XOR of PRPs in a Quantum World

Bart Mennink, Alan Szepieniec

Radboud University (The Netherlands),
KU Leuven (Belgium)

PQCrypto 2017
June 26, 2017

Introduction

PRP PRF

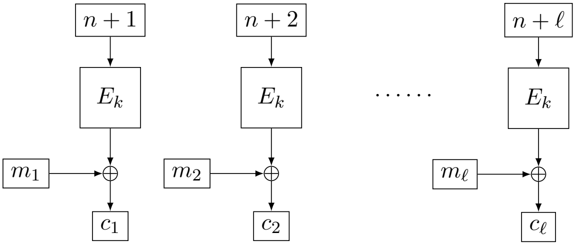
Introduction

$$\text{PRP} \xleftarrow{\text{Luby-Rackoff / Feistel}} \text{PRF}$$

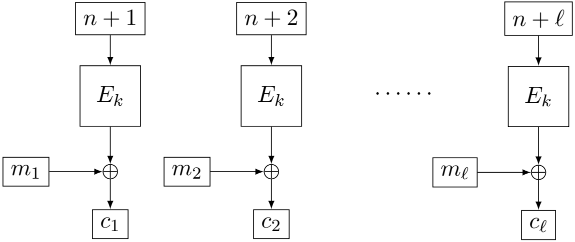
Introduction

$$\begin{tikzcd}[column sep=huge] \text{PRP} \arrow[r, bend right, red, "\text{Now}"'] & \text{PRF} \arrow[l, bend right, "\text{Luby-Rackoff / Feistel}"'] \end{tikzcd}$$

Counter Mode Based on Pseudorandom Permutation



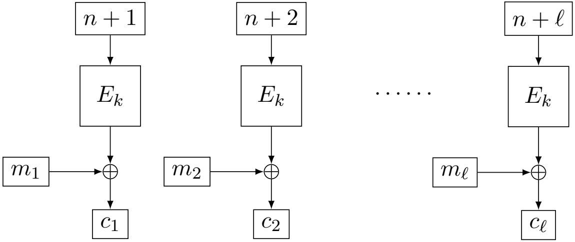
Counter Mode Based on Pseudorandom Permutation



- Security bound:

$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[E]}(q,t) \leq \mathsf{Adv}^{\mathrm{prp}}_{E}(q,t) + \binom{q}{2}/2^n$$

Counter Mode Based on Pseudorandom Permutation

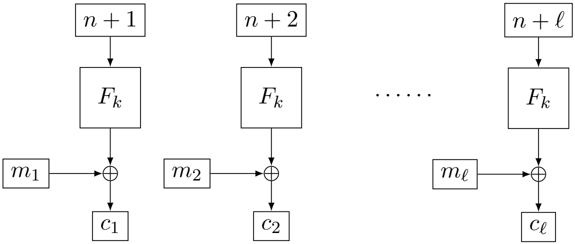


- Security bound:

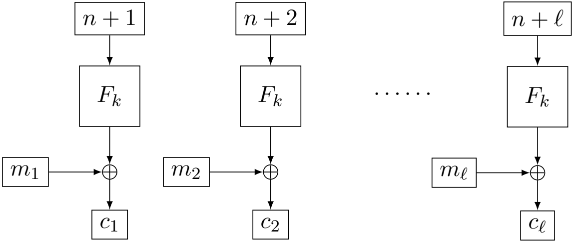
$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[E]}(q,t) \le \mathsf{Adv}^{\mathrm{prp}}_{E}(q,t) + \binom{q}{2}/2^n$$

- $\mathsf{CTR}[E]$ is secure as long as:
  - E_k is a secure PRP (typically $t \ll 2^\kappa$)
  - Number of encrypted blocks $q \ll 2^{n/2}$

Counter Mode Based on Pseudorandom Function



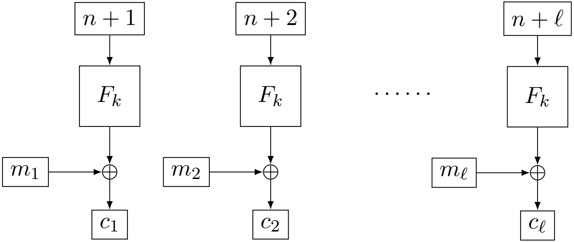
Counter Mode Based on Pseudorandom Function



- Security bound:

$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[F]}(q) \le \mathsf{Adv}^{\mathrm{prf}}_{F}(q)$$

Counter Mode Based on Pseudorandom Function

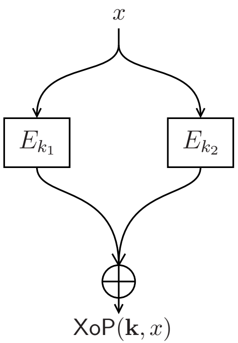


- Security bound:

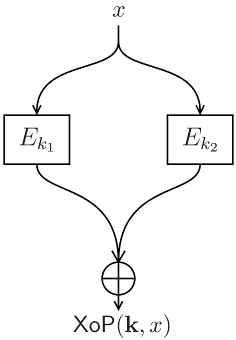
$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR}[F]}(q) \leq \mathsf{Adv}^{\mathrm{prf}}_{F}(q)$$

- $\mathsf{CTR}[F]$ is secure as long as F_k is a secure PRF
- Birthday bound security loss disappeared

XOR of PRPs

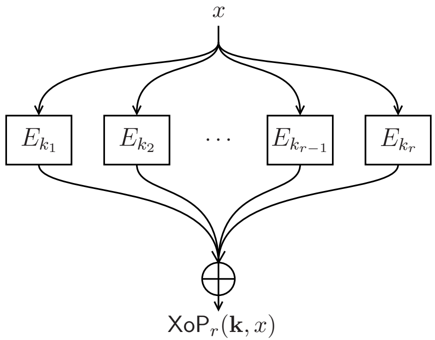


XOR of PRPs



- $\min\{2^\kappa, 2^n\}$ security [BI99,Luc00,Pat08]

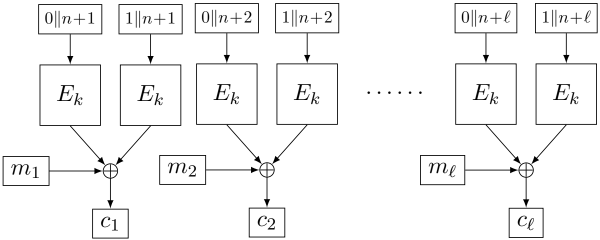
XOR of PRPs



- $\min\{2^\kappa, 2^n\}$ security [Bl99,Luc00,Pat08]
- Bound preserved for $r \geq 3$ [CLP14,MP15]

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q,t) \leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(q,t) + q/2^n$$

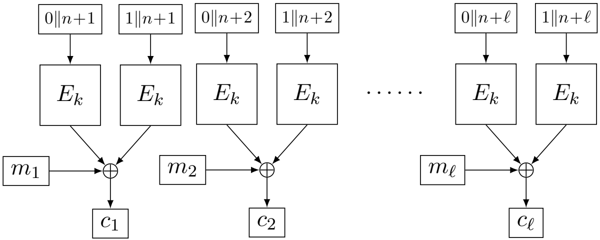
Counter Mode Based on XoP



- Security bound:

$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(q,t) \leq \mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q,t)$$

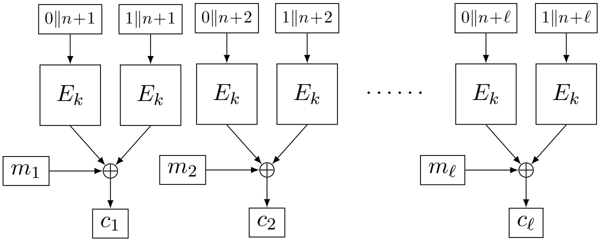
Counter Mode Based on XoP



- Security bound:

$$\begin{aligned}\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(q,t) &\leq \mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q,t)\\ &\leq \mathsf{Adv}^{\mathrm{prp}}_{E}(2q,t) + q/2^n\end{aligned}$$

Counter Mode Based on XoP



- Security bound:

$$\mathsf{Adv}^{\mathrm{cpa}}_{\mathsf{CTR[XoP]}}(q,t) \le \mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q,t)$$
$$\le \mathsf{Adv}^{\mathrm{prp}}_{E}(2q,t) + q/2^n$$

- $\min\{2^\kappa, 2^n\}$ security

Quantum Security Analysis?

Quantum Security Analysis?

Simon/Shor

- Poly-time period finding
- Used to attack Even-Mansour, CBC-MAC, ...
- Quantum interaction with keyed primitive

Quantum Security Analysis?

Simon/Shor

- Poly-time period finding
- Used to attack Even-Mansour, CBC-MAC, ...
- Quantum interaction with keyed primitive

Grover

- "Halves the key size"
- No quantum interaction needed

Quantum Security Analysis?

