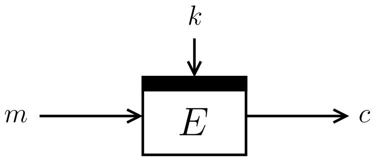
Optimally Secure Tweakable Blockciphers

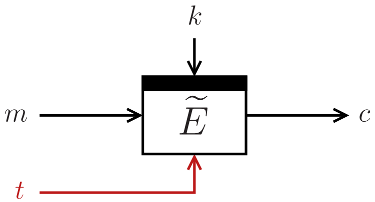
Bart Mennink
KU Leuven (Belgium)

Fast Software Encryption
March 10, 2015

Introduction

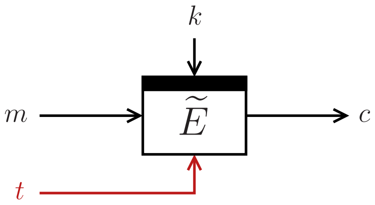


Introduction



- Tweak: flexibility to the cipher
- Each tweak gives different permutation

Introduction

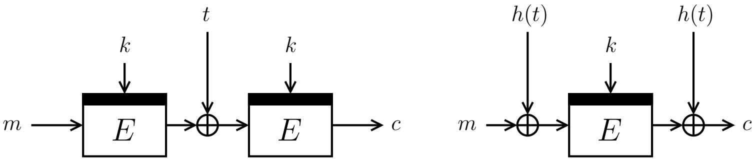


- Tweak: flexibility to the cipher
- Each tweak gives different permutation

- Dedicated constructions:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro01]
  - Threefish [FLS+07]

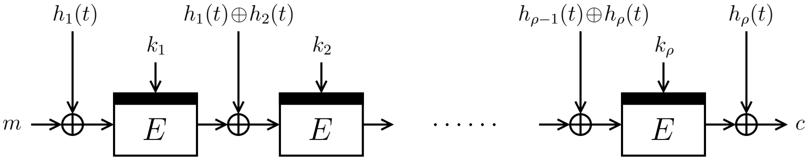
Introduction: Modular Designs

- LRW1 and LRW2 by Liskov et al. [LRW02]:



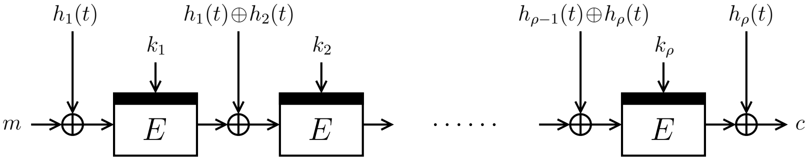
- h is XOR-universal hash
- Related: XEX
- Secure up to $2^{n/2}$ queries

Introduction: Modular Designs



- LRW2$[\rho]$: concatenation of ρ LRW2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

Introduction: Modular Designs



- LRW2$[\rho]$: concatenation of ρ LRW2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

- $\rho = 2$: secure up to $2^{2n/3}$ queries [LST12,Pro14]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [LS13]
- Conjecture: optimal $2^{\rho n/(\rho+1)}$ security

Introduction: State of the Art

scheme	security ($\log_2$)	key length	cost E	cost $\otimes/h$
LRW1	$n/2$	n	2	0
LRW2	$n/2$	$2n$	1	1
XEX	$n/2$	n	2	0
LRW2$[2]$	$2n/3$	$4n$	2	2
LRW2$[\rho]$	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ

Optimal 2^n security only if key length and cost $\rightarrow \infty$?

