A Fast and Key-Efficient Reduction from Chosen-Ciphertext to Known-Plaintext Security

Ueli Maurer
Johan Sjödin

Department of Computer Science
ETH Zurich, Switzerland

May 24, 2007

(Computational) Symmetric Cryptography

(Computational) Symmetric Cryptography

- *Efficient*

(Computational) Symmetric Cryptography

- *Efficient*
- *Short* key

(Computational) Symmetric Cryptography

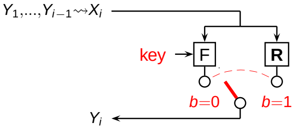
- *Efficient*
- *Short* key
- Conditional *security* (i.e., security is based on certain primitives)

(Computational) Symmetric Cryptography

- *Efficient*
- *Short* key
- Conditional *security* (i.e., security is based on certain primitives)

Pseudorandom Function (PRF)

$b = ?$



Adaptive Chosen-Plaintext Attack

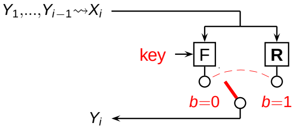
$$\mathbf{Adv}^{\text{CPA}}_{t,q}(\mathsf{F}, \mathbf{R})$$

(Computational) Symmetric Cryptography

- *Efficient*
- *Short* key
- Conditional *security* (i.e., security is based on certain primitives)

Pseudorandom Function (PRF)

$b = ?$



Adaptive Chosen-Plaintext Attack

$\mathbf{Adv}^{CPA}_{t,q}(\mathsf{F}, \mathbf{R})$

...but is AES really a pseudorandom permutation (and thus also a PRF)?

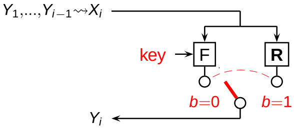
(Computational) Symmetric Cryptography

- *Efficient*
- *Short* key
- Conditional *security* (i.e., security is based on certain primitives)

Goal: weaken assumptions, improve efficiency

Pseudorandom Function (PRF)

$b = ?$



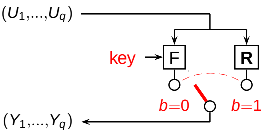
Adaptive Chosen-Plaintext Attack

$\mathbf{Adv}^{\mathrm{CPA}}_{t,q}(\mathrm{F}, \mathbf{R})$

...but is AES really a pseudorandom permutation (and thus also a PRF)?

This Paper: Weak PRFs

$b = ?$

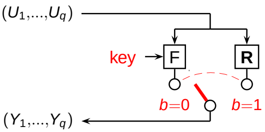


Known-Plaintext Attack

$$\mathbf{Adv}^{\mathsf{KPA}}_{t,q}(\mathsf{F}, \mathbf{R})$$

This Paper: Weak PRFs

$b = ?$



Known-Plaintext Attack

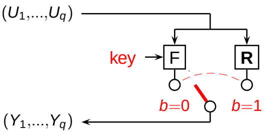
$\mathbf{Adv}^{\mathsf{KPA}}_{t,q}(\mathsf{F}, \mathbf{R})$

How weak are weak PRFs (under standard assumptions)?
E.g., they can:

- have large fraction of fix-points, i.e., $F_k(x) = x$ for many x.

This Paper: Weak PRFs

$b = ?$



Known-Plaintext Attack

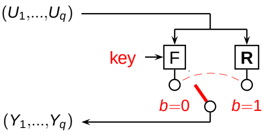
$\mathbf{Adv}^{\mathrm{KPA}}_{t,q}(\mathsf{F}, \mathbf{R})$

How weak are weak PRFs (under standard assumptions)?
E.g., they can:

- have large fraction of fix-points, i.e., $F_k(x) = x$ for many x.
- commute, i.e., $F_k(F_{k'}(x)) = F_{k'}(F_k(x))$.