Simon/Shor

- Poly-time period finding
- Used to attack Even-Mansour, CBC-MAC, ...
- Quantum interaction with keyed primitive

Grover

- "Halves the key size"
- No quantum interaction needed

This work: no quantum interaction

Our Contribution

Classical Versus Quantum Proofs

- Formalization of types of distinguishers
- Exposition of how classical proofs subsist quantumly
- Applicable to myriad cryptographic schemes

Our Contribution

Classical Versus Quantum Proofs

- Formalization of types of distinguishers
- Exposition of how classical proofs subsist quantumly
- Applicable to myriad cryptographic schemes

Quantum Security Analysis of XoP

- Application of subsistence: $\min\{2^{\kappa/2}, 2^n\}$ security

Our Contribution

Classical Versus Quantum Proofs

- Formalization of types of distinguishers
- Exposition of how classical proofs subsist quantumly
- Applicable to myriad cryptographic schemes

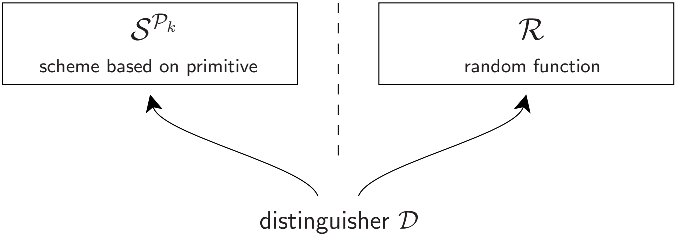
Quantum Security Analysis of XoP

- Application of subsistence: $\min\{2^{\kappa/2}, 2^n\}$ security

Key Recovery Attack on XoP

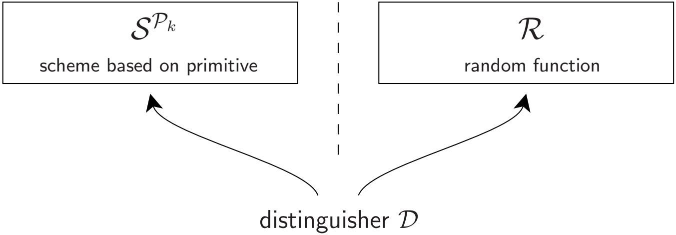
- Attack in complexity $2^{\kappa r/(r+1)}$ (improves over Grover)
- Relies on claw-finding algorithm

General Security Framework



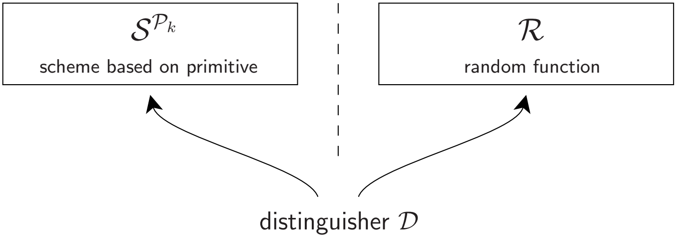
- Distinguishing advantage $\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t)$

General Security Framework



- Distinguishing advantage $\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t)$
- Online complexity: q oracle queries
- Offline complexity: t time

General Security Framework



- Distinguishing advantage $\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t)$
- Online complexity: q oracle queries
- Offline complexity: t time
- $\mathcal{D}$ knows $\mathcal{P}$: can make $\approx t$ offline evaluations

Distinguishers

set of $\mathcal{D}$'s	online	offline
$\mathbb{D}(q, t)$	q classical	t classical
$\mathbb{D}(q, \hat{t})$	q classical	t quantum
$\mathbb{D}(\hat{q}, \hat{t})$	q quantum	t quantum

Distinguishers

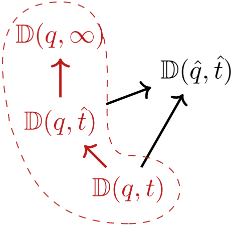
set of $\mathcal{D}$'s	online	offline	
$\mathbb{D}(q, t)$	q classical	t classical	$\longleftarrow$ classical distinguishers
$\mathbb{D}(q, \hat{t})$	q classical	t quantum	$\longleftarrow$ includes Grover
$\mathbb{D}(\hat{q}, \hat{t})$	q quantum	t quantum	$\longleftarrow$ includes Simon/Shor

Distinguishers

set of $\mathcal{D}$'s	online	offline	
$\mathbb{D}(q, t)$	q classical	t classical	$\longleftarrow$ classical distinguishers
$\mathbb{D}(q, \hat{t})$	q classical	t quantum	$\longleftarrow$ includes Grover
$\mathbb{D}(\hat{q}, \hat{t})$	q quantum	t quantum	$\longleftarrow$ includes Simon/Shor
$\mathbb{D}(q, \infty)$	q classical	∞	$\longleftarrow$ used a lot in classical crypto

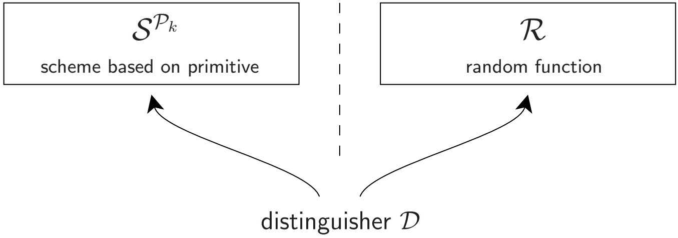
Distinguishers

set of $\mathcal{D}$'s	online	offline	
$\mathbb{D}(q,t)$	q classical	t classical	$\longleftarrow$ classical distinguishers
$\mathbb{D}(q,\hat{t})$	q classical	t quantum	$\longleftarrow$ includes Grover
$\mathbb{D}(\hat{q},\hat{t})$	q quantum	t quantum	$\longleftarrow$ includes Simon/Shor
$\mathbb{D}(q,\infty)$	q classical	∞	$\longleftarrow$ used a lot in classical crypto



