Improved Constructions of PRFs Secure Against Related-Key Attacks

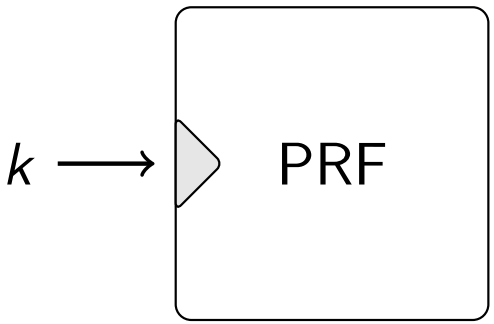
Kevin Lewi Hart Montgomery Ananth Raghunathan

Stanford University

Pseudorandom Functions (PRFs)

$k \xleftarrow{R} \mathcal{K}$

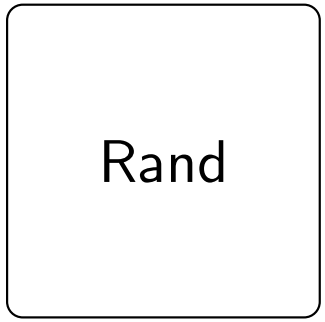
$x \in \{0,1\}^{\ell}$



x

$\mathrm{PRF}(k, x)$

$\approx$

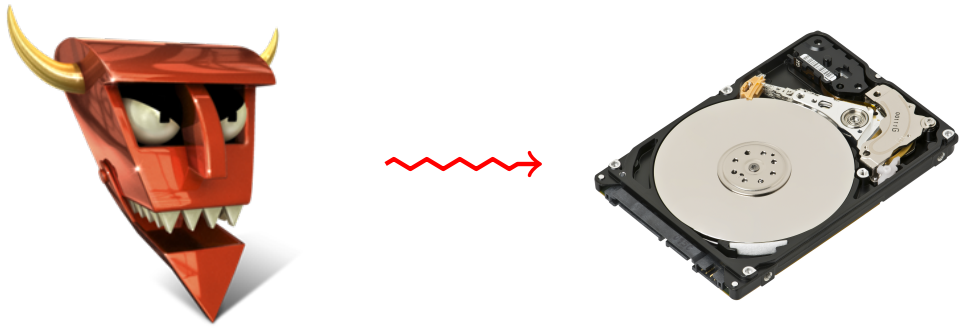


x

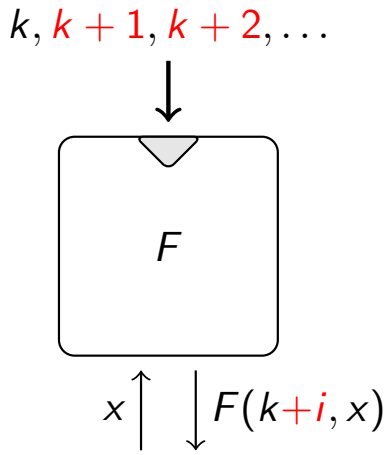
$\mathrm{Rand}(x)$

Related-Key Attacks

- With physical access, attacker can cause device to flip bits of the key



- Key update protocols that update the key using a known function



Related-Key Attacks on Blockciphers

RKAs on blockciphers have been effective in key recovery:

- 3-DES, DESX related-key slide and differential attacks
- AES-192 and AES-256 related-key differential attacks [Biryukov, Khovratovich 2009]

