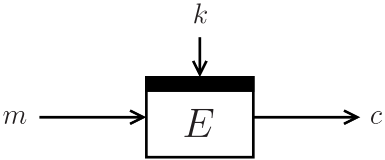
XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees

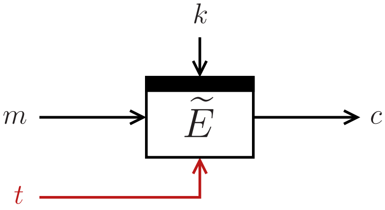
Bart Mennink
KU Leuven (Belgium)

CRYPTO 2016
August 15, 2016

Tweakable Blockciphers

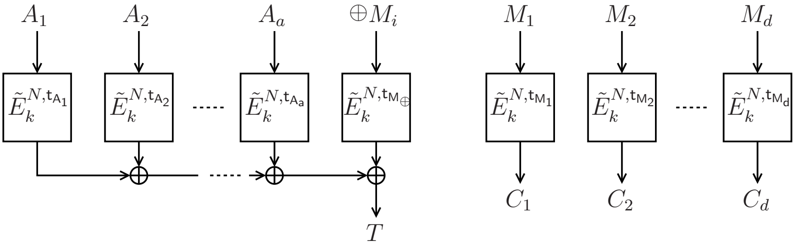


Tweakable Blockciphers



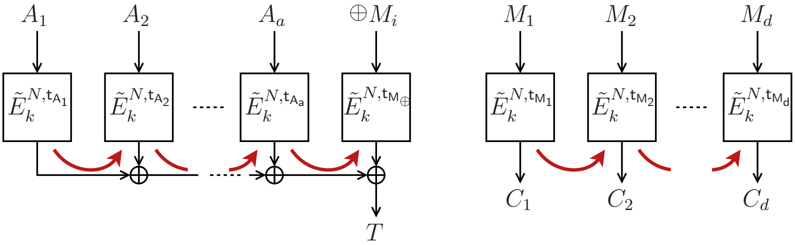
- Tweak: flexibility to the cipher
- Each tweak gives different permutation

Tweakable Blockciphers in OCBx



- OCBx by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak $(N, \text{position})$ is unique for every evaluation
  - Different blocks always transformed under different tweak

Tweakable Blockciphers in OCBx



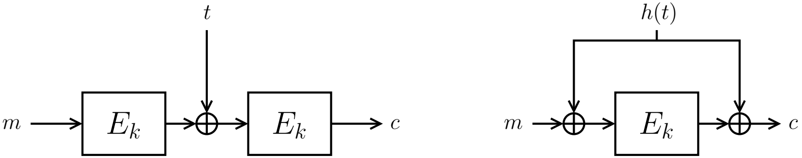
- OCBx by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak $(N, \text{position})$ is unique for every evaluation
  - Different blocks always transformed under different tweak
- Change of tweak should be efficient

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

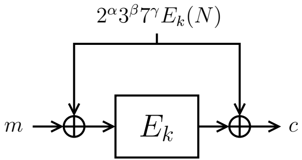
- LRW_1 and LRW_2 by Liskov et al. (2002):



- h is XOR-universal hash

Tweakable Blockciphers from Blockcipher

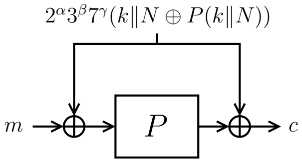
- XEX by Rogaway (2004):



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and in about 14 CAESAR submissions

Tweakable Blockciphers from Permutation

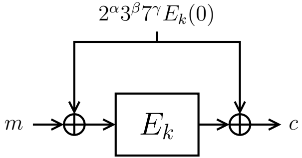
- Tweakable Even-Mansour (TEM):



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Introduced in CAESAR candidate Minalpher (2014)
- Generalized by Cogliati et al. (2015)

Tweakable Blockciphers from Permutation

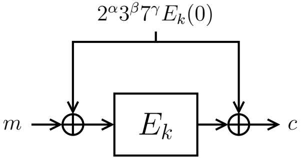
- Related to XEX with Even-Mansour:



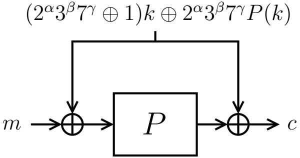
with $E_k(m) = P(m \oplus k) \oplus k$

Tweakable Blockciphers from Permutation

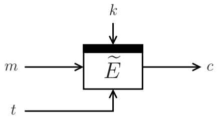
- Related to XEX with Even-Mansour:



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

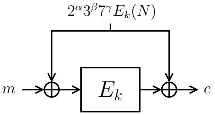


Tweakable Blockciphers in CAESAR



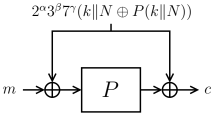
Dedicated

Deoxys,
Joltik,
KIASU,
SCREAM



XEX-inspired

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

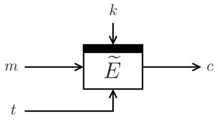


TEM-inspired

Minalpher,
Prøst

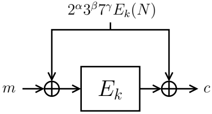
plain = first round, **bold** = **second round**

Tweakable Blockciphers in CAESAR



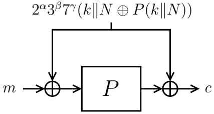
Dedicated

Deoxys,
Joltik,
KIASU,
SCREAM



XEX-inspired

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



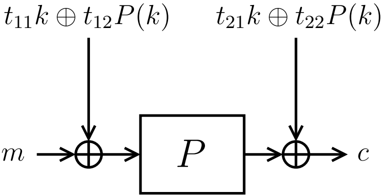
TEM-inspired

Minalpher,
Prøst

We generalize this

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

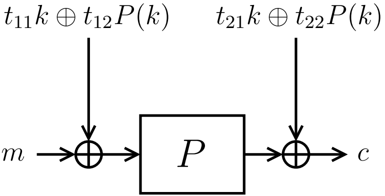
XPX



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

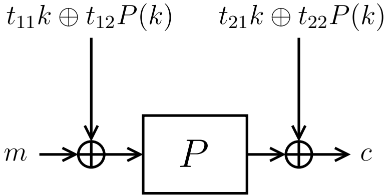


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ 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

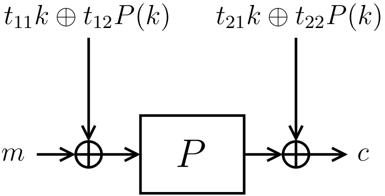


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ 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. "Weak" $\mathcal{T}$ $\longrightarrow$ insecure

XPX

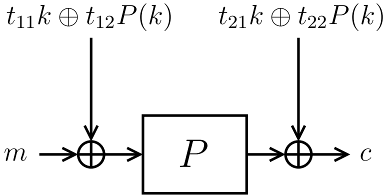


Tweak Set

- $(t_{11}, t_{12}, t_{21}, t_{22})$ 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. "Weak" $\mathcal{T}$ $\longrightarrow$ insecure
  2. "Normal" $\mathcal{T}$ $\longrightarrow$ single-key secure

XPX

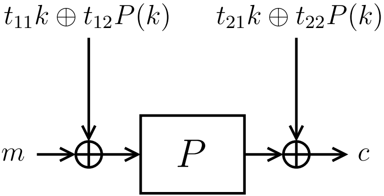


Tweak Set

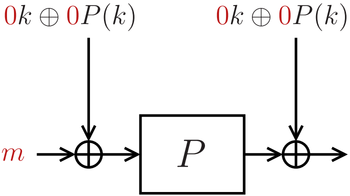
- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

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

XPX: Valid Tweaks

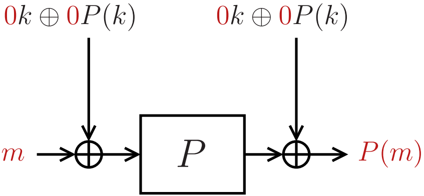


XPX: Valid Tweaks



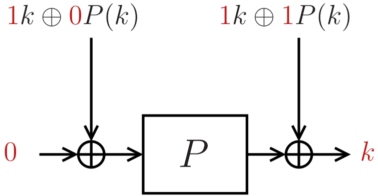
$(0, 0, 0, 0) \in \mathcal{T}$

XPX: Valid Tweaks



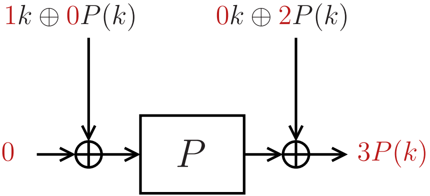
$$(0, 0, 0, 0) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((0, 0, 0, 0), m) = P(m)$$