This Paper: Weak PRFs

$b = ?$



Known-Plaintext Attack

$\mathbf{Adv}^{\mathrm{KPA}}_{t,q}(\mathsf{F}, \mathbf{R})$

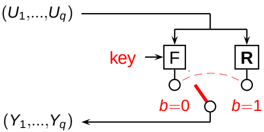
How weak are weak PRFs (under standard assumptions)?
E.g., they can:

- have large fraction of fix-points, i.e., $F_k(x) = x$ for many x.
- commute, i.e., $F_k(F_{k'}(x)) = F_{k'}(F_k(x))$.

$$\begin{array}{rcll} \exp : \mathbb{Z}_{|G|} \times G & \rightarrow & G & \text{(for DDH-group} G\text{)} \\ (k, x) & \mapsto & x^k & \end{array}$$

This Paper: Weak PRFs

$b = ?$



Known-Plaintext Attack

$\mathbf{Adv}^{\text{KPA}}_{t,q}(\mathsf{F}, \mathbf{R})$

How weak are weak PRFs (under standard assumptions)?
E.g., they can:

- have large fraction of fix-points, i.e., $F_k(x) = x$ for many x.
- commute, i.e., $F_k(F_{k'}(x)) = F_{k'}(F_k(x))$.

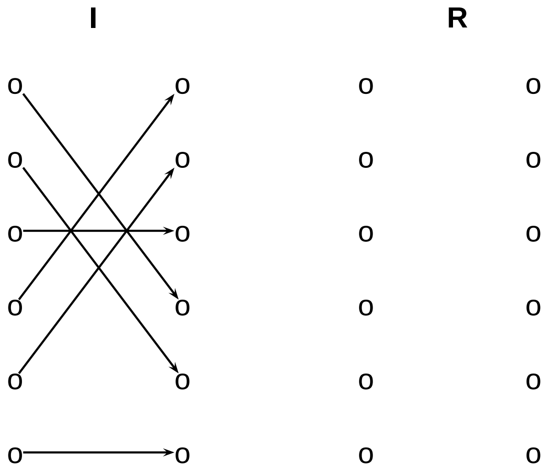
$$\begin{aligned} \exp : \mathbb{Z}_{|G|} \times G &\rightarrow G \qquad \text{(for DDH-group} G\text{)} \\ (k, x) &\mapsto x^k \end{aligned}$$

- be self inverse, i.e., $F_k(F_k(x)) = x$.

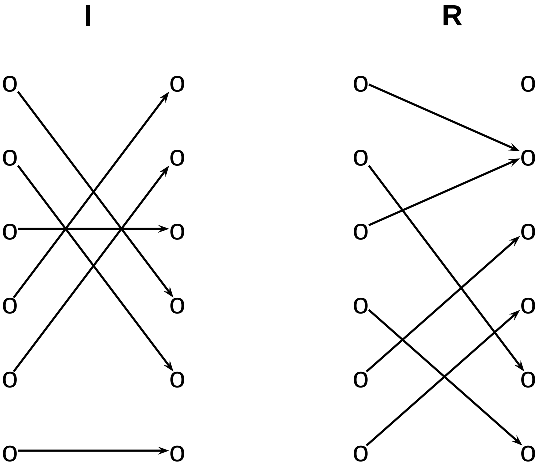
KPA vs. CPA: Example 1

I		R	
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

KPA vs. CPA: Example 1



KPA vs. CPA: Example 1



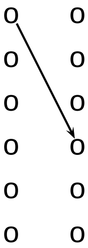
KPA vs. CPA: Example 1

- **I** or **R** under a CPA?

0	0
0	0
0	0
0	0
0	0
0	0

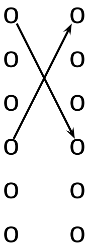
KPA vs. CPA: Example 1

- **I** or **R** under a CPA?



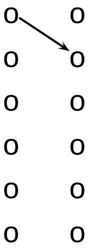
KPA vs. CPA: Example 1

- **I** or **R** under a CPA?



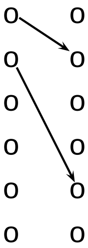
KPA vs. CPA: Example 1

- **I** or **R** under a CPA?



KPA vs. CPA: Example 1

- **I** or **R** under a CPA?



KPA vs. CPA: Example 1

- **I** or **R** under a CPA?

o	o
o	o
o	o
o	o
o	o
o	o

$\Rightarrow \quad \mathbf{I} \overset{\text{CPA}}{\not\approx} \mathbf{R}$

KPA vs. CPA: Example 1

- **I** or **R** under a CPA?

o	o
o	o
o	o
o	o
o	o
o	o

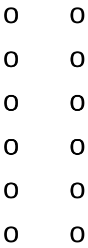
$\Rightarrow$ $\mathbf{I} \overset{\text{CPA}}{\not\approx} \mathbf{R}$

- **I** or **R** under a KPA?

o	o
o	o
o	o
o	o
o	o
o	o

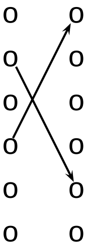
KPA vs. CPA: Example 1

- **I** or **R** under a CPA?