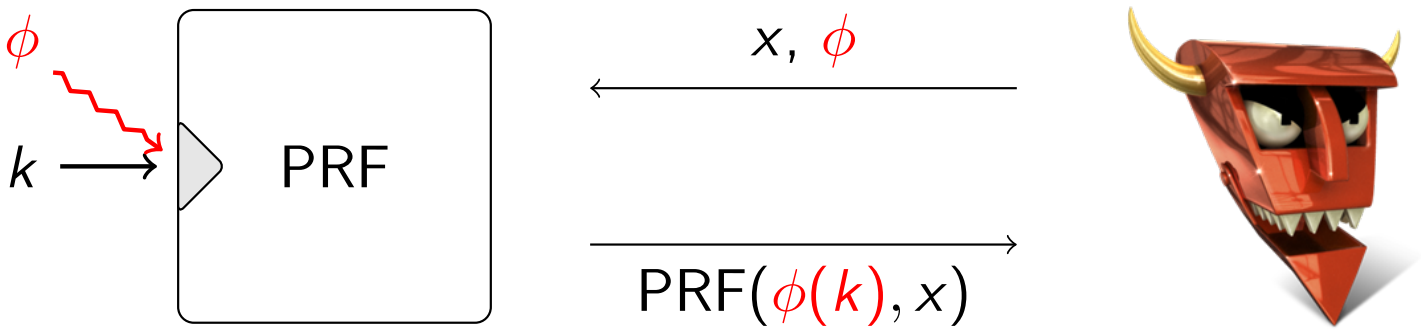
Other types of RKAs:

- boomerang attack, rectangle attack, SQUARE attack, and many more...

RKA-secure PRFs for a Class Φ [BK03]

For a fixed class Φ of related-key functions $\phi : \mathcal{K} \to \mathcal{K}$,

$k \xleftarrow{R} \mathcal{K}$ $\qquad$ $x \in \{0,1\}^\ell$, $\phi \in \Phi$

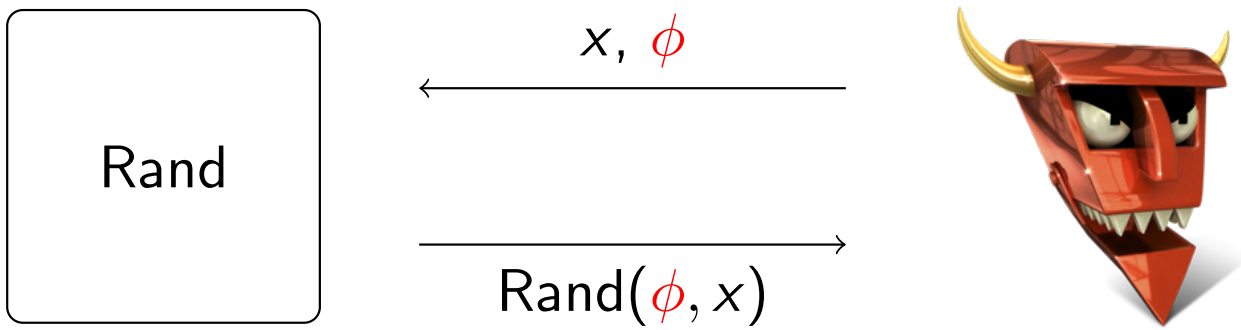


(Φ is the class of "related-key attacks" available to the adversary)

RKA-secure PRFs for a Class Φ [BK03]

For a fixed class Φ of related-key functions $\phi : \mathcal{K} \to \mathcal{K}$,

$$x \in \{0,1\}^\ell,\ \phi \in \Phi$$

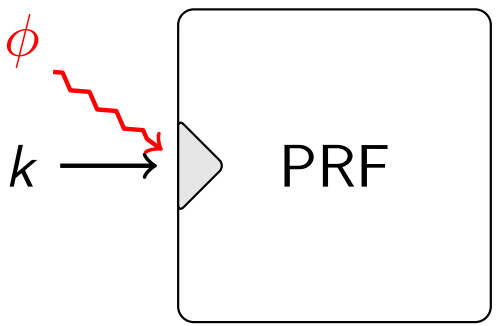


(Φ is the class of "related-key attacks" available to the adversary)

PRFs under Related-Key Attacks (Example)

