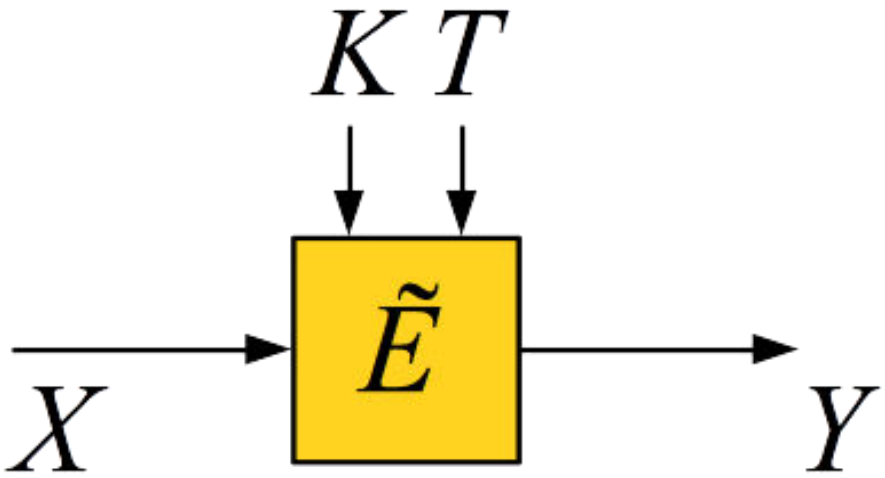
Tweakable Block Cipher Secure Beyond the Birthday Bound in the Ideal Cipher Model

Jooyoung Lee, Byeonghak Lee

KAIST

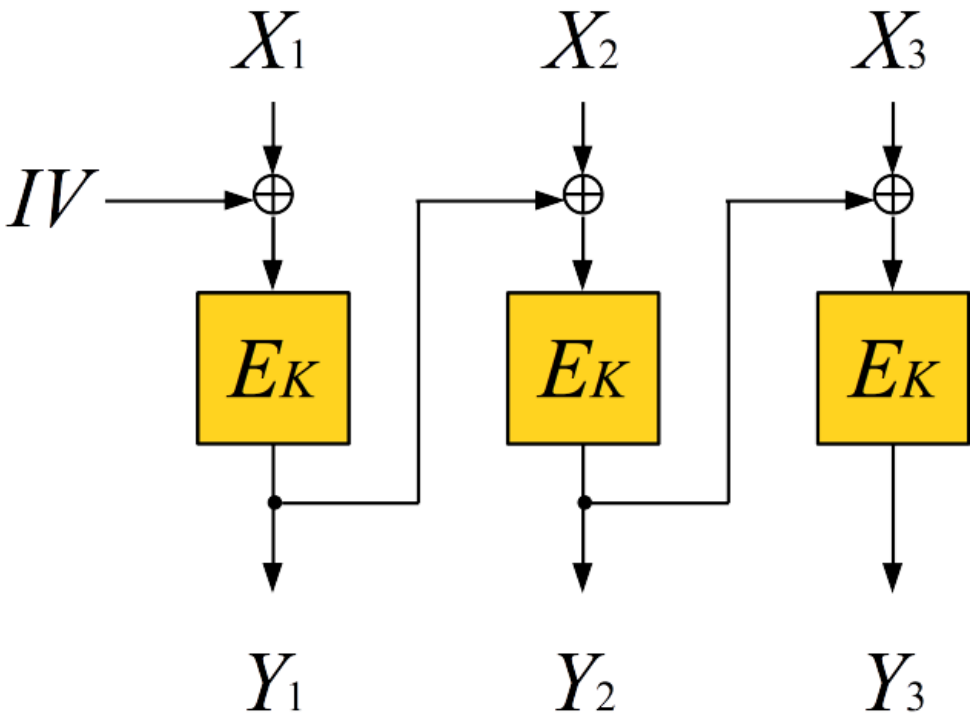
Tweakable Block Cipher



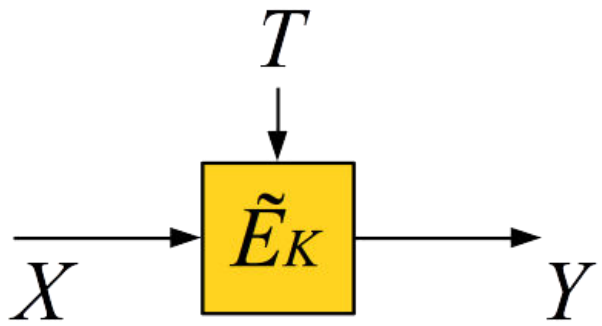
- A tweakable block cipher $\tilde{E}$ accepts an additional input "tweak"
  - Tweaks are publicly used (like IVs and nonces in modes of operation)
  - Changing tweaks should be efficient (compared to changing keys)

Motivation: why do we need tweaks

- Provide variability to the block cipher
- Can be used to construct various cryptographic schemes