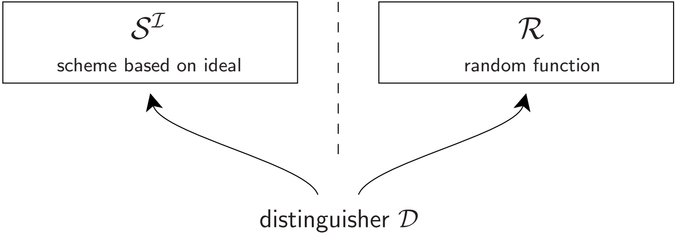
$$\mathbb{D}(q,t) \subseteq \mathbb{D}(q,\hat{t}) \subseteq \mathbb{D}(q,\infty)$$

Typical Classical Security Proof



$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t)$$

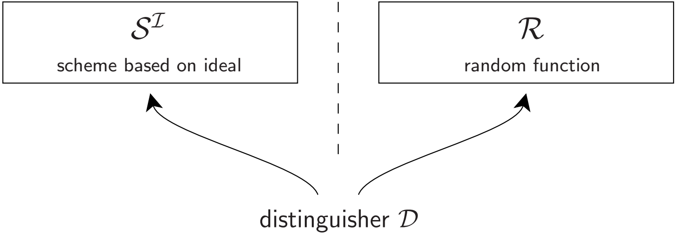
Typical Classical Security Proof



- Step 1: replace $\mathcal{P}_k$ by ideal equivalent $\mathcal{I}$

$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t) \leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',t') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,t)$$

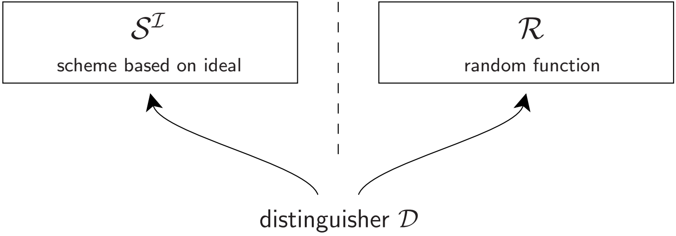
Typical Classical Security Proof



- Step 1: replace $\mathcal{P}_k$ by ideal equivalent $\mathcal{I}$
- Step 2: first term is primitive security (e.g., PRP)

$$\begin{aligned}\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t) &\leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',t') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,t) \\ &\leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',t') +\end{aligned}$$

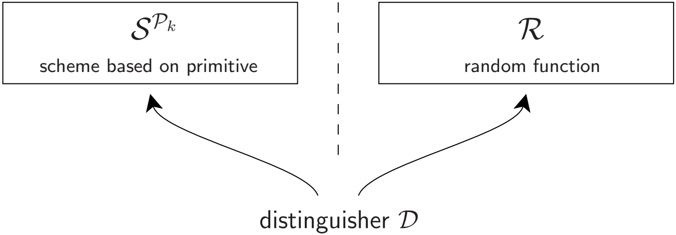
Typical Classical Security Proof



- Step 1: replace $\mathcal{P}_k$ by ideal equivalent $\mathcal{I}$
- Step 2: first term is primitive security (e.g., PRP)
- Step 3: second term $\mathcal{P}$-invariant: give $\mathcal{D}$ infinite time

$$\begin{aligned}\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,t) &\le \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',t') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,t) \\ &\le \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',t') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,\infty)\end{aligned}$$

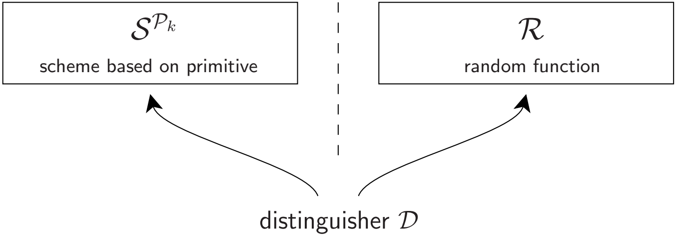
Conversion to Quantum



- Identical story holds for quantum distinguishers

$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,\hat{t}) \leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',\hat{t}') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,\infty)$$

Conversion to Quantum

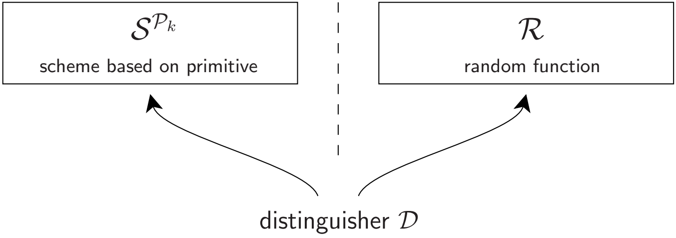


- Identical story holds for quantum distinguishers

$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q,\hat{t}) \leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q',\hat{t}') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q,\infty)$$

$t' \ll 2^{\kappa/2}$?