$\Rightarrow$ $\mathbf{I} \overset{\text{CPA}}{\not\approx} \mathbf{R}$

- **I** or **R** under a KPA?



KPA vs. CPA: Example 1

- **I** or **R** under a CPA?

o	o
o	o
o	o
o	o
o	o
o	o

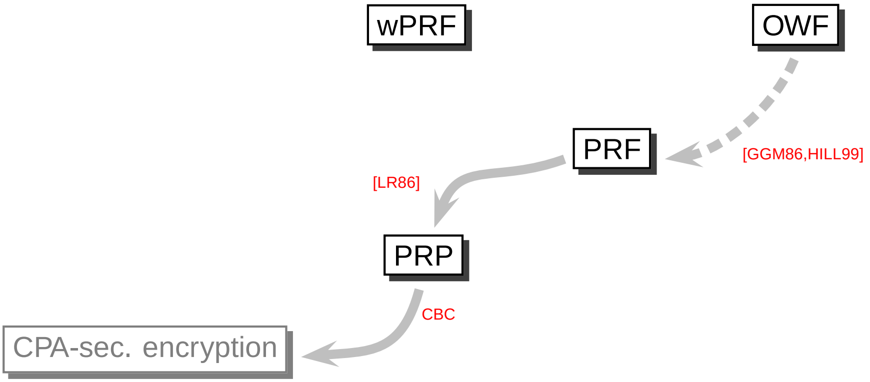
$\Rightarrow$ $\mathbf{I} \overset{\text{CPA}}{\not\approx} \mathbf{R}$

- **I** or **R** under a KPA?

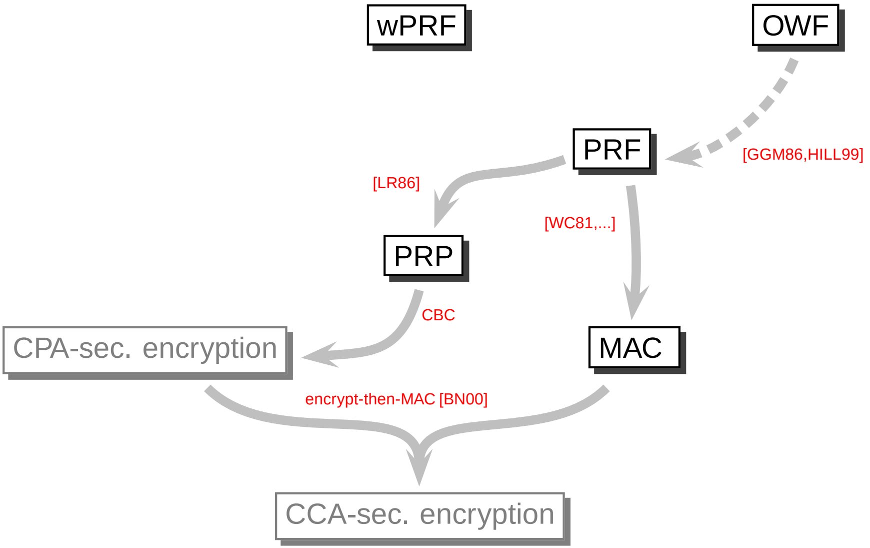
o	o
o	o
o	o
o	o
o	o
o	o

$\Rightarrow$ $\mathbf{I} \overset{\text{KPA}}{\approx} \mathbf{R}$

Efficient Symmetric Encryption based on wPRFs?

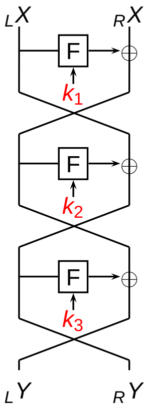


Efficient Symmetric Encryption based on wPRFs?



Feistel-Networks?

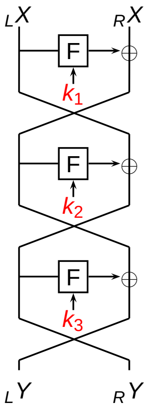
Feistel-Networks with PRFs do produce a PRP.



Feistel-Networks?

Feistel-Networks with wPRFs do not produce a PRP.

...even for infinitely many rounds!



