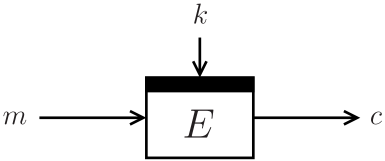
XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees

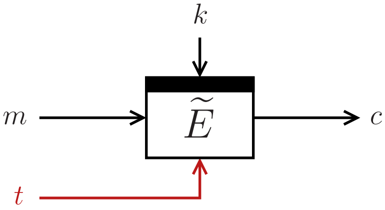
Bart Mennink
KU Leuven (Belgium)

ASK 2015
October 2, 2015

Tweakable Blockciphers

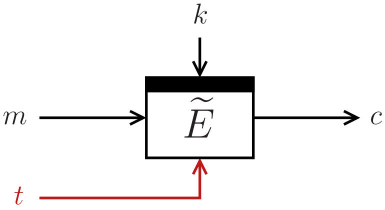


Tweakable Blockciphers



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

Tweakable Blockciphers



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

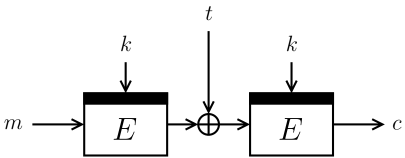
- Three approaches:
  - from scratch
  - from blockcipher
  - from permutation

Tweakable Blockciphers from Scratch

- Hasty Pudding Cipher [Sch98]
  - AES submission, "first tweakable cipher"
- Mercy [Cro01]
  - Disk encryption
- Threefish [FLS+07]
  - SHA-3 submission Skein
- TWEAKEY [JNP14]
  - CAESAR submissions Deoxys, Joltik, KIASU

Tweakable Blockciphers from Blockcipher

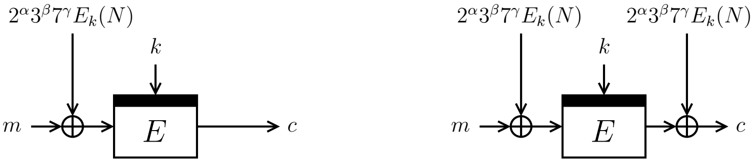
- LRW_1 and LRW_2 by Liskov et al. (2002):



- h is XOR-universal hash

Tweakable Blockciphers from Blockcipher

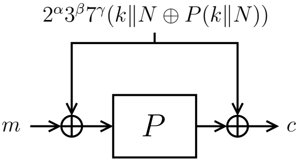
- XE and XEX by Rogaway (2004):



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

Tweakable Blockciphers from Permutation

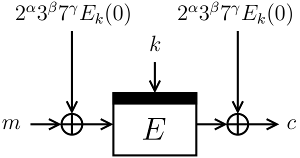
- Minalpher's TEM [STA+14]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

Tweakable Blockciphers from Permutation

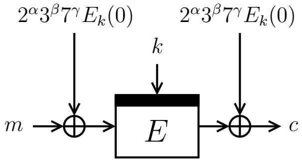
- Prøst [KLL+14] uses XE(X) with Even-Mansour:



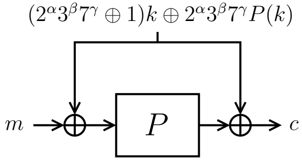
with $E_k(m) = P(m \oplus k) \oplus k$

Tweakable Blockciphers from Permutation

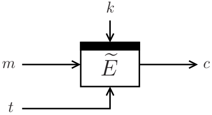
- Prøst [KLL+14] uses XE(X) with Even-Mansour:



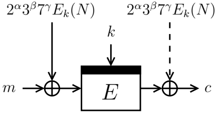
with $E_k(m) = P(m \oplus k) \oplus k$



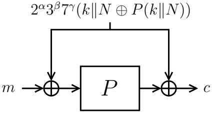
Tweakable Blockciphers in CAESAR



TWEAKEY

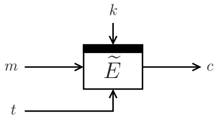


XE/XEX-inspired



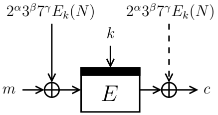
TEM-inspired

Tweakable Blockciphers in CAESAR



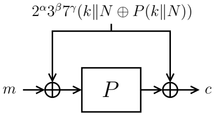
TWEAKEY

Deoxys,
Joltik,
KIASU



XE/XEX-inspired

AEZ, CBA, COBRA,
COPA, **ELmD**, iFeed,
Marble, **OCB**, **OMD**,
OTR, **POET**, **SHELL**

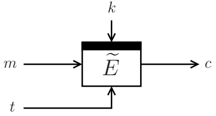


TEM-inspired

Minalpher,
Prøst

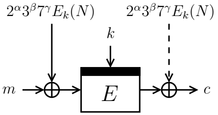
plain = first round, **bold = second round**

Tweakable Blockciphers in CAESAR



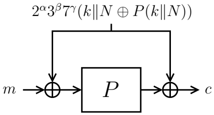
TWEAKEY

Deoxys, **Joltik**, KIASU



XE/XEX-inspired

AEZ, CBA, COBRA, **COPA**, **ELmD**, iFeed, Marble, **OCB**, **OMD**, **OTR**, **POET**, **SHELL**



