RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-T08**

Generic Attack on Iterated Tweakable FX Constructions

Ferdinand Sibleyras

Ph.D. Student

Inria, Paris, France

DGA

Inria informatiques mathématiques

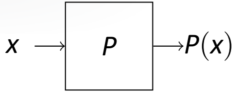
Introduction

Permutation

A bijective pseudorandom function.

$P : \{0,1\}^n \rightarrow \{0,1\}^n$

Example: Keccak-f

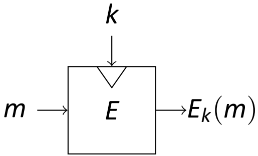


Block Cipher

A family of permutations indexed by a (secret) key.

$E : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$

Example: AES, DES



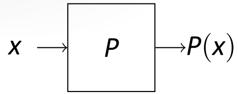
Introduction

Permutation

A bijective pseudorandom function.

$P : \{0,1\}^n \to \{0,1\}^n$

Example: Keccak-f

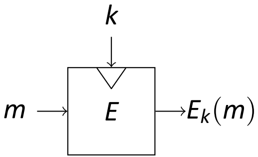


Block Cipher

A family of permutations indexed by a (secret) key.

$E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$

Example: AES, DES

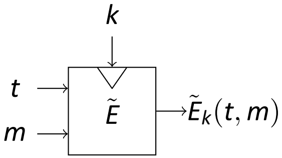


Tweakable Block Cipher

A family of permutations indexed by a key and a (public) tweak.

$\tilde{E} : \{0,1\}^\kappa \times \{0,1\}^\tau \times \{0,1\}^n \to \{0,1\}^n$

Example: Deoxys, Skinny



Introduction

All those primitives are used for Authenticated Encryption.

- Permutation: Sponge based modes (Monkey duplex, Beetle, ...)
- Block Cipher: Most common (GCM, CCM, ...)
- Tweakable Block Cipher: Needed for analysis of OCB, XTS, PMAC, ...

Introduction

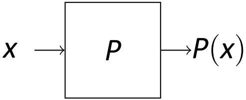
All those primitives are used for Authenticated Encryption.

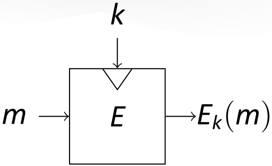
- Permutation: Sponge based modes (Monkey duplex, Beetle, ...)
- Block Cipher: Most common (GCM, CCM, ...)
- Tweakable Block Cipher: Needed for analysis of OCB, XTS, PMAC, ...

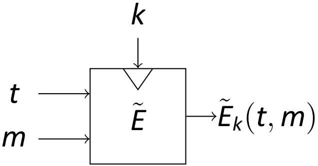
2-Step Proofs

First prove a mode is secure using a Tweakable Block Cipher.
Then build a Tweakable Block Cipher from an existing Block Cipher.