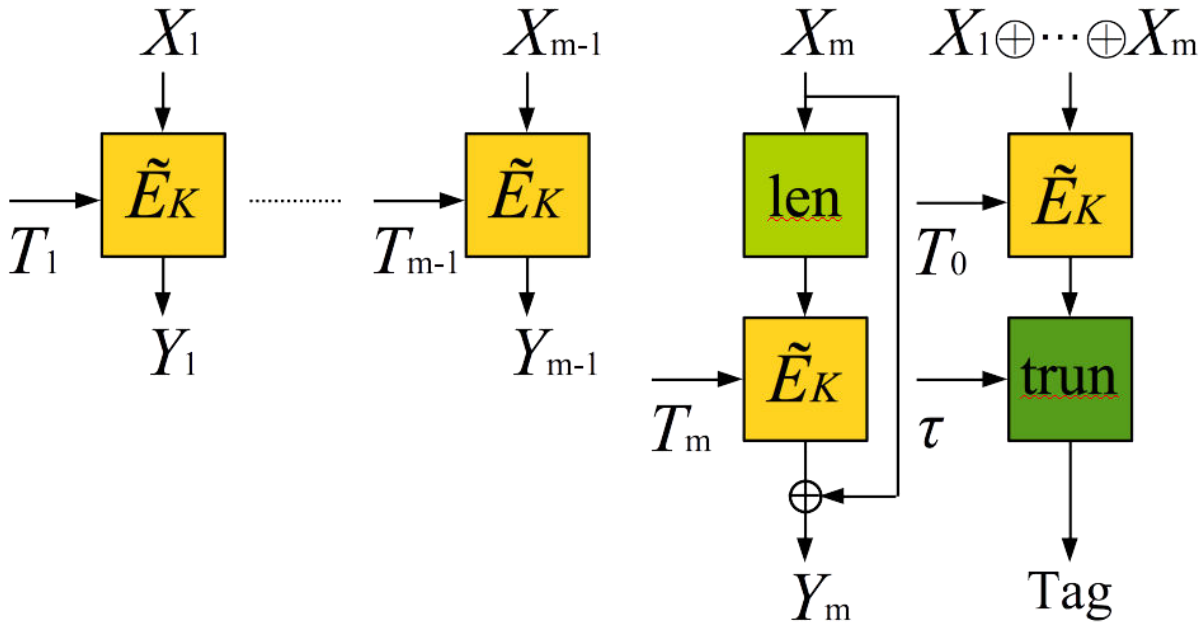


Vs.



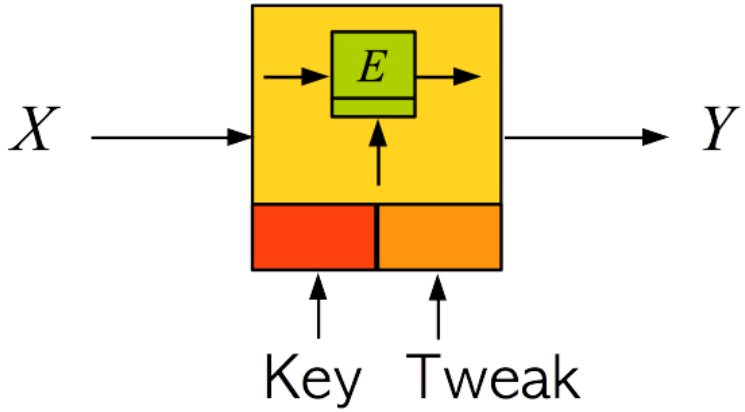
Application: Authenticated Encryption

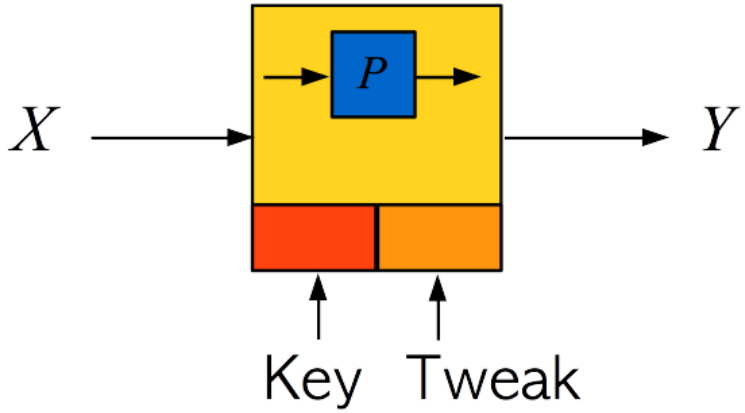
- Tweakable Authenticated Encryption (Liskov, Rivest, Wagner)
  - TAE can be proved to be secure if the underlying TBC is secure
  - Typically, the TBC is replaced by a block cipher-based construction (e.g., OCB modes of operation)



Construction of Tweakable Block Ciphers

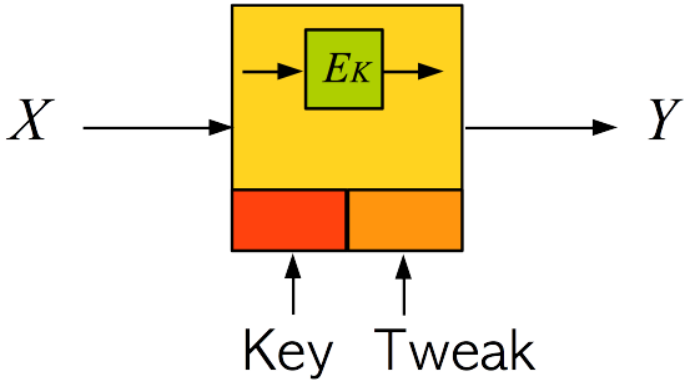
- Dedicated construction
  - Hasty Pudding, Mercy, Threefish, etc.
- Block cipher-based construction
  - LRW1, LRW2, XEX, XHX, etc.
- Permutation-based construction
  - TEM, XPX, etc.



