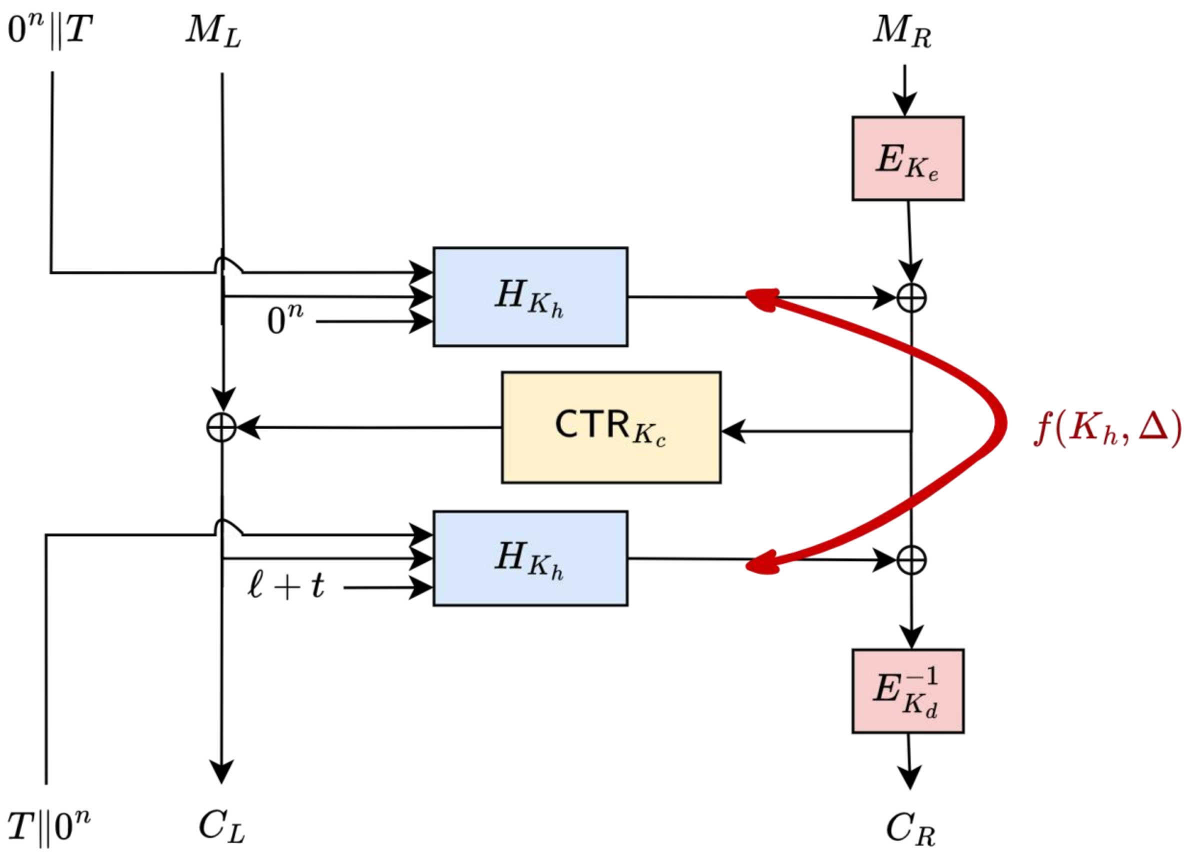
Repairing and Enhancing XCB



- XCB style

KU LEUVEN

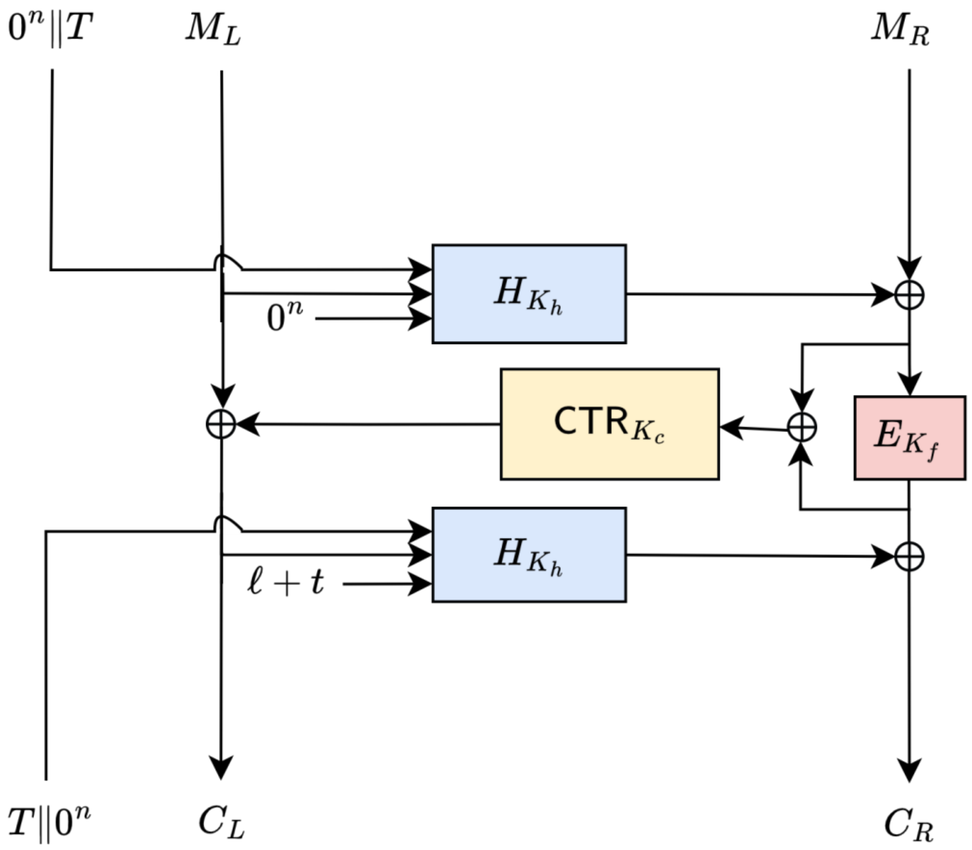
Repairing and Enhancing XCB



- XCB style
  - Insecure in current form

KU LEUVEN

Repairing and Enhancing XCB

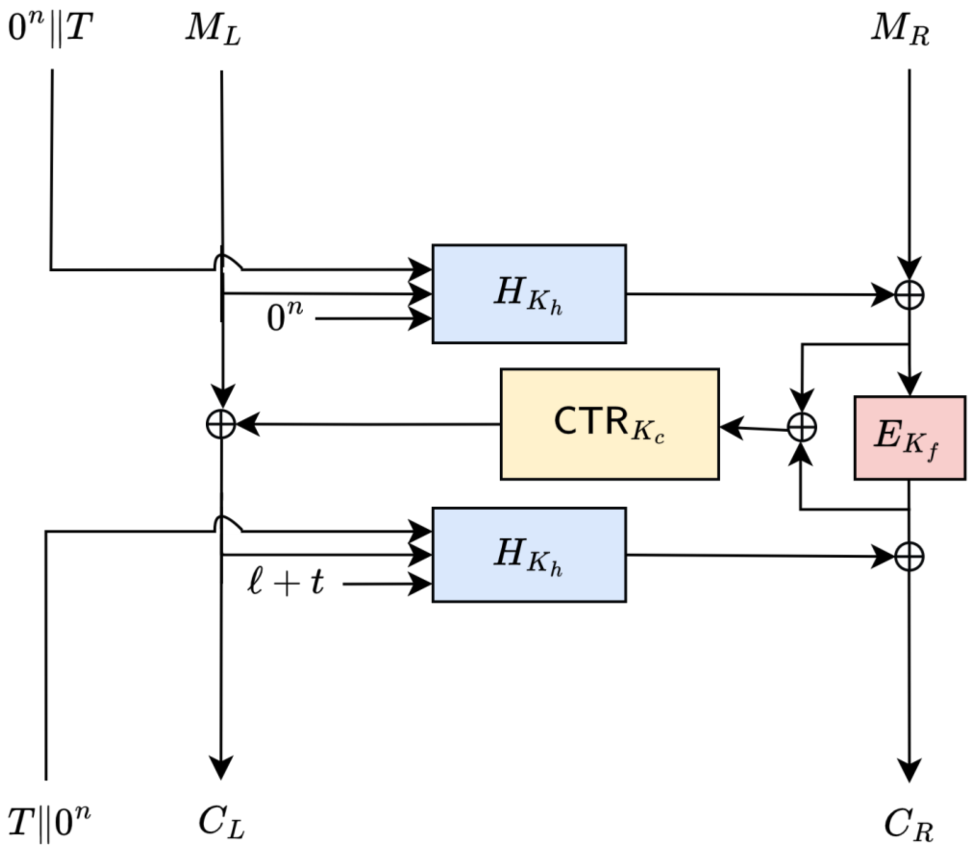


Avoid the Sum

- XCB style
  - Insecure in current form

KU LEUVEN

Repairing and Enhancing XCB

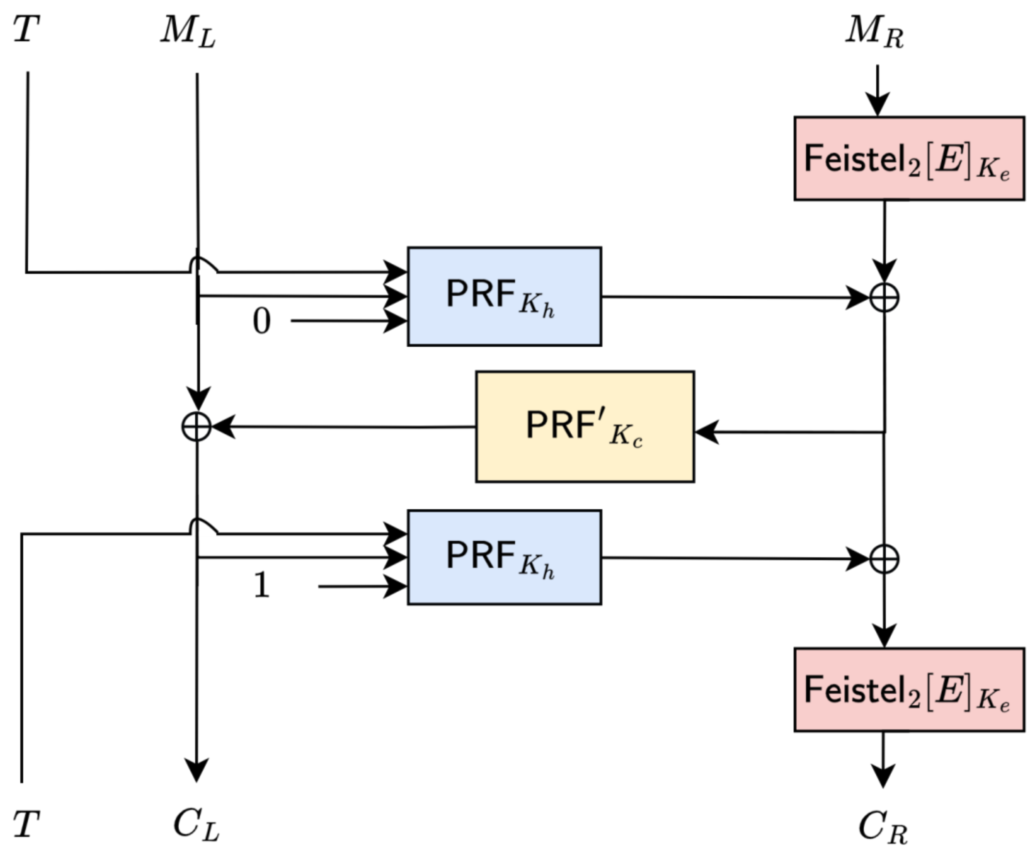


Avoid the Sum

- XCB style
  - Insecure in current form
- HCTR2 style [CHB23]
  - AES-128, PolyVal
  - 64-bit STPRP security
  - 1.1 cpb on Gracemont

KU LEUVEN

Repairing and Enhancing XCB

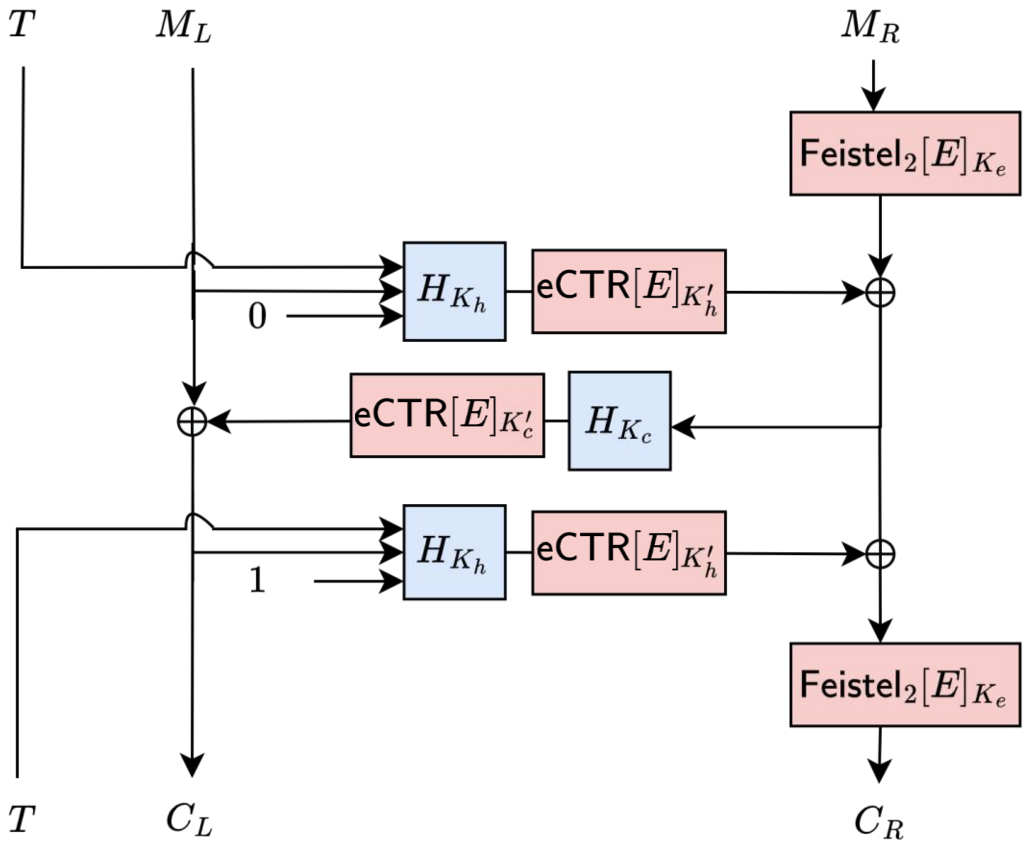


Use Inseparable Hashes

- XCB style
  - Insecure in current form
- HCTR2 style [CHB23]
  - AES-128, PolyVal
  - 64-bit STPRP security
  - 1.1 cpb on Gracemont
- GEM style [BVA24]

KU LEUVEN

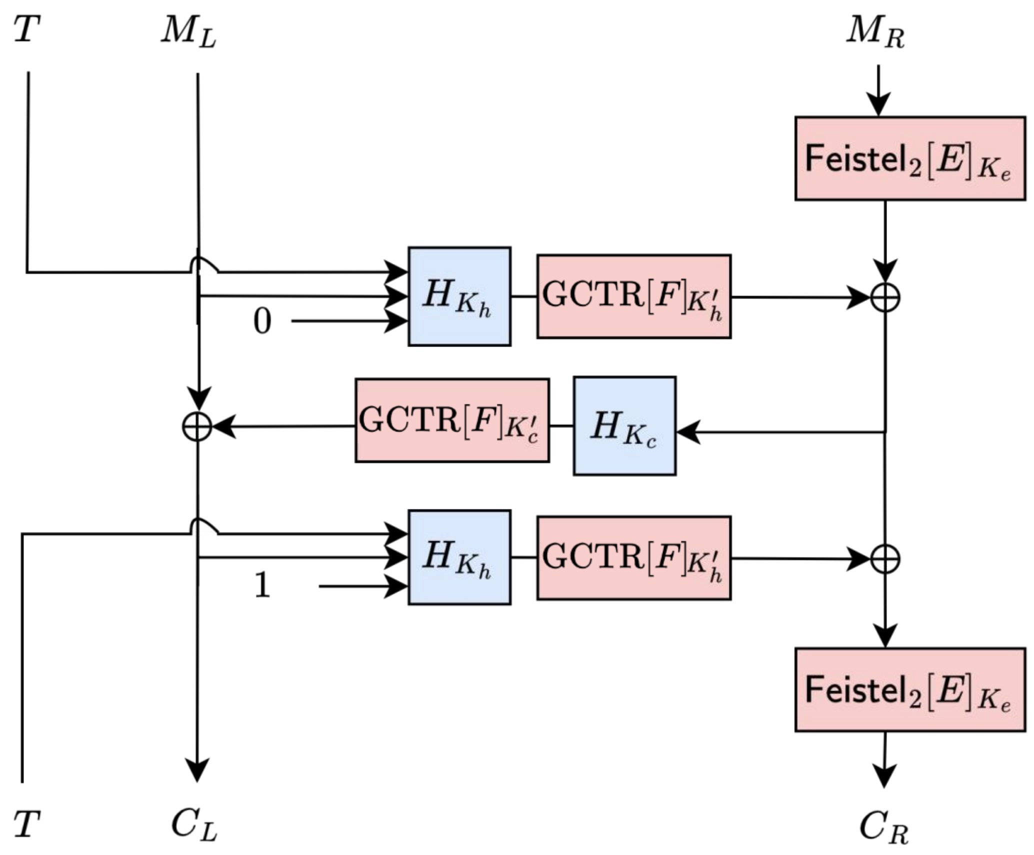
Repairing and Enhancing XCB



Use Inseparable Hashes

- XCB style
  - Insecure in current form
- HCTR2 style [CHB23]
  - AES-128, PolyVal
  - 64-bit STPRP security
  - 1.1 cpb on Gracemont
- GEM style [BVA24]
  - AES-128, PolyVal
  - 128-bit STPRP security
  - 1.4 cpb on Gracemont

Repairing and Enhancing XCB



Use Inseparable Hashes

- XCB style
  - Insecure in current form
- HCTR2 style [CHB23]
  - AES-128, PolyVal
  - 64-bit STPRP security
  - 1.1 cpb on Gracemont
- GEM style [BVA24]
  - Butterknife [ACL+22], PolyVal
  - 128-bit STPRP security
  - 1.1 cpb on Gracemont

Conclusion

Conclusion

1. Introduced shared difference attack against XCB
    - Breaking SPRP, STPRP, VIL-STPRP security of all XCB variants
    - Including XCB-AES; a 15 year old IEEE standard
2. Pinpointed exact flaw in existing analyses
3. Presented some countermeasures – HCTR2 and GEM

Impact: IEEE has officially removed XCB-AES from 1619.2 standard

Takeaway: 1. Efforts toward TEM design and analysis through NIST's accordion initiative are essential

2. To protect innovation, we must enforce clear professional consequences for reviewer misconduct

Thank You!