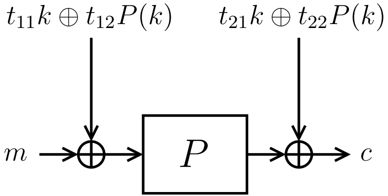
TEM-inspired

Minalpher, Prøst

We generalize this

plain = first round, **bold = second round**

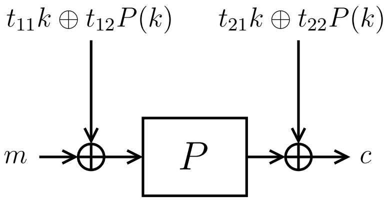
XPX



Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

XPX

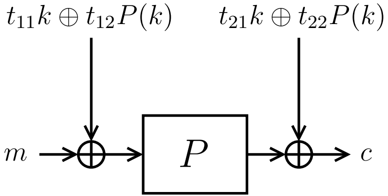


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

- Security of XPX strongly depends on choice of $\mathcal{T}$

XPX

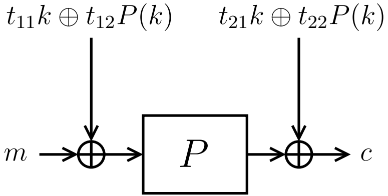


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

- Security of XPX strongly depends on choice of $\mathcal{T}$
  1. "Stupid" $\mathcal{T}$ $\longrightarrow$ insecure

XPX

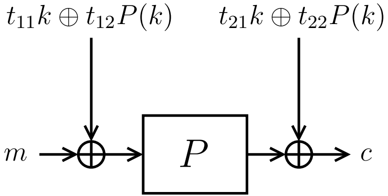


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

- Security of XPX strongly depends on choice of $\mathcal{T}$
  1. "Stupid" $\mathcal{T}$ $\longrightarrow$ insecure
  2. "Normal" $\mathcal{T}$ $\longrightarrow$ single-key secure

XPX

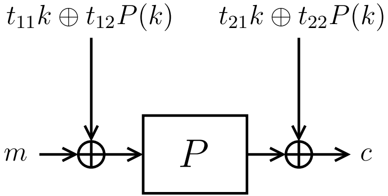


Tweak Set

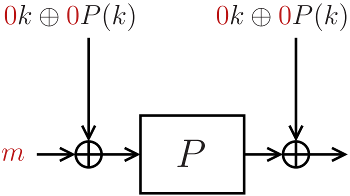
- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

- Security of XPX strongly depends on choice of $\mathcal{T}$
  1. "Stupid" $\mathcal{T}$ $\longrightarrow$ insecure
  2. "Normal" $\mathcal{T}$ $\longrightarrow$ single-key secure
  3. "Strong" $\mathcal{T}$ $\longrightarrow$ related-key secure

XPX: Valid Tweaks

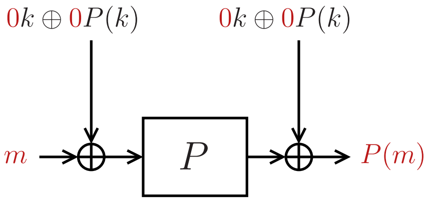


XPX: Valid Tweaks



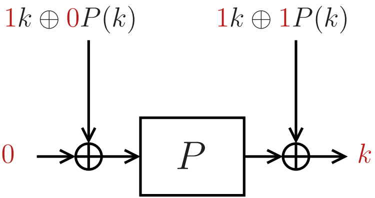
$(0, 0, 0, 0) \in \mathcal{T}$

XPX: Valid Tweaks



$$(0,0,0,0) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m)$$

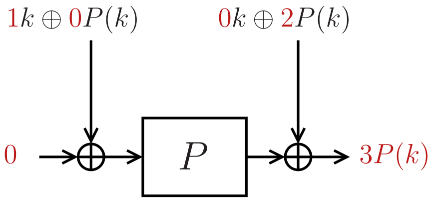
XPX: Valid Tweaks



$$(0,0,0,0) \in \mathcal{T} \implies \mathsf{XPX}_k((0,0,0,0),m) = P(m)$$

$$(1,0,1,1) \in \mathcal{T} \implies \mathsf{XPX}_k((1,0,1,1),0) = k$$

XPX: Valid Tweaks

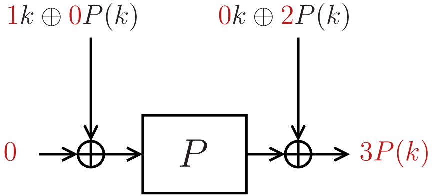


$$(0,0,0,0) \in \mathcal{T} \implies \mathsf{XPX}_k((0,0,0,0),m) = P(m)$$

$$(1,0,1,1) \in \mathcal{T} \implies \mathsf{XPX}_k((1,0,1,1),0) = k$$

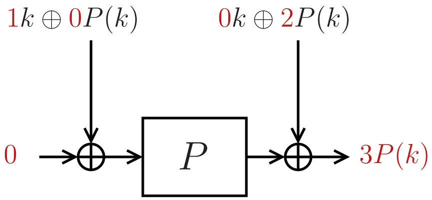
$$(1,0,0,2) \in \mathcal{T} \implies \mathsf{XPX}_k((1,0,0,2),0) = 3P(k)$$

XPX: Valid Tweaks



$$
\begin{aligned}
(0,0,0,0) \in \mathcal{T} &\implies \mathsf{XPX}_k((0,0,0,0),m) = P(m)\\
(1,0,1,1) \in \mathcal{T} &\implies \mathsf{XPX}_k((1,0,1,1),0) = k\\
(1,0,0,2) \in \mathcal{T} &\implies \mathsf{XPX}_k((1,0,0,2),0) = 3P(k)\\
\dots \quad &\dots \quad \dots
\end{aligned}
$$

XPX: Valid Tweaks

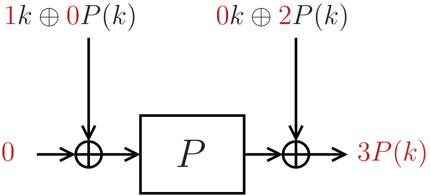


$$\begin{aligned}
(0,0,0,0) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m) \\
(1,0,1,1) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,1,1),0) = k \\
(1,0,0,2) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,0,2),0) = 3P(k) \\
\ldots \quad & \quad \ldots \quad \ldots
\end{aligned}$$

