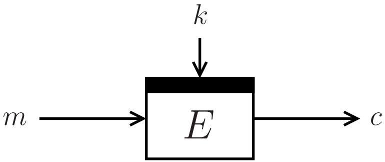
Tweakable Blockciphers: Theory and Application

Bart Mennink
KU Leuven (Belgium)

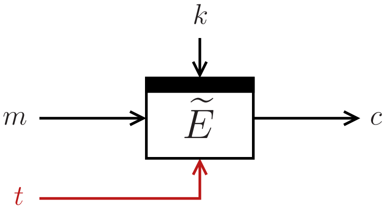
IACR School on Design and Security of Cryptographic Algorithms and Devices

October 21, 2015

Tweakable Blockciphers

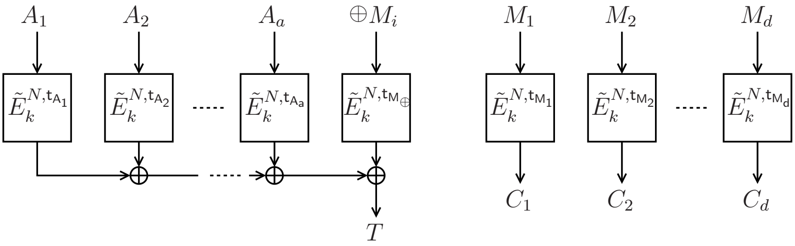


Tweakable Blockciphers



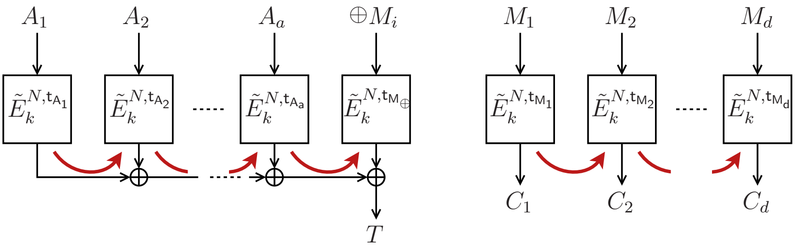
- Tweak: flexibility to the cipher
- Each tweak gives different permutation

Motivation: OCBx



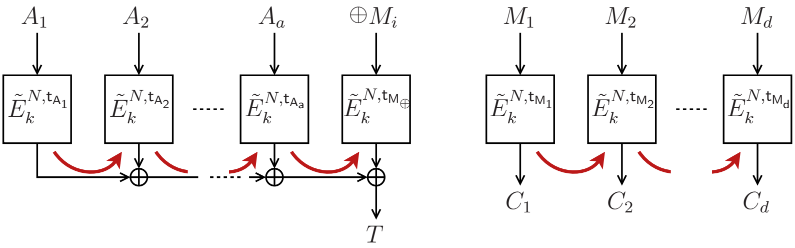
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, tweak) is unique for every evaluation

Motivation: OCBx



- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, tweak) is unique for every evaluation
- Change of tweak should be efficient

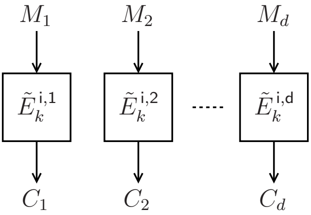
Motivation: OCBx



- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, tweak) is unique for every evaluation
- Change of tweak should be efficient

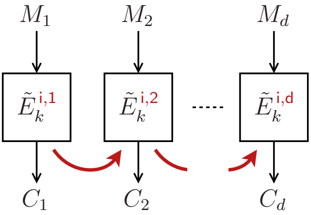
Tweakable blockcipher with efficient re-tweaking $\Longrightarrow$ efficient AE

Motivation: XTS



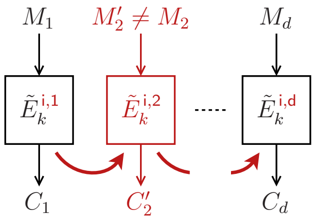
- XTS mode for disk encryption
- Tweak $(\mathsf{i}, \mathsf{j}) = (\mathsf{sector}, \mathsf{block})$ unique for every block

Motivation: XTS



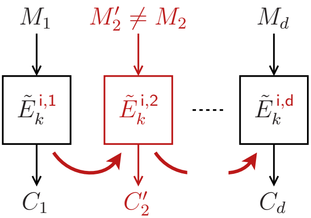
- XTS mode for disk encryption
- Tweak $(i, j) = (\text{sector}, \text{block})$ unique for every block
- Change of tweak should be efficient (as before)

Motivation: XTS



- XTS mode for disk encryption
- Tweak $(\mathsf{i},\mathsf{j}) = (\mathsf{sector},\mathsf{block})$ unique for every block
- Change of tweak should be efficient (as before)
- Incrementality: change in one (or few) blocks

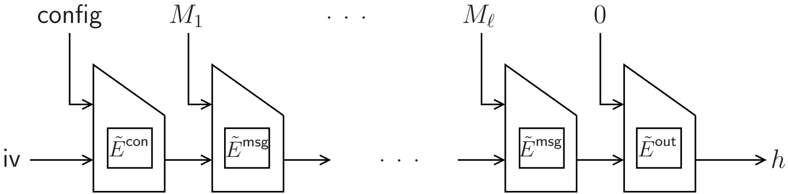
Motivation: XTS



- XTS mode for disk encryption
- Tweak $(\mathsf{i}, \mathsf{j}) = (\mathsf{sector}, \mathsf{block})$ unique for every block
- Change of tweak should be efficient (as before)
- Incrementality: change in one (or few) blocks

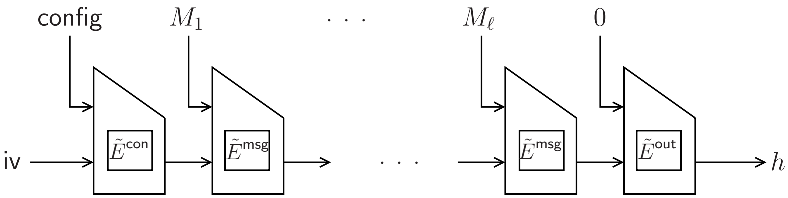
Tweakable blockcipher facilitates ECB-like modes $\Longrightarrow$ incrementality

Motivation: Skein



- Skein hash function by Ferguson et al. [FLS+07]
- Based on Threefish tweakable blockcipher
- Tweaks used for domain separation

Motivation: Skein



- Skein hash function by Ferguson et al. [FLS+07]
- Based on Threefish tweakable blockcipher
- Tweaks used for domain separation

Tweakable blockcipher $\Longrightarrow$ independent-looking blockciphers

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 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

Our focus: generic tweakable blockcipher design

Outline

Birthday Bound TBCs

Improved Security for Birthday Bound TBCs

Improved Efficiency for Birthday Bound TBCs

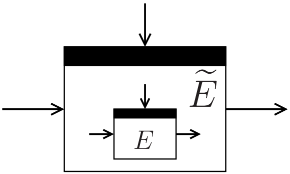
Beyond Birthday Bound TBCs

Conclusion

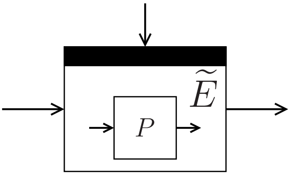
Outline

Tweakable Blockciphers from Blockciphers/Permutations

Blockcipher Based

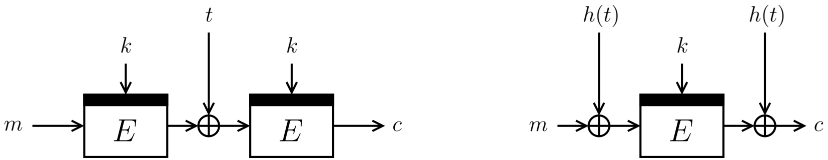


Permutation Based



Tweakable Blockciphers from Blockciphers

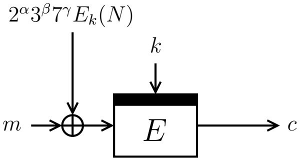
- LRW_1 and LRW_2 by Liskov et al. [LRW02]:

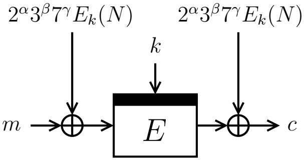


- h is XOR-universal hash
  - E.g., $h(t) = h \otimes t$ for n-bit "key" h

Tweakable Blockciphers from Blockciphers

- XE and XEX by Rogaway [Rog04]:

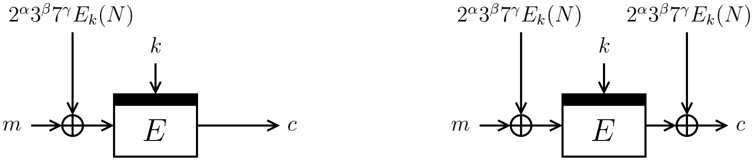




- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

Tweakable Blockciphers from Blockciphers

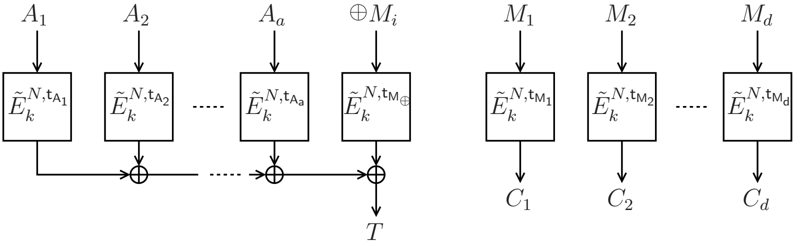
- XE and XEX by Rogaway [Rog04]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and XTS

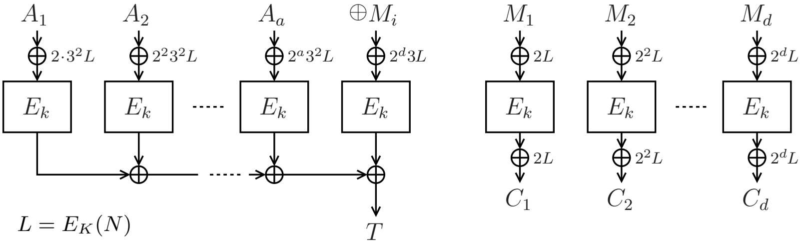
Example: XEX in OCB2 and XTS

OCB2:



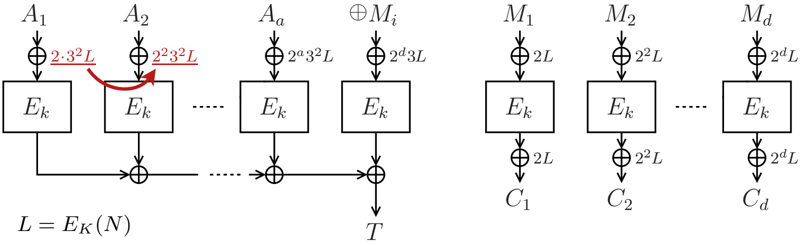
Example: XEX in OCB2 and XTS

OCB2:



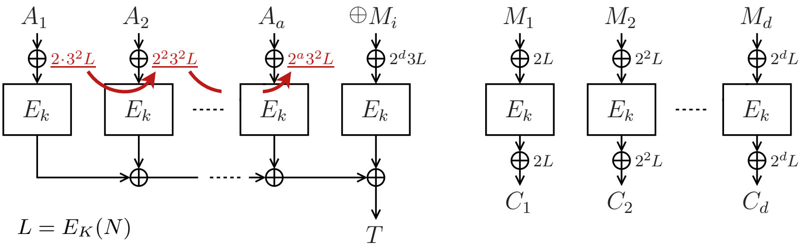
Example: XEX in OCB2 and XTS

OCB2:



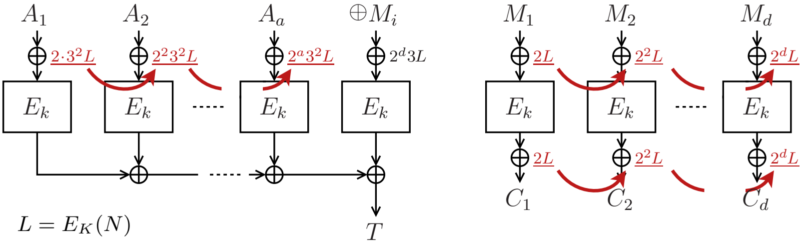
Example: XEX in OCB2 and XTS

OCB2:



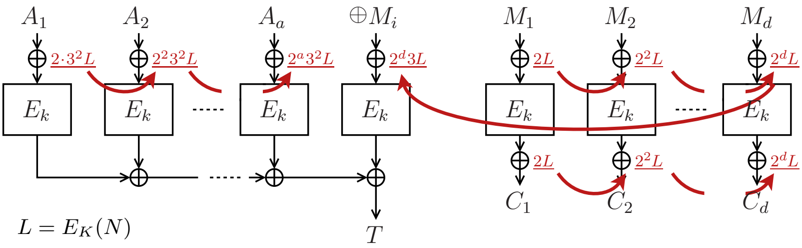
Example: XEX in OCB2 and XTS

OCB2:



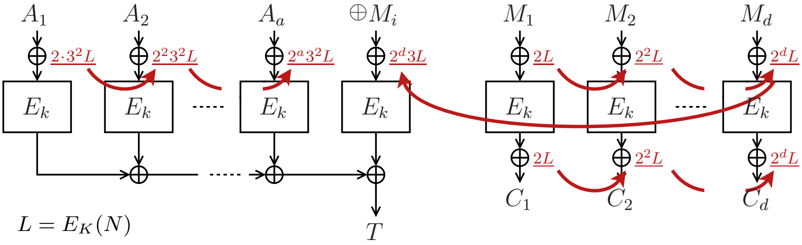
Example: XEX in OCB2 and XTS

OCB2:

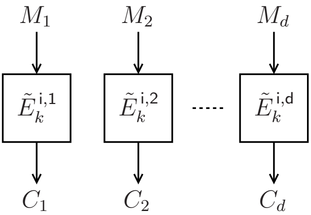


Example: XEX in OCB2 and XTS

OCB2:

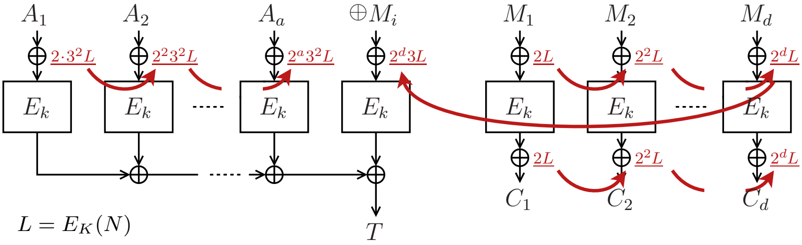


XTS:

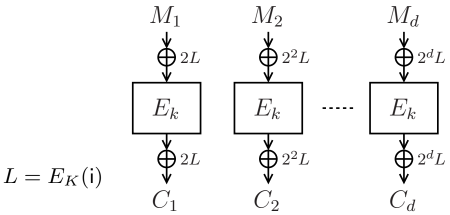


Example: XEX in OCB2 and XTS

OCB2:

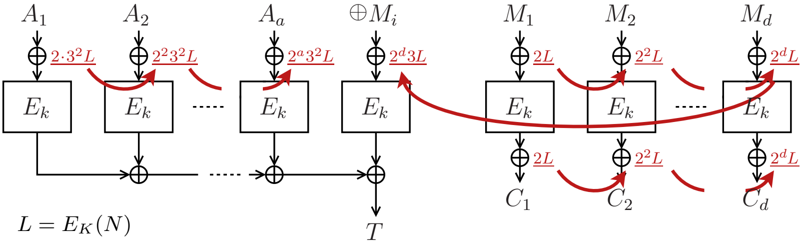


XTS:

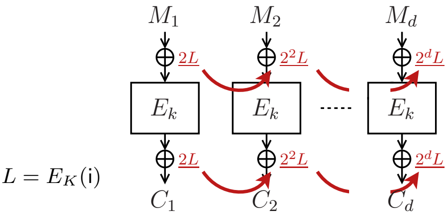


Example: XEX in OCB2 and XTS

OCB2:

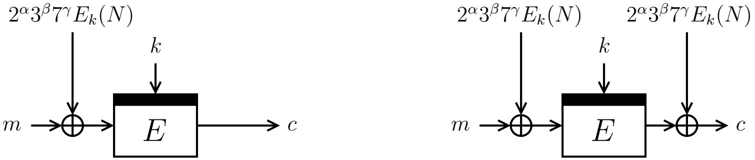


XTS:



Tweakable Blockciphers from Blockciphers

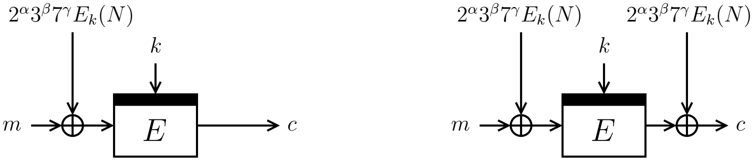
- XE and XEX by Rogaway [Rog04]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and XTS

Tweakable Blockciphers from Blockciphers

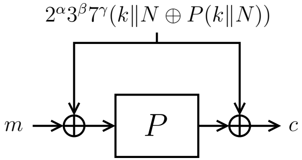
- XE and XEX by Rogaway [Rog04]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and XTS
- Generalized masking:
  - Chakraborty and Sarkar [CS06]: $\varphi^\alpha(E_k(N))$ for LFSR φ
  - Gray codes (used in OCB1 and OCB3)

Tweakable Blockciphers from Permutations

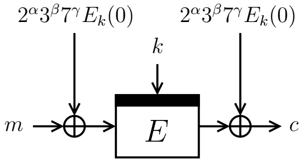
- Minalpher's TEM [STA+14]:



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

Tweakable Blockciphers from Permutations

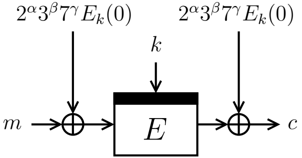
- Prøst [KLL+14] uses XE(X) with Even-Mansour:



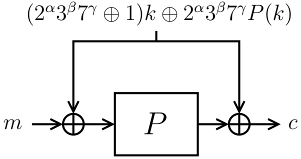
with $E_k(m) = P(m \oplus k) \oplus k$

Tweakable Blockciphers from Permutations

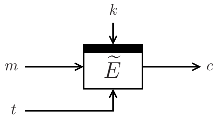
- Prøst [KLL+14] uses XE(X) with Even-Mansour:



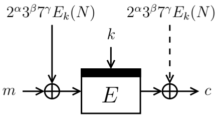
with $E_k(m) = P(m \oplus k) \oplus k$



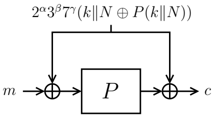
Tweakable Blockciphers in CAESAR



Dedicated

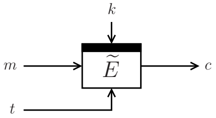


XE/XEX-inspired



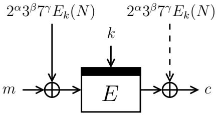
TEM-inspired

Tweakable Blockciphers in CAESAR



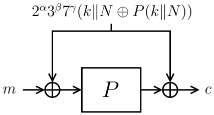
Dedicated

Deoxys,
Joltik,
KIASU,
SCREAM



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**

Outline

Birthday Bound TBCs

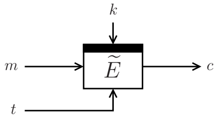
Improved Security for Birthday Bound TBCs

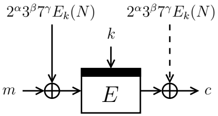
Improved Efficiency for Birthday Bound TBCs

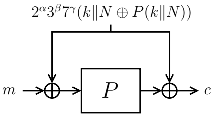
Beyond Birthday Bound TBCs

Conclusion

Tweakable Blockciphers in CAESAR







Dedicated

Deoxys,
Joltik,
KIASU,
SCREAM

XE/XEX-inspired

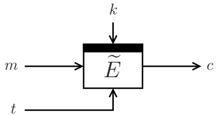
AEZ, CBA, COBRA,
COPA, **ELmD**, iFeed,
Marble, **OCB**, **OMD**,
OTR, **POET**, **SHELL**

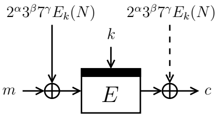
TEM-inspired

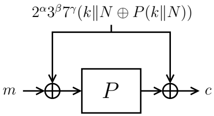
Minalpher,
Prøst

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

Tweakable Blockciphers in CAESAR







Dedicated

Deoxys, **Joltik**, KIASU, **SCREAM**

XE/XEX-inspired

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

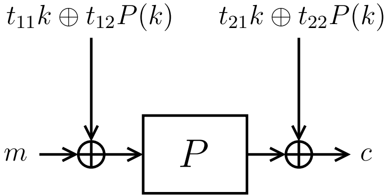
TEM-inspired

Minalpher, Prøst

XPX [Men15b], generalization of this

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

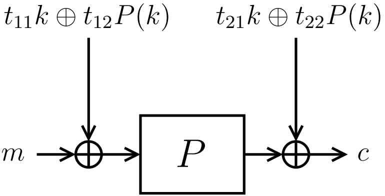
XPX



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

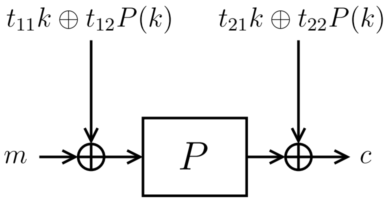


Tweak Set

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

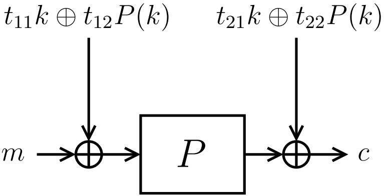


Tweak Set

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

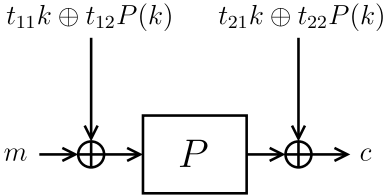


Tweak Set

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

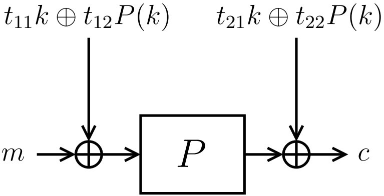


Tweak Set

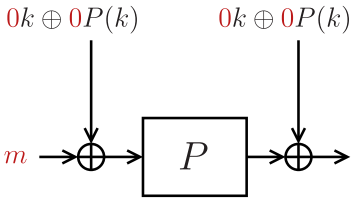
- $(t_{11}, t_{12}, t_{21}, t_{22})$ from some tweak set $\mathcal{T} \subseteq (\{0,1\}^n)^4$
- $\mathcal{T}$ can (still) be any set

- 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: Stupid Tweaks

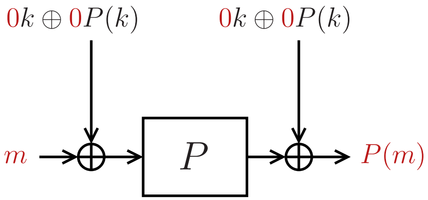


XPX: Stupid Tweaks



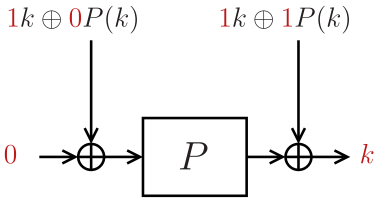
$(0, 0, 0, 0) \in \mathcal{T}$

XPX: Stupid Tweaks



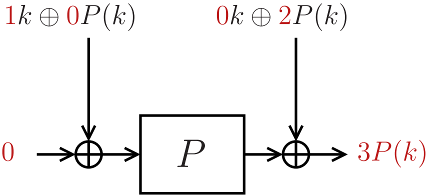
$$(0, 0, 0, 0) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((0, 0, 0, 0), m) = P(m)$$