Introduction: Tweak-Dependent Keys

Efficiency

tweak schedule lighter
than key schedule

Introduction: Tweak-Dependent Keys

Efficiency	**Security**
tweak schedule lighter than key schedule	tweak schedule stronger than key schedule

Introduction: Tweak-Dependent Keys

Efficiency	**Security**
tweak schedule lighter than key schedule	tweak schedule stronger than key schedule

Tweak and key change approximately equally expensive

Introduction: Tweak-Dependent Keys

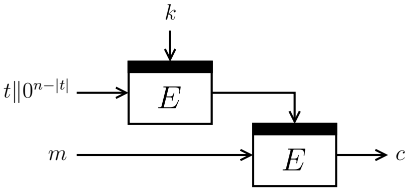
Efficiency	**Security**
tweak schedule lighter than key schedule	tweak schedule stronger than key schedule

$$\underbrace{\hspace{10em}}_{\text{Tweak and key change approximately equally expensive}}$$

- TWEAKEY [JNP14] key scheduling blends key and tweak

Introduction: Tweak-Dependent Keys

- Minematsu [Min09]:



- Secure up to $\max\{2^{n/2}, 2^{n-|t|}\}$ queries
- Beyond birthday bound for $|t| < n/2$

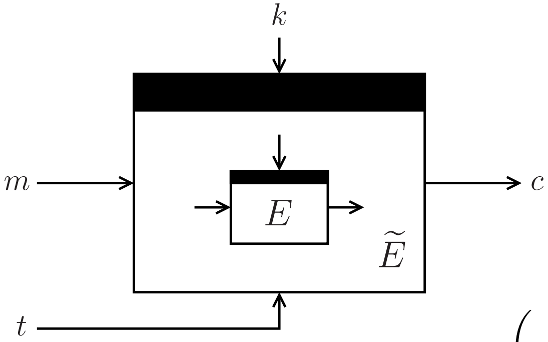
Introduction: State of the Art

scheme	security ($\log_2$)	key length	cost E	cost $\otimes/h$	cost tdk
LRW1	$n/2$	n	2	0	0
LRW2	$n/2$	$2n$	1	1	0
XEX	$n/2$	n	2	0	0
LRW2[2]	$2n/3$	$4n$	2	2	0
LRW2[ρ]	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ	0
Min	$\max\{n/2, n-\|t\|\}$	n	2	0	1

Our Goal

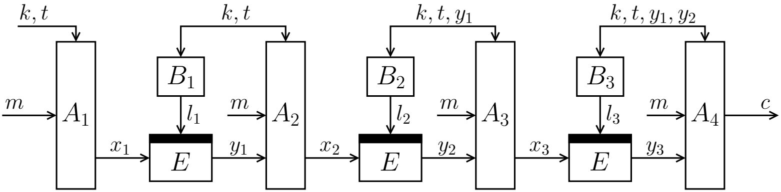
Given a blockcipher E,

construct optimally secure tweakable blockcipher $\widetilde{E}$



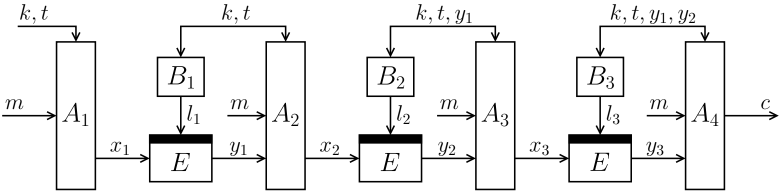
(all wires carry n bits)

Generic Design



$\widetilde{E}[\rho]$ (for $\rho \geq 1$)

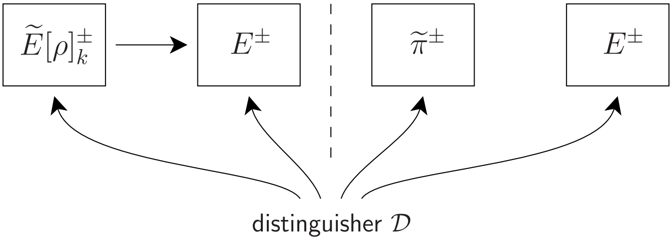
Generic Design



$\widetilde{E}[\rho]$ (for $\rho \geq 1$)