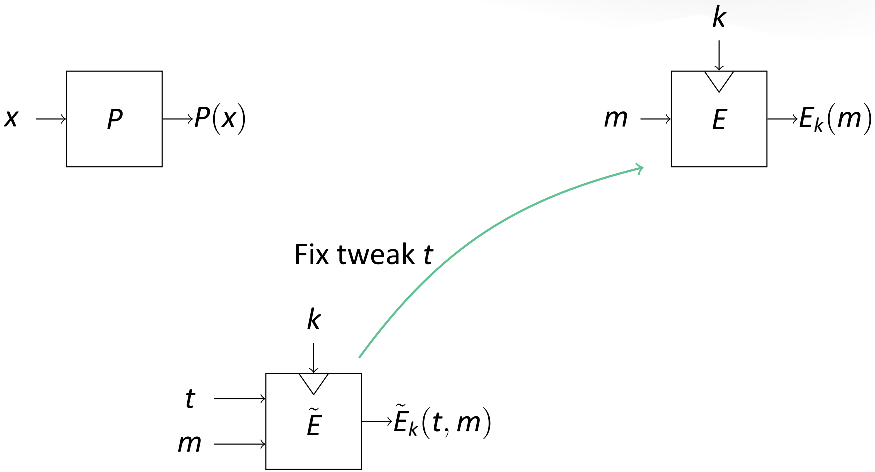
Introduction



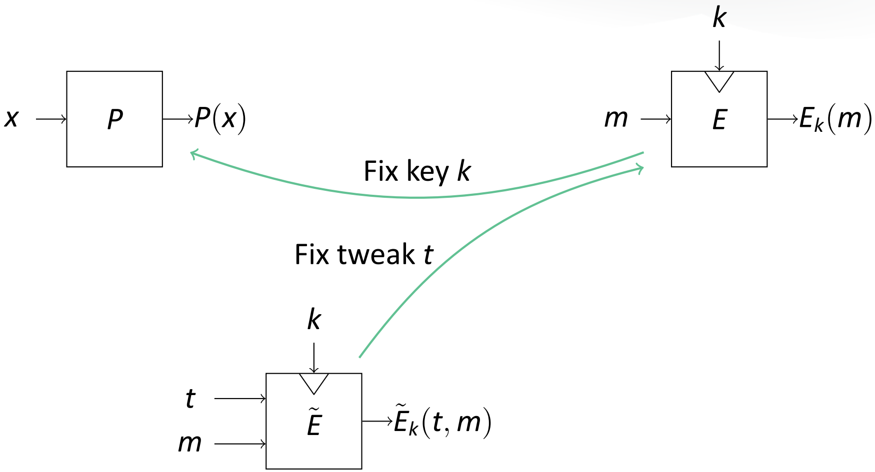




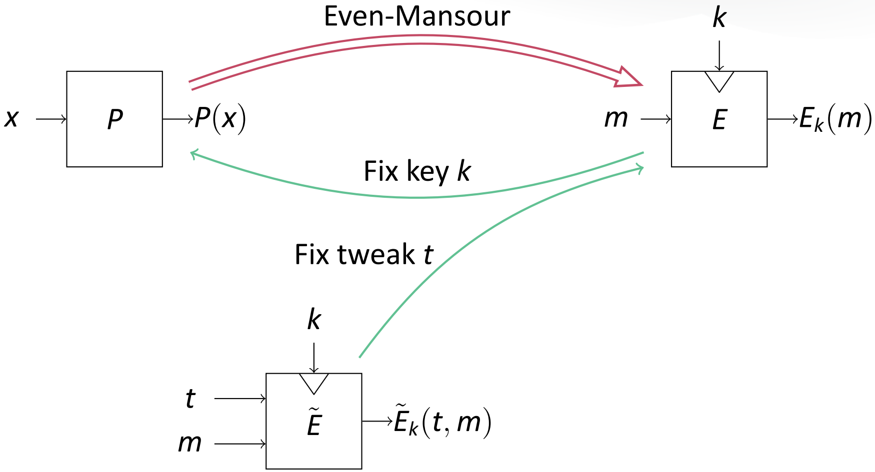
Introduction



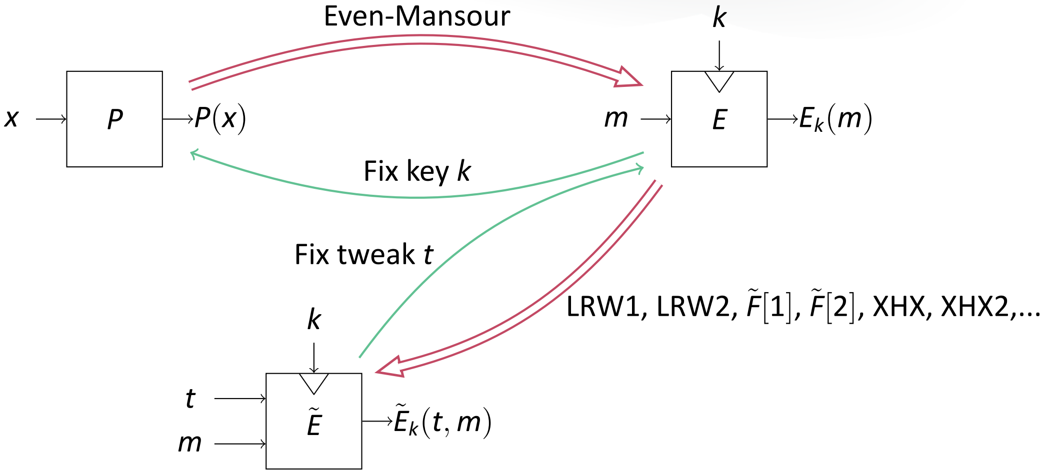
Introduction



Introduction



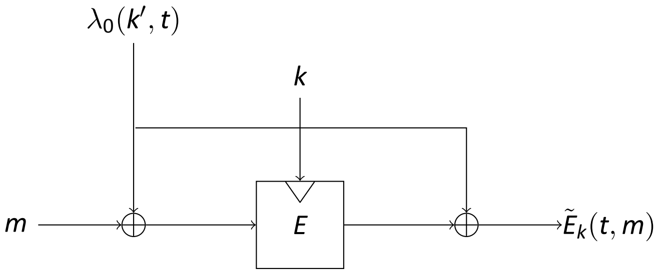
Introduction



LRW2 [Liskov, Rivest, Wagner, 2011]

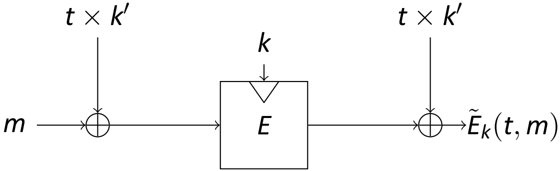
It uses:

- 1 n-bit AXU function $\lambda_0(k', t)$.
- 2 secret values k, k'.



