KAIST Graduate School of Information Security

Tweakable Block Cipher Secure Beyond the Birthday Bound in the Ideal Cipher Model

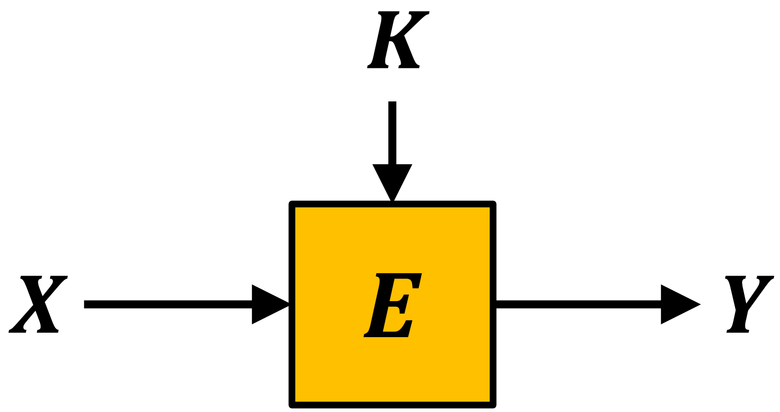
*Byeonghak Lee, Jooyoung Lee

KAIST

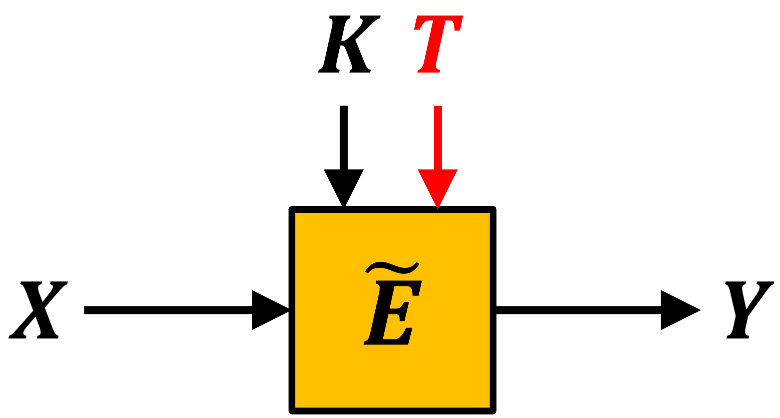
Outline

- Tweakable block ciphers
- Our contribution
- Proof overview
- Conclusion

Tweakable Block Ciphers (TBCs)



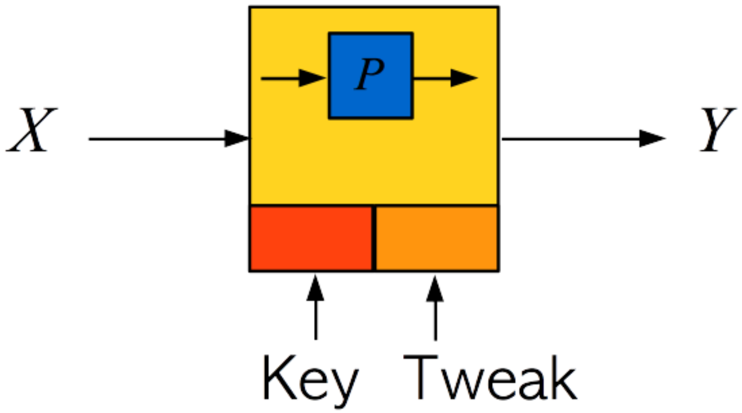
Tweakable Block Ciphers (TBCs)

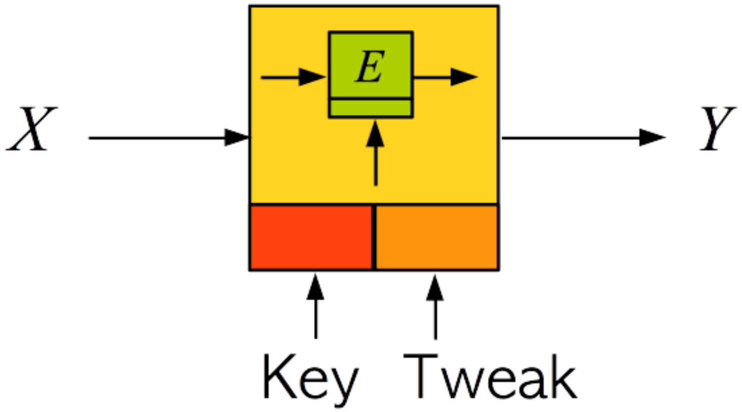


- A tweakable block cipher $\tilde{E}$ accepts an additional input "tweak"
  - Tweaks are publicly used (like IVs in modes of operation)
  - Changing tweaks should be efficient (compared to changing keys)
  - Each tweak should give an independent permutation
  - Can be used to construct various cryptographic schemes

Construction of TBCs

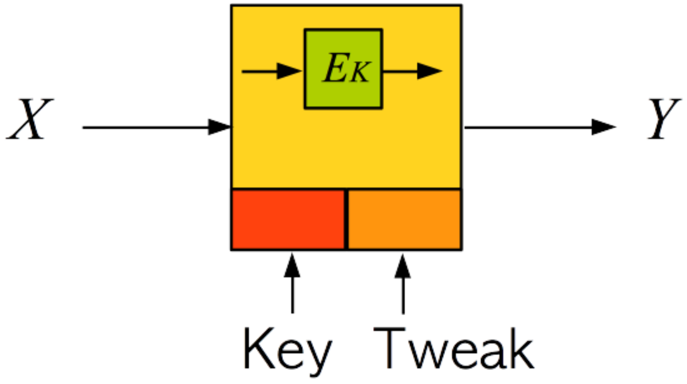
- Dedicated construction
  - Hasty Pudding, Mercy, Threefish, TWEAKEY framework, etc.
- Permutation-based construction
  - TEM, XPX, etc.
- Block cipher-based construction
  - LRW, XEX, XHX, etc.