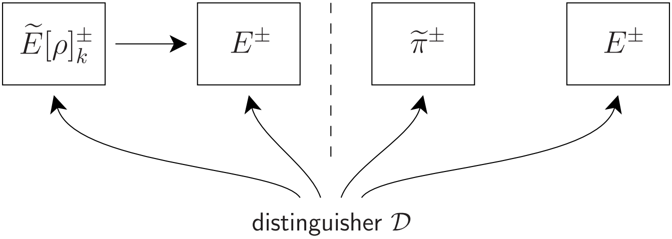
- Mixing functions A_i, B_i
  - should be such that $\widetilde{E}[\rho]$ is invertible
  - but can be anything otherwise

Security Model



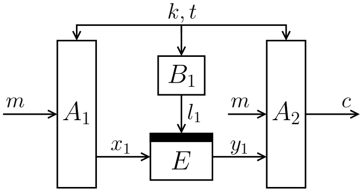
- Information-theoretic indistinguishability
  - $\widetilde{\pi}$ ideal tweakable cipher
  - E ideal cipher

Security Model

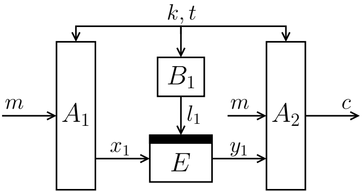


- Information-theoretic indistinguishability
  - $\widetilde{\pi}$ ideal tweakable cipher
  - E ideal cipher
- Complexity-theoretic indistinguishability?

One E-Call with Linear Mixing



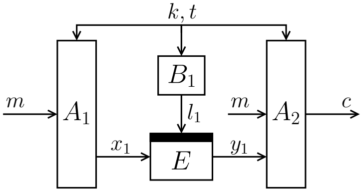
One E-Call with Linear Mixing



Theorem

- If A_1, B_1, A_2 are linear, $\widetilde{E}[1]$ can be distinguished from $\widetilde{\pi}$ in at most about $2^{n/2}$ queries

One E-Call with Linear Mixing



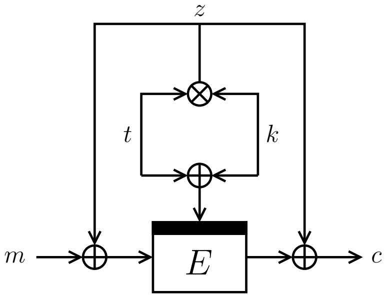
Theorem

- If A_1, B_1, A_2 are linear, $\widetilde{E}[1]$ can be distinguished from $\widetilde{\pi}$ in at most about $2^{n/2}$ queries

Proof idea

- Relation among queries to $\widetilde{E}[1]$?
- Case distinction based on how k, t, m are processed