Conversion to Quantum



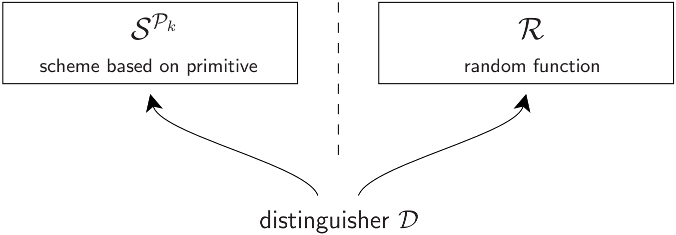
- Identical story holds for quantum distinguishers

$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q, \hat{t}) \leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q', \hat{t}') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q, \infty)$$

$t' \ll 2^{\kappa/2}$?

classical analysis carries over

Conversion to Quantum



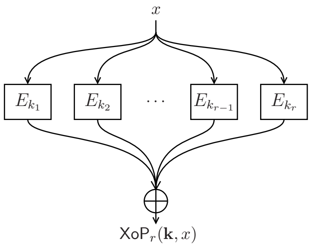
- Identical story holds for quantum distinguishers

$$\mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{P}_k}}(q, \hat{t}) \leq \mathsf{Adv}^{\mathcal{I}}_{\mathcal{P}_k}(q', \hat{t}') + \mathsf{Adv}^{\mathcal{R}}_{\mathcal{S}^{\mathcal{I}}}(q, \infty)$$

$t' \ll 2^{\kappa/2}$?   classical analysis carries over

- Conversion applies to all standard model proofs
  (not covered: permutation-based modes)

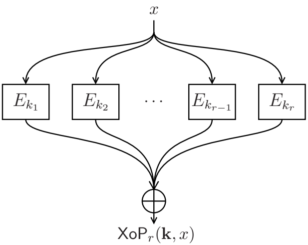
Quantum Security Analysis of XoP



Theorem [Pat08,MP15] For $r \geq 2$ and $q \leq 2^n/67$ we have

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}_r}(q,t) \leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(q,t) + q/2^n$$

Quantum Security Analysis of XoP



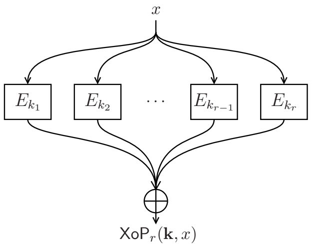
Theorem [Pat08,MP15] For $r \geq 2$ and $q \leq 2^n/67$ we have

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}_r}(q,t) \leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(q,t) + q/2^n$$

Theorem For $r \geq 2$ and $q \leq 2^n/67$ we have

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}_r}(q,\hat{t}) \leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(q,\hat{t}) + q/2^n$$

Key Recovery Attack on XoP

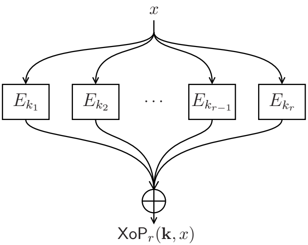


Theorem For $r \geq 1$, $\tau \geq 1$, $t = O(\tau \cdot 2^{\kappa r/(r+1)})$ we have

$$\mathsf{Adv}^{\text{key}}_{\mathsf{XoP}_r}(\tau, \hat{t}) \geq 1 - \varepsilon(r, \tau, n)$$

- ε monotonically decreasing in threshold τ

Key Recovery Attack on XoP

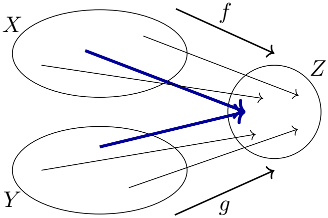


Theorem For $r \geq 1$, $\tau \geq 1$, $t = O(\tau \cdot 2^{\kappa r/(r+1)})$ we have

$$\mathsf{Adv}^{\text{key}}_{\mathsf{XoP}_r}(\tau, \hat{t}) \geq 1 - \varepsilon(r, \tau, n)$$