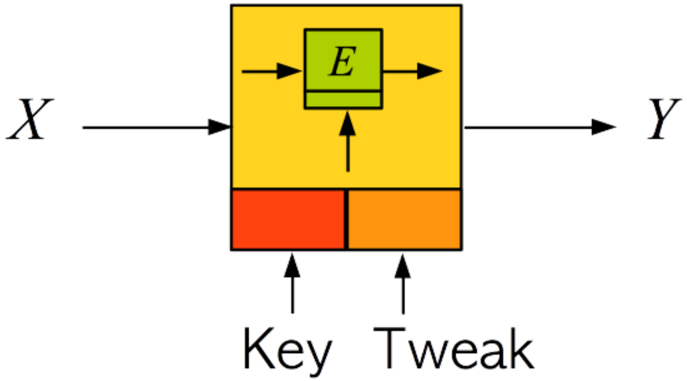


Block cipher-based Construction

- Using fixed keys (independent of tweaks)
  - Security is proved in the standard model
  - The underlying BC is replaced by an ideal random permutation (up to the security of TBC)



- Using tweak-dependent keys
  - Suitable when the underlying block cipher E uses a lightweight key schedule
  - Security is proved in the ideal cipher model
  - An adversary is allowed oracle access to E

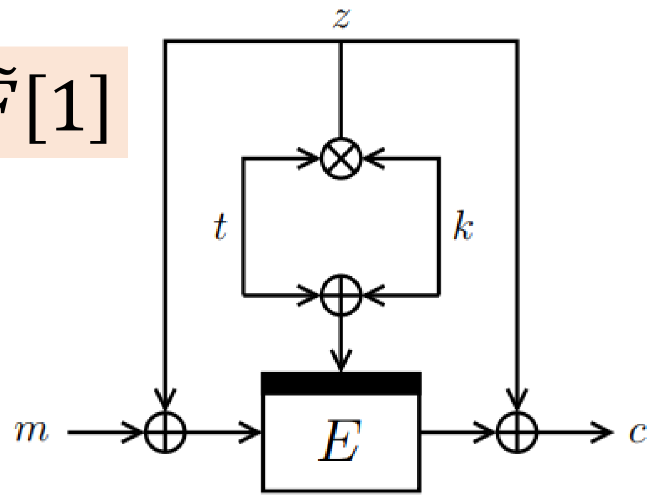


$\widetilde{F}[1]$, $\widetilde{F}[2]$ (Mennink, FSE 2015)

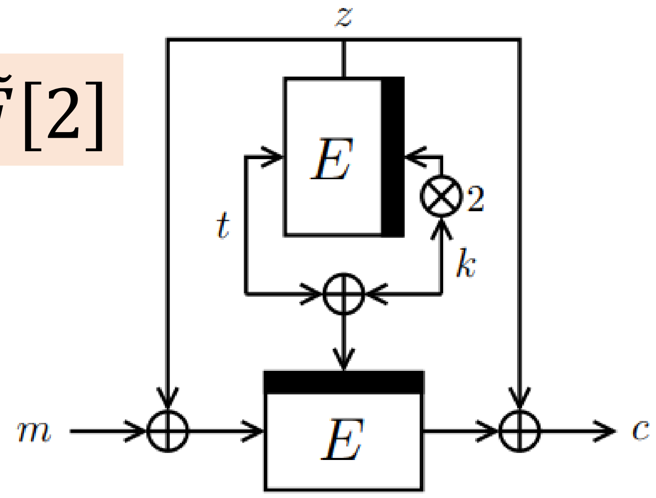
With n-bit block cipher using n-bit keys,

- $\tilde{F}[1]$ is secure up to $2^{2n/3}$ queries
  - BBB-secure with one BC call
- $\tilde{F}[2]$ is secure up to 2^{n} queries
  - Fully secure with two BC calls

$\tilde{F}[1]$



$\tilde{F}[2]$

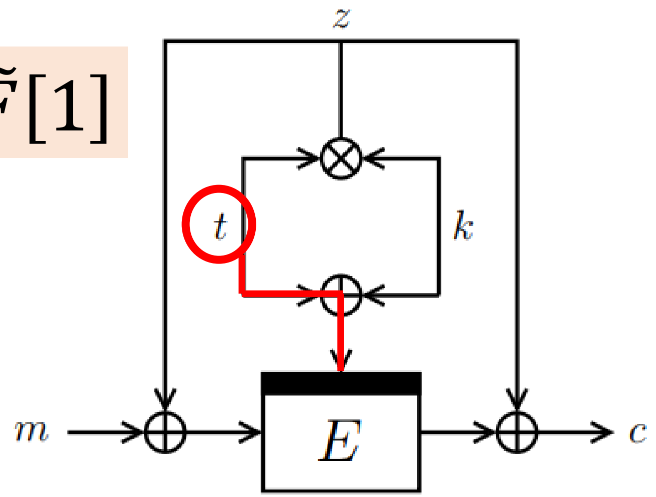


$\widetilde{F}[1]$, $\widetilde{F}[2]$ (Mennink, FSE 2015)

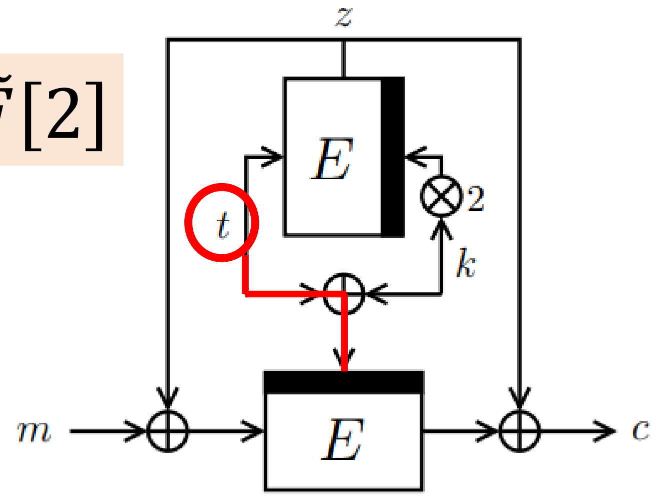
With n-bit block cipher using n-bit keys,