One E-Call with Polynomial Mixing

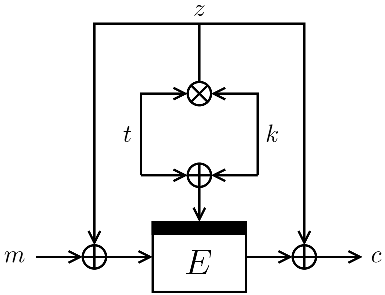


$$\widetilde{F}[1](k, t, m) = c$$

Idea

- Subkey $k \oplus t$
- Masking $k \otimes t$

One E-Call with Polynomial Mixing



$\widetilde{F}[1](k, t, m) = c$

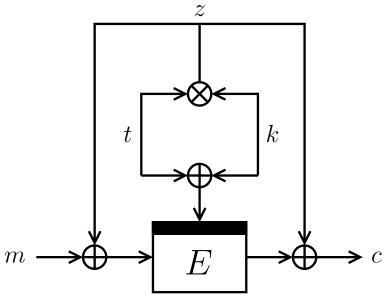
Idea

- Subkey $k \oplus t$
- Masking $k \otimes t$

Security

- Up to $2^{2n/3}$ queries

One E-Call with Polynomial Mixing



$\widetilde{F}[1](k,t,m) = c$

Idea

- Subkey $k \oplus t$
- Masking $k \otimes t$

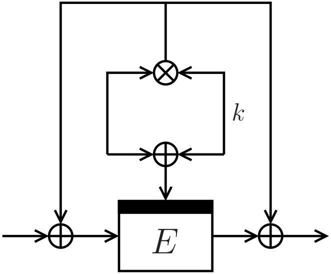
Security

- Up to $2^{2n/3}$ queries

Cost

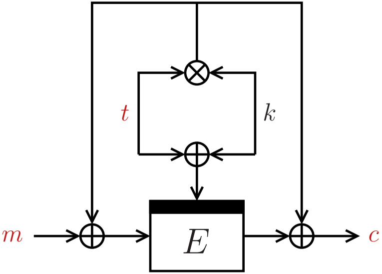
- One E-call
- One $\otimes$-evaluation
- One re-key

One E-Call with Polynomial Mixing: Proof Idea



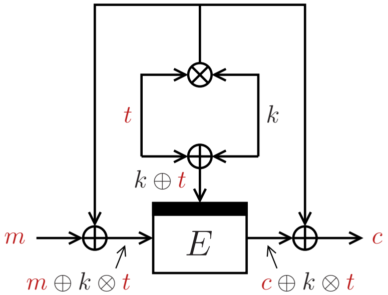
- Key k is secret

One E-Call with Polynomial Mixing: Proof Idea



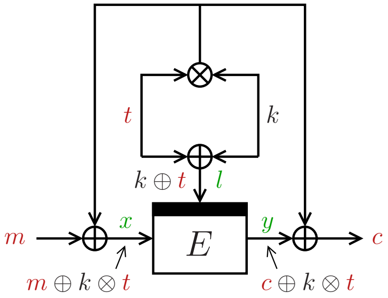
- Key k is secret
- Consider any construction query (t, m, c)

One E-Call with Polynomial Mixing: Proof Idea



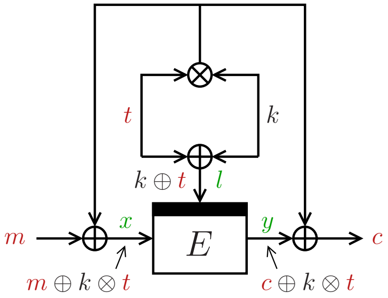
- Key k is secret
- Consider any construction query (t, m, c)

One E-Call with Polynomial Mixing: Proof Idea



- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

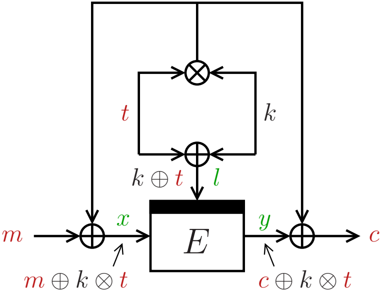
One E-Call with Polynomial Mixing: Proof Idea



- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

$k \oplus t = l$ and $m \oplus k \otimes t = x$

One E-Call with Polynomial Mixing: Proof Idea



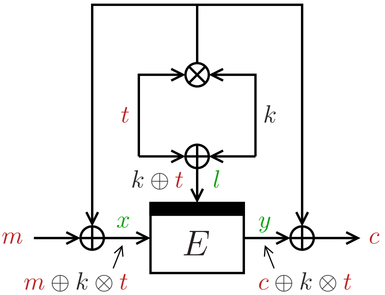
- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

$$k \oplus t = l \text{ and } m \oplus k \otimes t = x$$

or

$$k \oplus t = l \text{ and } c \oplus k \otimes t = y$$

One E-Call with Polynomial Mixing: Proof Idea



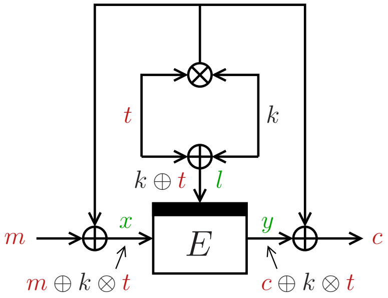
- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

$$k \oplus t = l \text{ and } m \oplus k \otimes t = x \iff k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

or

$$k \oplus t = l \text{ and } c \oplus k \otimes t = y \iff k = l \oplus t \text{ and } c \oplus (l \oplus t) \otimes t = y$$