- ε monotonically decreasing in threshold τ
- Goal: construct an adversary

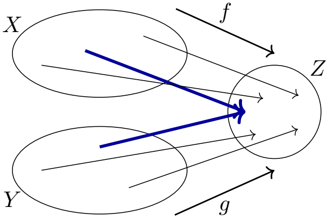
Quantum Claw-Finding



Claw-Finding

- Given $f : X \to Z$ and $g : Y \to Z$
- Find (x, y) s.t. $f(x) = g(y)$

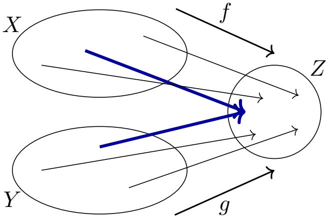
Quantum Claw-Finding



Claw-Finding

- Given $f : X \to Z$ and $g : Y \to Z$
- Find (x, y) s.t. $f(x) = g(y)$
- Tani (2009): algorithm with complexity $O\left((|X| \cdot |Y|)^{1/3}\right)$

Quantum Claw-Finding



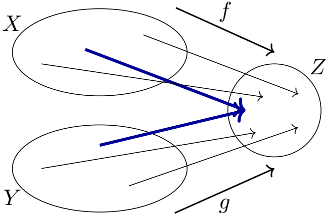
Claw-Finding

- Given $f : X \to Z$ and $g : Y \to Z$
- Find (x, y) s.t. $f(x) = g(y)$
- Tani (2009): algorithm with complexity $O\left((|X| \cdot |Y|)^{1/3}\right)$

Predicate-Finding

- Given $f : X \to Z$ and $g : Y \to Z$
- Given relation R
- Find $(x_1 \ldots x_p, y_1 \ldots y_q)$ s.t. $(f(x_1) \ldots f(x_p), g(y_1) \ldots g(y_q)) \in R$

Quantum Claw-Finding



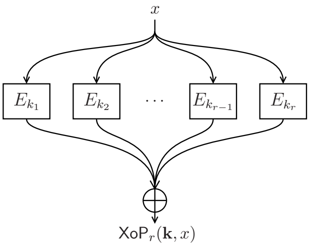
Claw-Finding

- Given $f : X \to Z$ and $g : Y \to Z$
- Find (x, y) s.t. $f(x) = g(y)$
- Tani (2009): algorithm with complexity $O\left((|X| \cdot |Y|)^{1/3}\right)$

Predicate-Finding

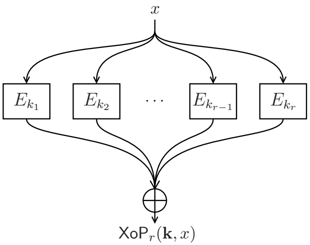
- Given $f : X \to Z$ and $g : Y \to Z$
- Given relation R
- Find $(x_1 \dots x_p, y_1 \dots y_q)$ s.t. $(f(x_1) \dots f(x_p), g(y_1) \dots g(y_q)) \in R$
- Tani (2009): algorithm with complexity $O\left((|X|^p \cdot |Y|^q)^{1/(p+q+1)}\right)$

Key Recovery Adversary



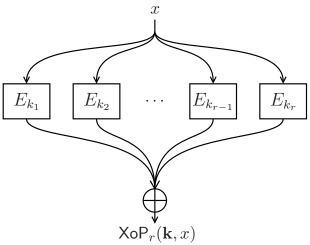
1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1$
2. Define $f(l) = E_l(1)$
   $g(m) = E_m(1) \oplus z_1$

Key Recovery Adversary



1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1$
2. Define $f(l) = E_l(1)$
   $g(m) = E_m(1) \oplus z_1$
3. Apply Tani's algorithm to find $l_1, \ldots, l_{r-1}, m$ s.t.
   $f(l_1) \oplus f(l_2) \oplus \ldots \oplus f(l_{r-1}) \oplus g(m) = 0$ (relation R)

Key Recovery Adversary



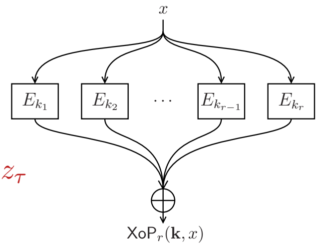
1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1$
2. Define $f(l) = E_l(1)$
   $g(m) = E_m(1) \oplus z_1$
3. Apply Tani's algorithm to find $l_1, \ldots, l_{r-1}, m$ s.t.

$$f(l_1) \oplus f(l_2) \oplus \ldots \oplus f(l_{r-1}) \oplus g(m) = 0 \qquad \text{(relation } R\text{)}$$

Complexity

- Online queries: 1
- Offline complexity: $O(2^{\kappa r/(r+1)})$
- Success probability: quite low due to false positives