“Valid” Tweak Sets

- Technical definition to eliminate trivial cases

XPX: Valid Tweaks



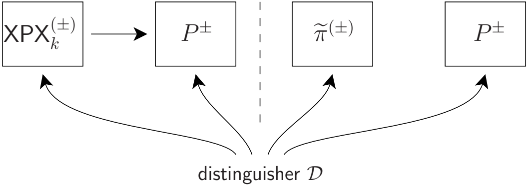
$$
\begin{aligned}
(0,0,0,0) \in \mathcal{T} &\implies \mathsf{XPX}_k((0,0,0,0),m) = P(m) \\
(1,0,1,1) \in \mathcal{T} &\implies \mathsf{XPX}_k((1,0,1,1),0) = k \\
(1,0,0,2) \in \mathcal{T} &\implies \mathsf{XPX}_k((1,0,0,2),0) = 3P(k) \\
\dots \quad &\quad \dots \quad \dots
\end{aligned}
$$

"Valid" Tweak Sets

- Technical definition to eliminate trivial cases
- Proven to be minimal: $\mathcal{T}$ invalid $\Rightarrow$ XPX insecure

XPX: Single-Key Security

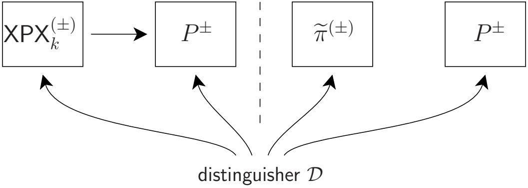
(Strong) Tweakable PRP



- Information-theoretic indistinguishability
  - $\widetilde{\pi}$ ideal tweakable permutation
  - P ideal permutation
  - k secret key

XPX: Single-Key Security

(Strong) Tweakable PRP

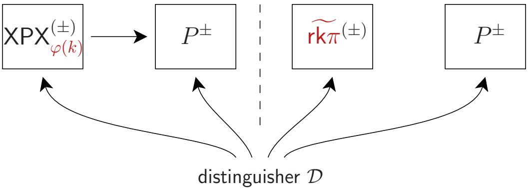


- Information-theoretic indistinguishability
  - $\widetilde{\pi}$ ideal tweakable permutation
  - P ideal permutation
  - k secret key

$$\mathcal{T} \text{ is valid} \quad \Longrightarrow \quad \text{XPX is (S)TPRP up to } \mathcal{O}\left(\frac{q^2+qr}{2^n}\right)$$

XPX: Related-Key Security

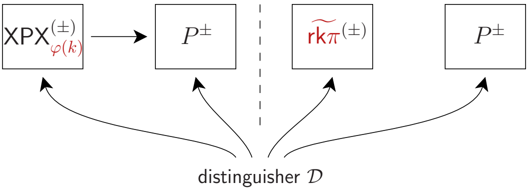
Related-Key (Strong) Tweakable PRP



- Information-theoretic indistinguishability
  - $\widetilde{\mathsf{rk}\pi}$ ideal tweakable related-key permutation
  - P ideal permutation
  - k secret key

XPX: Related-Key Security

Related-Key (Strong) Tweakable PRP



- Information-theoretic indistinguishability
  - $\widetilde{\mathsf{rk}\pi}$ ideal tweakable related-key permutation
  - P ideal permutation
  - k secret key

- $\mathcal{D}$ restricted to some set of key-deriving functions Φ

XPX: Related-Key Security

Key-Deriving Functions (Informal)

- $\Phi_{\oplus}$: all functions $k \mapsto k \oplus \delta$

XPX: Related-Key Security

Key-Deriving Functions (Informal)

- $\Phi_{\oplus}$: all functions $k \mapsto k \oplus \delta$
- $\Phi_{P\oplus}$: all functions $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$

XPX: Related-Key Security

Key-Deriving Functions (Informal)

- $\Phi_{\oplus}$: all functions $k \mapsto k \oplus \delta$
- $\Phi_{P\oplus}$: all functions $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$
- Note: maskings in XPX are $t_{i1}k \oplus t_{i2}P(k)$

XPX: Related-Key Security

Key-Deriving Functions (Informal)

- $\Phi_\oplus$: all functions $k \mapsto k \oplus \delta$
- $\Phi_{P\oplus}$: all functions $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$
- Note: maskings in XPX are $t_{i1}k \oplus t_{i2}P(k)$

Results

if $\mathcal{T}$ is valid, and for all tweaks:	security	Φ
$t_{12} \neq 0$	TPRP	$\Phi_\oplus$
$t_{12}, t_{22} \neq 0$ and $(t_{21}, t_{22}) \neq (0, 1)$	STPRP	$\Phi_\oplus$

XPX: Related-Key Security

Key-Deriving Functions (Informal)

- $\Phi_{\oplus}$: all functions $k \mapsto k \oplus \delta$
- $\Phi_{P\oplus}$: all functions $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$
- Note: maskings in XPX are $t_{i1}k \oplus t_{i2}P(k)$

Results

if $\mathcal{T}$ is valid, and for all tweaks:	security	Φ
$t_{12} \neq 0$	TPRP	$\Phi_{\oplus}$
$t_{12}, t_{22} \neq 0$ and $(t_{21}, t_{22}) \neq (0, 1)$	STPRP	$\Phi_{\oplus}$
$t_{11}, t_{12} \neq 0$	TPRP	$\Phi_{P\oplus}$
$t_{11}, t_{12}, t_{21}, t_{22} \neq 0$	STPRP	$\Phi_{P\oplus}$

XPX: Security Proof Techniques

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

XPX: Security Proof Techniques

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

$$\mathbf{Adv}_{\mathsf{XPX}}^{\text{rk-(s)prp}}(\mathcal{D}) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } (\widetilde{\mathsf{rk}\pi}, P)\right]$$

↰ prob. ratio for good transcripts

XPX: Security Proof Techniques

Patarin's H-coefficient Technique

- Each conversation defines a transcript
- Define good and bad transcripts

$$\mathbf{Adv}_{\mathsf{XPX}}^{\text{rk-(s)prp}}(\mathcal{D}) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } (\widetilde{\mathsf{rk}\pi}, P)\right]$$

↰ prob. ratio for good transcripts

- Trade-off: define bad transcripts smartly!