$k \xleftarrow{R} \mathcal{K}$

$x \in \{0,1\}^{\ell}$, $\phi \in \Phi$



x, $\phi(k) = k \oplus 011$ $\longleftarrow$

$\longrightarrow$ $\mathrm{PRF}(k \oplus 011, x)$

Example: Suppose the adversary can tamper with the key by flipping any of its last 3 bits. Then,

$$\Phi = \{\phi_z \mid z \in \{0,1\}^3, \phi_z(k) = k \oplus z\}$$

Related-Key Attacks from a Theoretical Perspective

- 2003: Bellare and Kohno established a theoretical foundation for building blockciphers and PRFs resistant against RKAs
- 2010: Bellare and Cash built the first PRFs secure against non-trivial RKAs
- 2011: Bellare, Cash, and Miller showed how to transfer RKA security to higher-level primitives (IBE, sigs, etc.)
- 2012: Bellare, Paterson, and Thomson showed how to get RKA security for more expressive classes of attacks

Types of Algebraic Φ (from [BPT12])

For a PRF whose key space is $\mathbb{F}$ (field):

- Linear:

$$\Phi = \{\phi(k) = k + z\}_{z \in \mathbb{F}}$$

- Affine:

$$\Phi = \{\phi(k) = a \cdot k + b\}_{a,b \in \mathbb{F}} \qquad (a \neq 0)$$

- Polynomial (bounded degree):

$$\Phi = \{\phi(k) = c_1 \cdot k^d + c_2 \cdot k^{d-1} + \cdots + c_d \cdot k + c_{d+1}\}_{c_1,\ldots,c_{d+1} \in \mathbb{F}}$$

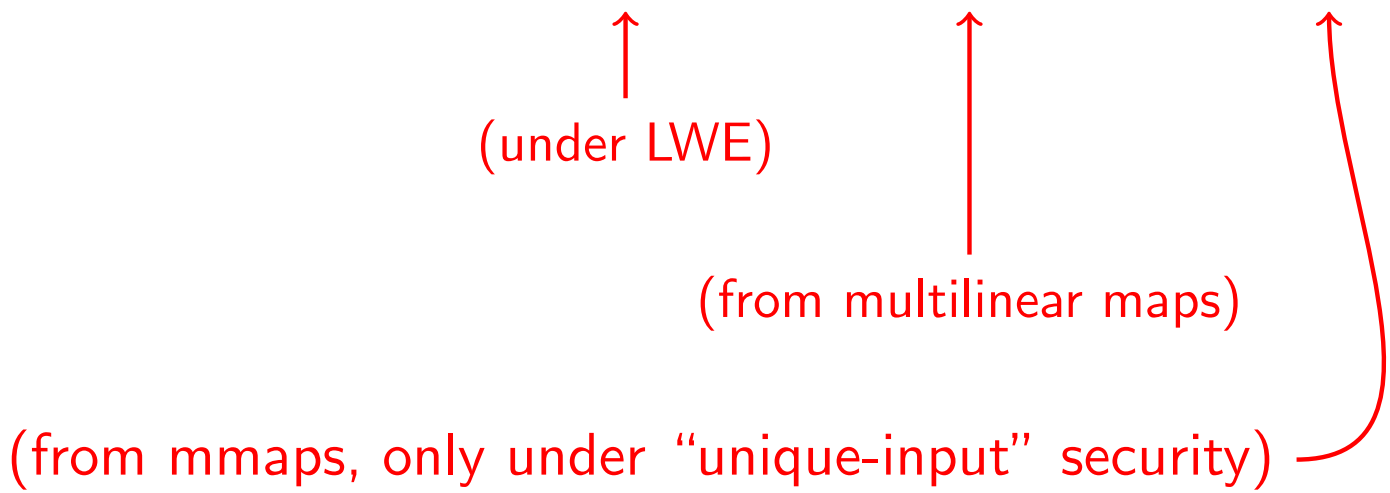
Related Work

[BC10] build RKA-secure PRFs for a non-trivial class of functions weaker than the linear class