One E-Call with Polynomial Mixing: Proof Idea



- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

$$k \oplus t = l \text{ and } m \oplus k \otimes t = x \iff \boxed{k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x}$$

$$\text{or} \qquad\qquad \text{or}$$

$$k \oplus t = l \text{ and } c \oplus k \otimes t = y \iff k = l \oplus t \text{ and } c \oplus (l \oplus t) \otimes t = y$$

One E-Call with Polynomial Mixing: Proof Idea

$k = l \oplus t$ and $m \oplus (l \oplus t) \otimes t = x$

One E-Call with Polynomial Mixing: Proof Idea

$$k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

Szemerédi-Trotter theorem [ST83]

Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ be a set of lines
- $P \subseteq \mathbb{F}^2$ be a set of points

point-line incidences $\leq \min\{|L|^{1/2}|P| + |L|, |L||P|^{1/2} + |P|\}$

One E-Call with Polynomial Mixing: Proof Idea

$$k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

Szemerédi-Trotter theorem [ST83]

Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ be a set of lines
- $P \subseteq \mathbb{F}^2$ be a set of points

point-line incidences $\leq \min\{|L|^{1/2}|P| + |L|, |L||P|^{1/2} + |P|\}$

- Construction queries = lines
- Primitive queries = points

One E-Call with Polynomial Mixing: Proof Idea

$$k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

Szemerédi-Trotter theorem [ST83]

Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ be a set of lines
- $P \subseteq \mathbb{F}^2$ be a set of points

point-line incidences $\leq \min\{|L|^{1/2}|P| + |L|, |L||P|^{1/2} + |P|\}$

- Construction queries = lines
- Primitive queries = points
- About $q^{3/2}$ solutions to $m \oplus (l \oplus t) \otimes t = x$

One E-Call with Polynomial Mixing: Proof Idea

$$k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

Szemerédi-Trotter theorem [ST83]

Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ be a set of lines
- $P \subseteq \mathbb{F}^2$ be a set of points

\# point-line incidences $\leq \min\{|L|^{1/2}|P| + |L|, |L||P|^{1/2} + |P|\}$

- Construction queries = lines
- Primitive queries = points
- About $q^{3/2}$ solutions to $m \oplus (l \oplus t) \otimes t = x$
- Every solution fixes one $l \oplus t$

One E-Call with Polynomial Mixing: Proof Idea

$$k = l \oplus t \text{ and } m \oplus (l \oplus t) \otimes t = x$$

Szemerédi-Trotter theorem [ST83]

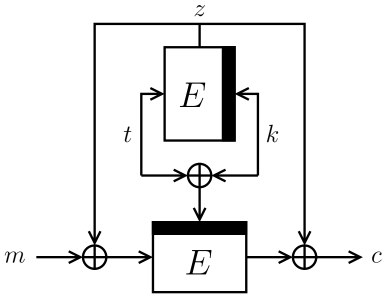
Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ be a set of lines
- $P \subseteq \mathbb{F}^2$ be a set of points

\# point-line incidences $\leq \min\{|L|^{1/2}|P| + |L|, |L||P|^{1/2} + |P|\}$

- Construction queries = lines
- Primitive queries = points
- About $q^{3/2}$ solutions to $m \oplus (l \oplus t) \otimes t = x$
- Every solution fixes one $l \oplus t$
- k is random n-bit key