XPX: Stupid 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: Stupid Tweaks

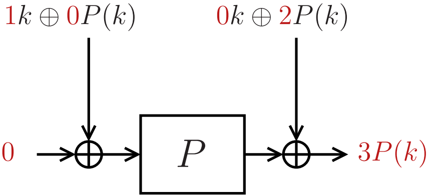


$$(0,0,0,0) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m)$$

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

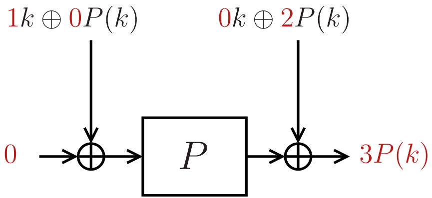
$$(1,0,0,2) \in \mathcal{T} \quad \Longrightarrow \quad \mathsf{XPX}_k((1,0,0,2),0) = 3P(k)$$

XPX: Stupid Tweaks



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

XPX: Stupid Tweaks

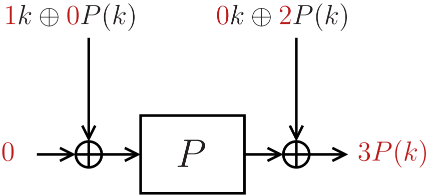


$$\begin{aligned}
(0,0,0,0) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((0,0,0,0),m) = P(m) \\
(1,0,1,1) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,1,1),0) = k \\
(1,0,0,2) \in \mathcal{T} \quad &\Longrightarrow \quad \mathsf{XPX}_k((1,0,0,2),0) = 3P(k) \\
\cdots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

"Valid" Tweak Sets

- Technical definition to eliminate trivial cases

XPX: Stupid Tweaks



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

"Valid" Tweak Sets

- Technical definition to eliminate trivial cases
- If $\mathcal{T}$ is invalid, then XPX is insecure

XPX: Normal and Strong Tweaks

Single-Key Security

- If $\mathcal{T}$ is valid, then XPX is STPRP

XPX: Normal and Strong Tweaks

Single-Key Security

- If $\mathcal{T}$ is valid, then XPX is STPRP

$\Phi_{\oplus}$-Related-Key Security (Simplified)

- $\mathcal{D}$ can influence key: $k \mapsto k \oplus \delta$

XPX: Normal and Strong Tweaks

Single-Key Security

- If $\mathcal{T}$ is valid, then XPX is STPRP

$\Phi_{\oplus}$-Related-Key Security (Simplified)

- $\mathcal{D}$ can influence key: $k \mapsto k \oplus \delta$

$\Phi_{P\oplus}$-Related-Key Security (Simplified)

- $\mathcal{D}$ can influence key: $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$
- Note: maskings in XPX are $t_{i1}k \oplus t_{i2}P(k)$

XPX: Normal and Strong Tweaks

Single-Key Security

- If $\mathcal{T}$ is valid, then XPX is STPRP

$\Phi_{\oplus}$-Related-Key Security (Simplified)

- $\mathcal{D}$ can influence key: $k \mapsto k \oplus \delta$

$\Phi_{P\oplus}$-Related-Key Security (Simplified)

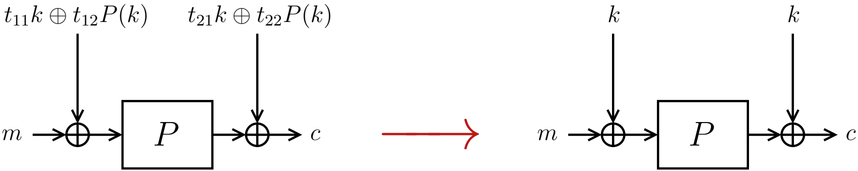
- $\mathcal{D}$ can influence key: $k \mapsto k \oplus \delta$ or $P(k) \mapsto P(k) \oplus \epsilon$
- Note: maskings in XPX are $t_{i1}k \oplus t_{i2}P(k)$

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

XPX Covers Even-Mansour

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

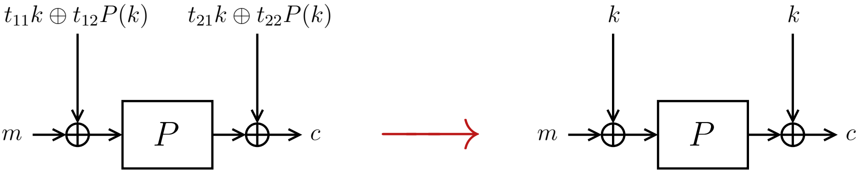
XPX Covers Even-Mansour



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

- Single-key STPRP secure (surprise?)

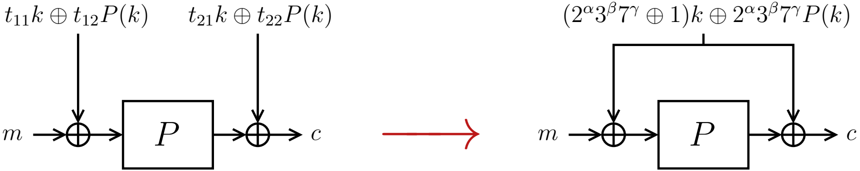
XPX Covers Even-Mansour



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

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

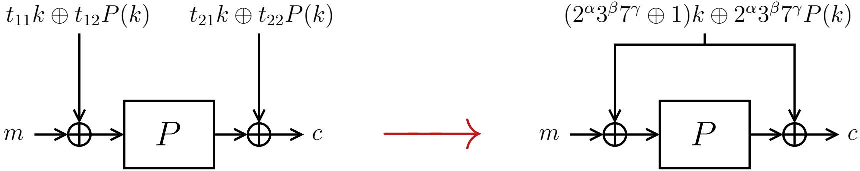
XPX Covers XEX With Even-Mansour



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

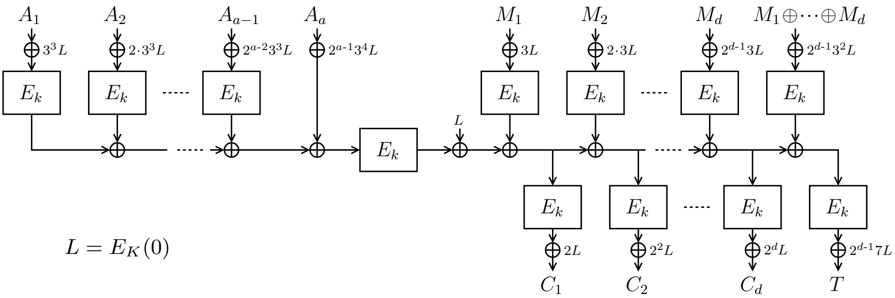
XPX Covers XEX With Even-Mansour



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

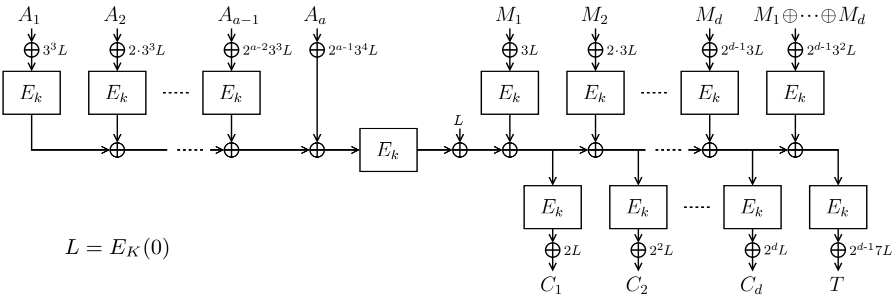
- (α, β, γ) is in fact the "real" tweak
- $\Phi_{P\oplus}$-rk STPRP secure (if $2^\alpha 3^\beta 7^\gamma \neq 1$)

Application of XPX to AE: COPA



- By Andreeva et al. [ABL+14]
- Implicitly based on XEX based on AES

Application of XPX to AE: COPA



- By Andreeva et al. [ABL+14]
- Implicitly based on XEX based on AES

- Prøst-COPA by Kavun et al. [KLL+14]:
  COPA based on XEX based on Even-Mansour

Application of XPX 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 of XPX 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 [Men15b])