(ia.cr/2024/1554)

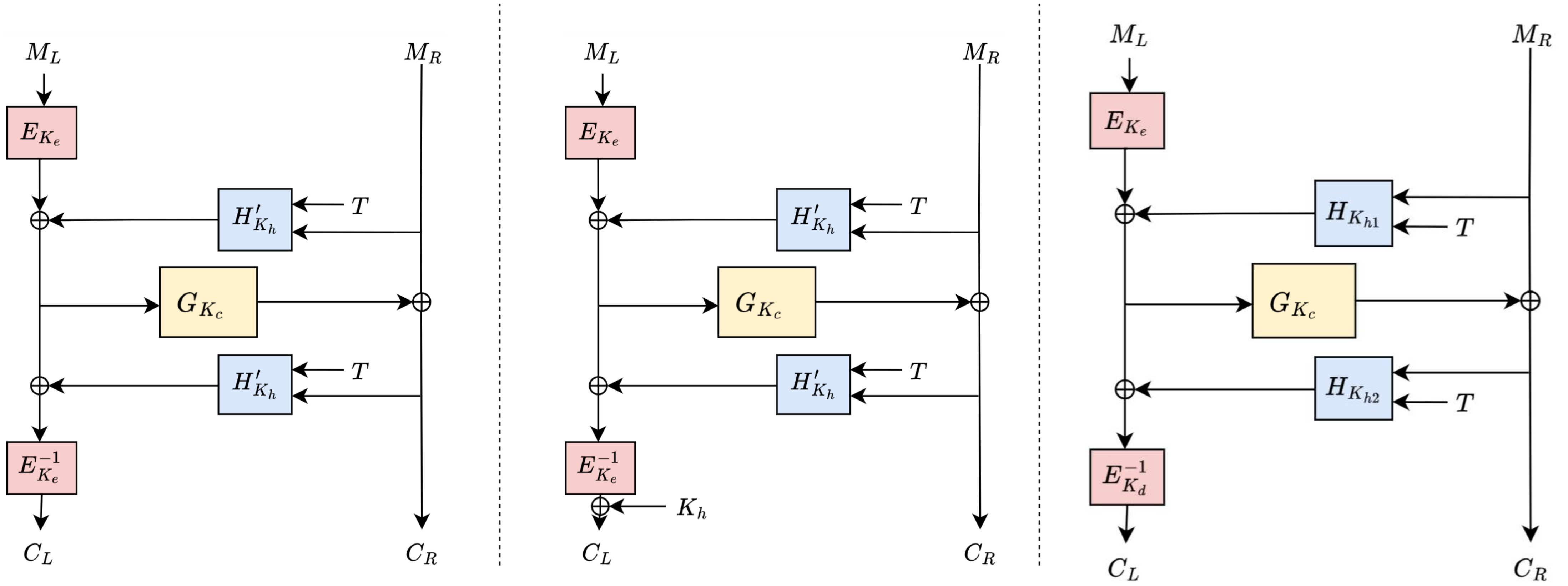
Contact:
Amitsingh.bhati@esat.kuleuven.be

“Knowledge gained without ethics is a loss, not a gain”

- Aristotle (attributed)

Backup Slides

Shared Difference Attack on Other XCB-style TEMs



HCI [Nan08]

MXCB [Nan08]

XCBv1 [MF07]

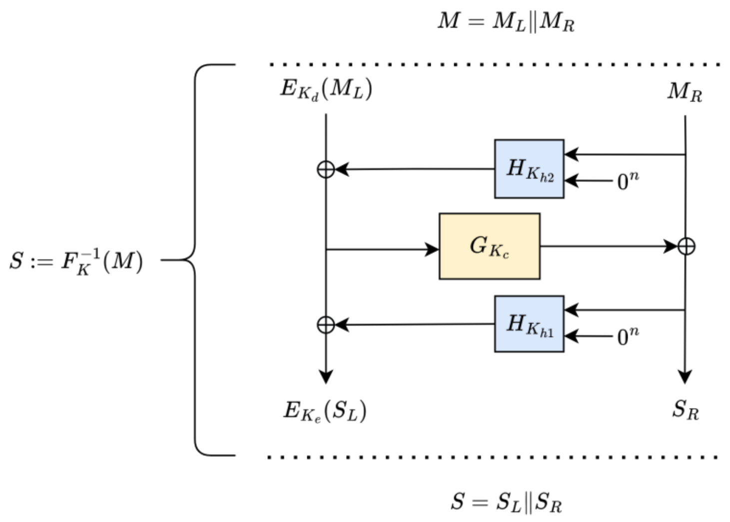
Mirrored XCB-AES,
Direct adaptation of our attack