XPX: Valid Tweaks



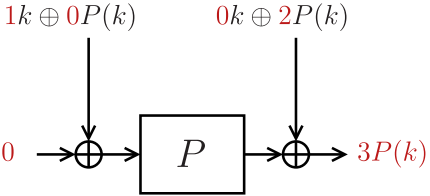
$$(0,0,0,0) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m)$$
$$(1,0,1,1) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((1,0,1,1),0) = k$$

XPX: Valid Tweaks



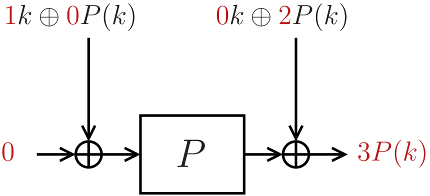
$$
\begin{aligned}
(0,0,0,0) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m) \\
(1,0,1,1) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,1,1),0) = k \\
(1,0,0,2) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,0,2),0) = 3P(k)
\end{aligned}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

XPX: Valid Tweaks



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

XPX: Valid Tweaks

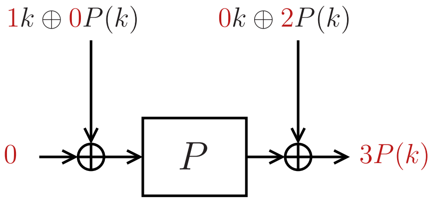


$$
\begin{array}{ccc}
(0,0,0,0) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((0,0,0,0), m) = P(m) \\
(1,0,1,1) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((1,0,1,1), 0) = k \\
(1,0,0,2) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((1,0,0,2), 0) = 3P(k) \\
\ldots & \ldots & \ldots
\end{array}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

"Valid" Tweak Sets

- Technical definition to eliminate weak cases

XPX: Valid Tweaks



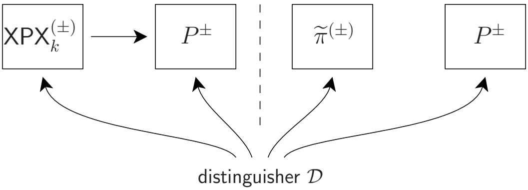
$$\begin{array}{ccc}
(0,0,0,0) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((0,0,0,0),m) = P(m) \\
(1,0,1,1) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((1,0,1,1),0) = k \\
(1,0,0,2) \in \mathcal{T} & \Longrightarrow & \mathsf{XPX}_k((1,0,0,2),0) = 3P(k) \\
\cdots & \cdots & \cdots
\end{array}$$

"Valid" Tweak Sets

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

XPX: Single-Key Security

(Strong) Tweakable PRP

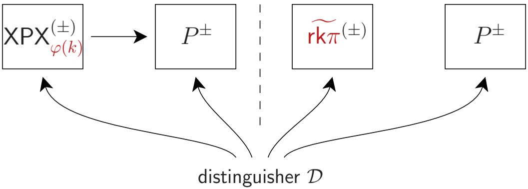


- Information-theoretic indistinguishability
  - $\widetilde{\pi}$ ideal tweakable permutation
  - P ideal permutation
  - k secret key

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

XPX: Related-Key Security

Related-Key (Strong) Tweakable PRP



- Information-theoretic indistinguishability
  - $\widetilde{\text{rk}\pi}$ 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

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

XPX: Related-Key Security

Key-Deriving Functions

- $\Phi_{\oplus}$: 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

- $\Phi_{\oplus}$: 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

- $\Phi_{\oplus}$: 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

- $\Phi_{\oplus}$: 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 $t_{i1}k \oplus t_{i2}P(k)$