Feistel-Networks?

Feistel-Networks with wPRFs do not produce a PRP.

...even for infinitely many rounds!

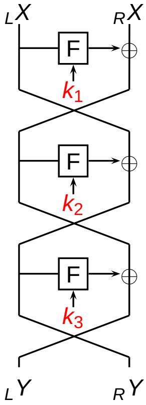
Reason

The wPRF F can have 0 as fixpoint,

$$\mathsf{F}_k(0) = 0 \qquad \text{(for all keys } k\text{)}$$

and hence

$$\psi[\mathsf{F}_{k_1}\mathsf{F}_{k_2}\mathsf{F}_{k_3}](0) = 0.$$



CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1\right]$ [NaoRei98]

CPA-Secure Encryption from any wPRF F

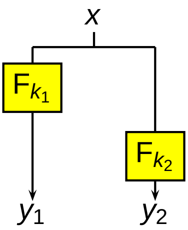
1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{c} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array} \right]$

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

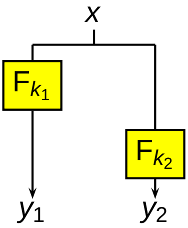
2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{c} \mathsf{F}_{k_1}(x) \oplus m_1 \\ \mathsf{F}_{k_2}(x) \oplus m_2 \end{array} \right]$



CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1\right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{c} \mathsf{F}_{k_1}(x) \oplus m_1 \\ \mathsf{F}_{k_2}(x) \oplus m_2 \end{array}\right]$

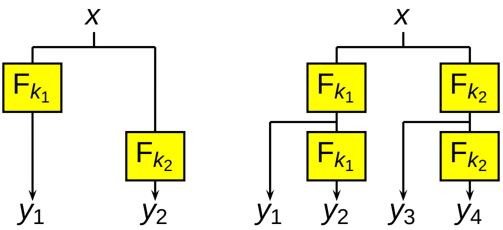


⇒ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{l} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array} \right]$

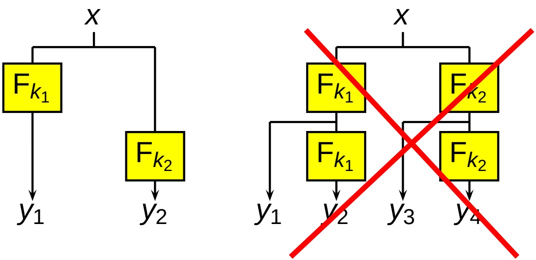


⇒ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{l} \mathsf{F}_{k_1}(x) \oplus m_1 \\ \mathsf{F}_{k_2}(x) \oplus m_2 \end{array} \right]$

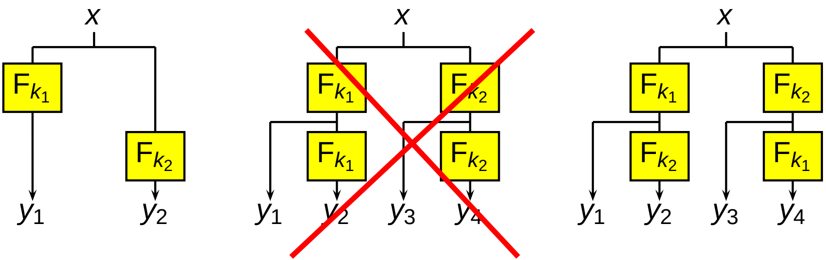


⇒ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{l} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array} \right]$

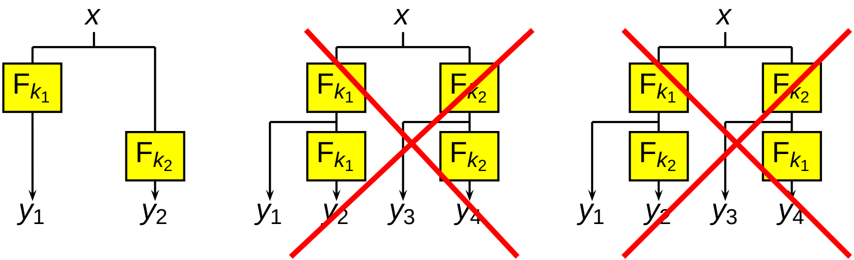


⇒ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1\right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{c} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array}\right]$