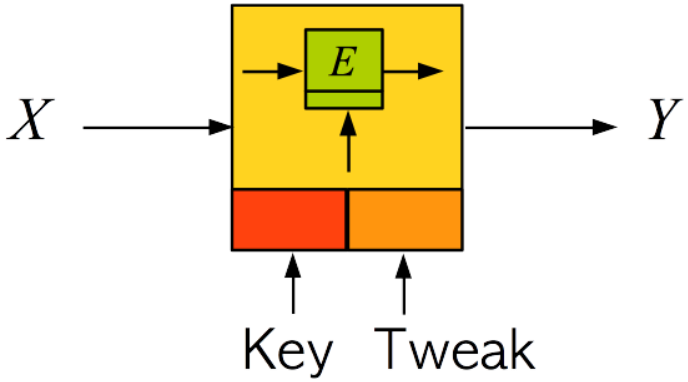


Block cipher-based Construction

- 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)

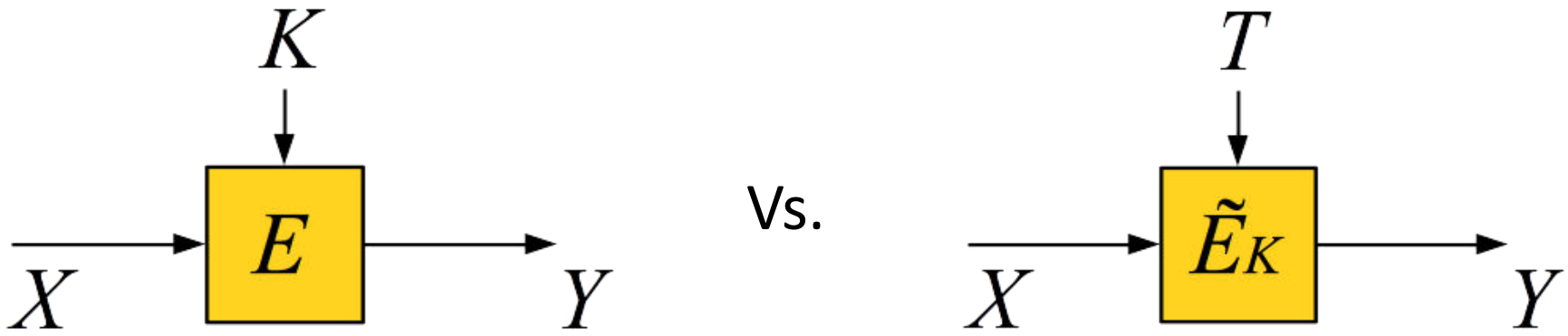


- Using tweak-dependent keys
  - Security is proved in the ideal cipher model
  - An adversary is allowed oracle access to the primitive



Security Notion

- How should we model secure tweakable block ciphers?
  - When a secret key is chosen uniformly at random, each tweak should make the keyed block cipher behave like an independent random permutation
  - This model is similar to the ideal cipher model, but an adversary is not allowed oracle access to the underlying tweakable block cipher



Security Notion

- A tweakable block cipher on $\{0,1\}^n$ with key space $\mathcal{K}$ and tweak space $\mathcal{T}$ is a function

$$\widetilde{E}\colon \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$$

such that $\tilde{E}(K,T,\cdot)$ (also denoted $\tilde{E}_K(T,\cdot)$) is a permutation on $\{0,1\}^n$ for each pair of key and tweak (K,T).

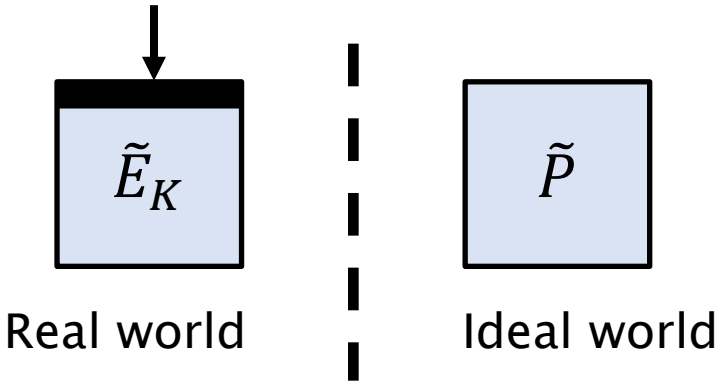
- A tweakable permutation on $\{0,1\}^n$ with tweak space $\mathcal{T}$ is a function

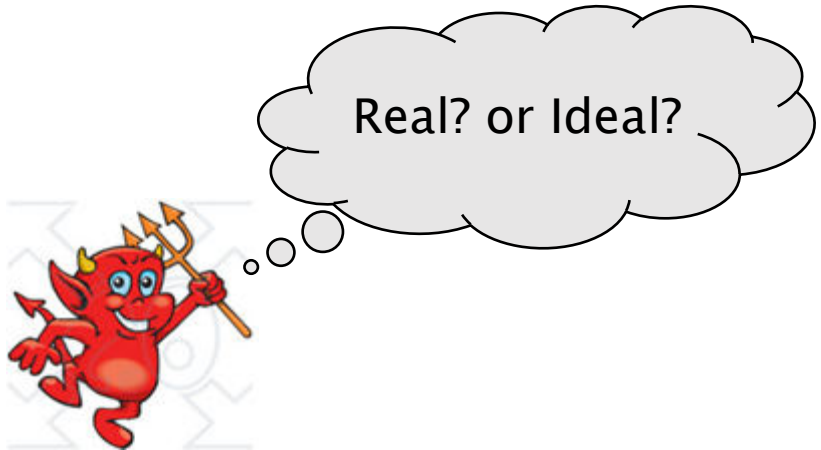
$$\widetilde{P}\colon \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$$

such that $\tilde{P}(T,\cdot)$ is a permutation on $\{0,1\}^n$ for each tweak T.