Key Recovery Adversary

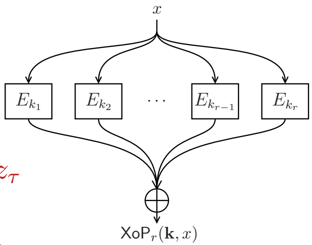


1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1$, $\ldots$, $\mathsf{XoP}_r(\mathbf{k}, \tau) = z_\tau$
2. Define $f(l) = E_l(1)$
   $g(m) = E_m(1) \oplus z_1$
3. Apply Tani's algorithm to find $l_1, \ldots, l_{r-1}, m$ s.t.
   $$f(l_1) \oplus f(l_2) \oplus \ldots \oplus f(l_{r-1}) \oplus g(m) = 0 \qquad \text{(relation } R\text{)}$$

Complexity

- Online queries: $\cancel{1}$ τ
- Offline complexity: $O(2^{\kappa r/(r+1)})$
- Success probability: quite low due to false positives

Key Recovery Adversary

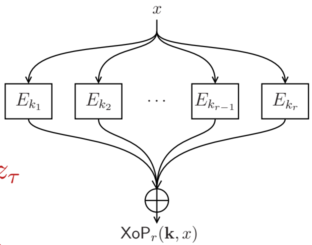


1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1, \ldots, \mathsf{XoP}_r(\mathbf{k}, \tau) = z_\tau$
2. Define $f(l) = E_l(1) \parallel \cdots \parallel E_l(\tau)$
   $g(m) = E_m(1) \oplus z_1 \parallel \cdots \parallel E_m(\tau) \oplus z_\tau$
3. Apply Tani's algorithm to find $l_1, \ldots, l_{r-1}, m$ s.t.
   $$f(l_1) \oplus f(l_2) \oplus \ldots \oplus f(l_{r-1}) \oplus g(m) = 0 \qquad \text{(relation } R\text{)}$$

Complexity

- Online queries: $\cancel{1}$ τ
- Offline complexity: $\cancel{O(2^{\kappa r/(r+1)})}$ $O(\tau \cdot 2^{\kappa r/(r+1)})$
- Success probability: quite low due to false positives

Key Recovery Adversary



1. Query $\mathsf{XoP}_r(\mathbf{k}, 1) = z_1, \ldots, \mathsf{XoP}_r(\mathbf{k}, \tau) = z_\tau$
2. Define $f(l) = E_l(1) \parallel \cdots \parallel E_l(\tau)$
   $g(m) = E_m(1) \oplus z_1 \parallel \cdots \parallel E_m(\tau) \oplus z_\tau$
3. Apply Tani's algorithm to find $l_1, \ldots, l_{r-1}, m$ s.t.
   $$f(l_1) \oplus f(l_2) \oplus \ldots \oplus f(l_{r-1}) \oplus g(m) = 0 \qquad \text{(relation } R\text{)}$$

Complexity

- Online queries: $\cancel{1}$ τ
- Offline complexity: $\cancel{O(2^{\kappa r/(r+1)})}$ $O(\tau \cdot 2^{\kappa r/(r+1)})$
- Success probability: ~~quite low due to false positives~~ approaching 1 for increasing τ

Conclusion

Proof subsistence

- Simple and natural
- Broadly applicable

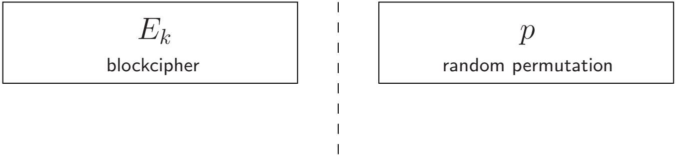
Primitive isolation step

- Tight if there is only one key
- Loose if multiple keys are involved
- Non-trivial to get around

Thank you for your attention!

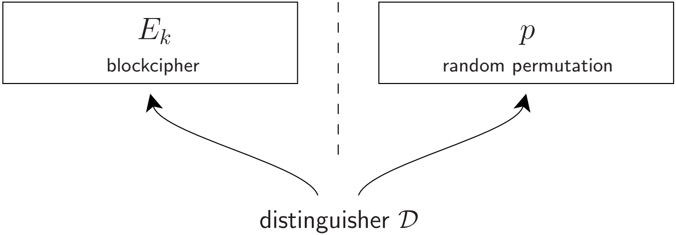
SUPPORTING SLIDES

Pseudorandom Permutation



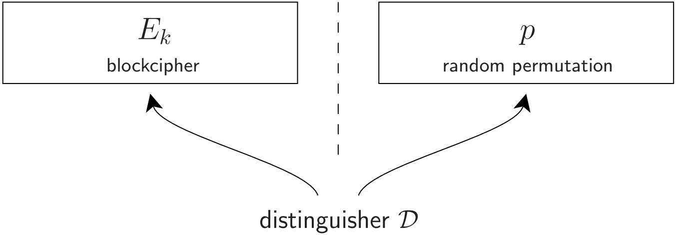
- Two oracles: E_k (for secret random key k) and p

Pseudorandom Permutation



- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p
- $\mathcal{D}$ tries to determine which oracle it communicates with