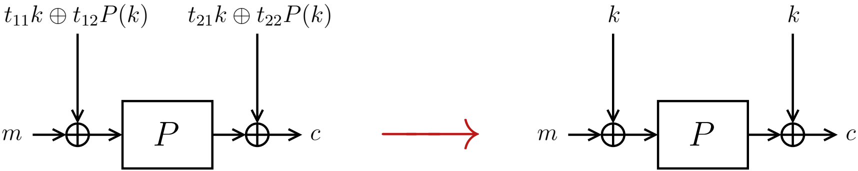
Results

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 Covers Even-Mansour

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

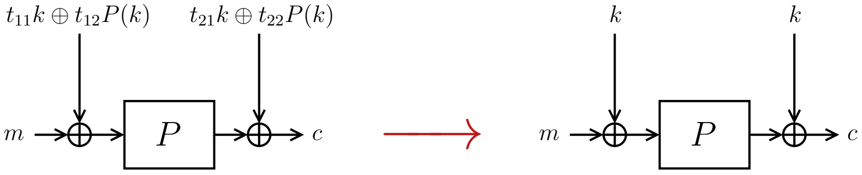
XPX Covers Even-Mansour



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

- Single-key STPRP secure (surprise?)

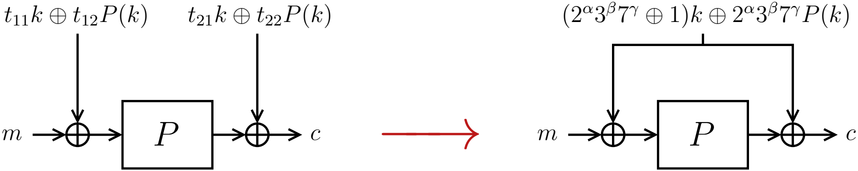
XPX Covers Even-Mansour



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

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

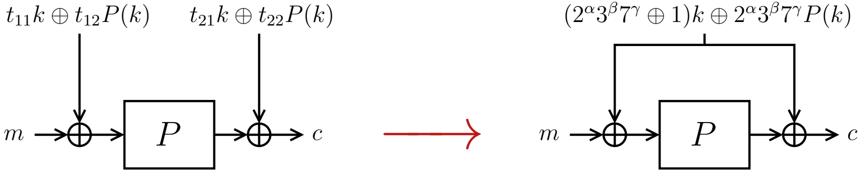
XPX Covers XEX With Even-Mansour



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

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

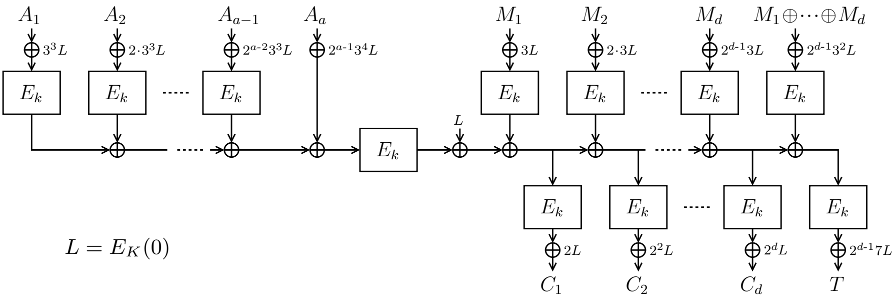
XPX Covers XEX With Even-Mansour



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

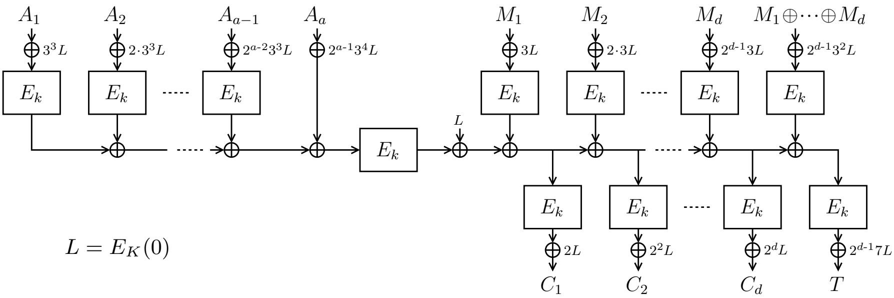
- (α, β, γ) is in fact the "real" tweak
- $\Phi_{P\oplus}$-related-key STPRP secure (if $2^\alpha 3^\beta 7^\gamma \neq 1$)

Application to AE: COPA and Prøst-COPA



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

Application to AE: COPA and Prøst-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 and Prøst-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 and Prøst-COPA

Single-Key Security of Prøst-COPA

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

Application to AE: COPA and 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: COPA and 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 COPA