- $\tilde{F}[1]$ is secure up to $2^{2n/3}$ queries
  - BBB-secure with one BC call
- $\tilde{F}[2]$ is secure up to 2^{n} queries
  - Fully secure with two BC calls
- Both uses tweak dependent keys

$\tilde{F}[1]$



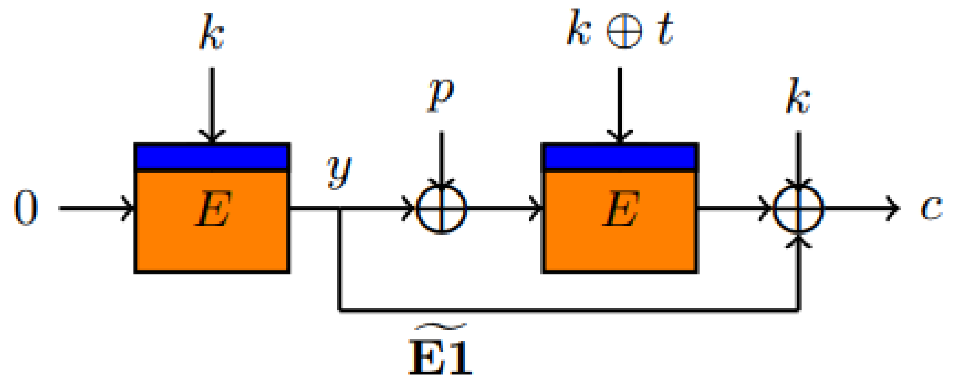
$\tilde{F}[2]$



$\widetilde{E1}, \ldots, \widetilde{E32}$ (Wang, et. al., AC 2016)

With n-bit block cipher using n-bit keys,

- only xor operation is used
- secure up to 2^n queries
  - Fully secure with two BC calls

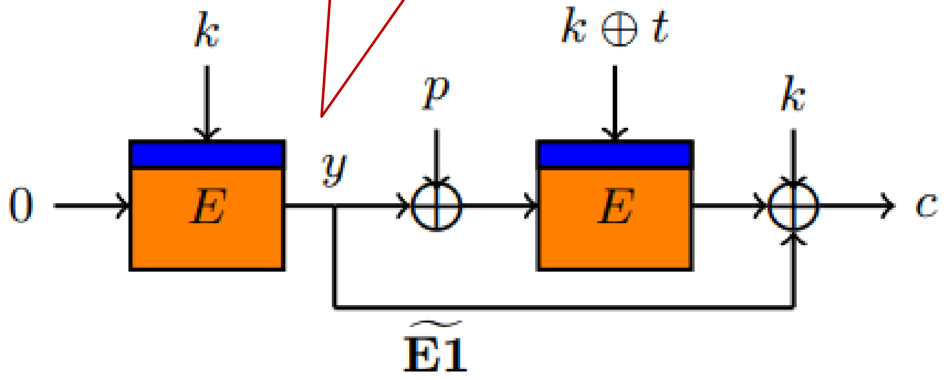


$\widetilde{E1}, \ldots, \widetilde{E32}$ (Wang, et. al., AC 2016)

With n-bit block cipher using n-bit keys,

- only xor operation is used
- secure up to 2^n queries
  - Fully secure with two BC calls
  - One call can be saved by precomputation

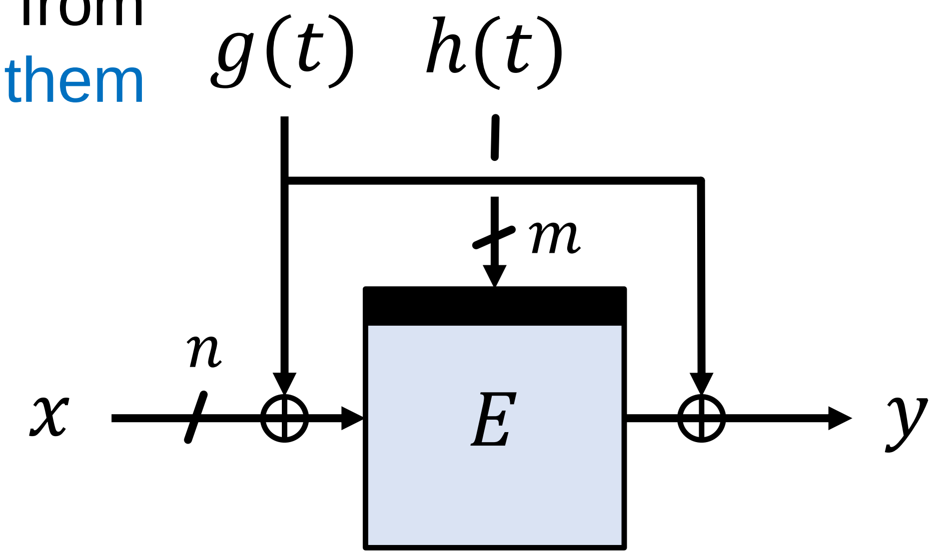
Can be precomputed
and viewed as a subkey



XHX (Jha, et. al., Latincrypt 2017)

- XHX uses two types of hash functions
  - g: δ-almost xor-universal and uniform hash function
  - h: δ'-almost universal and uniform hash function
  - Accepts arbitrary length tweak
- g and h are keyed hash function generated from the master key, but we omit the key and view them as secret key of the construction
- With n-bit block cipher using m-bit keys,