Security Notion

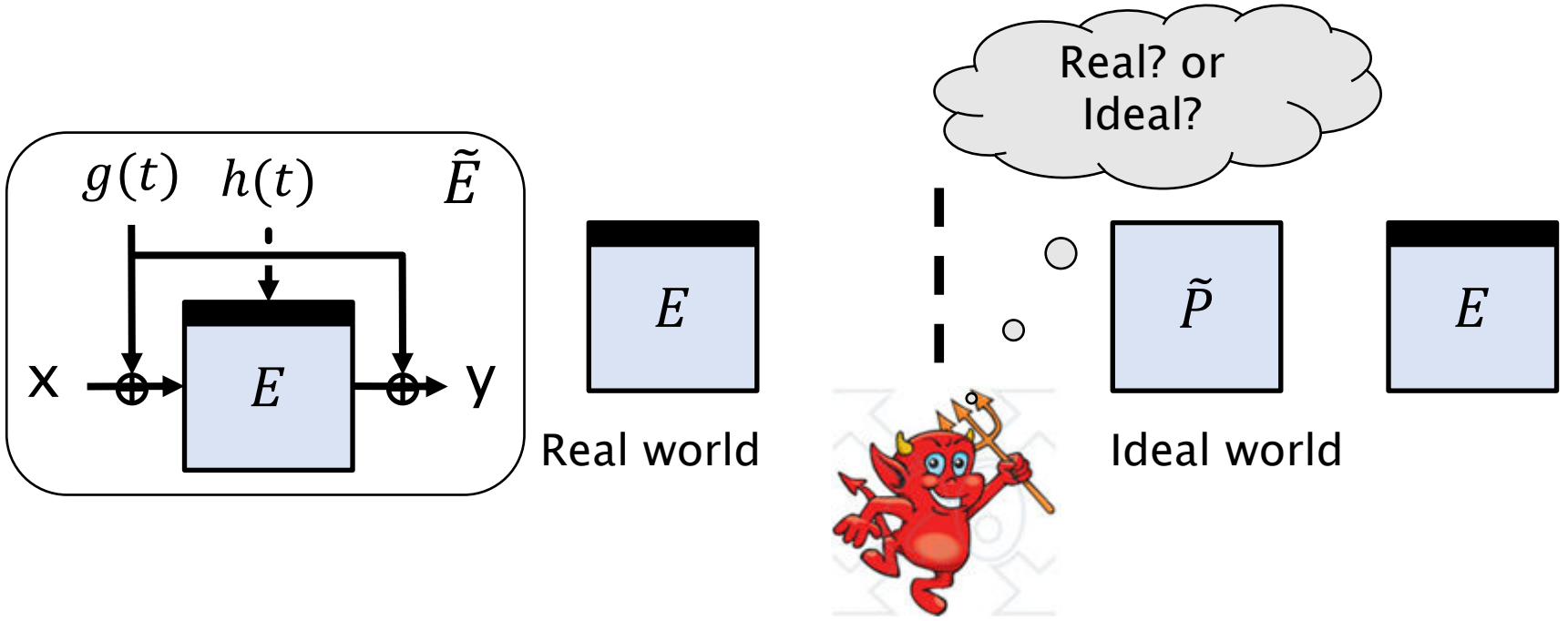
- An ideal tweakable permutation is a tweakable permutation that has been chosen uniformly at random from the set of all possible tweakable permutations.
- Any distinguisher should not be able to distinguish a tweakable block cipher with a secret random key and an ideal tweakable permutation by making a certain number of oracle queries.





Security Notion for Ideal Cipher-based Construction

- An (information-theoretic) adversary is allowed oracle access to both the construction and the ideal cipher



Security Notion for Ideal Cipher-based Construction

- For a distinguisher $\mathcal{D}$, its distinguishing advantage is defined by

$$\mathbf{Adv}_{\tilde{E}}(\mathcal{D}) = \left|\Pr\left[1 \xleftarrow{\$} \mathcal{D}^{\tilde{P},E}\right] - \Pr\left[1 \xleftarrow{\$} \mathcal{D}^{\tilde{E}_K,E}\right]\right|$$

  where $\tilde{P}$ is an ideal random tweakable permutation and a key K is uniform random

- For positive integers p and q,

$$\mathbf{Adv}_{\tilde{E}}(p,q) = \max_{\mathcal{D}}\{\mathbf{Adv}_{\tilde{E}}(\mathcal{D})\},$$