Primitive	Linear	Affine	Polynomial
IBE	[BCM11]	[BPT12]	[BPT12]
Sig	[BCM11]	[BPT12]	[BPT12]
CCA-secure PKE	[Wee12]	[BPT12]	[BPT12]
CPA-secure SKE	[AHI11]	[GNR11]	[GNR11]
PRF	—	—	—

Our Results

Primitive	Linear	Affine	Polynomial
IBE	[BCM11]	[BPT12]	[BPT12]
Sig	[BCM11]	[BPT12]	[BPT12]
CCA-secure PKE	[Wee12]	[BPT12]	[BPT12]
CPA-secure SKE	[AHI11]	[GNR11]	[GNR11]
PRF	**[this work]***	**[this work]**	**[this work]**



- The Bellare-Cash Framework
- Unique-Input RKA Security

Bellare-Cash Framework

Theorem (Bellare, Cash 2010)

PRF + "key transformer for Φ" + "fingerprint" $\rightarrow$ *RKA-secure PRF for* Φ

given $\phi \in \Phi$ and $F(k, \cdot)$, can compute $F(\phi(k), \cdot)$

an input w s.t. for all k and distinct $\phi_1, \phi_2 \in \Phi$, $F(\phi_1(k), w) \neq F(\phi_2(k), w)$

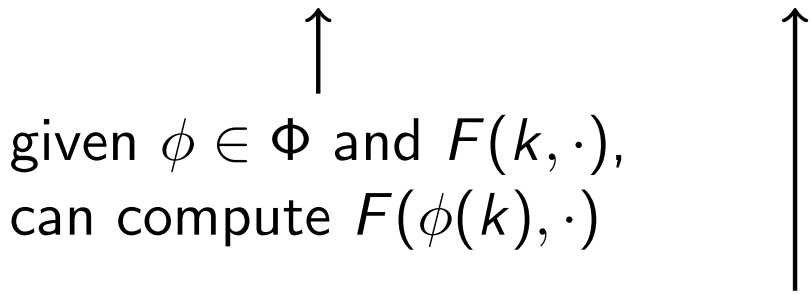
[BC10] Construction: $F_{\mathsf{rka}}(k, x) = F_{\mathsf{prf}}(k, H(x \| F_{\mathsf{prf}}(k, w)))$

("compatible" CR hash function)

Bellare-Cash Framework

Theorem (Bellare, Cash 2010)

PRF + "key transformer for Φ" + "fingerprint" $\rightarrow$ RKA-secure PRF for Φ



given $\phi \in \Phi$ and $F(k, \cdot)$,
can compute $F(\phi(k), \cdot)$

an input w s.t. for all k and distinct
$\phi_1, \phi_2 \in \Phi$, $F(\phi_1(k), w) \neq F(\phi_2(k), w)$

[BC10] Construction: $F_{\mathsf{rka}}(k, x) = F_{\mathsf{prf}}(k, H(x \| F_{\mathsf{prf}}(k, w)))$

("compatible" CR hash function)

Our Main Tool: Key Homomorphic PRFs [BLMR13]

For a PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$:

Key Homomorphism

We say F is key homomorphic if for all inputs x and keys k_1, k_2,

$$F(k_1, x) + F(k_2, x) = F(k_1 + k_2, x)$$

Our Main Tool: Key Homomorphic PRFs [BLMR13]

For a PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$:

Key Homomorphism

We say F is key homomorphic if for all inputs x and keys k_1, k_2,

$$F(k_1, x) + F(k_2, x) = F(k_1 + k_2, x)$$

Key Homomorphism $\Rightarrow$ Key Transformers for Linear Φ

For x and $\phi(k) = k + c$, key transformer queries for $F(k, x)$ and computes $F(c, x)$ to form $F(\phi(k), x)$.