  XHX is secure up to $2^{\frac{n+m}{2}}$ queries



Outline

- Tweakable block ciphers
- Our contribution
- Proof overview
- Conclusion

Motivation

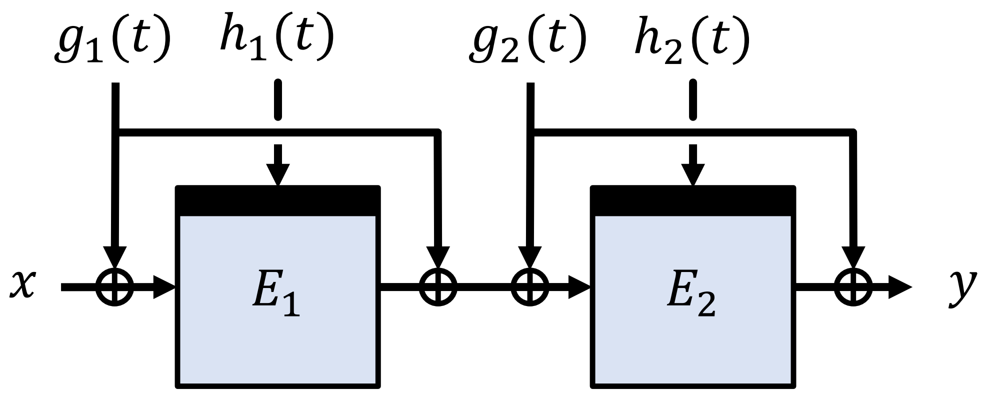
- The input size of an n-bit block cipher using m-bit key is $n + m$ bits
- In the ideal cipher model, its information-theoretic security cannot go beyond $n + m$ bits (due to key exhaustive search)
- With respect to this size, the birthday bound should be $\frac{n+m}{2}$
  - If $m = n$, it become n, so previous results are birthday bound in this view

Motivation

- The input size of an n-bit block cipher using m-bit key is $n + m$ bits
- In the ideal cipher model, its information-theoretic security cannot go beyond $n + m$ bits (due to key exhaustive search)
- With respect to this size, the birthday bound should be $\frac{n+m}{2}$
  - If $m = n$, it become n, so previous results are birthday bound in this view
- Can we go beyond the birthday bound?

XHX2

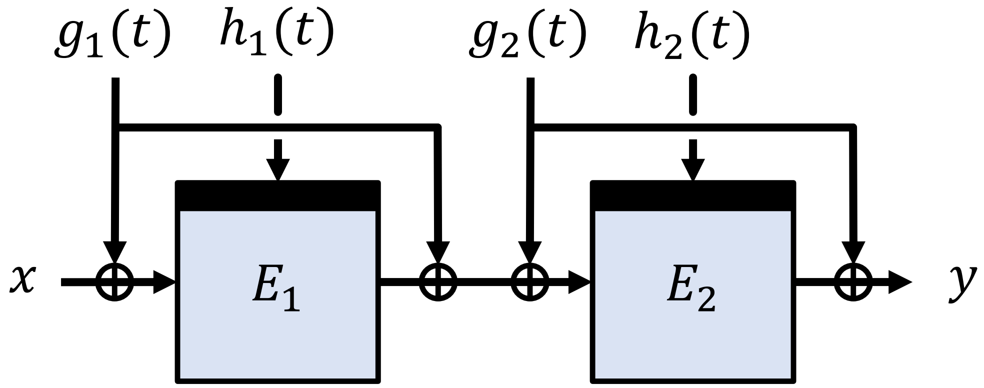
- Cascade of two independent copies of XHX
  - E_1 and E_2 are n-bit block ciphers using m-bit keys
  - g_1 and g_2 are δ-almost uniform and xor-universal functions, and
  - h_1 and h_2 are δ'-almost uniform and universal function
  - Accepts arbitrary length tweak



XHX2

- Cascade of two independent copies of XHX
  - E_1 and E_2 are n-bit block ciphers using m-bit key
  - g_1 and g_2 are δ-almost uniform and xor-universal functions, and
  - h_1 and h_2 are δ'-almost uniform and universal function
  - Accepts arbitrary length tweak

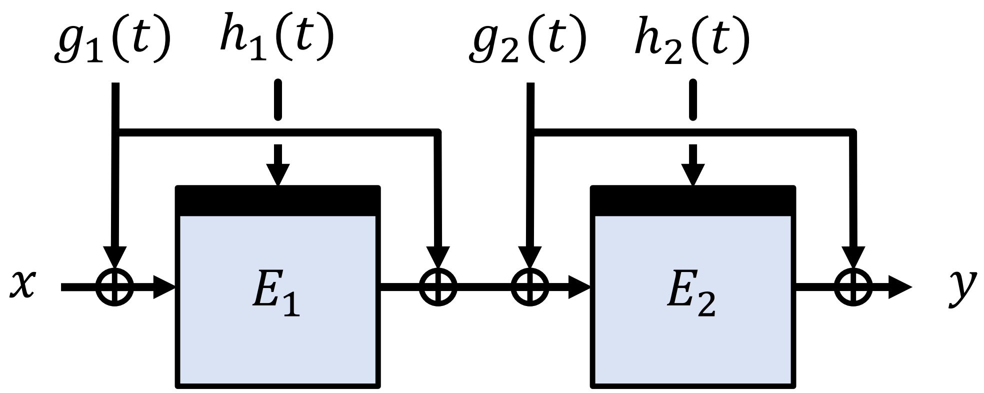
$\otimes$ (finite field mult) can be used



XHX2

- Cascade of two independent copies of XHX
  - E_1 and E_2 are n-bit block ciphers using m-bit keys
  - g_1 and g_2 are δ-almost uniform and xor-univers
  - h_1 and h_2 are δ'-almost uniform and universal function
  - Accepts arbitrary length tweak