Secure Tweakable Block Cipher up to $2^{n/2}$ calls.

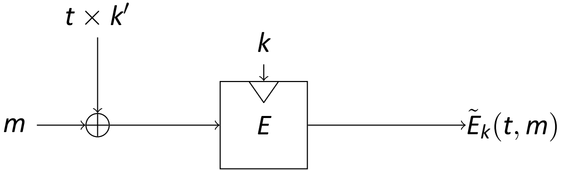
XEX[Rogaway, 2004]



Uses Galois field multiplication $t \times k'$ for a secret value k'.
Preserves CCA security.

Secure Tweakable Block Cipher up to $2^{n/2}$ calls.

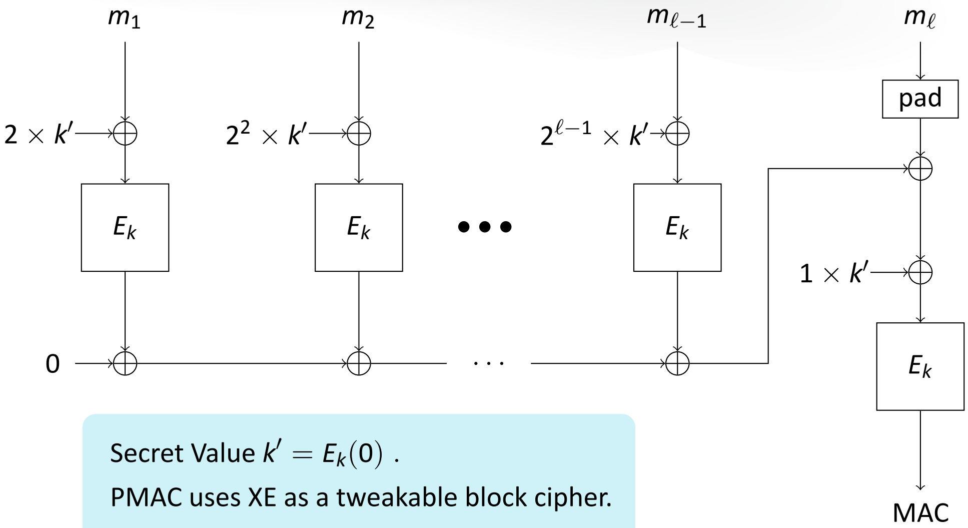
XE [Rogaway, 2004]



Uses Galois field multiplication $t \times k'$ for a secret value k'.
Preserves CPA security.

Secure Tweakable Block Cipher up to $2^{n/2}$ calls.

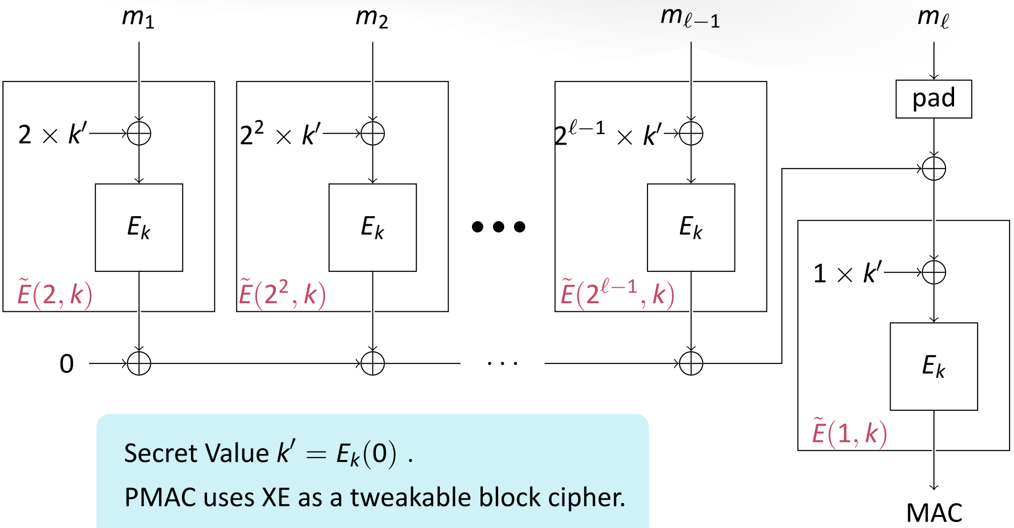
2-step proof for PMAC



Secret Value $k' = E_k(0)$.

PMAC uses XE as a tweakable block cipher.