Two Key Homomorphic PRFs [BLMR13]

- For integers $m, n, q, p > 0$, $\mathbf{k} \in \mathbb{Z}_q^n$, $x \in \{0,1\}^\ell$, $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{R} \{0,1\}^{m \times n}$,

$$pp = \mathbf{A}_0, \mathbf{A}_1, \qquad F_{\mathrm{LWE}}(\mathbf{k}, x) = \left\lfloor \prod_{i=1}^{\ell} \mathbf{A}_{x_i} \cdot \mathbf{k} \right\rfloor_p$$

- For integers $m, q > 0$, groups $\mathbb{G}_1, \ldots, \mathbb{G}_\ell$ with a multilinear map, $\mathbf{K} \in \mathbb{Z}_q^{m \times m}$, $x \in \{0,1\}^\ell$, $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{R} \{0,1\}^{m \times m}$,

$$pp = (g_1)^{\mathbf{A}_0}, (g_1)^{\mathbf{A}_1}, \qquad F_{\mathrm{DLIN}}(\mathbf{K}, x) = (g_\ell)^{\mathbf{K} \cdot \prod_{i=1}^{\ell} \mathbf{A}_{x_i}}$$

(here, g_i is a generator for group $\mathbb{G}_i$)

Key Homomorphic PRFs + BC framework

$$pp = \mathbf{A}_0, \mathbf{A}_1 \qquad pp = (g_1)^{\mathbf{A}_0}, (g_1)^{\mathbf{A}_1}$$

$$F_{\mathrm{LWE}}(\mathbf{k}, x) = \left\lfloor \prod_{i=1}^{\ell} \mathbf{A}_{x_i} \cdot \mathbf{k} \right\rfloor_p \qquad F_{\mathrm{DLIN}}(\mathbf{K}, x) = (g_\ell)^{\mathbf{K} \cdot \prod_{i=1}^{\ell} \mathbf{A}_{x_i}}$$

Theorem

Applying the BC framework to F_{LWE} yields a PRF secure against linear related-key attacks.*

Theorem

Applying the BC framework to F_{DLIN} yields a PRF secure against affine related-key attacks.

Key Homomorphic PRFs + BC framework

$$pp = \mathbf{A}_0, \mathbf{A}_1 \qquad pp = (g_1)^{\mathbf{A}_0}, (g_1)^{\mathbf{A}_1}$$

$$F_{\mathrm{LWE}}(\mathbf{k}, x) = \left\lfloor \prod_{i=1}^{\ell} \mathbf{A}_{x_i} \cdot \mathbf{k} \right\rfloor_p \qquad F_{\mathrm{DLIN}}(\mathbf{K}, x) = (g_\ell)^{\mathbf{K} \cdot \prod_{i=1}^{\ell} \mathbf{A}_{x_i}}$$

Theorem

Applying the BC framework to F_{LWE} yields a PRF secure against linear related-key attacks.*

Theorem

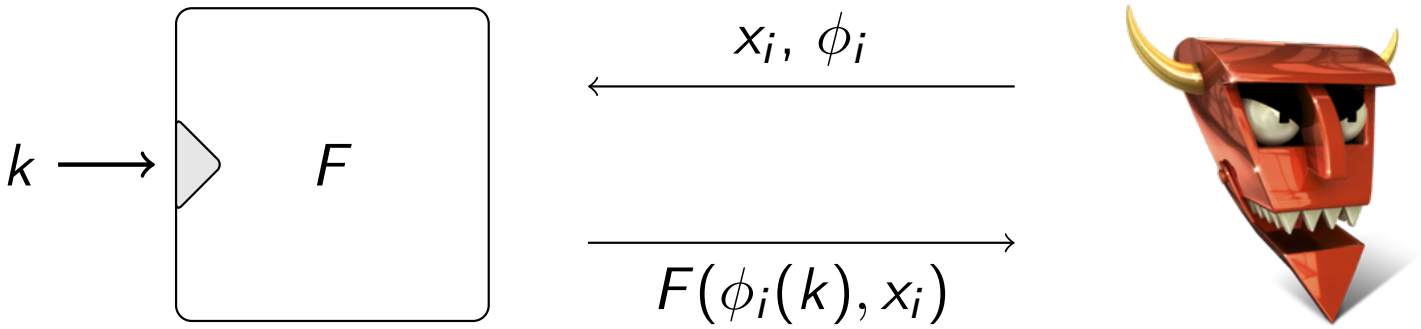
Applying the BC framework to F_{DLIN} yields a PRF secure against affine related-key attacks.