XPX: Security Proof Techniques

Before the Interaction

- Reveal dedicated construction queries

After the Interaction

- Reveal key information
  - Single-key: k and $P(k)$
  - $\Phi_{\oplus}$-related-key: k and $P(k \oplus \delta)$
  - $\Phi_{P\oplus}$-related-key: k and $P(k \oplus \delta)$ and $P^{-1}(P(k) \oplus \varepsilon)$

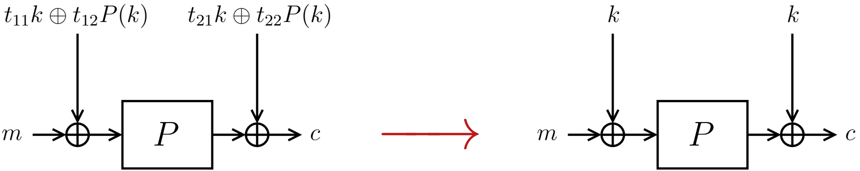
Bounding the Advantage

- Smart definition of bad transcripts

XPX Covers Even-Mansour

for $\mathcal{T} = \{(1, 0, 1, 0)\}$

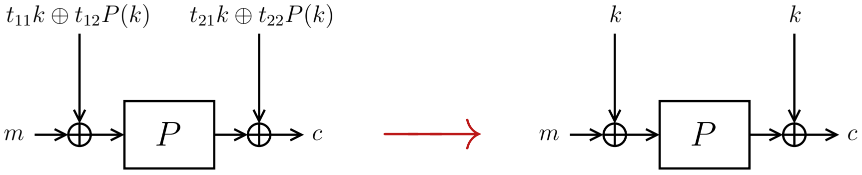
XPX Covers Even-Mansour



for $\mathcal{T} = \{(1,0,1,0)\}$

- Single-key STPRP secure (surprise?)

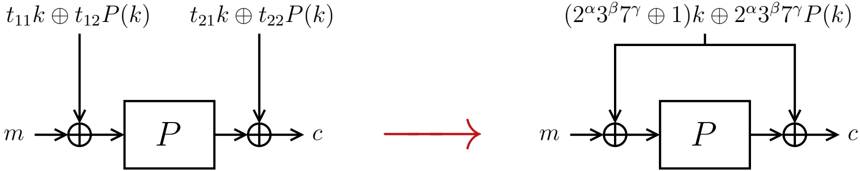
XPX Covers Even-Mansour



for $\mathcal{T} = \{(1,0,1,0)\}$

- Single-key STPRP secure (surprise?)
- Generally, if $|\mathcal{T}| = 1$, XPX is a normal blockcipher

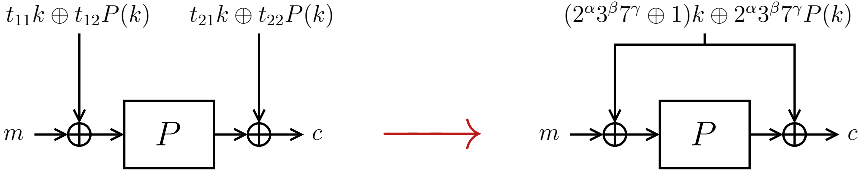
XPX Covers XEX With Even-Mansour



$$\text{for } \mathcal{T} = \left\{ \begin{array}{l} (\,2^\alpha 3^\beta 7^\gamma \oplus 1\,,\, 2^\alpha 3^\beta 7^\gamma\,, \\ \;\; 2^\alpha 3^\beta 7^\gamma \oplus 1\,,\, 2^\alpha 3^\beta 7^\gamma\,) \end{array} \;\middle|\; (\alpha, \beta, \gamma) \in \{\text{XEX-tweaks}\} \right\}$$

- (α, β, γ) is in fact the "real" tweak

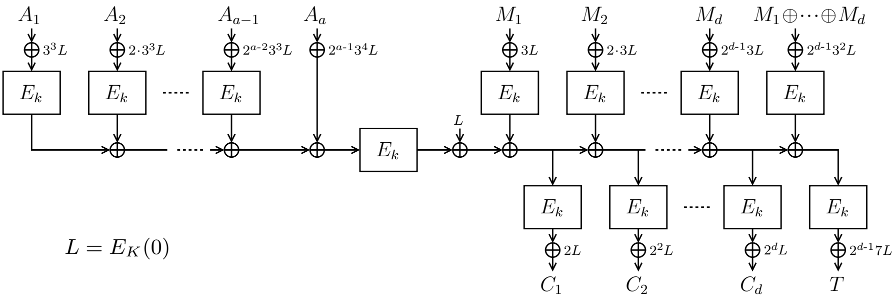
XPX Covers XEX With Even-Mansour



for $\mathcal{T} = \left\{ \begin{array}{l} (2^\alpha 3^\beta 7^\gamma \oplus 1\,,\, 2^\alpha 3^\beta 7^\gamma\,, \\ \;2^\alpha 3^\beta 7^\gamma \oplus 1\,,\, 2^\alpha 3^\beta 7^\gamma\,) \end{array} \;\middle|\; (\alpha, \beta, \gamma) \in \{\text{XEX-tweaks}\} \right\}$