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

Application of XPX to AE: Prøst-COPA

Single-Key Security of Prøst-COPA

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

Application of XPX 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 of XPX 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

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

Application of XPX 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 of XPX to AE: Prøst-COPA

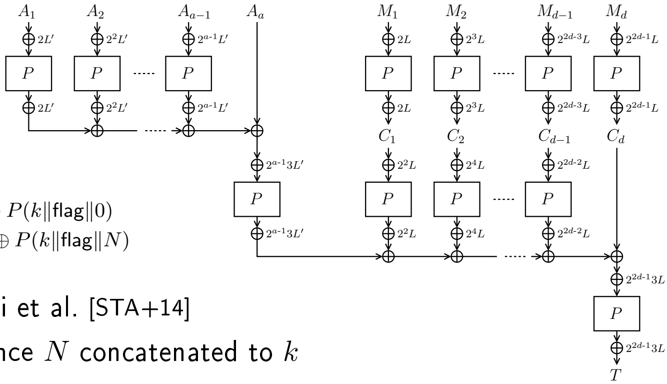
Single-Key Security of Prøst-COPA

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

Related-Key Security of Prøst-COPA

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

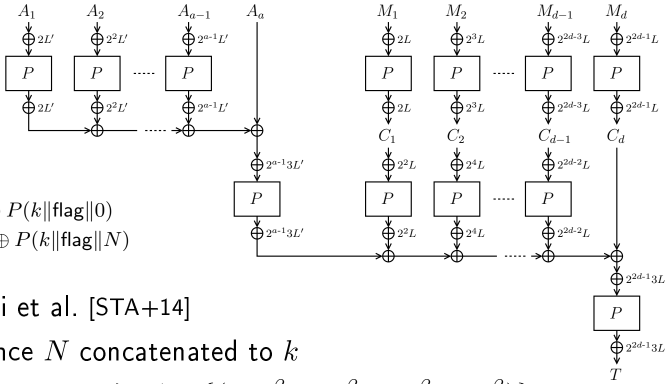
Application of XPX to AE: Minalpher



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

- By Sasaki et al. [STA+14]
- Extra nonce N concatenated to k

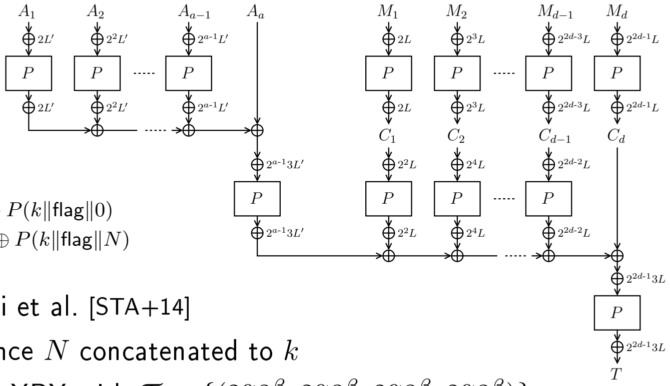
Application of XPX to AE: Minalpher



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

- By Sasaki et al. [STA+14]
- 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 of XPX to AE: Minalpher

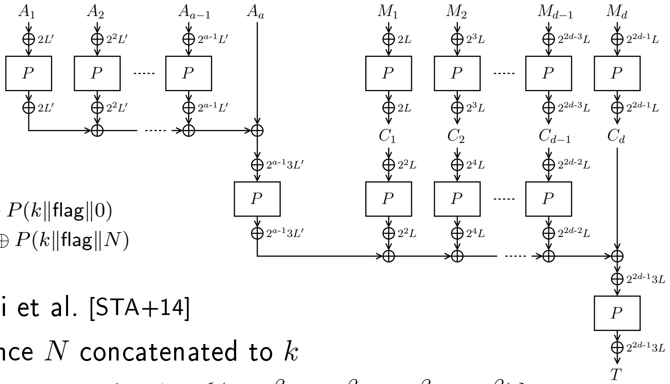


$L' = k\|\text{flag}\|0 \oplus P(k\|\text{flag}\|0)$
$L \;= k\|\text{flag}\|N \oplus P(k\|\text{flag}\|N)$

- By Sasaki et al. [STA+14]
- Extra nonce N concatenated to k
- Based on XPX with $\mathcal{T} = \{(2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta)\}$

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

Application of XPX to AE: Minalpher

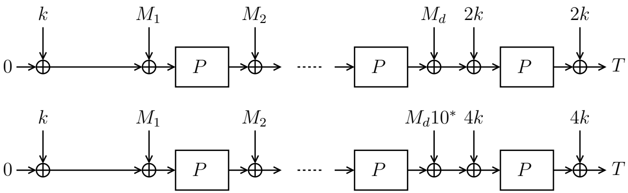


$$L' = k\|\text{flag}\|0 \oplus P(k\|\text{flag}\|0)$$
$$L = k\|\text{flag}\|N \oplus P(k\|\text{flag}\|N)$$

- By Sasaki et al. [STA+14]
- Extra nonce N concatenated to k
- Based on XPX with $\mathcal{T} = \{(2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta, 2^\alpha 3^\beta)\}$

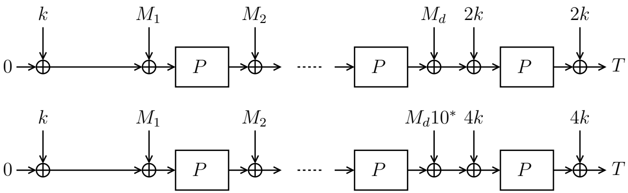
$$\boxed{\text{Minalph.}} \xrightarrow[\Phi\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\Phi_{P\oplus}\text{-rk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application of XPX to MAC: Chaskey



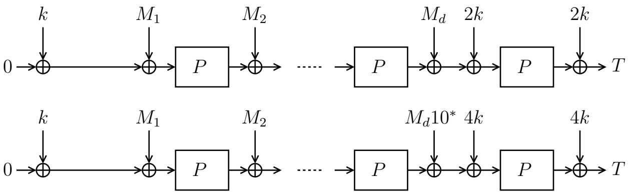
- By Mouha et al. [MMV+14]

Application of XPX to MAC: Chaskey



- By Mouha et al. [MMV+14]
- Based on XPX with $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

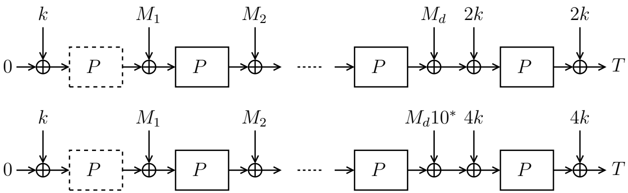
Application of XPX to MAC: Chaskey



- By Mouha et al. [MMV+14]
- Based on XPX with $\mathcal{T} = \{(1,0,1,0),(3,0,2,0),(5,0,4,0)\}$

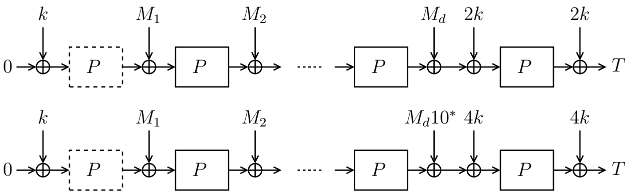
$$\boxed{\text{Chaskey}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{\text{XPX}} \xrightarrow[\text{sk}]{\mathcal{O}\left(\frac{\sigma^2}{2^n}\right)} \boxed{P}$$

Application to MAC: Adjusted Chaskey



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

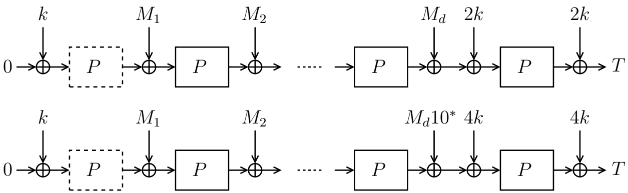
Application to MAC: Adjusted Chaskey



- 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 also applies to Keyed Sponges