2-step proof for PMAC



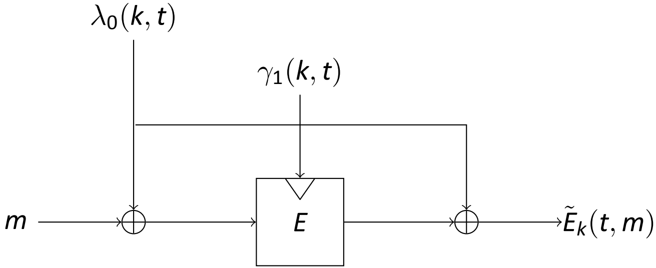
Secret Value $k' = E_k(0)$.

PMAC uses XE as a tweakable block cipher.

XHX[Jha, List, Minematsu, Mishra, Nandi]

It uses:

- 1 n-bit subkey $\lambda_0(k,t)$.
- 1 κ-bit subkey $\gamma_1(k,t)$.

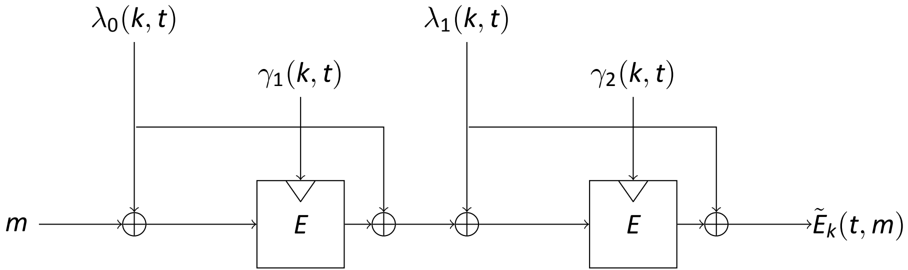


Typically λ_0 and γ_1 can use field multiplication with a secret derived with k.
Allowing rekeying improves the security up to $2^{\frac{n+\kappa}{2}}$.

XHX2 [Lee, Lee]

It uses:

- 2 n-bit subkeys $\lambda_0(k,t)$, $\lambda_1(k,t)$.
- 2 κ-bit subkeys $\gamma_1(k,t)$, $\gamma_2(k,t)$.

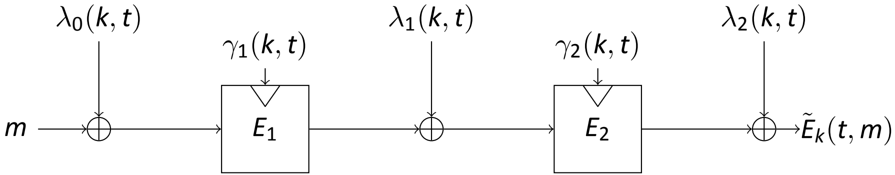


Cascade of two independant XHX.
Cascading improves the security up to $2^{\frac{2}{3}(n+\kappa)}$.

2-Round Tweakable FX

It uses:

- 3 n-bit subkeys $\lambda_0(k,t)$, $\lambda_1(k,t)$, $\lambda_2(k,t)$.
- 2 κ-bit subkeys $\gamma_1(k,t)$, $\gamma_2(k,t)$.



Generalization

We don't assume anything on subkey functions.

$\Longrightarrow$ Attack works for any 2-round schemes !

Information Theoretic Setting

Proofs say an attacker needs at least this much data.
Proofs can get better, it is a lower bound.
Information Theoretic cryptanalysis shows an upper bound on the provable security.
A proof is tight when cryptanalysis matches.
Computations are irrelevant.

Information Theoretic Setting

Proofs say an attacker needs at least this much data.

Proofs can get better, it is a lower bound.

Information Theoretic cryptanalysis shows an upper bound on the provable security.

A proof is tight when cryptanalysis matches.

Computations are irrelevant.

Information Theoretic Key Recovery

It's all about the query complexity.

We count calls to tweakable block cipher $\tilde{E}_k(\cdot,\cdot)$ and block ciphers $E_1(\cdot,\cdot), E_2(\cdot,\cdot)$.

Computation of subkey functions are not counted.

GOAL: Recover the master key k.

Our Result

How far can we hope to go by cascading and rekeying?

Is the proof for XHX2 tight?

Our Result

How far can we hope to go by cascading and rekeying?

Is the proof for XHX2 tight?

This work

Information theoretic cryptanalysis.

Query complexity of $\mathcal{O}(2^{\frac{r}{r+1}(n+\kappa)})$.

Show that XHX and XHX2 proofs are tight.

Our Strategy

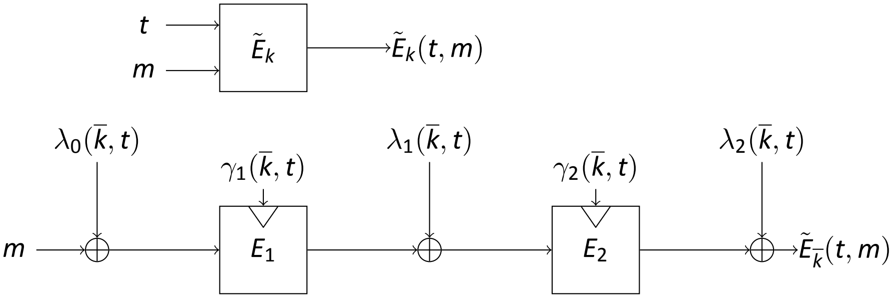
We follow the same strategy as [Gaži, 2013] to improve and apply it in the tweakable block cipher setting.