Two-hash-key XCB-AES,
Attack applied by contradiction

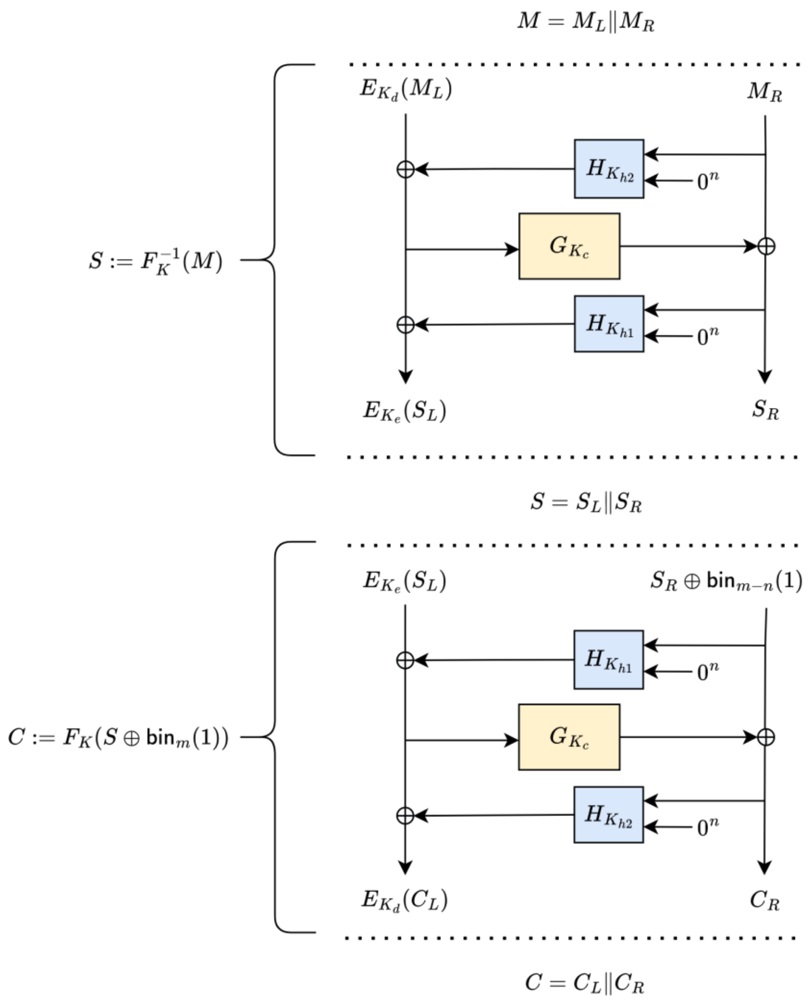
KU LEUVEN

Shared Difference Attack by Contradiction on XCBv1

Attack by Contradiction on XCBv1

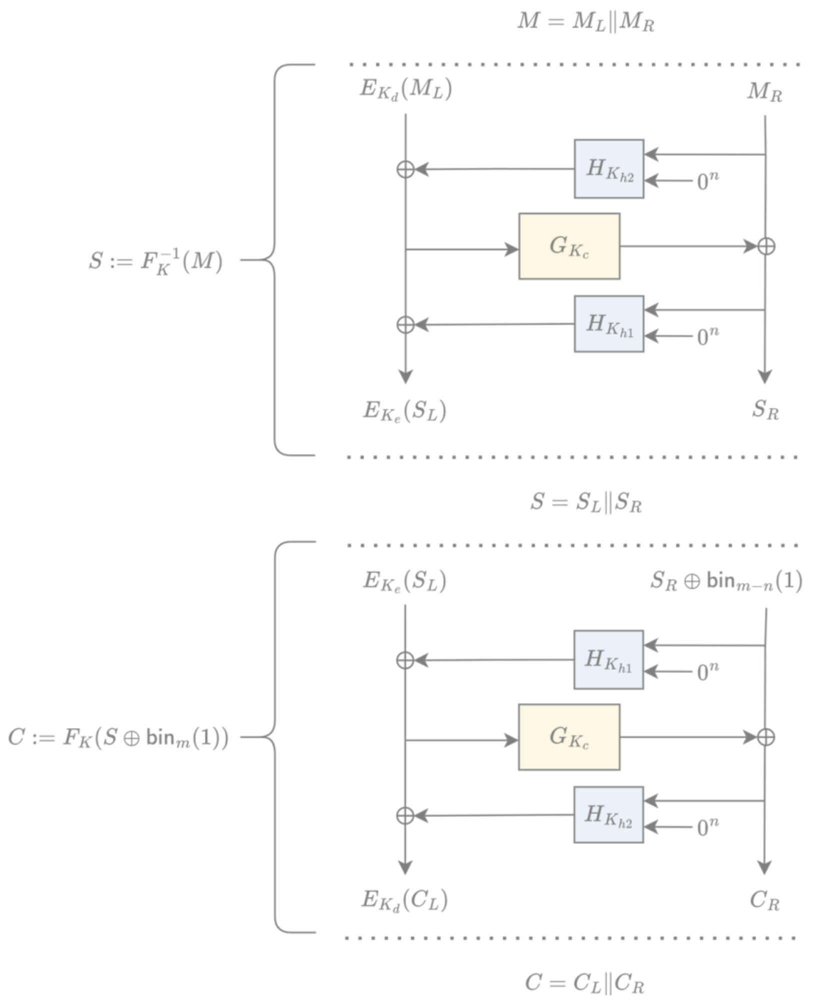


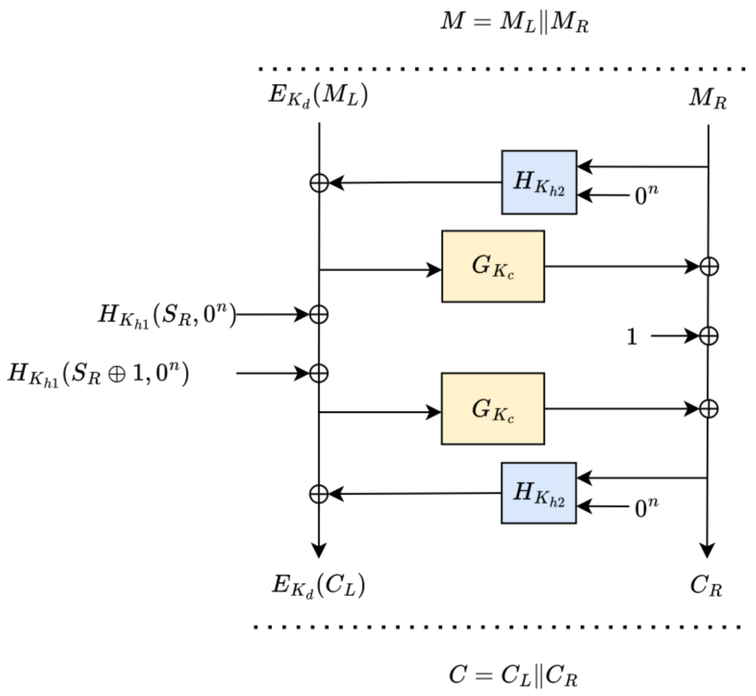
Attack by Contradiction on XCBv1



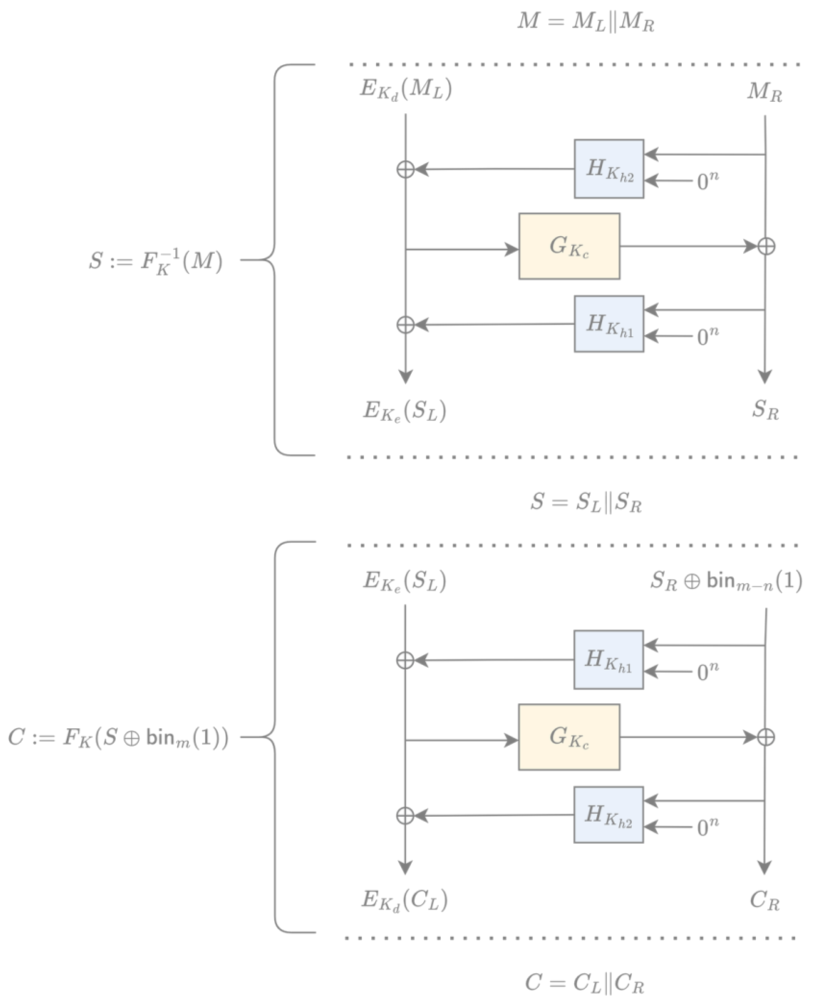
KU LEUVEN

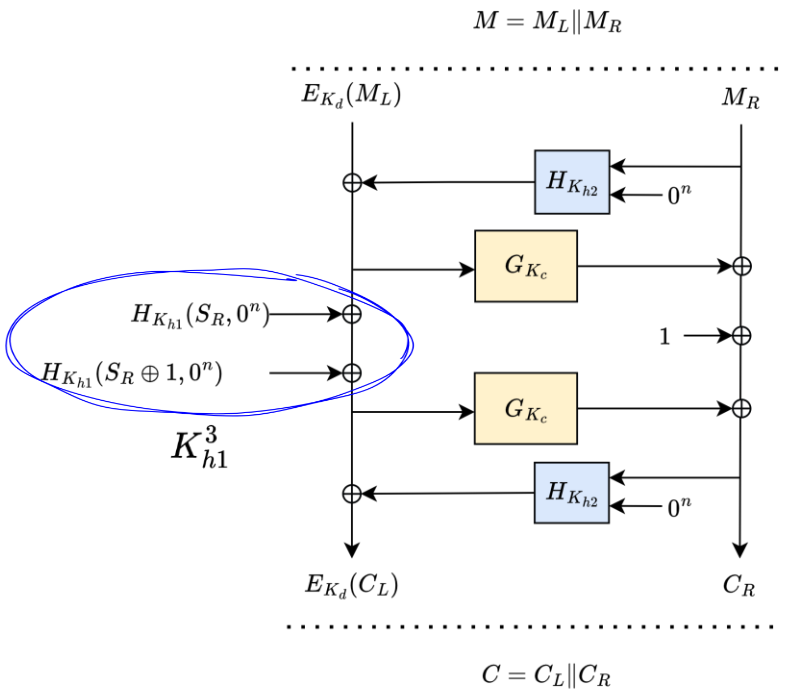
Attack by Contradiction on XCBv1



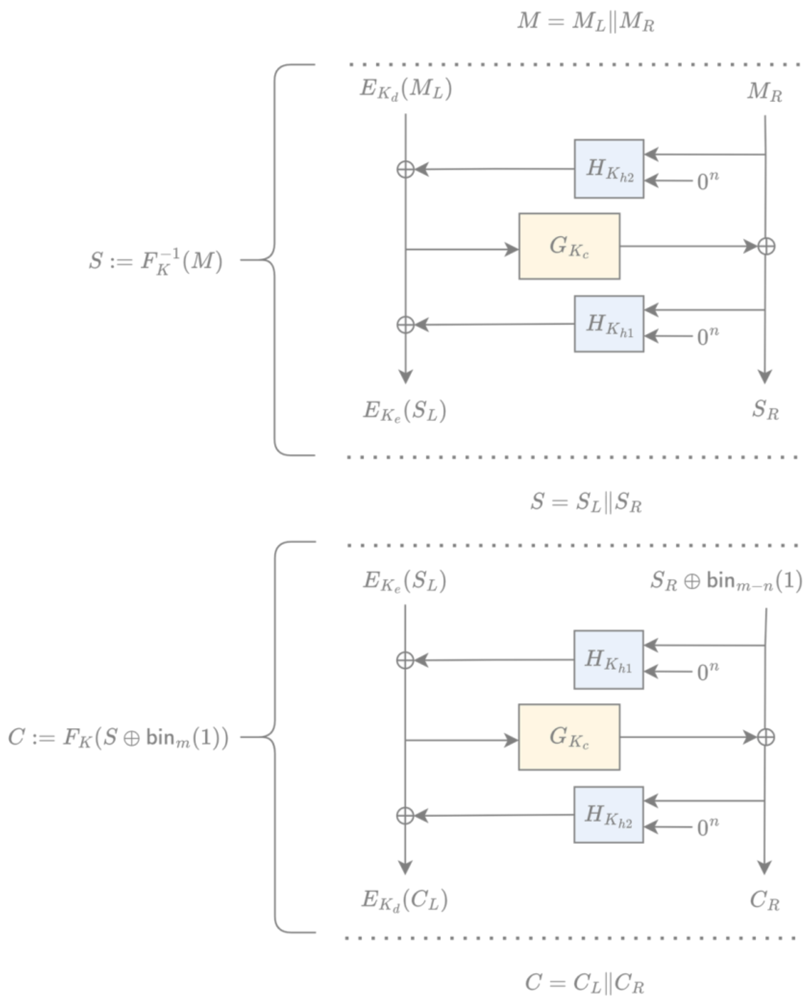


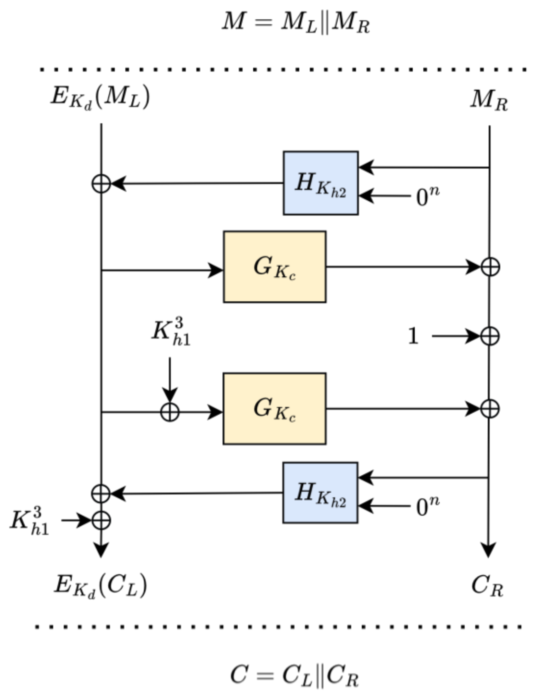
Attack by Contradiction on XCBv1





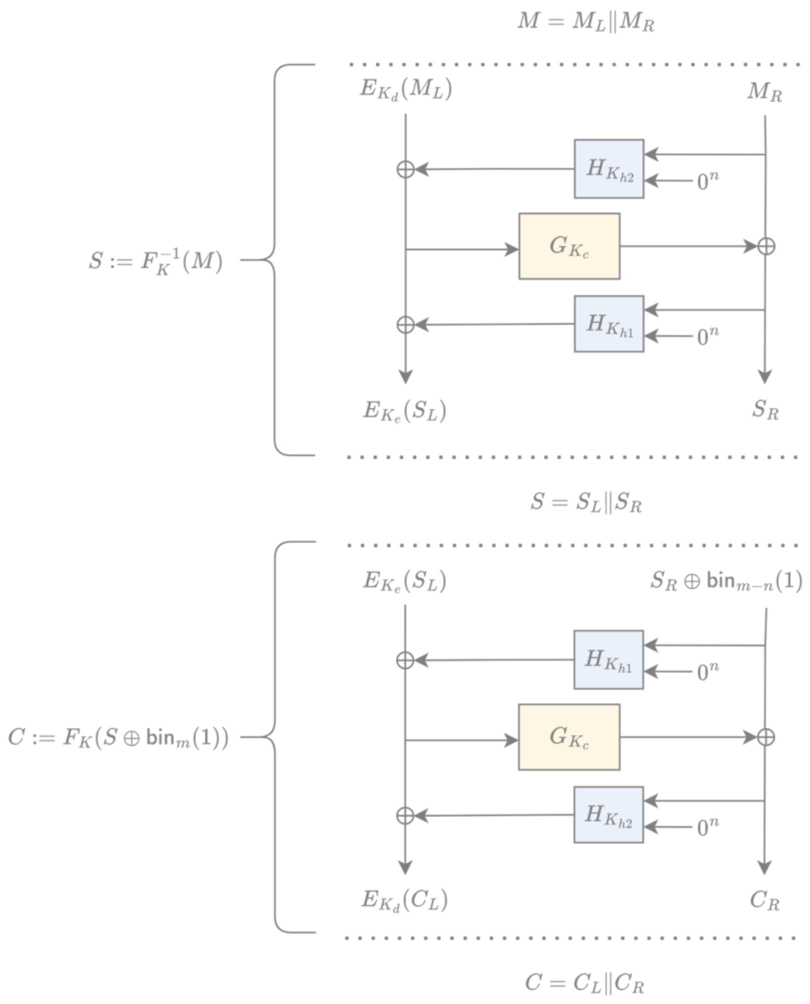
Attack by Contradiction on XCBv1