...what about a PRF secure against *polynomial* related-key attacks?

Unique-Input Security [BC10]

$k \xleftarrow{R} \{0,1\}^\lambda$

$x_i \in \{0,1\}^\ell,\ \phi_i \in \Phi$



Unique-Input Security: The inputs x_i are unique

Unique-Input Security For Polynomials

$$pp = (g_1)^{\mathbf{A}_0}, (g_1)^{\mathbf{A}_1}$$

$$F_{\mathrm{DLIN}}(\mathbf{K}, x) = (g_\ell)^{\mathbf{K} \cdot \prod_{i=1}^{\ell} \mathbf{A}_{x_i}}$$

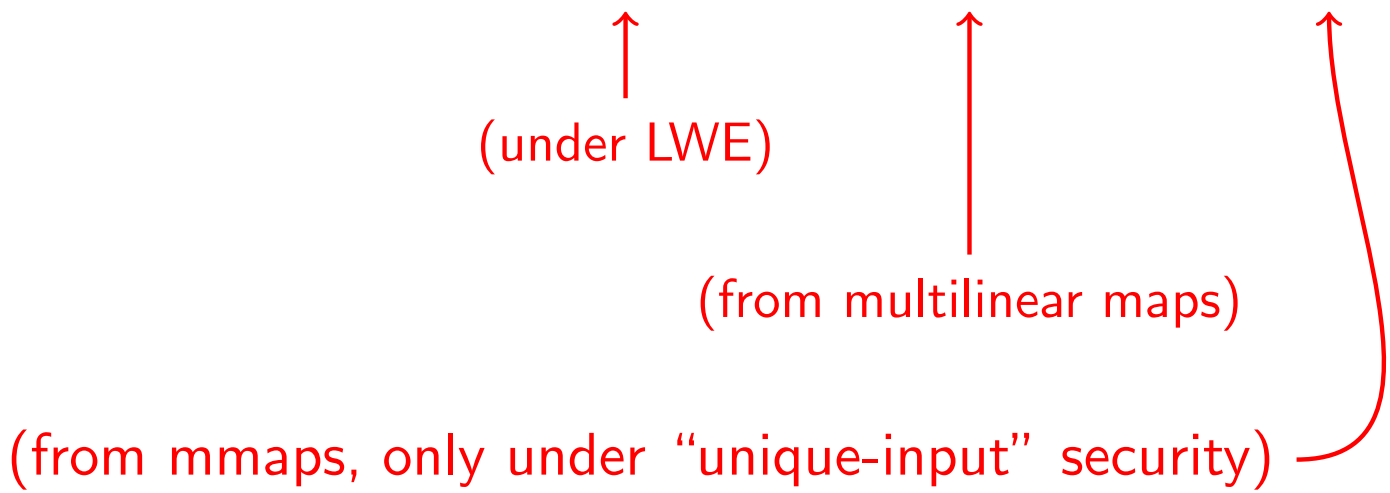
Theorem

F_{DLIN} is a PRF secure against polynomial related-key attacks (unique-input).

Open Problem: Can we show that F_{DLIN} is secure against polynomial RKAs without the unique-input restriction?

Our Results

Primitive	Linear	Affine	Polynomial
IBE	[BCM11]	[BPT12]	[BPT12]
Sig	[BCM11]	[BPT12]	[BPT12]
CCA-secure PKE	[Wee12]	[BPT12]	[BPT12]
CPA-secure SKE	[AHI11]	[GNR11]	[GNR11]
PRF	**[this work]***	**[this work]**	**[this work]**



Thanks!