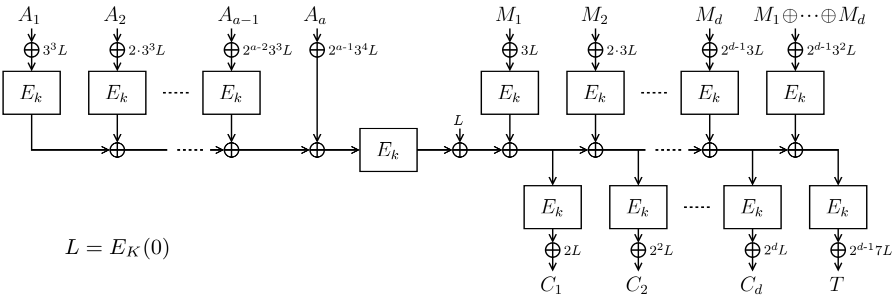
- (α, β, γ) is in fact the "real" tweak
- $\Phi_{P\oplus}$-related-key STPRP secure (if $2^\alpha 3^\beta 7^\gamma \neq 1$)

Application to AE: COPA



- By Andreeva et al. (2014)
- Implicitly based on XEX based on AES

Application to AE: COPA



- By Andreeva et al. (2014)
- Implicitly based on XEX based on AES

- Prøst-COPA by Kavun et al. (2014):
  COPA based on XEX based on Even-Mansour

Application to AE: COPA

Single-Key Security of COPA

$$\boxed{\text{COPA}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E}$$

Application to AE: COPA

Single-Key Security of COPA

$$\boxed{\text{COPA}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E}$$

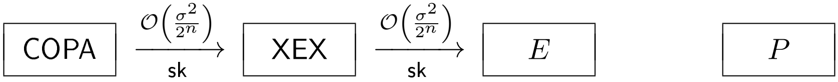
Related-Key Security of COPA

- Approach generalizes for any Φ (proof in paper)

$$\boxed{\text{COPA}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E}$$

Application to AE: Prøst-COPA

Single-Key Security of Prøst-COPA



Application to AE: Prøst-COPA

Single-Key Security of Prøst-COPA

$$\boxed{\text{COPA}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application to AE: Prøst-COPA

Single-Key Security of Prøst-COPA

$$\boxed{\text{COPA}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Related-Key Security of Prøst-COPA

$$\boxed{\text{COPA}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E} \qquad \boxed{P}$$

Application to AE: Prøst-COPA

Single-Key Security of Prøst-COPA

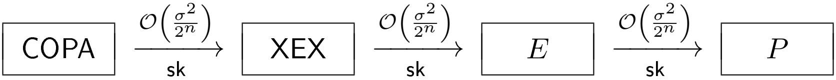
$$\boxed{\text{COPA}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Related-Key Security of Prøst-COPA

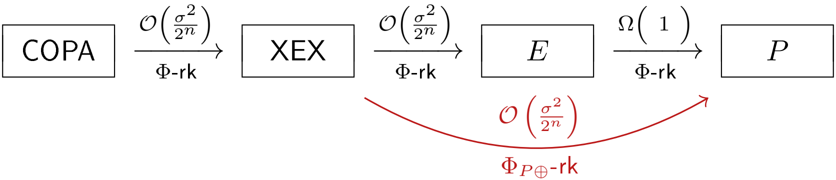
$$\boxed{\text{COPA}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XEX}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E} \xrightarrow[\Phi\text{-rk}]{\Omega\left(\ 1\ \right)} \boxed{P}$$

Application to AE: Prøst-COPA

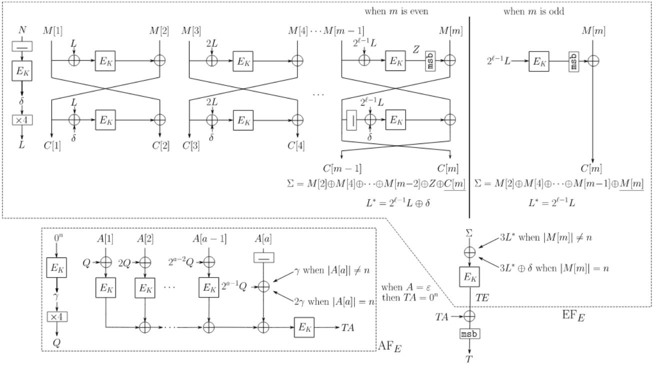
Single-Key Security of Prøst-COPA



Related-Key Security of Prøst-COPA

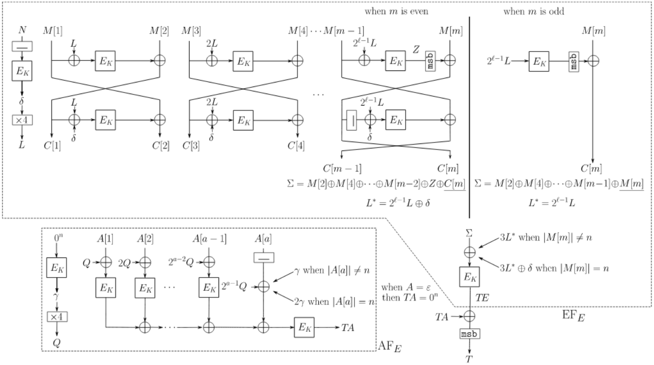


Application to AE: Prøst-OTR



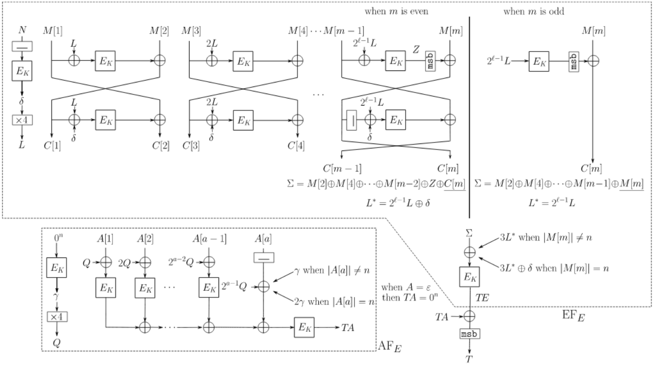
- Prøst-OTR by Kavun et al. (2014):
  OTR based on XE based on Even-Mansour