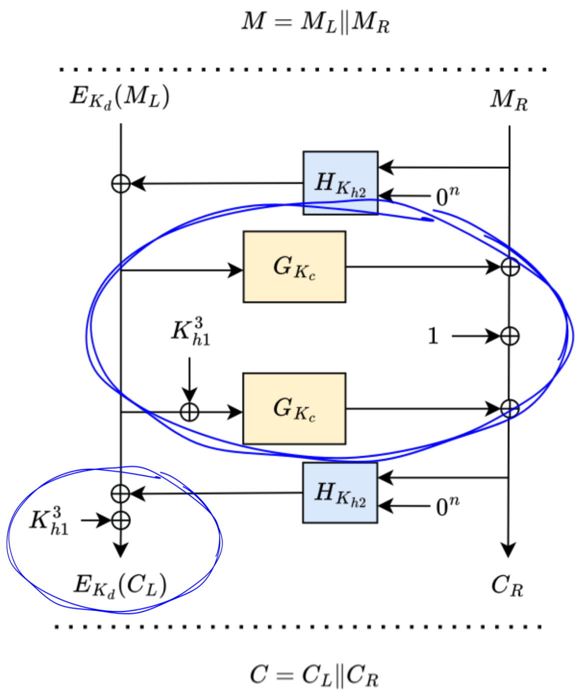




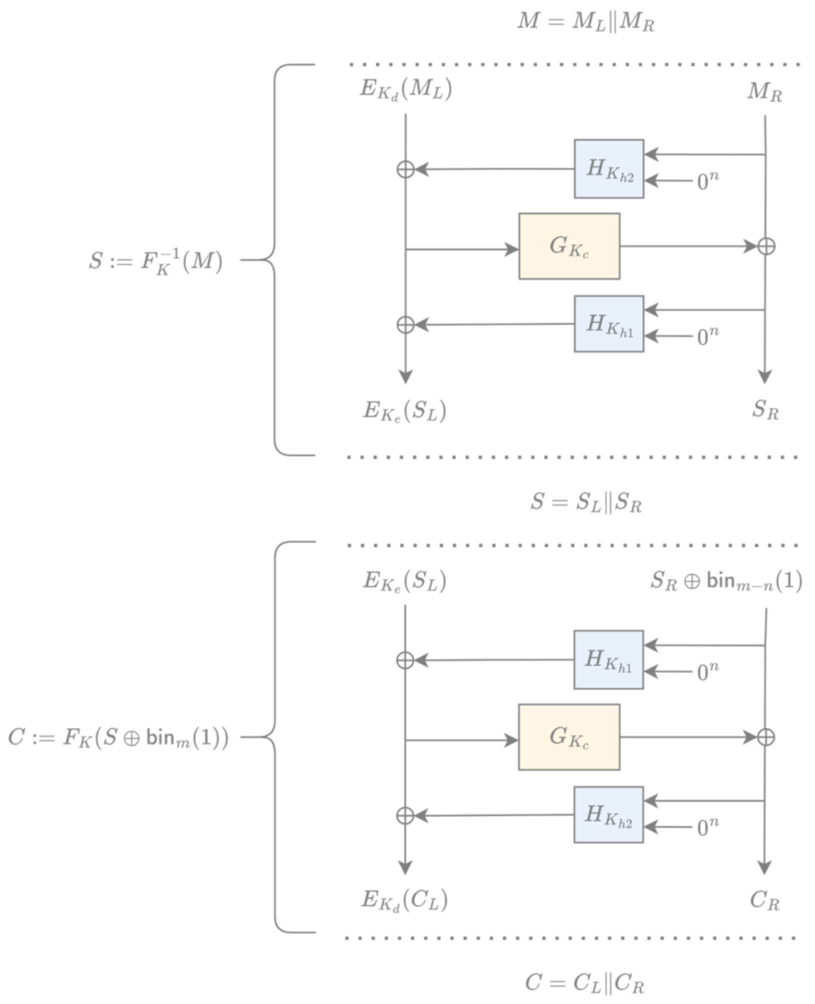
KU LEUVEN

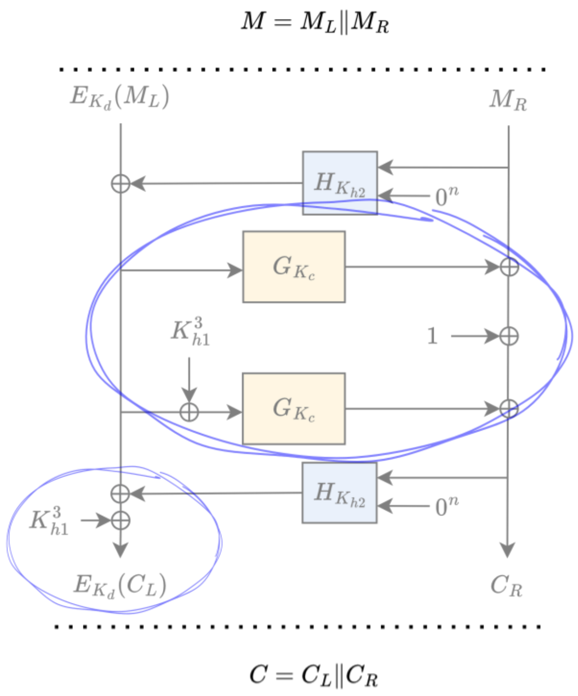
Attack by Contradiction on XCBv1

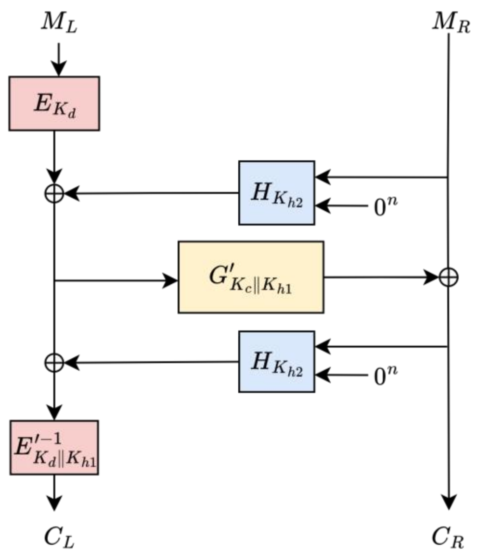




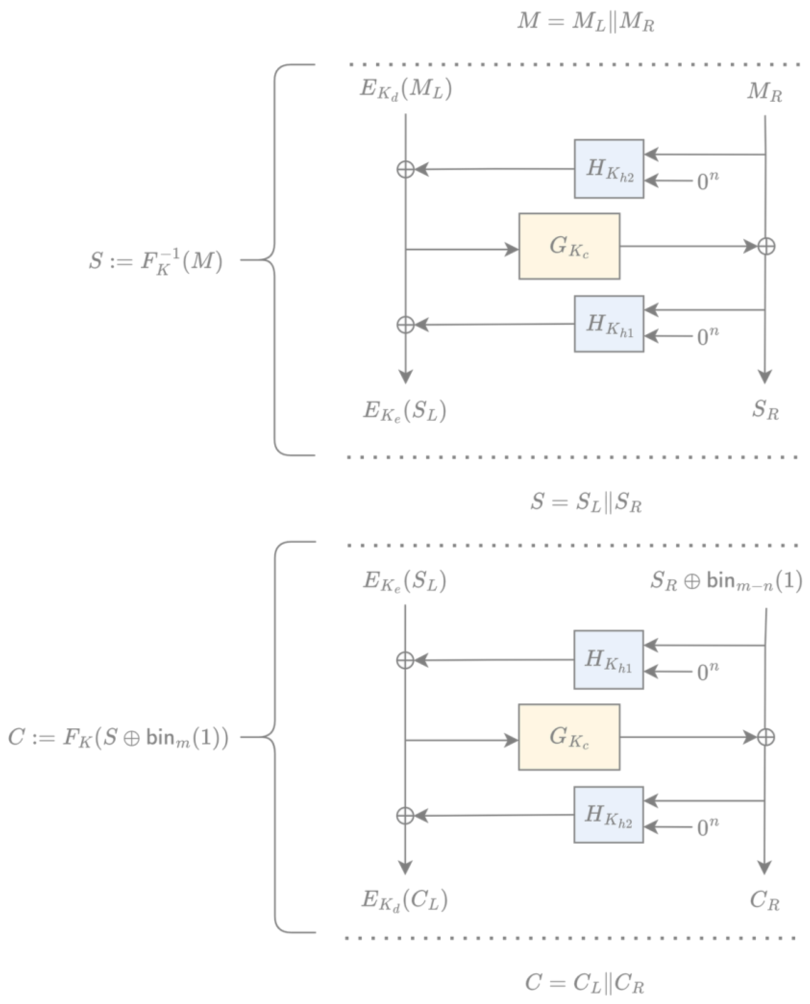
Attack by Contradiction on XCBv1

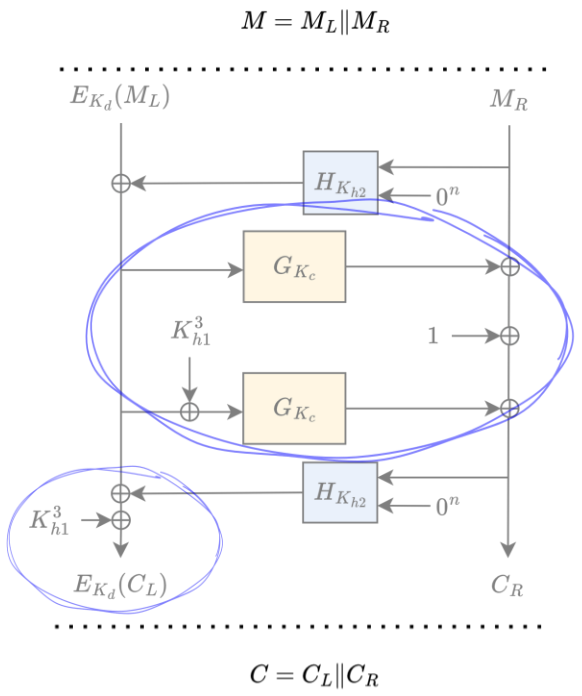


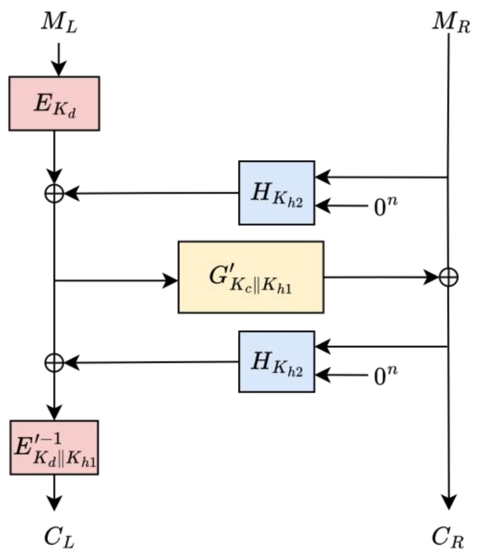




Attack by Contradiction on XCBv1



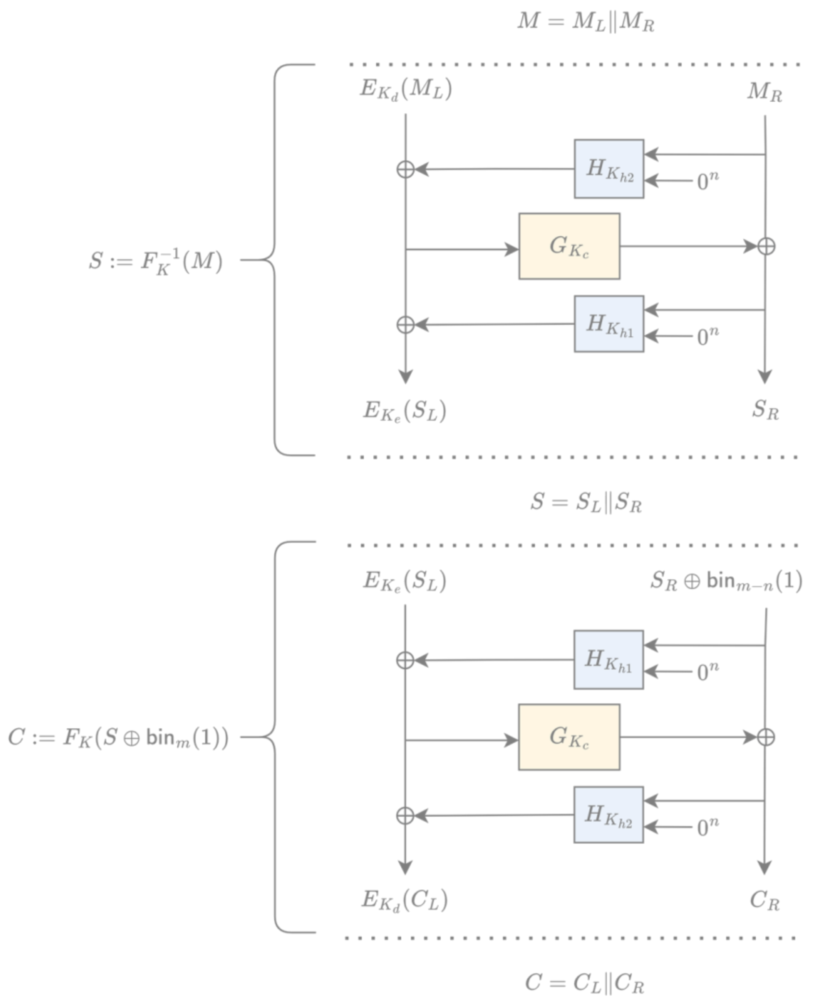


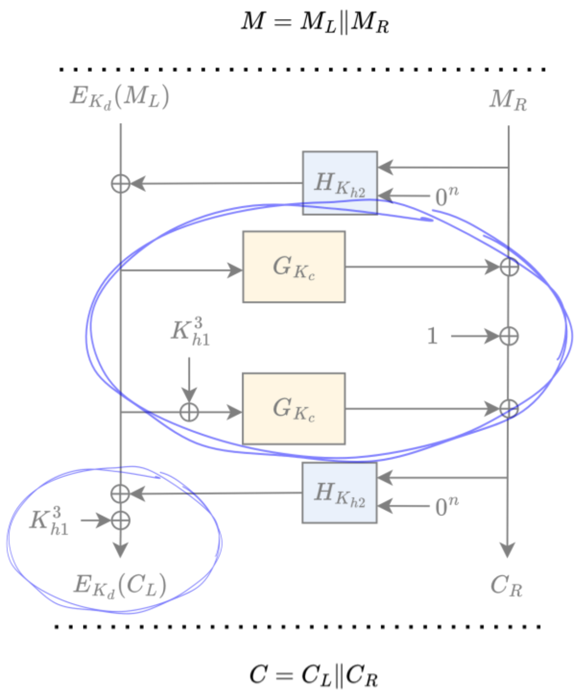


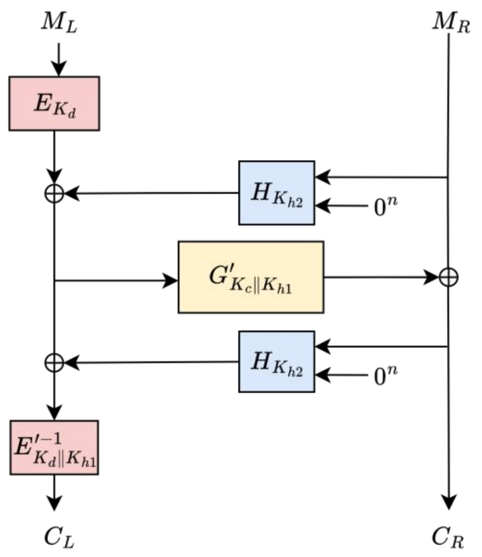
SPRP(SPRP^{-1}(M) $\oplus\gamma$) ⟶ Naor-Reingold, 2002 ⟶ PRI(M)

KU LEUVEN