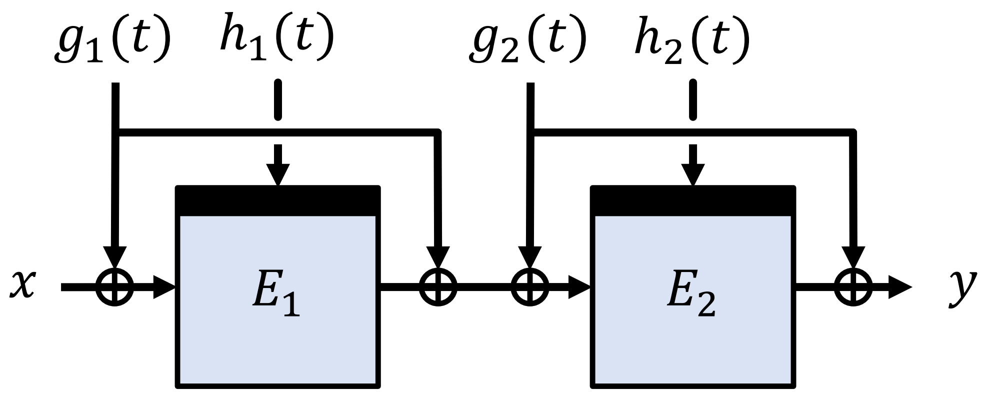
If $\|t\| = m$, $\oplus$ can be used
else, $\otimes$ can be used



XHX2

- Cascade of two independent copies of XHX
  - E_1 and E_2 are n-bit block ciphers using m-bit keys
  - g_1 and g_2 are δ-almost uniform and xor-universal functions, and
  - h_1 and h_2 are δ'-almost uniform and universal function
  - Accepts arbitrary length tweak

- Secure up to $2^{\min\left(\frac{2(n+m)}{3}, n+\frac{m}{2}\right)}$ queries
  - If $m \le 2n$, $\min\left(\frac{2(n+m)}{3}, n+\frac{m}{2}\right) = \frac{2(n+m)}{3}$



Security of XHX2

When g_1 and g_2 are n-bit δ-almost uniform and xor-universal hash functions, and h_1 and h_2 are m-bit δ'-almost uniform and universal hash functions, one has

$$\boxed{\begin{aligned}\mathbf{Adv}_{\mathsf{XHX2}}(p,q) \leq\ & 64p^{\frac{2}{3}}q^{\frac{2}{3}}\delta\delta' + \frac{256(8q^3+2pq^2)^{\frac{1}{2}}\delta^{\frac{1}{2}}\delta'}{N^{\frac{1}{2}}} + \frac{160(16q^3+8pq^2+p^2q)^{\frac{1}{2}}\delta'}{N} \\ & + 256(16q^3+8pq^2+2q^2+3p^2q)\delta^2(\delta')^2 + \frac{131072n^2q^2\delta'}{N^2}\end{aligned}}$$

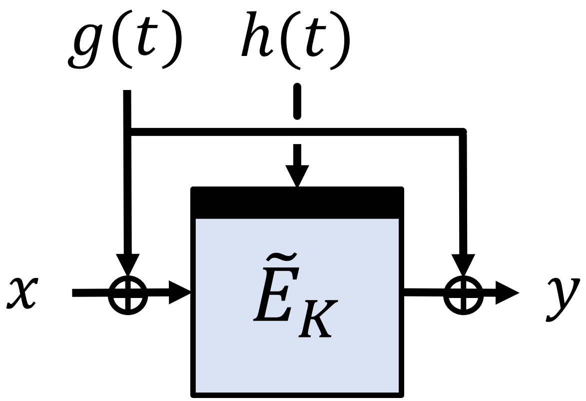
where $\delta \approx \frac{1}{2^n}$, $\delta' \approx \frac{1}{2^m}$, p and q are the number of queries to underlying block ciphers and construction

Comparison

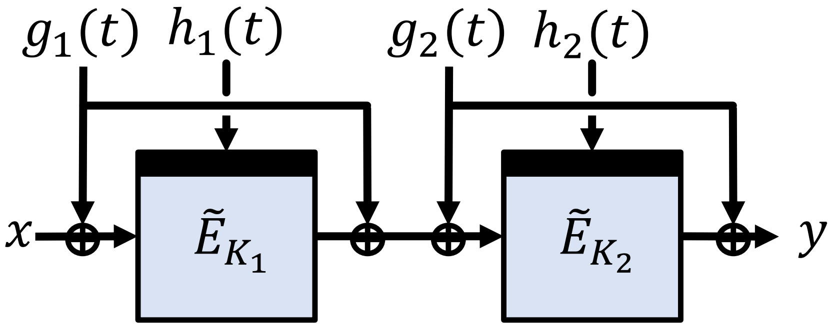
Construction	Key size	Security	Efficiency		Ref.
			E	$\otimes$/H	
LRW	$2n$	$n/2$	1	1	[LRW02]
LRW[2]	$4n$	$2n/3$, (or $3n/4$)	2	2	[LST12, Men18]
LRW[s]	$2sn$	$sn/(s+2)$	s	s	[LS13]
$\tilde{F}[1]$	n	$2n/3$	1	1	[Men15]
$\tilde{F}[2]$	n	n	2	0	[Men15]
$\widetilde{E1}, \cdots, \widetilde{E32}$	n	n	2	0	[Lei+16]
XHX	$n+m$	$(n+m)/2$	1	1	[Jha+ 17]
XHX2	$2n+2m$	$min(2(n+m)/3,\ n+m/2)$	2	2	Our work

Security of the 2-round XTX

- XTX is a tweak-length extension scheme (Minematsu and Iwata, IMACC 2015)