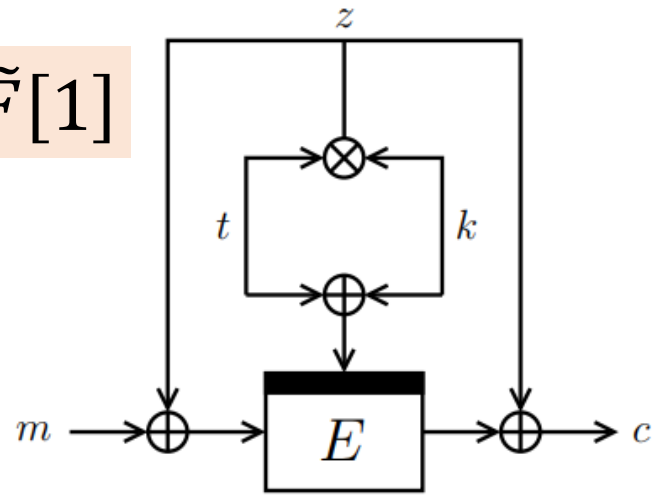
  where the maximum is taken over all the distinguishers making p block cipher queries and q construction queries

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

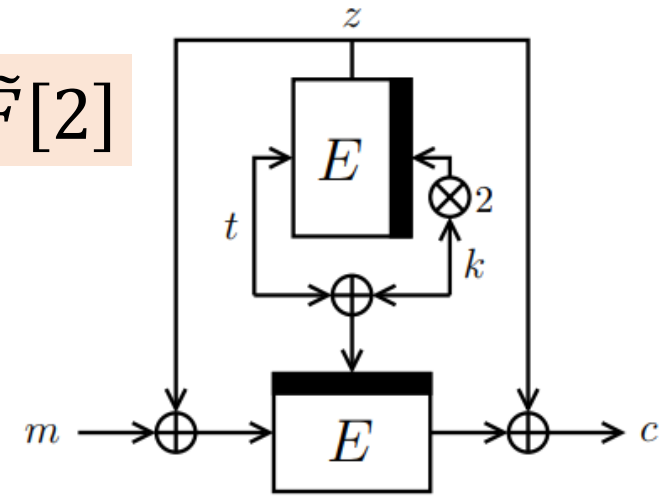
When it is based on an n-bit block block cipher using n-bit keys,

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

$\tilde{F}[1]$



$\tilde{F}[2]$

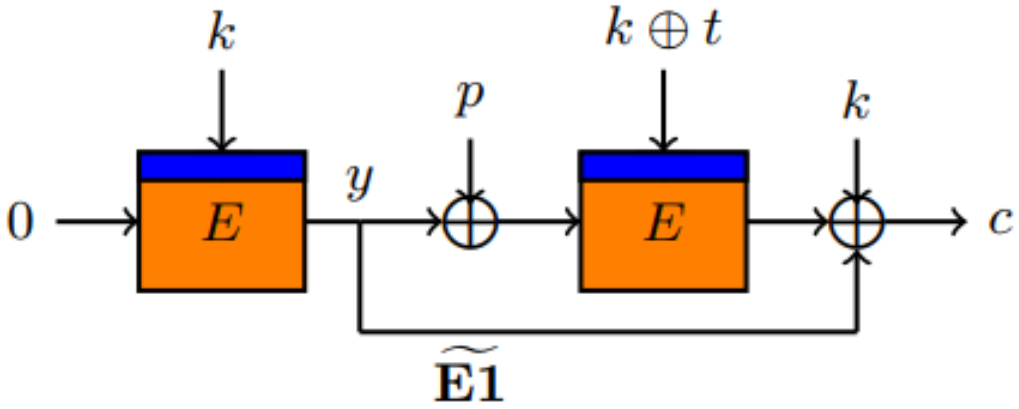


$\widetilde{E1}, \ldots, \widetilde{E32}$ (Wang, et. al., Aisacrypt 2016)

When it is based on an n-bit block block cipher using n-bit keys,

- $\widetilde{E}$i is secure up to 2^n queries

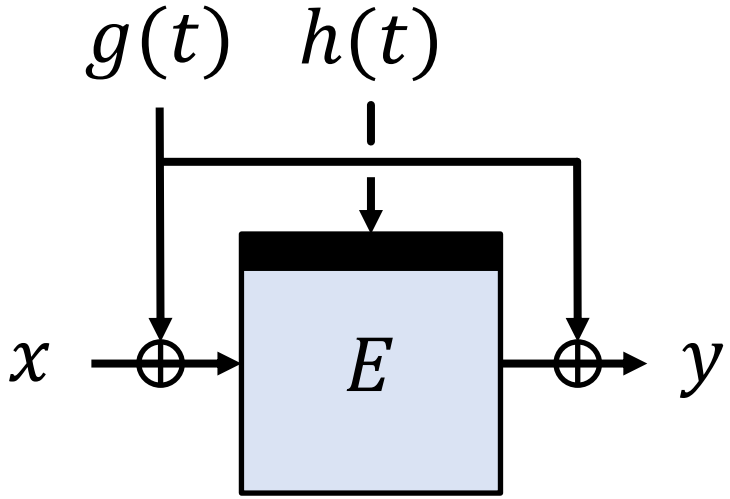
- Make two block cipher calls (or a single block cipher call by precomputation)
- Only xor operation is used



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
- When it is based on an n-bit block block cipher using m-bit keys,