Strategy

Build a contradictory path for each wrong key guesses until one is left.

Contradictory Path

1. Query $c = \tilde{E}_k(t, m)$ for some (t, m).
2. Make a guess $\overline{k}$ of the master key k.
3. Compute $\overline{c} = \tilde{E}_{\overline{k}}(t, m)$.
4. If $c \neq \overline{c}$ then Contradictory Path then $\overline{k} \neq k$.



Counting queries

- No issue with guessing all the keys in information theoretic setting.
- However we can't make a block cipher query for each guess, it's too much !
- We need to store and reuse previous queries as much as we can.

Tweakable Block Cipher

As we can have security $\gg 2^n$ we also can have online queries $\gg 2^n$!

Notations

- n and κ the block ciphers state and key size respectively.
- ℓ_0 the number of online queries to $\tilde{E}_k(t, m)$.
- ℓ the number of offline queries to $E(\overline{k}, m)$..

Total Asymptotic Query Complexity is $\mathcal{O}(\ell_0 + \ell)$.

Notations

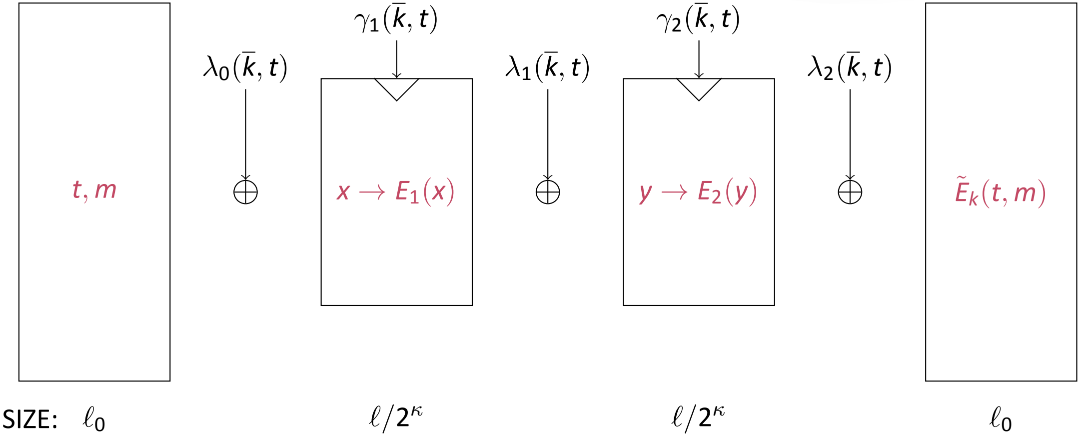
- n and κ the block ciphers state and key size respectively.
- ℓ_0 the number of online queries to $\tilde{E}_k(t, m)$.
- ℓ the number of offline queries to $E(\overline{k}, m)$..

Total Asymptotic Query Complexity is $\mathcal{O}(\ell_0 + \ell)$.

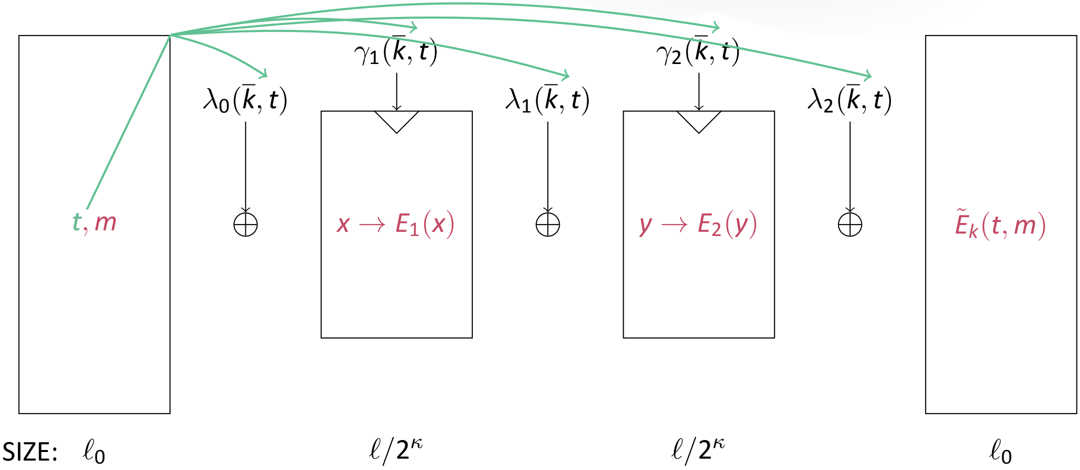
Non-Adaptative Known Plaintext Attack

Observed ℓ_0 tweak/plaintext/ciphertext triples.
Compute random $\ell/2^\kappa$ input/output of block ciphers under each κ-bit subkey.