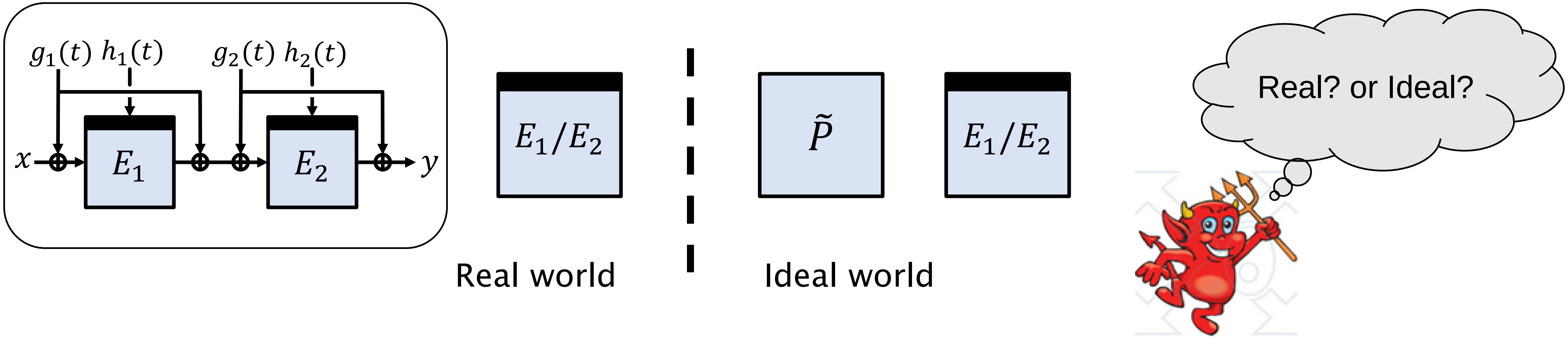
- Without allowing block cipher queries ($p = 0$), we can prove beyond-birthday-bound security for the cascade of two independent XTX constructions.



Outline

- Tweakable block ciphers
- Our contribution
- Proof overview
- Conclusion

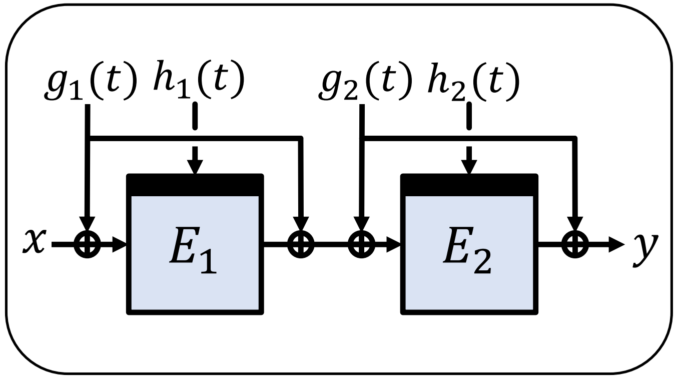
Distinguishing game

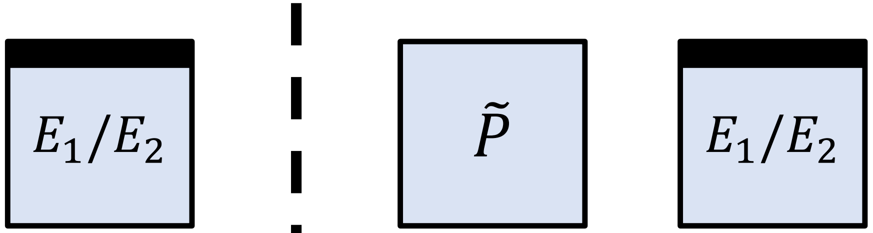


- Adversary tries to distinguish two worlds by making oracle queries
- All the information obtained during the attack is represented by a transcript:

$$\tau = \left(Q_C = \{(t_1, x_1, y_1), \cdots, (t_q, x_q, y_q)\}, Q_{E_j} = \{(j, k_1, u_1, v_1), \cdots, (j, k_p, u_p, v_p)\}\right)$$

Distinguishing game





Real world

Ideal world

Assume to be revealed
after the attack is finished

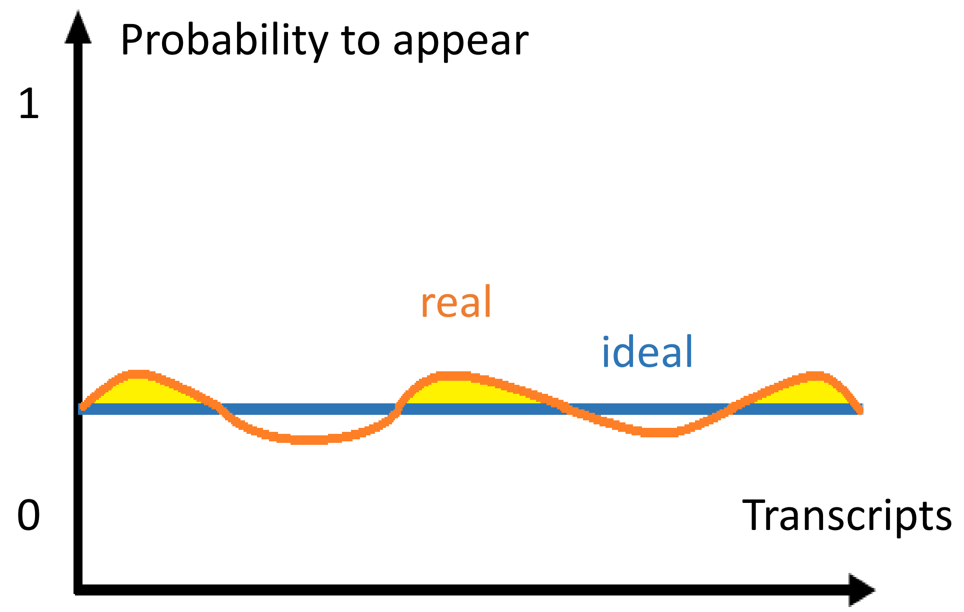
- Adversary tries to distinguish t
- All the information obtained during th ... ript:

$$\tau = \Big(Q_C = \{(t_1, x_1, y_1), \cdots, (t_q, x_q, y_q)\}, Q_{E_j} = \{(j, k_1, u_1, v_1), \cdots, (j, k_p, u_p, v_p)\}, g_1, g_2, h_1, h_2\Big)$$

Upper Bounding the Distinguishing Advantage

- $\mathrm{T_{id}}$: Probability distribution of τ in the ideal world
- $\mathrm{T_{re}}$: Probability distribution of τ in the real world

$$\mathbf{Adv}_{\tilde{E}}(\mathcal{D}) \leq \|\mathrm{T_{id}} - \mathrm{T_{re}}\|$$