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



Uniform/Universal Hash Functions

For (small) $\delta > 0$,

- A keyed function h is δ-almost uniform if for any x and y,

$$\Pr[h(x) = y] \leq \delta.$$

- A keyed function h is δ-almost universal if for any x and x',

$$\Pr[h(x) = h(x')] \leq \delta.$$

- A keyed function h is δ-almost xor-universal if for any x and y,

$$\Pr[h(x) \oplus h(x') = y] \leq \delta.$$

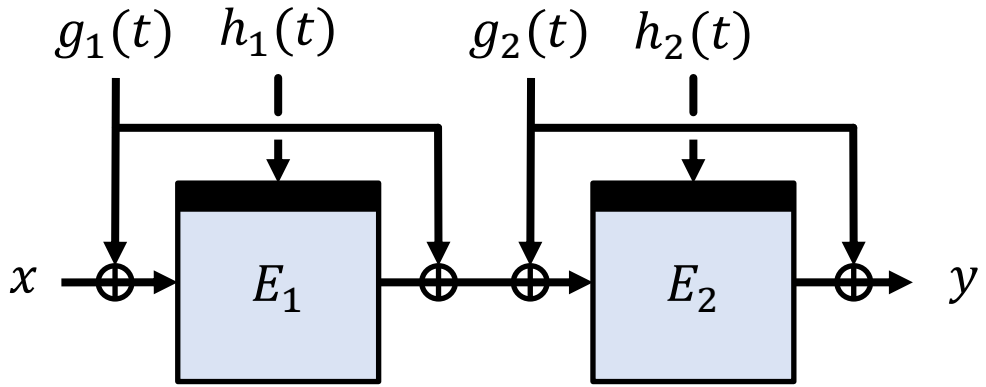
➢ These functions can be defined as polynomials over a finite field.

XHX2: Motivation

- The input size of an n-bit block 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 $\frac{n+m}{2}$.
- Can we go beyond the birthday bound?

XHX2: Construction

- 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 universal hash functions
  - h_1 and h_2 is δ'-almost uniform and xor-universal hash functions



Provable Security of XHX2

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

$$\mathbf{Adv}_{XHX2}(p,q)$$

$$\leq 64p^{\frac{2}{3}}q^{\frac{2}{3}}\delta\delta' + \frac{256(8q^3+2pq^2)^{\frac{1}{2}}\delta^{\frac{1}{2}}\delta'}{2^{\frac{n}{2}}} + \frac{160(16q^3+8pq^2+p^2q)^{\frac{1}{2}}\delta'}{2^n}$$

$$+ 256(16q^3+8pq^2+2q^2+3p^2q)\delta^2(\delta')^2 + \frac{131072n^2q^2\delta'}{2^{2n}},$$

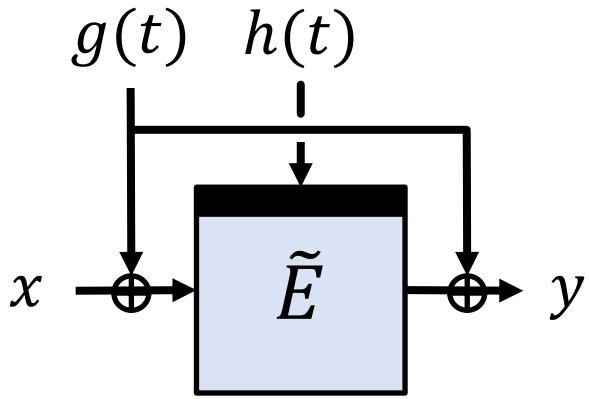
where $\delta \approx \frac{1}{2^n}$, $\delta' \approx \frac{1}{2^m}$

Comparison

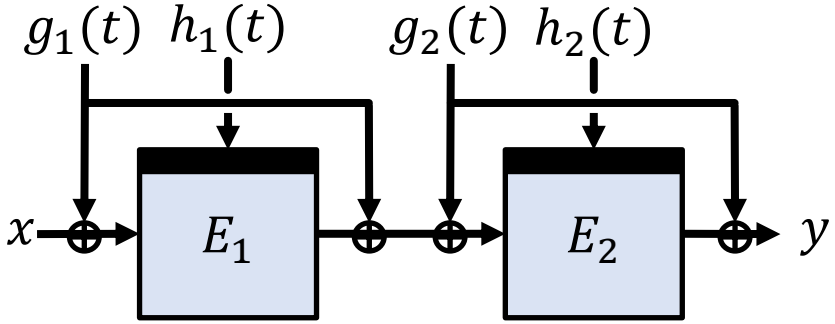
Construction	Key size	Security	Efficiency		Ref.
			E	⊗/**H**	
LRW	$2n$	$n/2$	1	1	[LRW02]
LRW[2]	$4n$	$2n/3$	2	2	[LST12]
LRW[s]	$2sn$	$sn/(s+2)$	s	s	[LS13]
$\tilde{F}[1]$	n	$2n/3$	1	1	[Men15]
$\tilde{F}[2]$	n	n	2	0	[Men15]
$\widetilde{E1}, \cdots, \widetilde{E32}$	n	n	2	0	[Lei+16]
XHX	$n+m$	$(n+m)/2$	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)



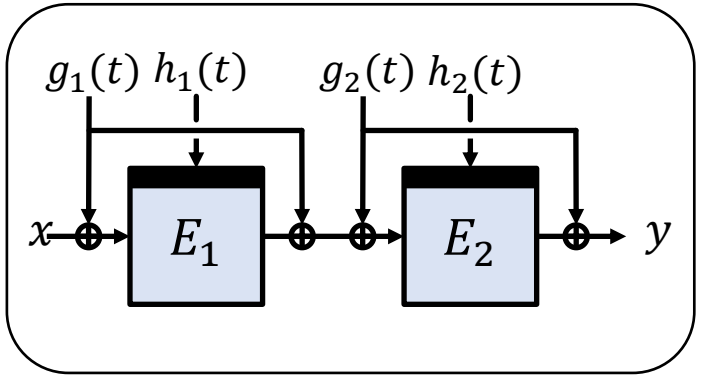
- Without allowing block cipher queries ($p = 0$), we can prove beyond-birthday-bound security for the cascade of two independent XTX constructions.