Application to AE: Prøst-OTR



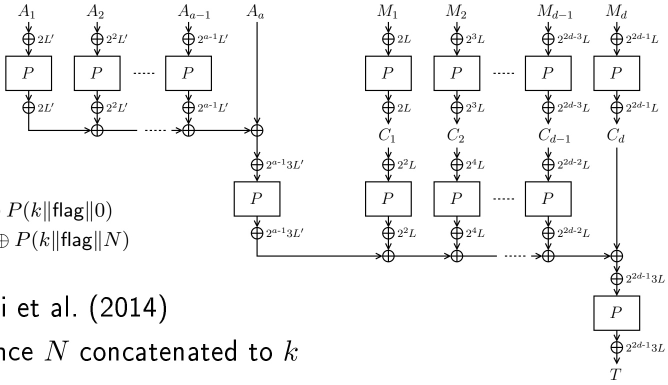
- Prøst-OTR by Kavun et al. (2014):
  OTR based on XE based on Even-Mansour
- Dobraunig et al. (2015): related-key attack on Prøst-OTR

Application to AE: Prøst-OTR



- Prøst-OTR by Kavun et al. (2014):
  OTR based on XE based on Even-Mansour
- Dobraunig et al. (2015): related-key attack on Prøst-OTR
- Nonce-based masking: $t_{11}k \oplus t_{11}P(k \oplus N)$

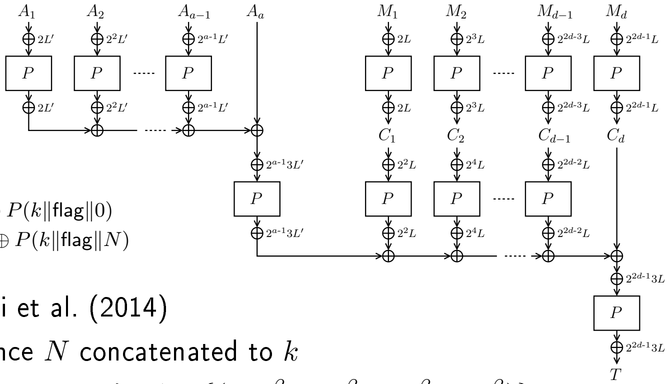
Application to AE: Minalpher



$$L' = k\|\mathsf{flag}\|0 \oplus P(k\|\mathsf{flag}\|0)$$
$$L \ = k\|\mathsf{flag}\|N \oplus P(k\|\mathsf{flag}\|N)$$

- By Sasaki et al. (2014)
- Extra nonce N concatenated to k

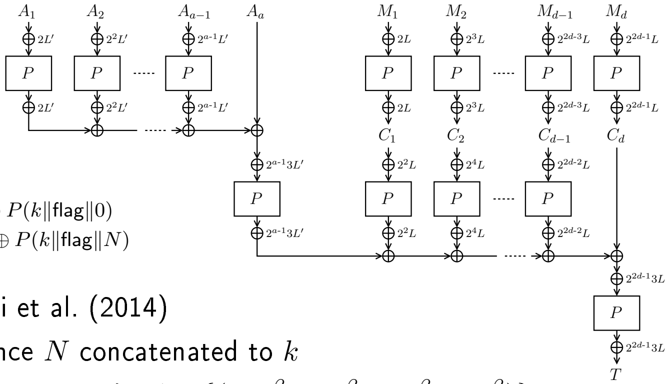
Application to AE: Minalpher



$$L' = k\|\text{flag}\|0 \oplus P(k\|\text{flag}\|0)$$
$$L = k\|\text{flag}\|N \oplus P(k\|\text{flag}\|N)$$

- By Sasaki et al. (2014)
- Extra nonce N concatenated to k
- Based on XPX with $\mathcal{T} = \{(2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta)\}$

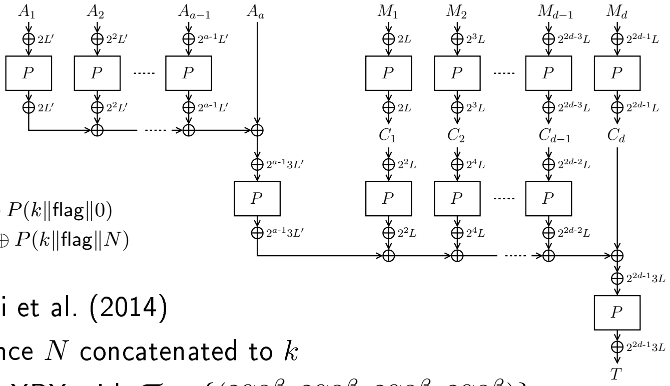
Application to AE: Minalpher



$L' = k\|\mathsf{flag}\|0 \oplus P(k\|\mathsf{flag}\|0)$
$L \;= k\|\mathsf{flag}\|N \oplus P(k\|\mathsf{flag}\|N)$

- By Sasaki et al. (2014)
- Extra nonce N concatenated to k
- Based on XPX with $\mathcal{T} = \{(2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta)\}$