Two E-Calls with Linear Mixing

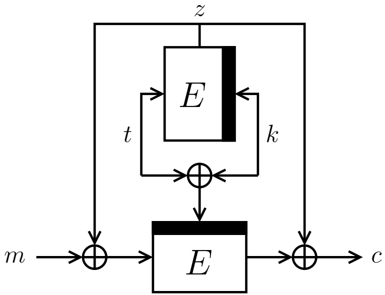


$\widetilde{F}[2](k,t,m) = c$

Idea

- Subkey $k \oplus t$
- Masking $E(k,t)$

Two E-Calls with Linear Mixing



$\widetilde{F}[2](k, t, m) = c$

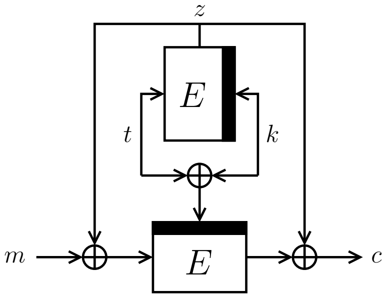
Idea

- Subkey $k \oplus t$
- Masking $E(k, t)$

Security

- Up to 2^n queries

Two E-Calls with Linear Mixing



$\widetilde{F}[2](k, t, m) = c$

Idea

- Subkey $k \oplus t$
- Masking $E(k, t)$

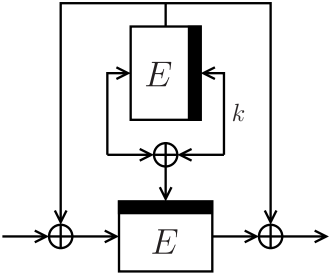
Security

- Up to 2^n queries

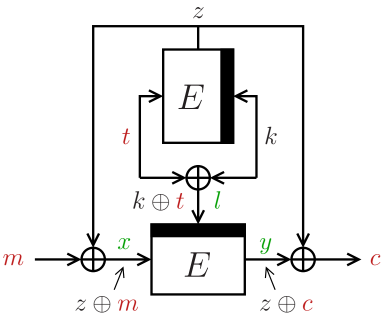
Cost

- Two E-calls
- Zero $\otimes$-evaluations
- One re-key

Two E-Calls with Linear Mixing: Proof Idea



Two E-Calls with Linear Mixing: Proof Idea



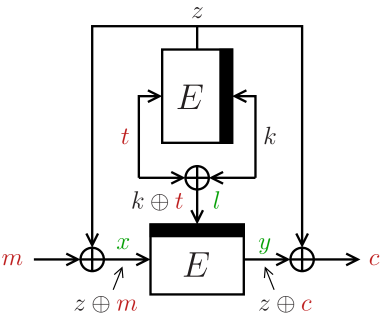
- Construction query (t, m, c) "hits" primitive query (l, x, y) if

$$k \oplus t = l \text{ and } z \oplus m = x$$

or

$$k \oplus t = l \text{ and } z \oplus c = y$$

Two E-Calls with Linear Mixing: Proof Idea



- Construction query (t, m, c) "hits" primitive query (l, x, y) if

$$k \oplus t = l \text{ and } z \oplus m = x$$
or
$$k \oplus t = l \text{ and } z \oplus c = y$$

- k is random key, z is almost-random subkey

Comparison

scheme	security ($\log_2$)	key length	cost		
			E	$\otimes/h$	tdk
LRW1	$n/2$	n	2	0	0
LRW2	$n/2$	$2n$	1	1	0
XEX	$n/2$	n	2	0	0
LRW2[2]	$2n/3$	$4n$	2	2	0
LRW2[ρ]	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ	0
Min	$\max\{n/2, n-\lvert t\rvert\}$	n	2	0	1
$\widetilde{F}[1]$	$2n/3$ *	n	1	1	1
$\widetilde{F}[2]$	n *	n	2	0	1