- Existing proof generalizes for any Φ

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

Application to AE: COPA and 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

- Existing proof generalizes for any Φ

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

Application to AE: COPA and 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

- Existing proof generalizes for any Φ

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

Application to AE: COPA and Prøst-COPA

Single-Key Security of Prøst-COPA

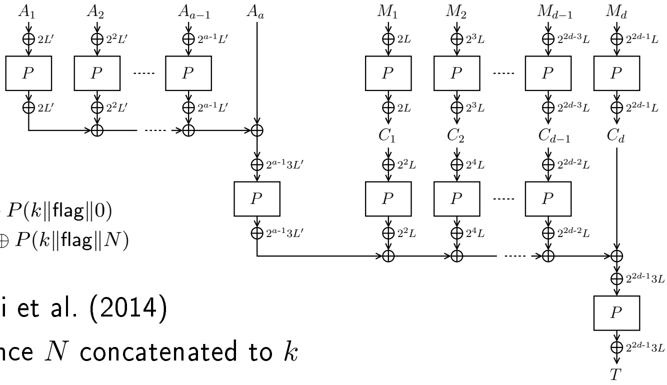
$$
\begin{tikzcd}
\boxed{\text{COPA}} \arrow[r, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)", "\text{sk}"'] & \boxed{\text{XEX}} \arrow[r, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)", "\text{sk}"'] & \boxed{E} \arrow[r, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)", "\text{sk}"'] & \boxed{P}
\end{tikzcd}
$$

Related-Key Security of Prøst-COPA

- Existing proof generalizes for any Φ

$$
\begin{tikzcd}
\boxed{\text{COPA}} \arrow[r, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)", "\Phi\text{-rk}"'] & \boxed{\text{XEX}} \arrow[r, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)", "\Phi\text{-rk}"'] \arrow[rr, bend right, "\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)"', "\Phi_{P\oplus}\text{-rk}"'] & \boxed{E} \arrow[r, "\Omega\left(1\right)", "\Phi\text{-rk}"'] & \boxed{P}
\end{tikzcd}
$$

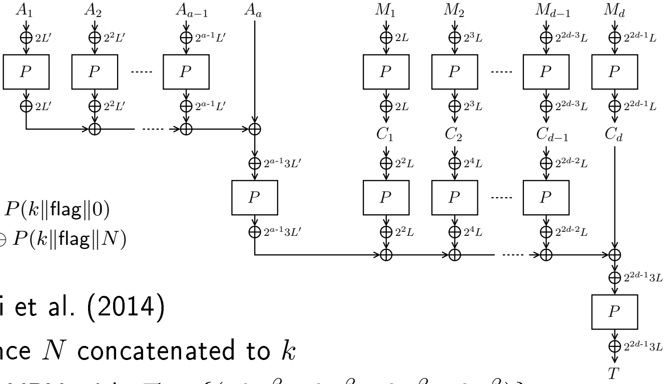
Application to AE: Minalpher



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

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

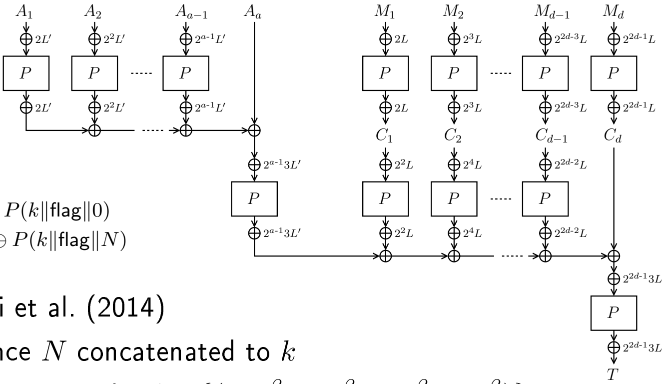
Application to AE: Minalpher



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

- 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

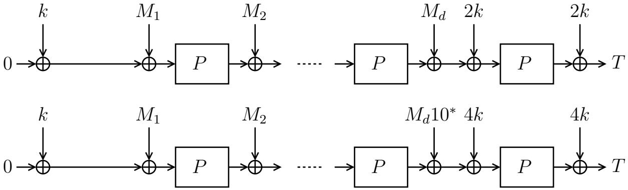


$$L' = k\|\mathsf{flag}\|0 \oplus P(k\|\mathsf{flag}\|0)$$
$$L = k\|\mathsf{flag}\|N \oplus P(k\|\mathsf{flag}\|N)$$