Proof technique

We can use following lemma to upper bound the statistical distance

Patarin's H-coefficient lemma (informal)

1) Define bad transcripts Θ_{bad}
   - $\Pr[\mathrm{T_{id}} \in \Theta_{\mathrm{bad}}] \leq \epsilon_1$
2) With $\tau \notin \Theta_{\mathrm{bad}}$
   - $\frac{\Pr[\mathrm{T_{re}}=\tau]}{\Pr[\mathrm{T_{id}}=\tau]} \geq 1 - \epsilon_2$

$\Rightarrow$ $\parallel \mathrm{T_{id}} - \mathrm{T_{re}} \parallel \leq \epsilon_1 + \epsilon_2$

Security Proof of XHX2 (Sketch)

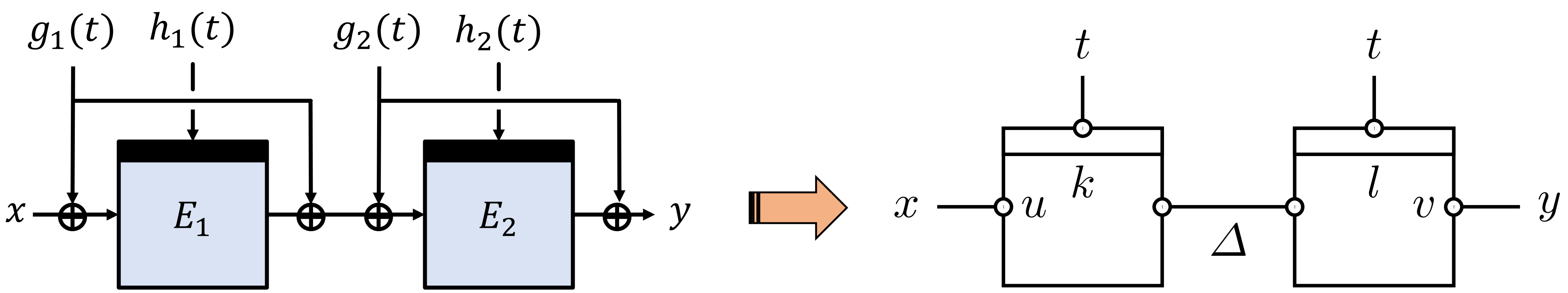
1) Give free queries to the adversary

2) Define bad transcripts

3) Lower bound the ratio of probabilities of obtaining a good transcript in the real world and in the ideal world
   - $\Pr[T_{id} = \tau]$ is easy to compute, while $\Pr[T_{re} = \tau]$ is challenging

4) Apply the H-coefficient lemma

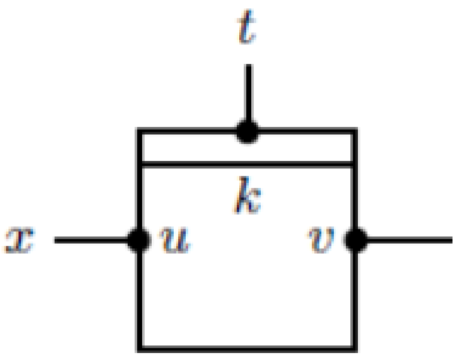
Representation of Construction Queries



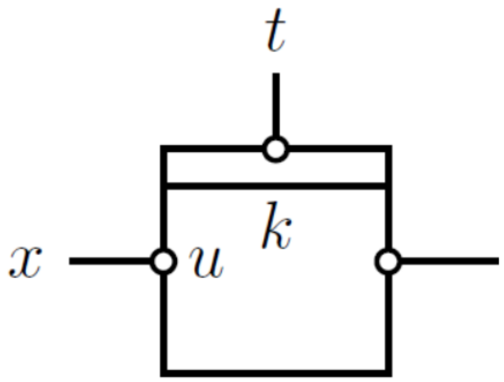
- Reduced query: combine keys and construction queries

$$(t, x, y) \mapsto \big(h_1(t), h_2(t), x \oplus g_1(t), y \oplus g_2(t), g_1(t) \oplus g_2(t)\big)$$
$$= (k, l, u, v, \Delta)$$

Representation of Construction Queries



$(k, u, v) \in Q_{E_i}$



$(k, u, *) \notin Q_{E_i}$

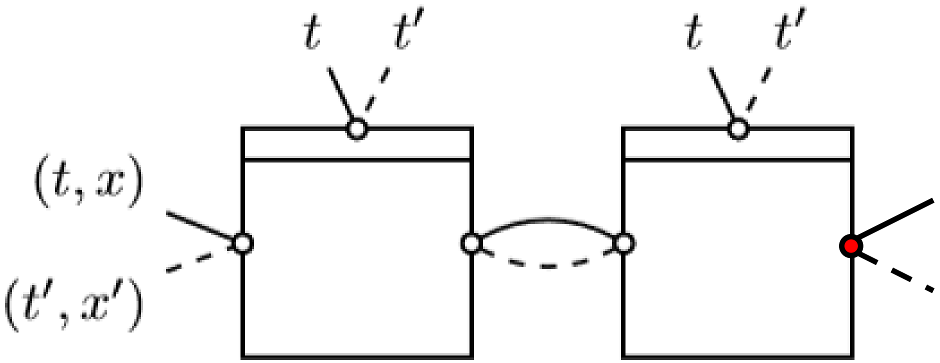
- Black dots represent values fixed by block cipher queries, while white dots are “free”