Application to AE: Minalpher

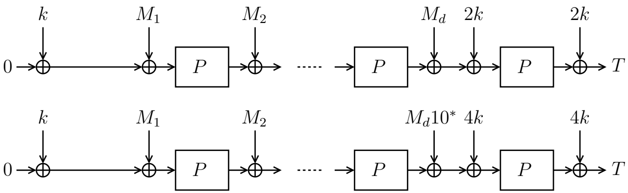


$L' = k\|\text{flag}\|0 \oplus P(k\|\text{flag}\|0)$

$L = k\|\text{flag}\|N \oplus P(k\|\text{flag}\|N)$

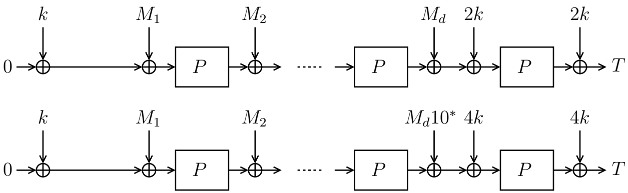
- By Sasaki et al. (2014)
- Extra nonce N concatenated to k
- Based on XPX with $\mathcal{T} = \{(2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta)\}$

Application to MAC: Chaskey



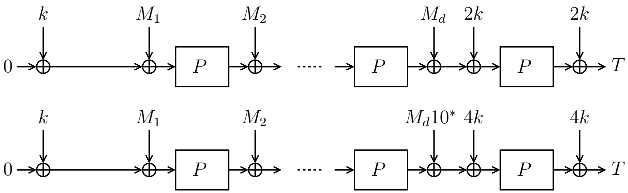
- By Mouha et al. (2014)
- Original proof based on 3 EM's: $\begin{cases} E_k(m) = P(m \oplus k) \oplus k \\ E_k(m) = P(m \oplus 3k) \oplus 2k \\ E_k(m) = P(m \oplus 5k) \oplus 4k \end{cases}$

Application to MAC: Chaskey



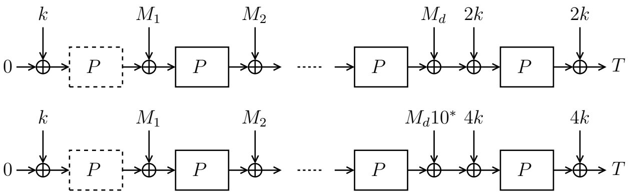
- By Mouha et al. (2014)
- Original proof based on 3 EM's: $\begin{cases} E_k(m) = P(m \oplus k) \oplus k \\ E_k(m) = P(m \oplus 3k) \oplus 2k \\ E_k(m) = P(m \oplus 5k) \oplus 4k \end{cases}$
- Equivalent to XPX with $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

Application to MAC: Chaskey



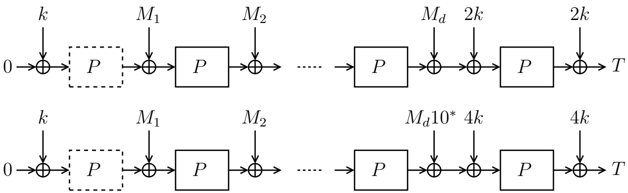
- By Mouha et al. (2014)
- Original proof based on 3 EM's: $\begin{cases} E_k(m) = P(m \oplus k) \oplus k \\ E_k(m) = P(m \oplus 3k) \oplus 2k \\ E_k(m) = P(m \oplus 5k) \oplus 4k \end{cases}$
- Equivalent to XPX with $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

Application to MAC: Adjusted Chaskey



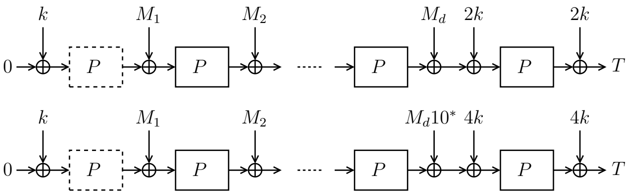
- Extra P-call

Application to MAC: Adjusted Chaskey



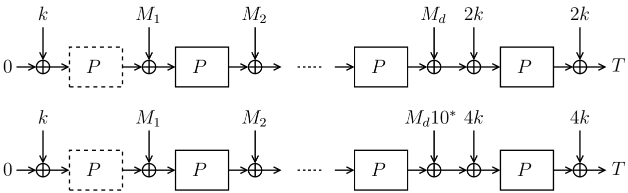
- Extra P-call
- Based on XPX with $\mathcal{T}' = \{(0,1,0,1),(2,1,2,0),(4,1,4,0)\}$

Application to MAC: Adjusted Chaskey



- Extra P-call
- Based on XPX with $\mathcal{T}' = \{(0,1,0,1),(2,1,2,0),(4,1,4,0)\}$

Application to MAC: Adjusted Chaskey



- Extra P-call
- Based on XPX with $\mathcal{T}' = \{(0,1,0,1),(2,1,2,0),(4,1,4,0)\}$

- Approach also applies to Keyed Sponges

Security Beyond Birthday Bound?

- All results so far: up to birthday bound

Security Beyond Birthday Bound?

- All results so far: up to birthday bound
- Security of AE's is mostly dominated by security of $\widetilde{E}$

Security Beyond Birthday Bound?