* Information-theoretic model

Towards Complexity-Theoretic Model

$\widetilde{F}[\alpha]$ with ideal cipher E

ideal tweakable cipher $\widetilde{\pi}$

current proof

Towards Complexity-Theoretic Model

$\widetilde{F}[\alpha]$ with any cipher E	$\widetilde{F}[\alpha]$ with ideal cipher E	ideal tweakable cipher $\widetilde{\pi}$

current proof

Towards Complexity-Theoretic Model

$$
\begin{tikzcd}
\boxed{\begin{array}{c}\widetilde{F}[\alpha] \text{ with} \\ \text{any cipher } E\end{array}} \arrow[r, bend right, "\text{security of } E"'] & \boxed{\begin{array}{c}\widetilde{F}[\alpha] \text{ with} \\ \text{ideal cipher } E\end{array}} \arrow[r, bend right, "\text{current proof}"'] & \boxed{\begin{array}{c}\text{ideal tweakable} \\ \text{cipher } \widetilde{\pi}\end{array}}
\end{tikzcd}
$$

Towards Complexity-Theoretic Model

$\widetilde{F}[\alpha]$ with any cipher E

$\widetilde{F}[\alpha]$ with ideal cipher E

ideal tweakable cipher $\widetilde{\pi}$

$\oplus$-rk security of E

current proof

Towards Complexity-Theoretic Model

$\widetilde{F}[\alpha]$ with any cipher E

$\widetilde{F}[\alpha]$ with ideal cipher E

ideal tweakable cipher $\widetilde{\pi}$

$\oplus$-rk security of E

current proof

- First step unnecessarily loose
- Tweak change influences key and message input
- Details in paper

Conclusions

$\widetilde{F}[1]$ and $\widetilde{F}[2]$

- Simple and few primitive calls
- High security level
- Efficient if key renewal is relatively cheap

Conclusions

$\widetilde{F}[1]$ and $\widetilde{F}[2]$

- Simple and few primitive calls
- High security level
- Efficient if key renewal is relatively cheap

Future Research

- One-call tweakable cipher with improved security?
- Avoiding related-key security condition?
- Implementations?

Conclusions

$\widetilde{F}[1]$ and $\widetilde{F}[2]$

- Simple and few primitive calls
- High security level
- Efficient if key renewal is relatively cheap

Future Research

- One-call tweakable cipher with improved security?
- Avoiding related-key security condition?
- Implementations?

Thank you for your attention!

SUPPORTING SLIDES

Generic Design: Inverse

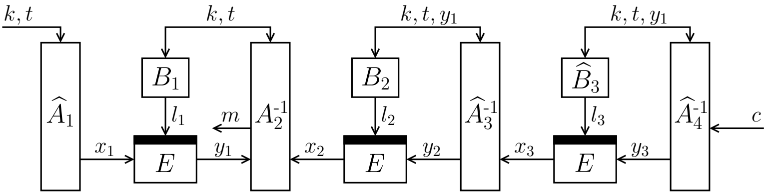
Valid Mixing Functions (informal)

A_i, B_i are valid if there is one A_{i^*} that processes m, s.t.

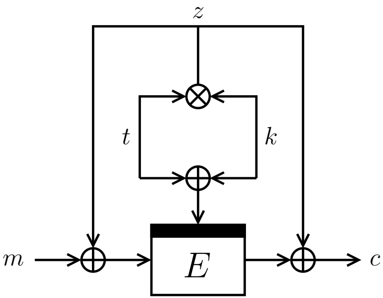
- first $i^* - 1$ rounds computable in forward direction
- last $\rho - (i^* - 1)$ rounds computable in inverse direction

both without usage of m

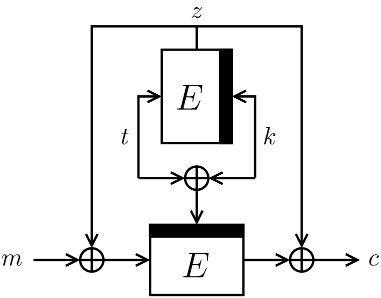
Example for $i^* = 2$



Both Designs on One Slide



$$\widetilde{F}[1](k, t, m) = c$$



$$\widetilde{F}[2](k, t, m) = c$$