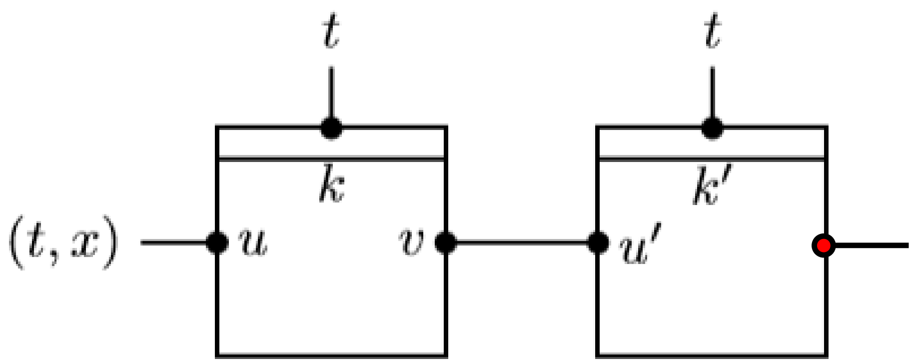
Free additional queries

- To avoid the extreme cases;
  - if there exists $2^n/4$ or more queries to E_i with same key, give full evaluation of the block cipher with that key
  - if there exists $2^n/16$ or more queries to the construction with same tweak, give full evaluation of the construction with that tweak
- This increases the advantage by a constant factor, but it helps the computation of probability

Bad Transcripts (1/2)

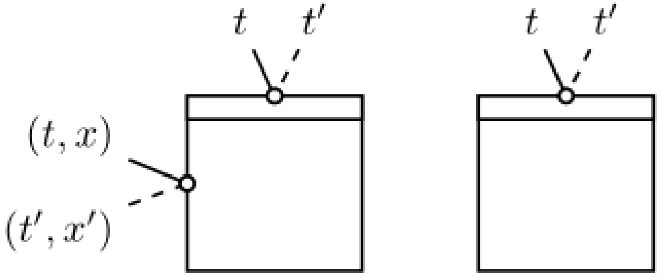
- Avoid revealing any colliding internal path
  - If two query collides in all internal path, (white or black dots) it will fix the choice of remaining values (red dots)





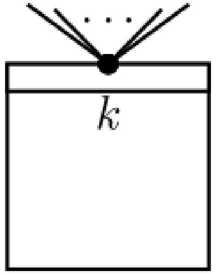
Bad Transcripts (2/2)

- Avoid large number of collisions
  - Upper bound the number of colliding pairs



$$\leq \frac{q^2}{2^{n+2m}}$$

  - Avoid a multi-collision with a large multiplicity

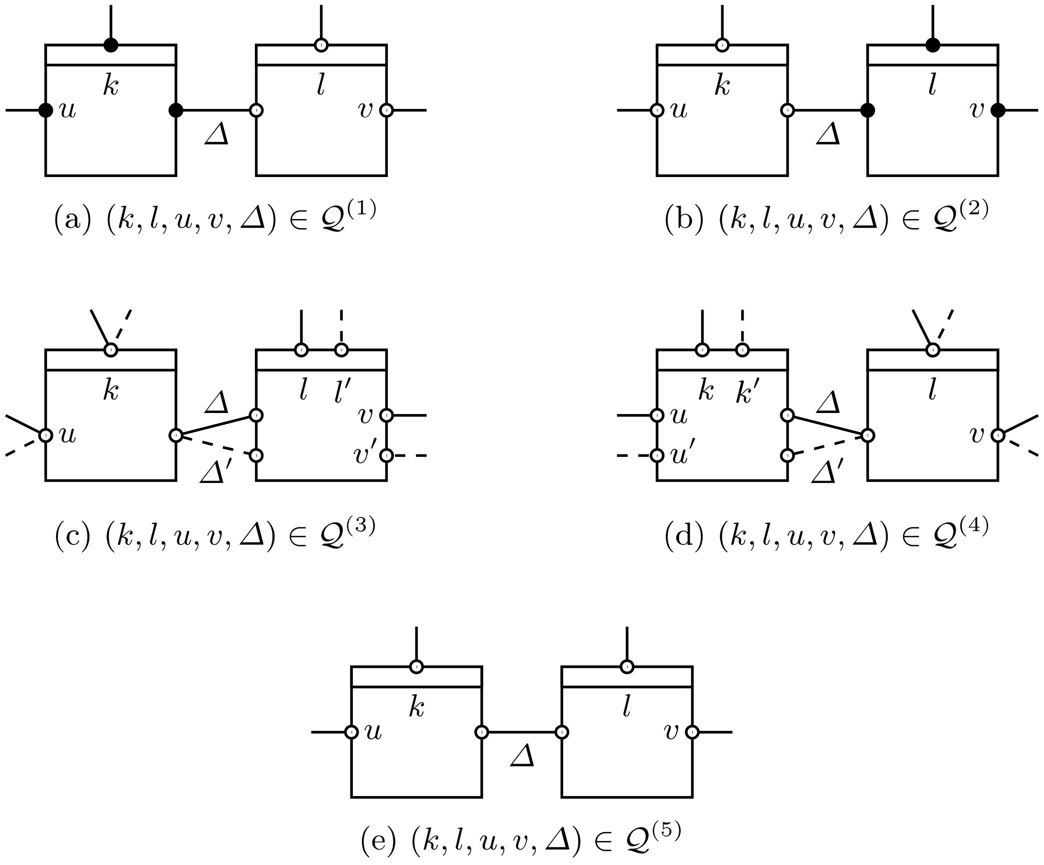


$$\leq 2^n/4$$

  - Otherwise, too large proportion of E_1 and E_2 become incompatible

Analyzing Good Transcripts

- Classify good queries into 5 classes
- Estimate the probability of completing the queries in each class
- In this way, we can lower bound $\Pr[\mathrm{T}_{\mathrm{re}} = \tau]$



(a) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$ (b) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(2)}$

(c) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(3)}$ (d) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(4)}$

(e) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(5)}$

Conclusion

- XHX2 is a TBC that is based on an n-bit block cipher using m-bit key providing $\min\left(\frac{2(n+m)}{3}, n+\frac{m}{2}\right)$-bit security in the ideal cipher model

As open problems;

- Can we improve our security bound using an alternative approach (e.g., the expectation method)?
- What is the security of the 3-round XHX?
- Is our bound tight? (Generic attacks matching the provable security?)

Thank You

Q&A