- All results so far: up to birthday bound

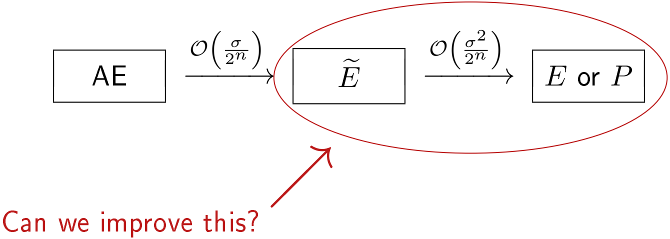
- Security of AE's is mostly dominated by security of $\widetilde{E}$
- For some AE's (e.g., OCB, pOMD, ...):

$$\boxed{\text{AE}} \xrightarrow{\mathcal{O}\left(\frac{\sigma}{2^n}\right)} \boxed{\widetilde{E}} \xrightarrow{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{E \text{ or } P}$$

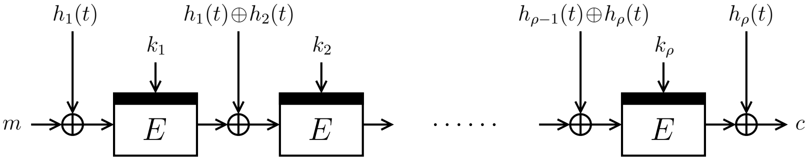
Security Beyond Birthday Bound?

- All results so far: up to birthday bound

- Security of AE's is mostly dominated by security of $\widetilde{E}$
- For some AE's (e.g., OCB, pOMD, . . .):

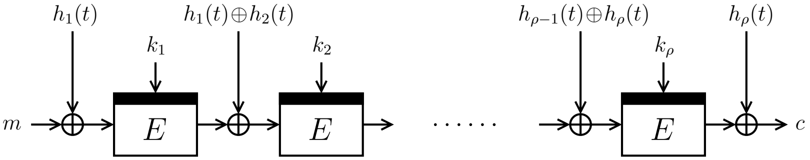


BBB Tweakable Blockciphers from Blockcipher



- $\text{LRW}_2[\rho]$: concatenation of ρ LRW_2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

BBB Tweakable Blockciphers from Blockcipher

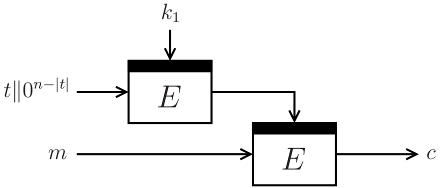


- $\mathsf{LRW}_2[\rho]$: concatenation of ρ LRW_2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

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

BBB Tweakable Blockciphers from Blockcipher

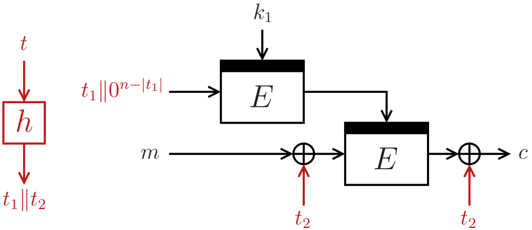
- Minematsu [Min09]:



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

BBB Tweakable Blockciphers from Blockcipher

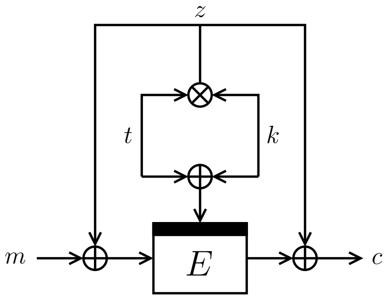
- Minematsu [Min09]:



- Secure up to $\max\{2^{n/2}, 2^{n-|t|}\}$ queries
- Beyond birthday bound for $|t| < n/2$
- Tweak-length extension possible by recent XTX [MI09]

BBB Tweakable Blockciphers from Blockcipher

- Mennink [Men15]:



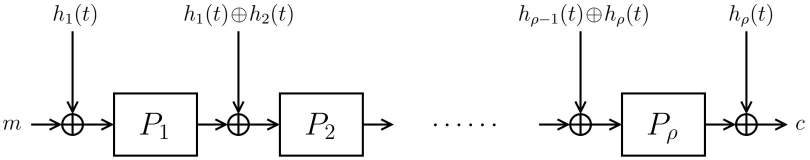
Secure up to $2^{2n/3}$ queries

(one $\otimes$, one E)

Secure up to 2^n queries

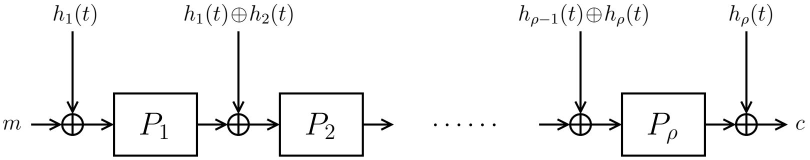
(two E's)

BBB Tweakable Blockciphers from Permutation



- TEM$[\rho]$: concatenation of ρ TEM-like's
- $P_1, \ldots, P_\rho$ and $h_1, \ldots, h_\rho$ independent

BBB Tweakable Blockciphers from Permutation



- TEM$[\rho]$: concatenation of ρ TEM-like's
- $P_1, \ldots, P_\rho$ and $h_1, \ldots, h_\rho$ independent

- $\rho = 2$: secure up to $2^{2n/3}$ queries [CLS15]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [CLS15]

Conclusions

XPX

- Generalized tweakable Even-Mansour
- Various levels of security
  - Single-key to related-key
- Many applications to AE and MAC

Optimal Secure AE?

- AE with cascaded LRW_2 or TEM: $2^{\rho n/(\rho+2)}$ security,
  but using ρ calls to E/P
- AE with Men_2: 2^n security,
  using 2 calls but ICM security proof

Conclusions

XPX

- Generalized tweakable Even-Mansour
- Various levels of security
  - Single-key to related-key
- Many applications to AE and MAC

Optimal Secure AE?

- AE with cascaded LRW_2 or TEM: $2^{\rho n/(\rho+2)}$ security,
  but using ρ calls to E/P
- AE with Men_2: 2^n security,
  using 2 calls but ICM security proof

Thank you for your attention!