Attack by Contradiction on XCBv1





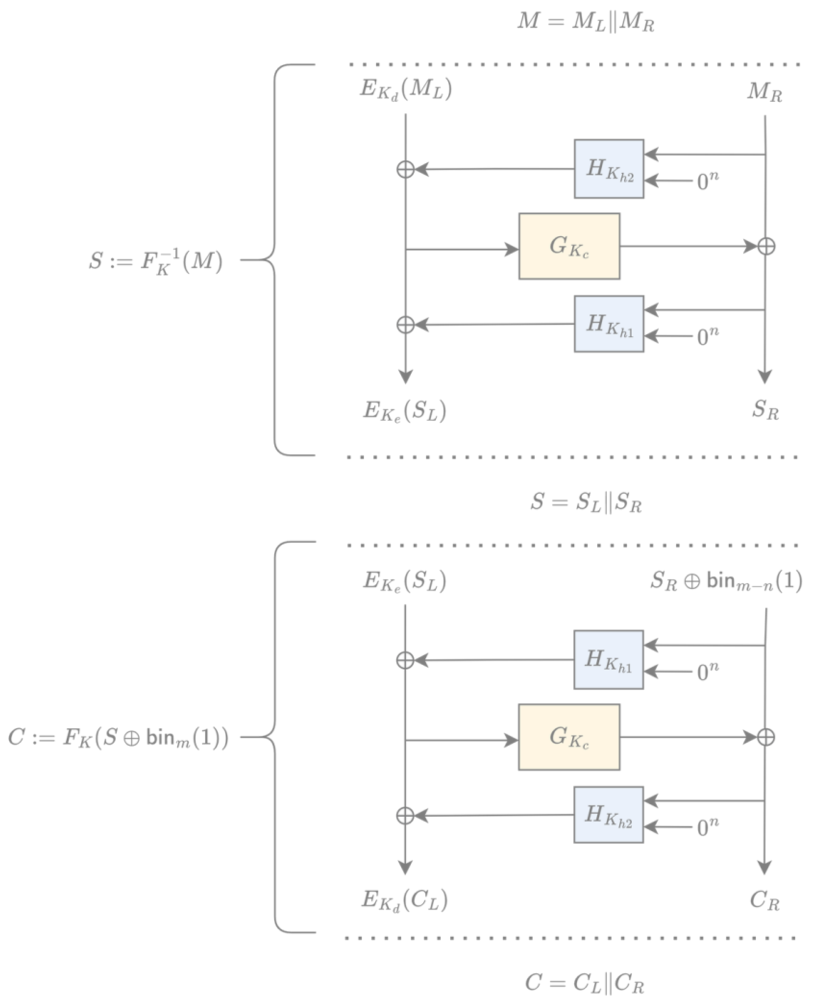


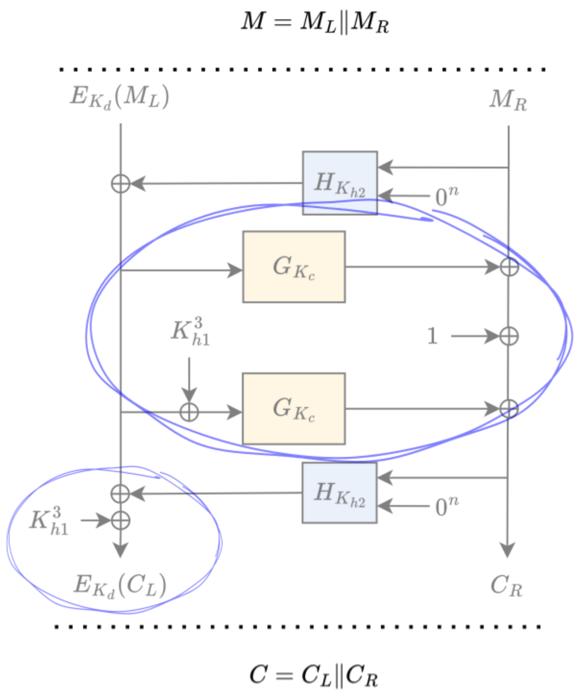
SPRP(SPRP$^{-1}(M) \oplus \gamma$) → Naor-Reingold, 2002 → ~~PRI~~(M)

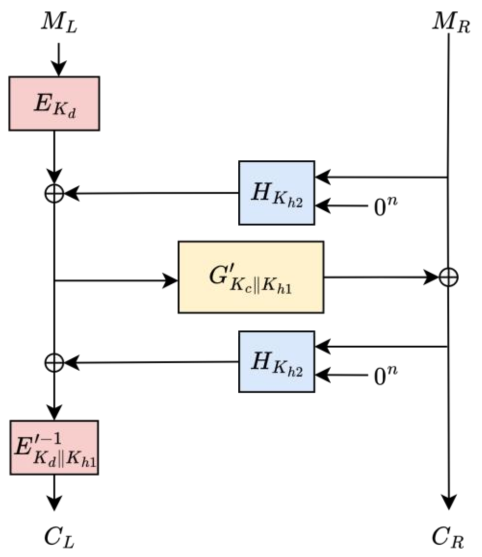
Shared Difference Attack

KU LEUVEN

Attack by Contradiction on XCBv1







~~SPRP~~(~~SPRP^{-1}~~$(M) \oplus \gamma$) —— Naor-Reingold, 2002 ——→ ~~PRI~~(M)

Shared Difference Attack

Separability contradicts XOR-Universality of Sum

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \epsilon_1$$

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

H_1 is XOR-universal

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

H_1 is XOR-universal

- For any two inputs $(T,C) \neq (T',C')$, output Y, and random secret key K,

$$\Pr(H_2(K,T,C) \oplus H_2(K,T',C') = Y) \leq \ell/2^n$$

H_2 is XOR-universal

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

H_1 is XOR-universal

- For any two inputs $(T,C) \neq (T',C')$, output Y, and random secret key K,

$$\Pr(H_2(K,T,C) \oplus H_2(K,T',C') = Y) \leq \ell/2^n$$

H_2 is XOR-universal

- For any two inputs $(T,M,C) \neq (T',M',C')$, output Y, and random secret key K,

$$\Pr(H_{\text{sum}}(K,T,M,C) \oplus H_{\text{sum}}(K,T',M',C') = 0) \leq \epsilon_{\text{sum}}$$