Outline

Birthday Bound TBCs

Improved Security for Birthday Bound TBCs

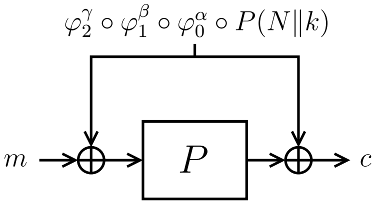
Improved Efficiency for Birthday Bound TBCs

Beyond Birthday Bound TBCs

Conclusion

MEM

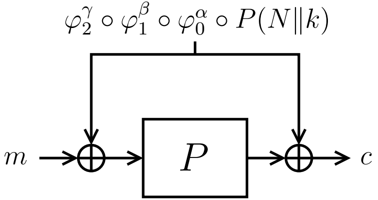
- MEM by Granger et al. [GJMN15]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

MEM

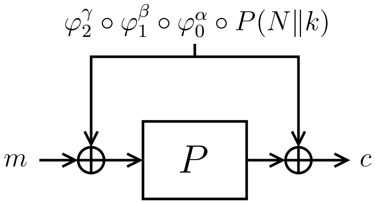
- MEM by Granger et al. [GJMN15]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Masking combines advantages of:
  - Powering-up masking
  - LFSR masking

MEM

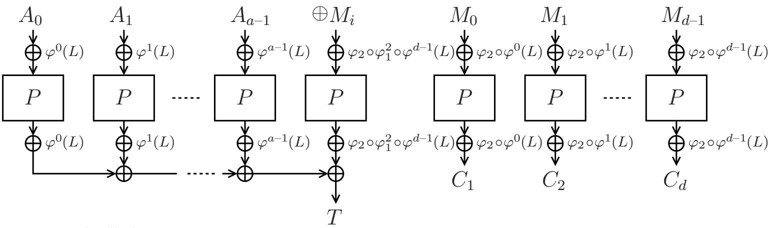
- MEM by Granger et al. [GJMN15]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Masking combines advantages of:
  - Powering-up masking
  - LFSR masking

New masking is simpler, constant-time (by default), more efficient

Application of MEM to AE: OPP

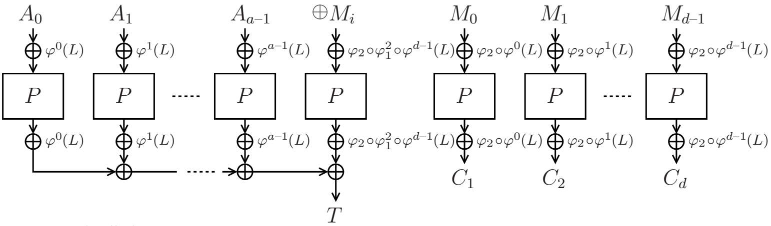


$L = P(N \| k)$

$\varphi_1 = \varphi \oplus id$, $\varphi_2 = \varphi^2 \oplus \varphi \oplus id$

- Offset Public Permutation (OPP) [GJMN15]
- Generalization of OCB3:
  - Permutation-based
  - More efficient MEM-masking
- Security against nonce-respecting adversaries

Application of MEM to AE: OPP



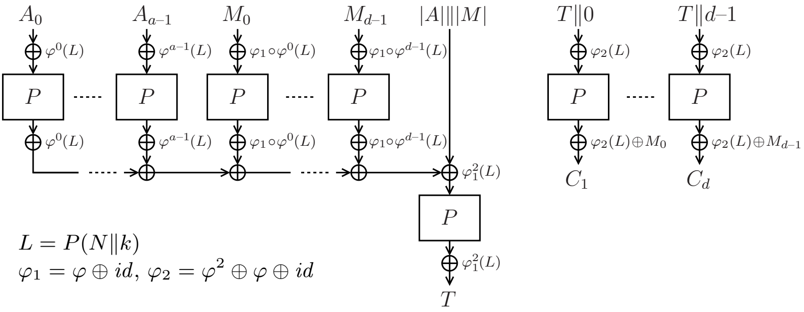
$L = P(N \| k)$

$\varphi_1 = \varphi \oplus id$, $\varphi_2 = \varphi^2 \oplus \varphi \oplus id$

- Offset Public Permutation (OPP) [GJMN15]
- Generalization of OCB3:
  - Permutation-based
  - More efficient MEM-masking
- Security against nonce-respecting adversaries

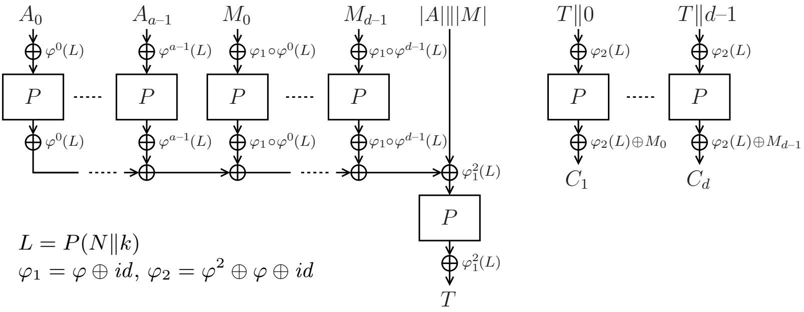
0.55 cpb with reduced-round BLAKE2b

Application of MEM to AE: MRO



- Misuse-Resistant OPP (MRO) [GJMN15]
- Fully nonce-misuse resistant version of OPP

Application of MEM to AE: MRO



- Misuse-Resistant OPP (MRO) [GJMN15]
- Fully nonce-misuse resistant version of OPP

1.06 cpb with reduced-round BLAKE2b

Outline

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, OPP, ...):

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

Security Beyond Birthday Bound?

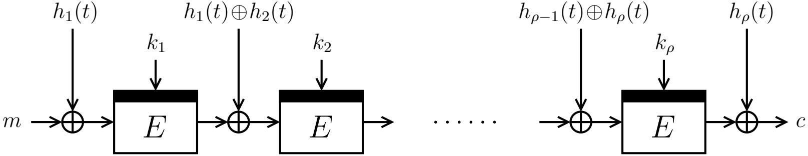
- All results so far: up to birthday bound

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

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

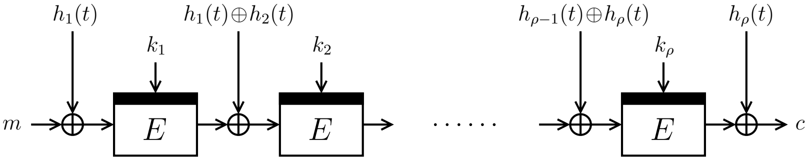
Can we improve this?

BBB Tweakable Blockciphers from Blockciphers



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

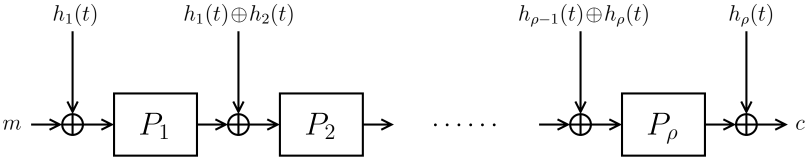
BBB Tweakable Blockciphers from Blockciphers



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

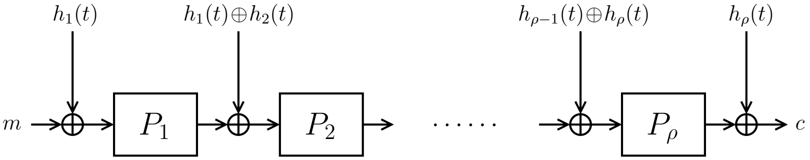
- $\rho = 2$: secure up to $2^{2n/3}$ queries [LST12,Pro14]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [LS13]
- Conjecture: optimal $2^{\rho n/(\rho+1)}$ security

BBB Tweakable Blockciphers from Permutations



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

BBB Tweakable Blockciphers from Permutations



- 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]
- Conjecture: optimal $2^{\rho n/(\rho+1)}$ security