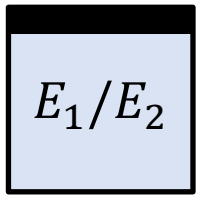


XHX2 from a Practical Viewpoint

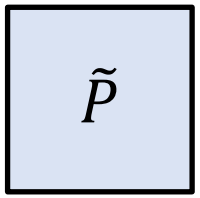
- In the ideal cipher model, each key should define an independent random permutation
- The BBB bound might be useful when the underlying block cipher is relatively small (lightweight)
- Such a small block cipher might be vulnerable to related key attacks (i.e., does not fit the ideal cipher model)
- XHX2 is suitable for a block cipher with the small block size (with a strong key schedule):
  - when $n = 64$ and $m = 128$, XHX2 provides 128 bit security

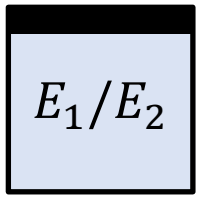
Transcripts





Real world





Ideal world

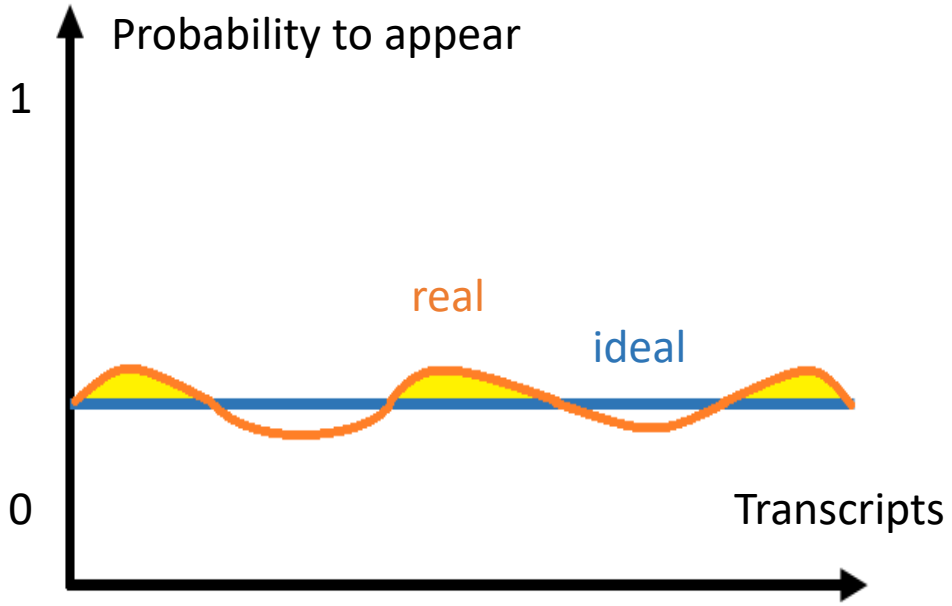
- Adversary tries to distinguish two worlds by making oracle queries
- All the information obtained during the attack is represented by a transcript:

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

Upper Bounding the Distinguishing Advantage

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

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



H-Coefficient Lemma

We can use following lemma to upper bound the statistical distance.

Let $\Theta = \Theta_{\text{good}} \sqcup \Theta_{\text{bad}}$ be a partition of the set of transcripts. Assume that there exist $\epsilon_1, \epsilon_2 > 0$ such that $\Pr[\mathrm{T}_{\text{id}} \in \Theta_{\text{bad}}] \leq \epsilon_2$, and for any $\tau \in \Theta_{\text{good}}$,

$$\frac{\Pr[\mathrm{T}_{\text{re}} = \tau]}{\Pr[\mathrm{T}_{\text{id}} = \tau]} \geq 1 - \epsilon_1.$$

Then one has

$$\| \mathrm{T}_{\text{id}} - \mathrm{T}_{\text{re}} \| \leq \epsilon_1 + \epsilon_2.$$

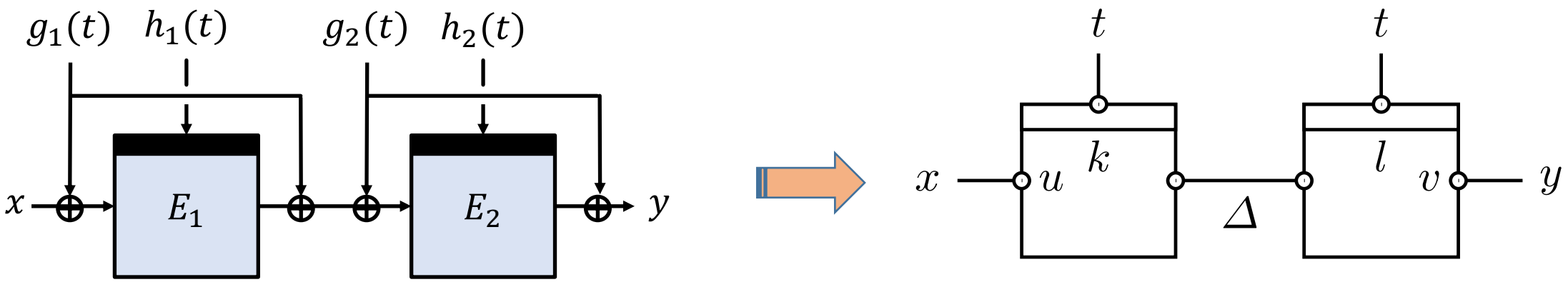
Security Proof of XHX2 (Sketch)