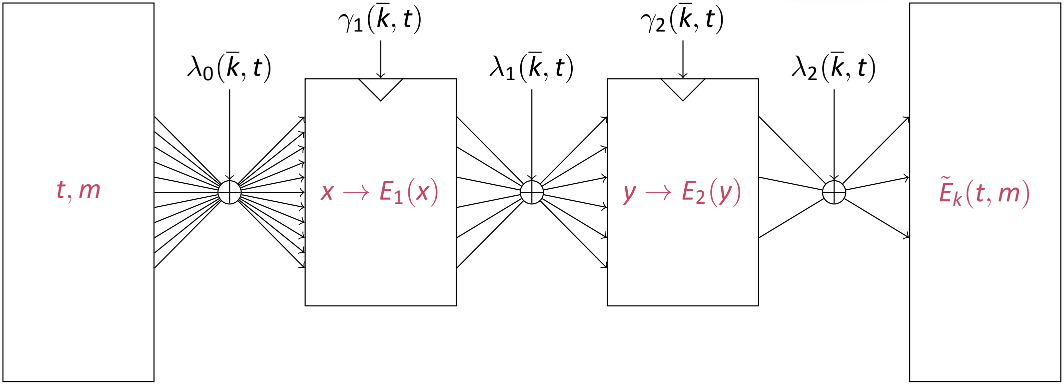
Random Path Reconstrution for 2 Rounds



Random Path Reconstrution for 2 Rounds

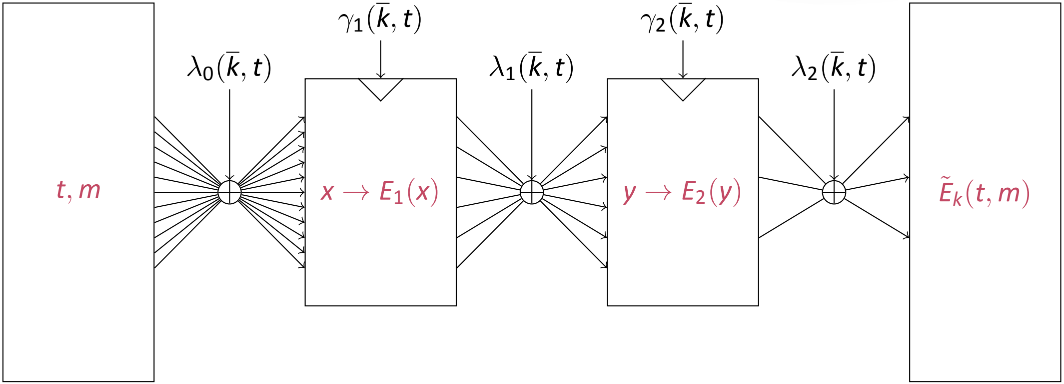


Random Path Reconstrution for 2 Rounds



SIZE: ℓ_0 $\ell/2^\kappa$ $\ell/2^\kappa$ ℓ_0

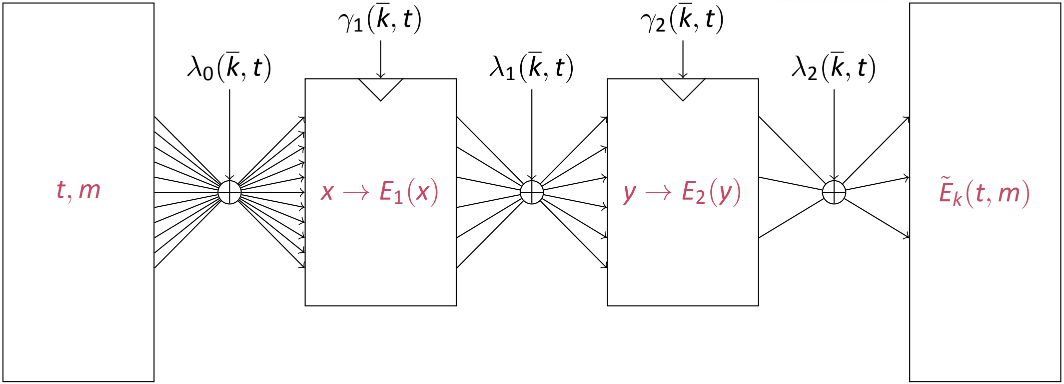
Random Path Reconstrution for 2 Rounds



SIZE: ℓ_0 $\ell/2^\kappa$ $\ell/2^\kappa$ ℓ_0

#PATH: ℓ_0

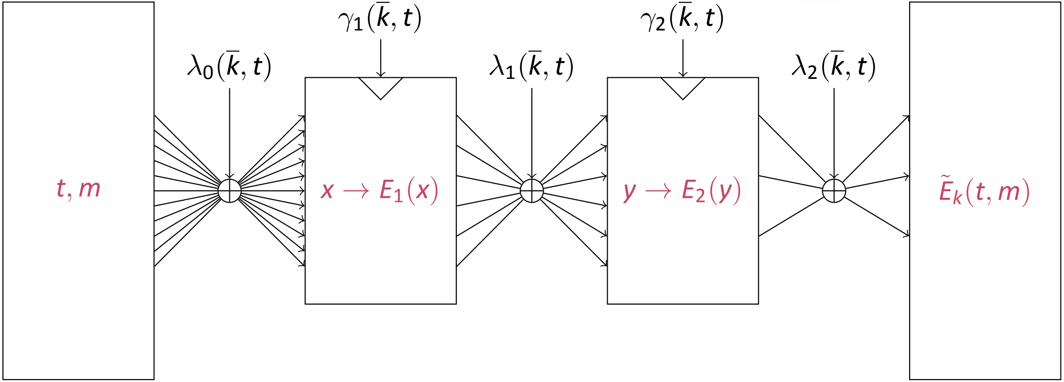
Random Path Reconstrution for 2 Rounds



SIZE: ℓ_0 $\ell/2^\kappa$ $\ell/2^\kappa$ ℓ_0

#PATH: ℓ_0 $\ell_0\ell/2^{\kappa+n}$

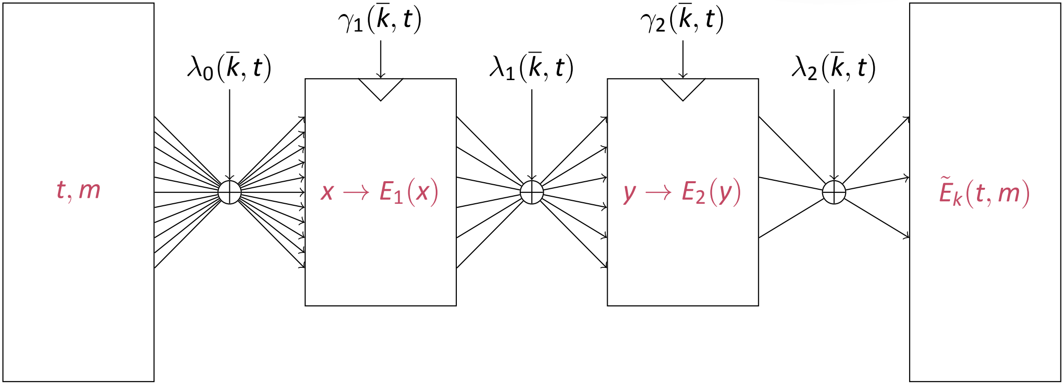
Random Path Reconstrution for 2 Rounds



SIZE: ℓ_0 $\ell/2^\kappa$ $\ell/2^\kappa$ ℓ_0

#PATH: ℓ_0 $\ell_0\ell/2^{\kappa+n}$ $\ell_0\ell^2/2^{2\kappa+2n}$

Random Path Reconstrution for 2 Rounds



SIZE:	ℓ_0		$\ell/2^\kappa$		$\ell/2^\kappa$		ℓ_0