State of the Art (Blockcipher Based)

scheme	security ($\log_2$)	key length	cost	
			E	$\otimes/h$
LRW_1	$n/2$	n	2	0
LRW_2	$n/2$	$2n$	1	1
XEX	$n/2$	n	2	0
$\text{LRW}_2[2]$	$2n/3$	$4n$	2	2
$\text{LRW}_2[\rho]$	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ

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

Tweak-Dependent Keys

Efficiency

tweak schedule lighter
than key schedule

Tweak-Dependent Keys

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

Tweak-Dependent Keys

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

Tweak and key change approximately equally expensive

Tweak-Dependent Keys

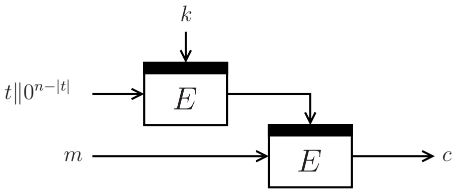
Efficiency	**Security**
tweak schedule lighter than key schedule	tweak schedule stronger than key schedule

Tweak and key change approximately equally expensive

- TWEAKEY [JNP14] key scheduling blends key and tweak

Tweak-Dependent Keys

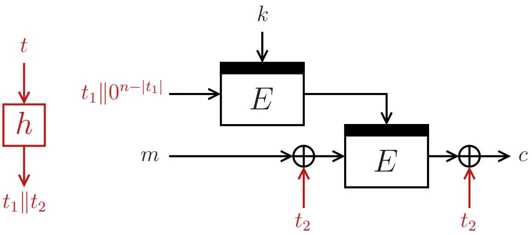
- Minematsu [Min09]:



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

Tweak-Dependent Keys

- Minematsu [Min09]:



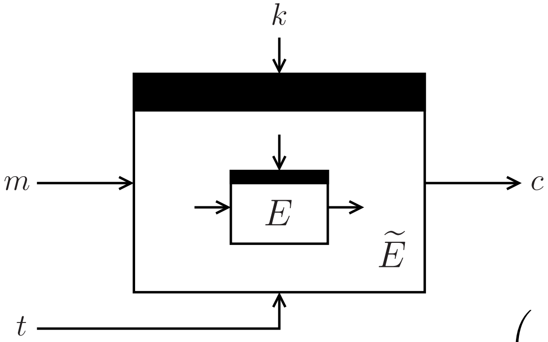
- Secure up to $\max\{2^{n/2}, 2^{n-|t|}\}$ queries
- Beyond birthday bound for $|t| < n/2$
- Tweak-length extension possible by XTX [MI15]

State of the Art (Blockcipher Based)

scheme	security ($\log_2$)	key length	cost		
			E	$\otimes/h$	tdk
LRW_1	$n/2$	n	2	0	0
LRW_2	$n/2$	$2n$	1	1	0
XEX	$n/2$	n	2	0	0
$\text{LRW}_2[2]$	$2n/3$	$4n$	2	2	0
$\text{LRW}_2[\rho]$	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ	0
Min	$\max\{n/2, n-\lvert t\rvert\}$	n	2	0	1
Min-XTX	$2n/3$	$7n/3$	2	1	1

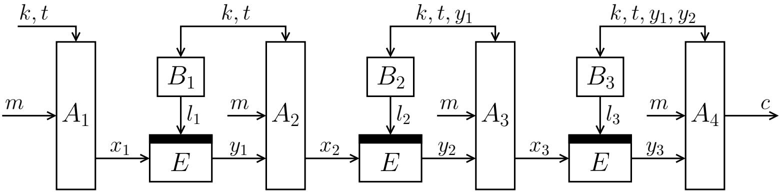
Goal

Given a blockcipher E,
construct optimally secure tweakable blockcipher $\widetilde{E}$



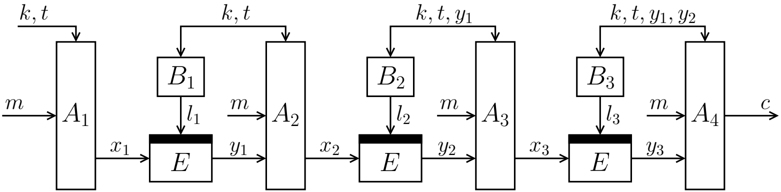
$\left(\begin{array}{c}\text{all wires}\\ \text{carry } n \text{ bits}\end{array}\right)$

Generic Design



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

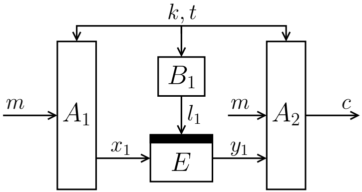
Generic Design



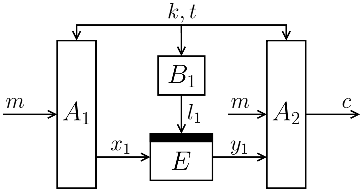
$\widetilde{E}[\rho]$ (for $\rho \geq 1$)

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

One E-Call with Linear Mixing



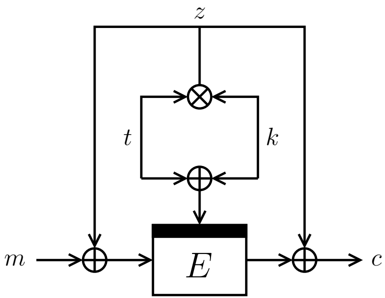
One E-Call with Linear Mixing



Theorem [Men15a]

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

One E-Call with Polynomial Mixing

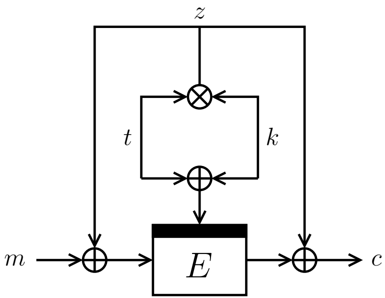


$\text{Men}_1(k, t, m) = c$ [Men15a]

Idea

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

One E-Call with Polynomial Mixing



$\mathsf{Men}_1(k, t, m) = c$ [Men15a]

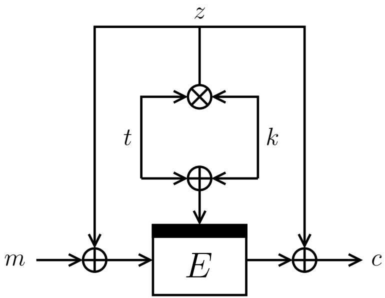
Idea

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

Security

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

One E-Call with Polynomial Mixing



$\text{Men}_1(k, t, m) = c$ [Men15a]

Idea

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

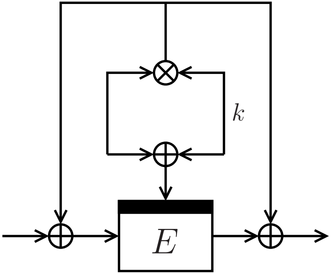
Security

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

Cost

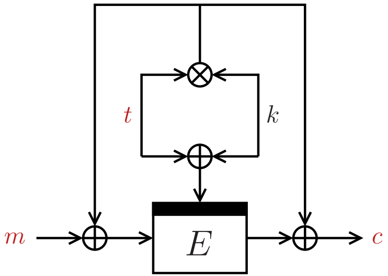
- One E-call
- One $\otimes$-evaluation
- One re-key

One E-Call with Polynomial Mixing: Proof Idea



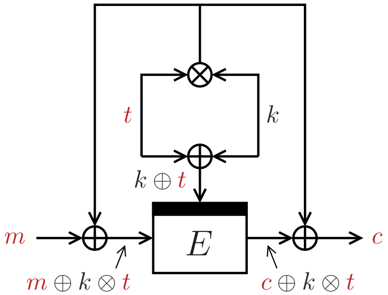
- Key k is secret

One E-Call with Polynomial Mixing: Proof Idea



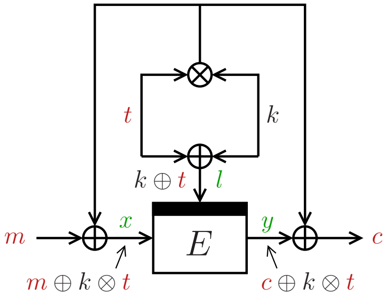
- Key k is secret
- Consider any construction query (t, m, c)