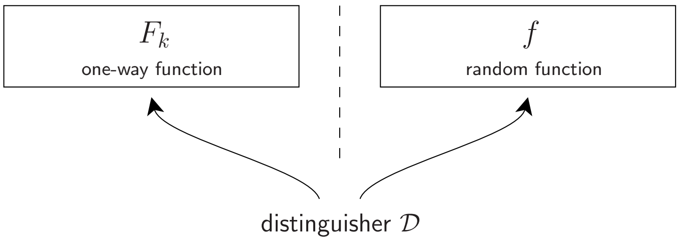
Pseudorandom Permutation



- Two oracles: E_k (for secret random key k) and p
- Distinguisher $\mathcal{D}$ has query access to either E_k or p
- $\mathcal{D}$ tries to determine which oracle it communicates with

$$\mathsf{Adv}_E^{\mathrm{prp}}(\mathcal{D}) = \left|\mathbf{P}\left(\mathcal{D}^{E_k} = 1\right) - \mathbf{P}\left(\mathcal{D}^{p} = 1\right)\right|$$

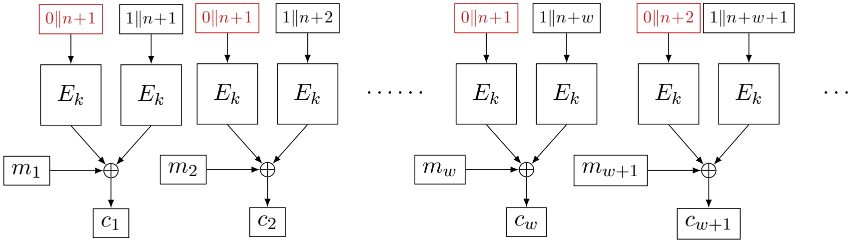
Pseudorandom Function



- Two oracles: F_k (for secret random key k) and f
- Distinguisher $\mathcal{D}$ has query access to either F_k or f
- $\mathcal{D}$ tries to determine which oracle it communicates with

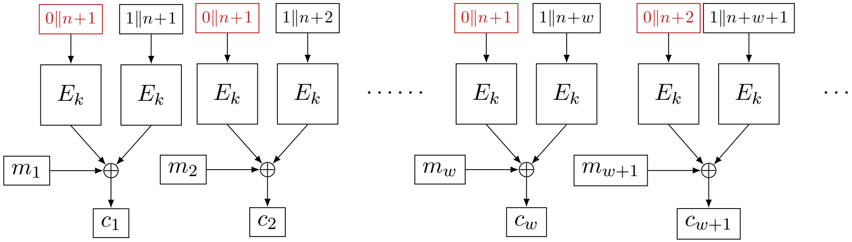
$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left| \mathbf{P}\left(\mathcal{D}^{F_k} = 1\right) - \mathbf{P}\left(\mathcal{D}^{f} = 1\right) \right|$$

CENC by Iwata [Iwa06]



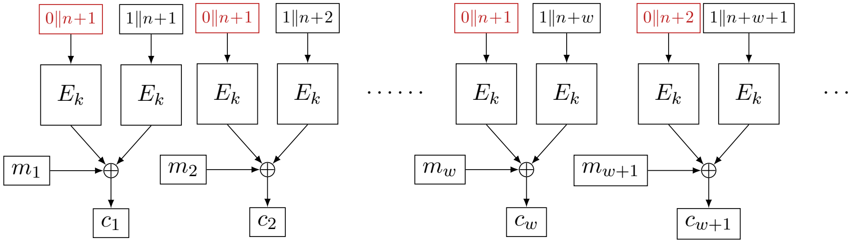
- One subkey used for $w \geq 1$ encryptions

CENC by Iwata [Iwa06]



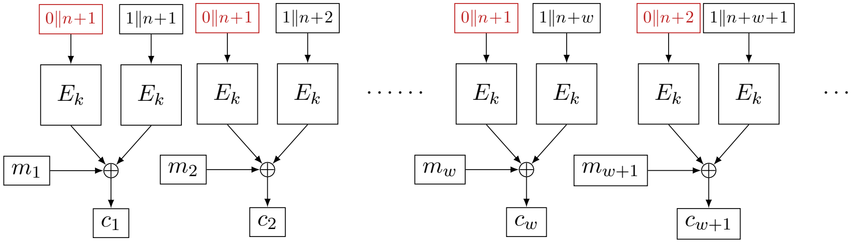
- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$

CENC by Iwata [Iwa06]



- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$
- 2006: $2^{2n/3}$ security, $2^n/w$ conjectured [Iwa06]

CENC by Iwata [Iwa06]



- One subkey used for $w \geq 1$ encryptions
- Almost as expensive as CTR$[E]$
- 2006: $2^{2n/3}$ security, $2^n/w$ conjectured [Iwa06]
- 2016: $2^n/w$ security [IMV16]