#PATH:		ℓ_0		$\ell_0\ell/2^{\kappa+n}$		$\ell_0\ell^2/2^{2\kappa+2n}$	$\bar{k} = k$?

Query Complexity

The number of path we can reconstruct is $\ell_0\ell^2/2^{2\kappa+2n}$ on average for all guesses $\overline{k}$.
We put $\ell_0 = \ell$ to minimize $\ell_0 + \ell$.

$$
\begin{aligned}
\ell_0\ell^2/2^{2\kappa+2n} &= 1\\
\ell^3/2^{2\kappa+2n} &= 1\\
\ell^3 &= 2^{2\kappa+2n}\\
\ell &= 2^{\frac{2}{3}(\kappa+n)} = \ell_0
\end{aligned}
$$

Query Complexity

The number of path we can reconstruct is $\ell_0 \ell^2 / 2^{2\kappa+2n}$ on average for all guesses $\bar{k}$.
We put $\ell_0 = \ell$ to minimize $\ell_0 + \ell$.

$$\begin{aligned} \ell_0 \ell^2 / 2^{2\kappa+2n} &= 1 \\ \ell^3 / 2^{2\kappa+2n} &= 1 \\ \ell^3 &= 2^{2\kappa+2n} \\ \ell &= 2^{\frac{2}{3}(\kappa+n)} = \ell_0 \end{aligned}$$

Result

The query complexity of the attack is $\mathcal{O}(2^{\frac{2}{3}(\kappa+n)})$.