One E-Call with Polynomial Mixing: Proof Idea



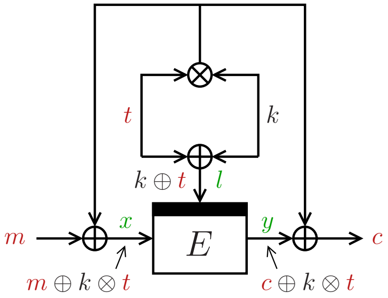
- Key k is secret
- Consider any construction query (t, m, c)

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)

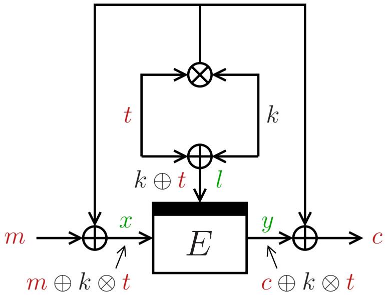
One E-Call with Polynomial Mixing: Proof Idea



- 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



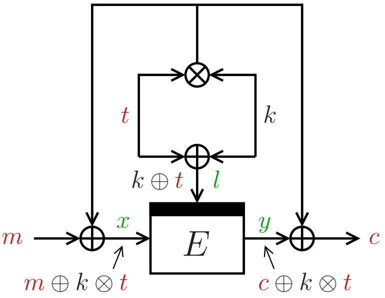
- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

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

or

$k \oplus t = l$ and $c \oplus k \otimes t = y$

One E-Call with Polynomial Mixing: Proof Idea



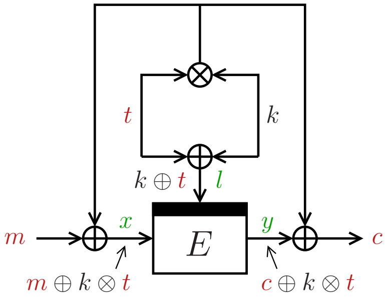
- Key k is secret
- Consider any construction query (t, m, c)
- May "hit" any primitive query (l, x, y)

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

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

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

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)

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

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

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

One E-Call with Polynomial Mixing: Proof Idea

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

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]

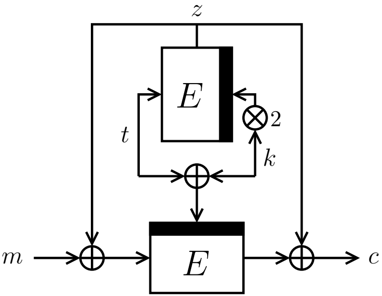
Consider a finite field $\mathbb{F}$. Let

- $L \subseteq \mathbb{F}^2$ 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

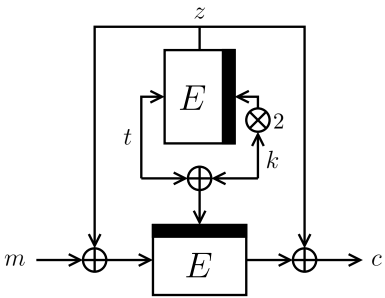


$\mathsf{Men}_2(k, t, m) = c$

Idea

- Subkey $k \oplus t$
- Masking $E(2k, t)$

Two E-Calls with Linear Mixing



$\mathsf{Men}_2(k, t, m) = c$

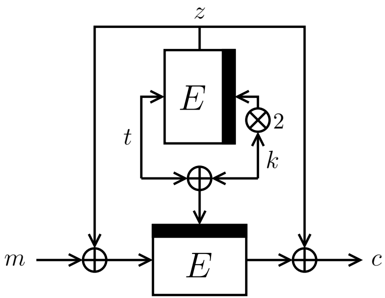
Idea

- Subkey $k \oplus t$
- Masking $E(2k, t)$

Security

- Up to 2^n queries

Two E-Calls with Linear Mixing



$\mathsf{Men}_2(k, t, m) = c$

Idea

- Subkey $k \oplus t$
- Masking $E(2k, t)$

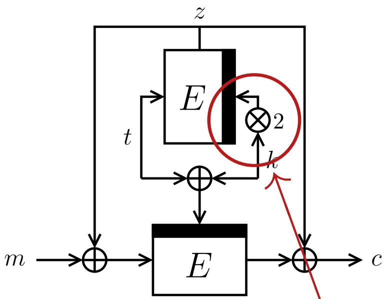
Security

- Up to 2^n queries

Cost

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

Two E-Calls with Linear Mixing



$\mathsf{Men}_2(k, t, m) = c$

Idea

- Subkey $k \oplus t$
- Masking $E(2k, t)$

Security

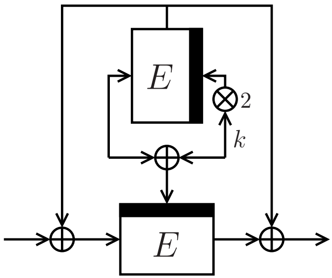
- Up to 2^n queries

Cost

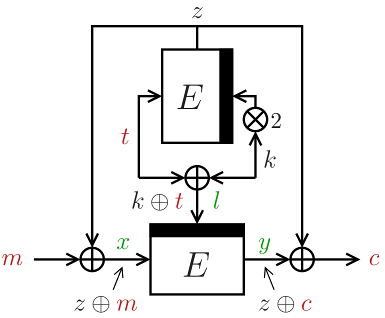
- Two E-calls
- Zero $\otimes$-evaluations
- One re-key

New after observation by Guo et al.
(original proof only for $t \neq 0$)

Two E-Calls with Linear Mixing: Proof Idea



Two E-Calls with Linear Mixing: Proof Idea



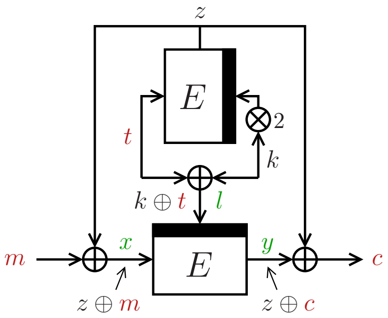
- Construction query (t, m, c) "hits" primitive query (l, x, y) if

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

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
LRW_1	$n/2$	n	2	0	0
LRW_2	$n/2$	$2n$	1	1	0
XEX	$n/2$	n	2	0	0
$\mathsf{LRW}_2[2]$	$2n/3$	$4n$	2	2	0
$\mathsf{LRW}_2[\rho]$	$\rho n/(\rho+2)$	$2\rho n$	ρ	ρ	0
Min	$\max\{n/2, n-\lvert t\rvert\}$	n	2	0	1
Min-XTX	$2n/3$	$7n/3$	2	1	1
Men_1	$2n/3$ *	n	1	1	1
Men_2	n *	n	2	0	1

* Information-theoretic model

Outline

Birthday Bound TBCs

Improved Security for Birthday Bound TBCs

Improved Efficiency for Birthday Bound TBCs

Beyond Birthday Bound TBCs

Conclusion

Conclusion

Birthday Bound Tweakable Blockciphers

- Myriad applications to AE, MAC, encryption, ...
- Various solutions for different problems:
    - Efficiency
    - Related-key security
    - ...

Conclusion

Birthday Bound Tweakable Blockciphers

- Myriad applications to AE, MAC, encryption, . . .
- Various solutions for different problems:
  - Efficiency
  - Related-key security
  - . . .

Beyond Birthday Bound Tweakable Blockciphers

- Allow for beyond birthday bound secure AE
- Efficient scheme without re-keying?
- One-call tweakable cipher with improved security?
- Optimal security in standard model?

Conclusion

Birthday Bound Tweakable Blockciphers

- Myriad applications to AE, MAC, encryption, ...
- Various solutions for different problems:
  - Efficiency
  - Related-key security
  - ...

Beyond Birthday Bound Tweakable Blockciphers

- Allow for beyond birthday bound secure AE
- Efficient scheme without re-keying?
- One-call tweakable cipher with improved security?
- Optimal security in standard model?

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 $i^* = 2$