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

H_1 is XOR-universal

- For any two inputs $(T,C) \neq (T',C')$, output Y, and random secret key K,

$$\Pr(H_2(K,T,C) \oplus H_2(K,T',C') = Y) \leq \ell/2^n$$

H_2 is XOR-universal

- For any two inputs $(T,M,C) \neq (T',M',C')$, output Y, and random secret key K,

$$\Pr(H_{\text{sum}}(K,T,M,C) \oplus H_{\text{sum}}(K,T',M',C') = 0) \leq \epsilon_{\text{sum}}$$

$M \oplus \Delta, C \oplus \Delta$

Flaw in Existing Analysis

- For any two inputs $(T,M) \neq (T',M')$, output Y, and random secret key K,

$$\Pr(H_1(K,T,M) \oplus H_1(K,T',M') = Y) \leq \ell/2^n$$

H_1 is XOR-universal

- For any two inputs $(T,C) \neq (T',C')$, output Y, and random secret key K,

$$\Pr(H_2(K,T,C) \oplus H_2(K,T',C') = Y) \leq \ell/2^n$$

H_2 is XOR-universal

- For any two inputs $(T,M,C) \neq (T',M',C')$, output Y, and random secret key K,

$$\Pr(H_{\text{sum}}(K,T,M,C) \oplus H_{\text{sum}}(K,T',M',C') = 0) = 1$$

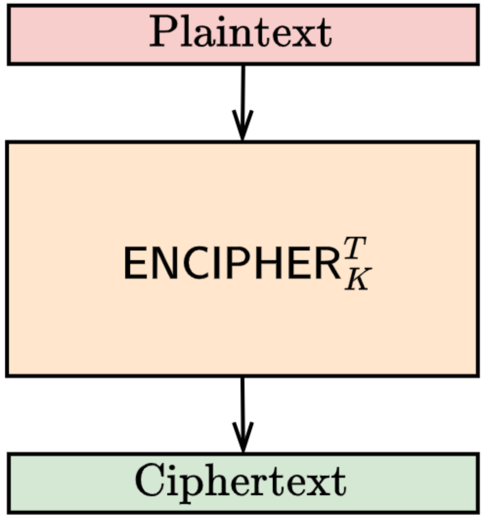
H_{sum} is not XOR-universal

$$M \oplus \Delta, C \oplus \Delta$$

KU LEUVEN

Where are TEMs Used in Real-World?

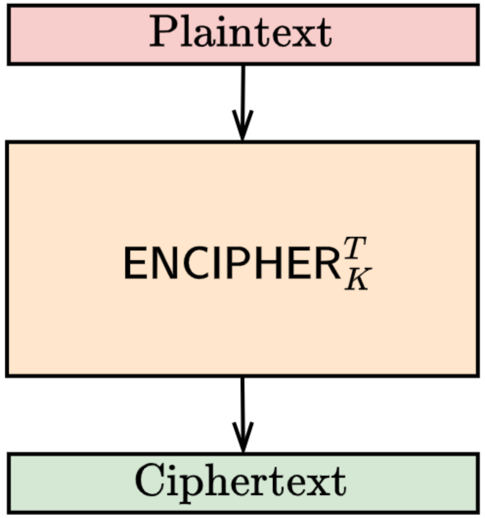
Primary Applications



1. Key-wrapping and swap-file encryption

2. Disk-sector and full-disk encryption

Primary Applications

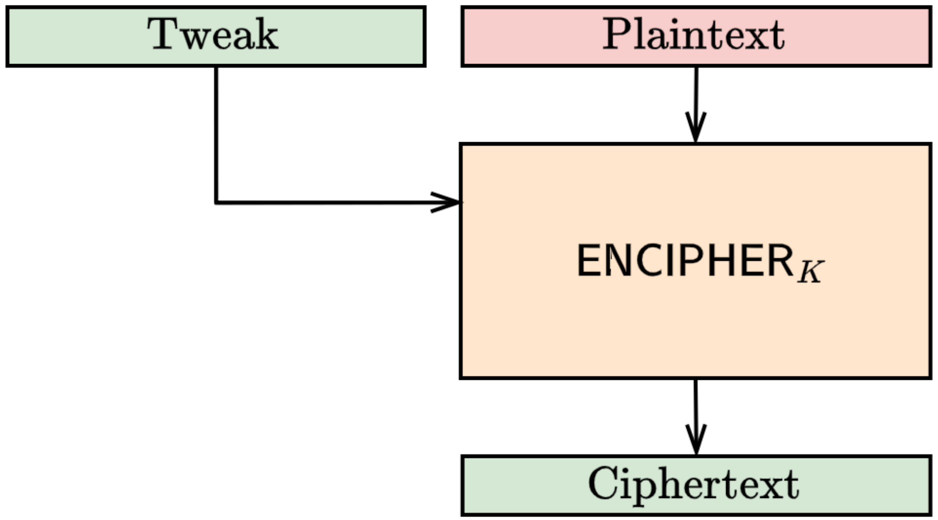


1. Key-wrapping and swap-file encryption

2. Disk-sector and full-disk encryption

VeraCrypt
Windows BitLocker
vmware vSphere
AWS KMS
Microsoft Azure Key Vault
OpenSSL Cryptography and SSL/TLS Toolkit
LUKS Linux Unified Key Setup
Encrypting Drives in Linux

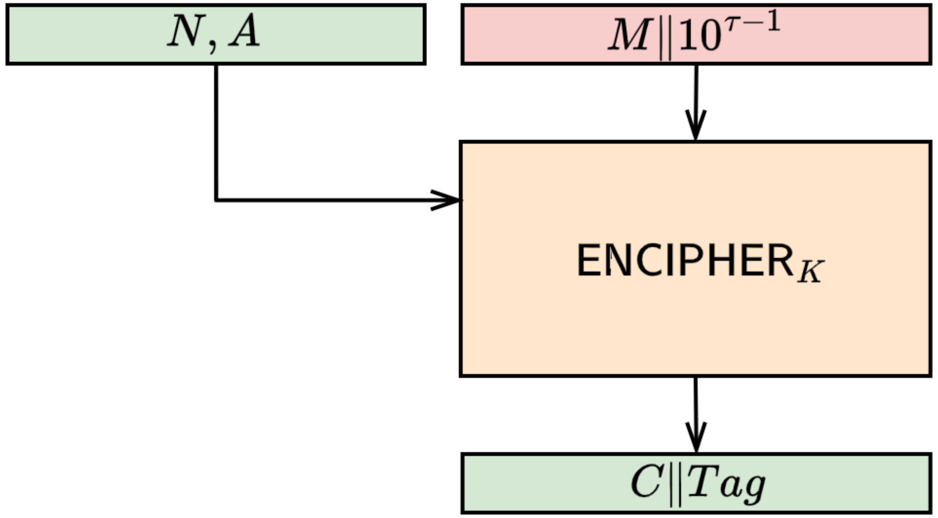
Primary Applications



1. Key-wrapping and swap-file encryption

2. Disk-sector and full-disk encryption

Primary Applications

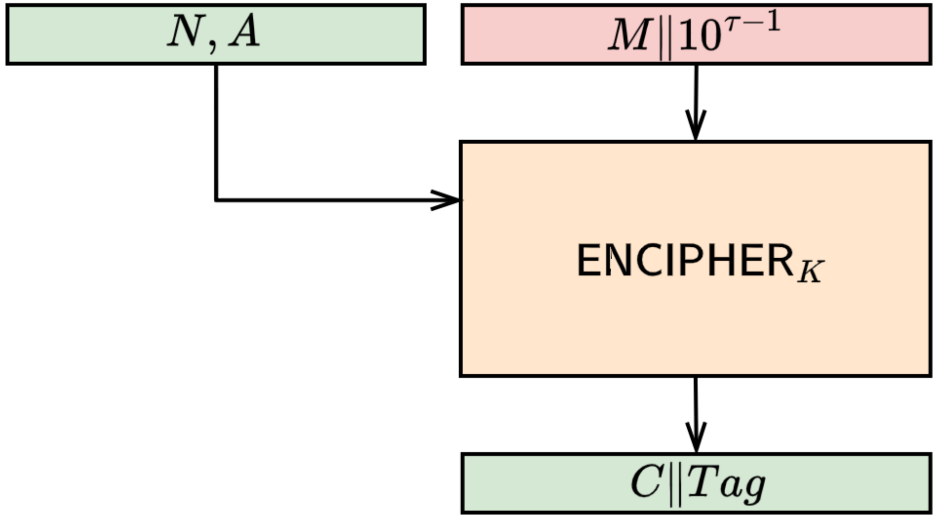


Encode-then-Encipher (EtE) [BR00]

1. Key-wrapping and swap-file encryption
2. Disk-sector and full-disk encryption
3. Robust authenticated encryption [HKR17]
    1. Resisting nonce-misuse and
    2. Decryptional leakage (RUP) [AB+14]

KU LEUVEN

Primary Applications



Encode-then-Encipher (EtE) [BR00]

1. Key-wrapping and swap-file encryption
2. Disk-sector and full-disk encryption
3. Robust authenticated encryption [HKR17]
    1. Resisting nonce-misuse and
    2. Decryptional leakage (RUP) [AB+14]

Goals also covered under NIST's accordion call

KU LEUVEN