1) Define bad transcripts

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

3) Apply the H-coefficients Lemma

Representation of Construction Queries



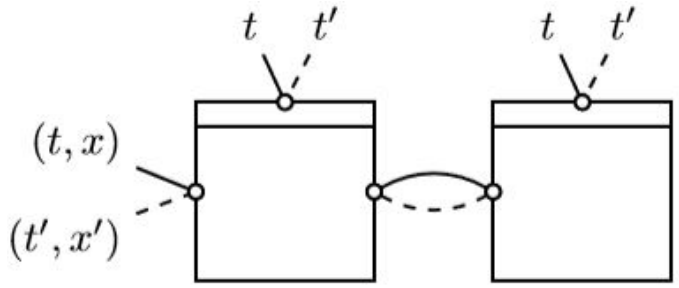
- Reduced query: combine keys and construction queries

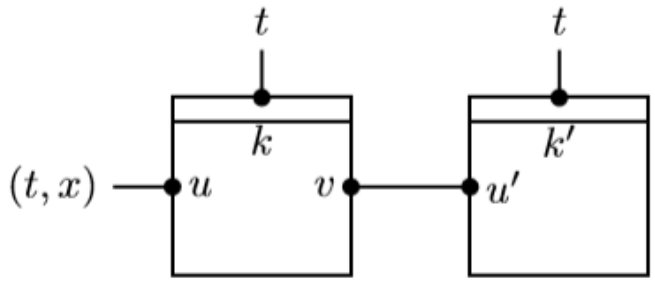
$$(t, x, y) \mapsto (h_1(t), h_2(t), x \oplus g_1(t), y \oplus g_2(t), g_1(t) \oplus g_2(t))$$

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

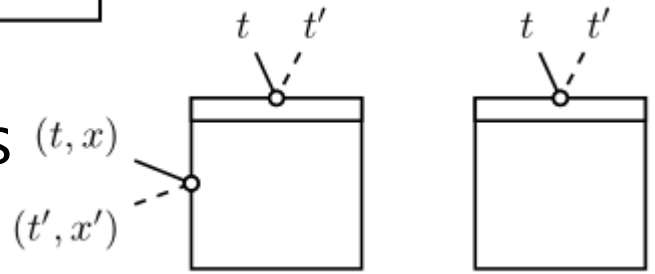
Bad Transcripts

- Avoid revealing any colliding internal path



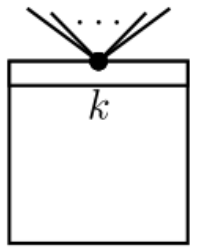


- Upper bound the number of colliding pairs



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

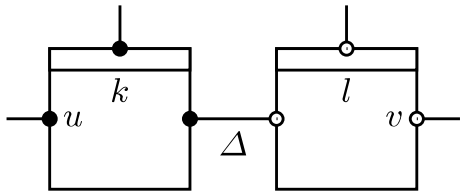
- Avoid a multi-collision with a large multiplicity



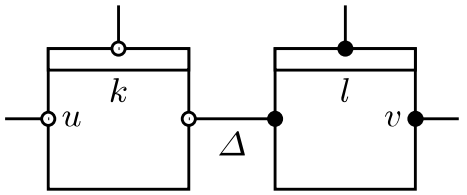
$\leq N/4$

Analyzing Good Transcripts

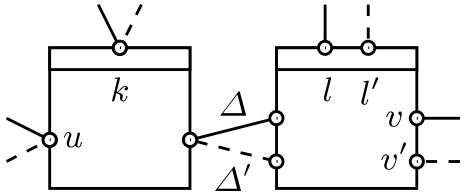
- Classify good queries into 5 classes
- Estimate the probability of completing the queries in each class
- In this way, we can lower bound $\Pr[\mathrm{T}_{\mathrm{re}} = \tau]$



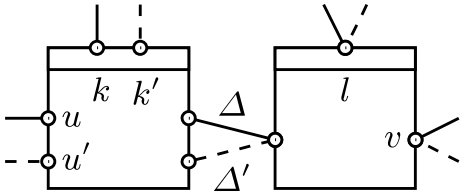
(a) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$



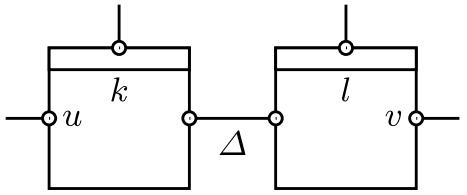
(b) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(2)}$



(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 m-bit key n-bit block cipher providing $min(\frac{2(n+m)}{3}, n+\frac{m}{2})$ 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?

Thank You

Q&A