Parameter Constraint

There is no issue with having $\ell_0 > 2^n$ as the tweak can be of arbitrary size. However we need $\ell/2^\kappa \geq 1$ for our previous reasoning to hold.

$$\begin{aligned} \ell/2^\kappa &\geq 1 \\ 2^{\frac{2}{3}(\kappa+n)}/2^\kappa &\geq 1 \\ \frac{2}{3}\kappa + \frac{2}{3}n - \kappa &\geq 0 \\ -\kappa + 2n &\geq 0 \\ \kappa &\leq 2n \end{aligned}$$

Parameter Constraint

There is no issue with having $\ell_0 > 2^n$ as the tweak can be of arbitrary size. However we need $\ell/2^\kappa \geq 1$ for our previous reasoning to hold.

$$\begin{aligned} \ell/2^\kappa &\geq 1 \\ 2^{\frac{2}{3}(\kappa+n)}/2^\kappa &\geq 1 \\ \frac{2}{3}\kappa + \frac{2}{3}n - \kappa &\geq 0 \\ -\kappa + 2n &\geq 0 \\ \kappa &\leq 2n \end{aligned}$$

Constraint

Cryptanalysis works when the block cipher key size is less or equal to twice the state size.

Generalization for *r* rounds

The attack works for any number r of rounds.

Result

The query complexity of the attack is $\mathcal{O}(2^{\frac{r}{r+1}(\kappa+n)})$.

Constraint

Cryptanalysis works when $\kappa \leq rn$.

Technical Details

Need to ensure that the right key *k* is detected while all the wrong guesses be dismissed.
Possible false positive when the master key *k* is large !

Technical Details

Need to ensure that the right key k is detected while all the wrong guesses be dismissed.
Possible false positive when the master key k is large !
Let k be a $\tilde{\kappa}$-bit value then:

Affined query complexity

The asymptotic query complexity is $\mathcal{O}(2^{\frac{r}{r+1}(n+\kappa)} \cdot \sqrt[r+1]{\tilde{\kappa}/n})$.

It is still $\mathcal{O}(2^{\frac{r}{r+1}(n+\kappa)})$ whenever $\tilde{\kappa}$ is a multiple of n.

Each tweak must give different subkey values for this key recovery to work but if not, then, we have a distinguisher.

Results

Ref	Scheme	r	Proof	Known Attack	Our Generic Attack
[LisRivWag11]	LRW2	1	$2^{n/2}$	$2^{n/2}$	$2^{\frac{1}{2}(n+\kappa)}$
[Mennink15]	$\tilde{F}[1]$	1	$2^{\frac{2}{3}n}$	2^n	2^n (as $\kappa = n$)
[Mennink16]	XPX	1	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$ (as $\kappa = 0$)
[JLMMN17]	XHX	1	$2^{\frac{1}{2}(n+\kappa)}$	$2^{\frac{1}{2}(n+\kappa)}$	$2^{\frac{1}{2}(n+\kappa)}$
[JLMMN17]	GXHX	1	$2^{\frac{1}{2}(n+\kappa)}$	none	$2^{\frac{1}{2}(n+\kappa)}$
[Mennink15]	$\tilde{F}[2]$	1	2^n	2^n	N.A.
[LisRivWag11]	LRW1	2	$2^{n/2}$	$2^{n/2}$	$2^{\frac{2}{3}(n+\kappa)}$
[LanShrTer12]	CLRW2	2	$2^{3n/4}$	$2^{3n/4}$	$2^{\frac{2}{3}(n+\kappa)}$
[LeeLee18]	XHX2	2	$2^{\frac{2}{3}(n+\kappa)}$	none	$2^{\frac{2}{3}(n+\kappa)}$

Take-Aways

- Cryptanalysis of the generalized tweakable FX construction for $r \geq 1$ rounds in $\mathcal{O}(2^{\frac{r}{r+1}(n+\kappa)})$ query complexity under standard assumptions.
- Shows tightness of proofs of GXHX and XHX2 which in turn show it is information theoretically optimal for $r = 1, 2$ rounds.
- Gives a security upper-bound for this strategy with $r \geq 3$ rounds.

Take-Aways

- Cryptanalysis of the generalized tweakable FX construction for $r \geq 1$ rounds in $\mathcal{O}(2^{\frac{r}{r+1}(n+\kappa)})$ query complexity under standard assumptions.
- Shows tightness of proofs of GXHX and XHX2 which in turn show it is information theoretically optimal for $r = 1, 2$ rounds.
- Gives a security upper-bound for this strategy with $r \geq 3$ rounds.

Open Questions:

- How simple can the subkey functions be while maintaining security?
- Can we prove security for $r \geq 3$ rounds?
- What concrete application for those improved schemes?