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

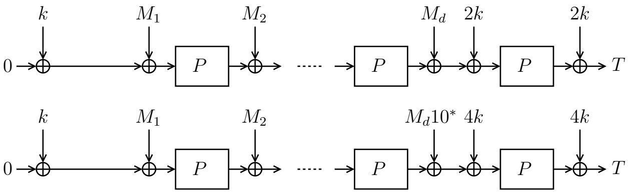
$$\boxed{\text{Minalph.}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\Phi_{P\oplus}\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application to MAC: Chaskey



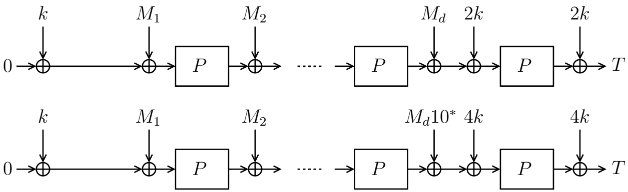
- By Mouha et al. (2014)
- Original proof based on 3 EM's: $\begin{cases} E_k(m) = P(m \oplus k) \oplus k \\ E_k(m) = P(m \oplus 3k) \oplus 2k \\ E_k(m) = P(m \oplus 5k) \oplus 4k \end{cases}$

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 $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

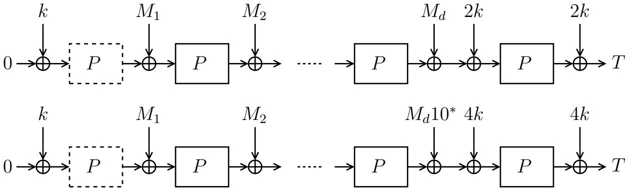
Application to MAC: Chaskey



- 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 $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

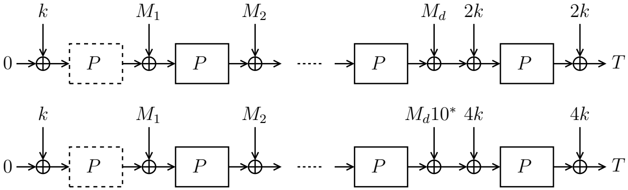
$$\boxed{\text{Chaskey}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application to MAC: Adjusted Chaskey



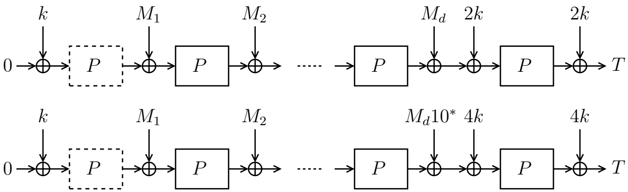
- Extra P-call

Application to MAC: Adjusted Chaskey



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

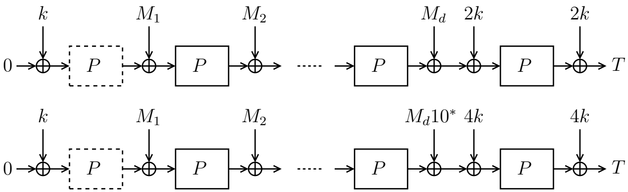
Application to MAC: Adjusted Chaskey



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

$$\boxed{\text{Chaskey}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\Phi_{\oplus}\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application to MAC: Adjusted Chaskey



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

$$\boxed{\text{Chaskey}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\Phi_{\oplus}\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

- Approach can also be applied to:
  - Keyed Sponge and Duplex
  - 10 Sponge-inspired CAESAR candidates

Conclusions

XPX

- Generalized tweakable Even-Mansour
- Various levels of security
  - Single-key to related-key
- Applications to
  - AE schemes (including 12 CAESAR candidates)
  - MAC functions

Further Research

- Beyond birthday bound?
- Other related-key settings?

Thank you for your attention!

SUPPORTING SLIDES

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

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

$\uparrow$ prob. ratio for good transcripts

- Trade-off: define bad transcripts smartly!

XPX: Security Proof Techniques

Before the Interaction

- Reveal "dedicated" oracle 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