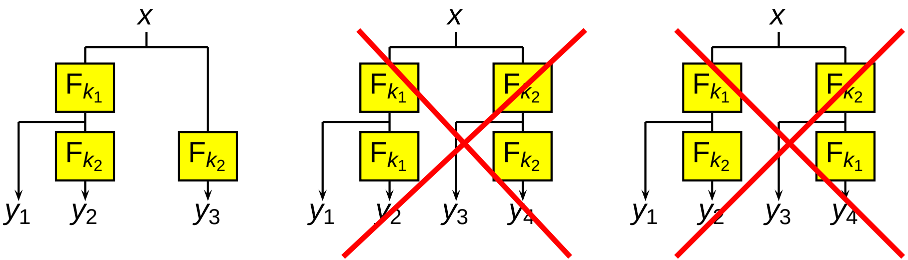


$\Rightarrow$ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1 \right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{l} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array} \right]$

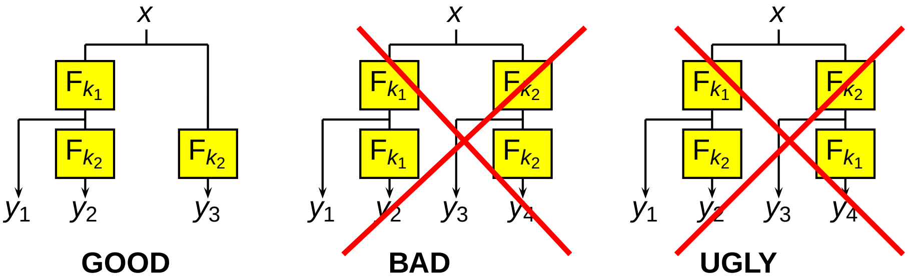


⇒ How to extend this further (using as few keys as possible)?

CPA-Secure Encryption from any wPRF F

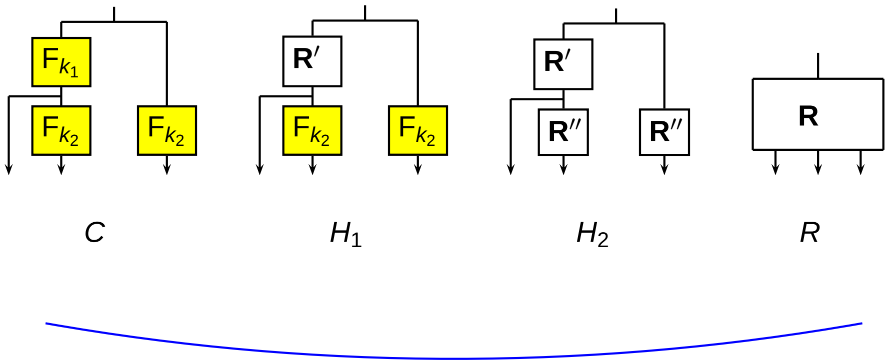
1 block of data: $Enc_{k_1}(m_1) := \left[x, F_{k_1}(x) \oplus m_1\right]$ [NaoRei98]

2 blocks of data: $Enc_{k_1,k_2}(m_1, m_2) := \left[x, \begin{array}{l} F_{k_1}(x) \oplus m_1 \\ F_{k_2}(x) \oplus m_2 \end{array}\right]$



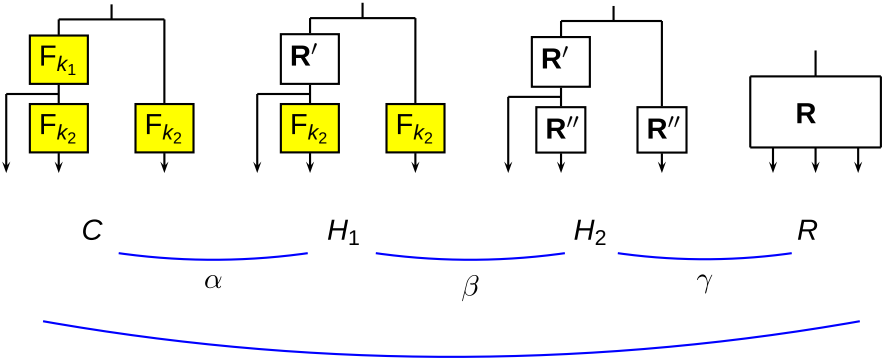
$\Rightarrow$ How to extend this further (using as few keys as possible)?

Proof (of the “Good” range extension for wPRFs)



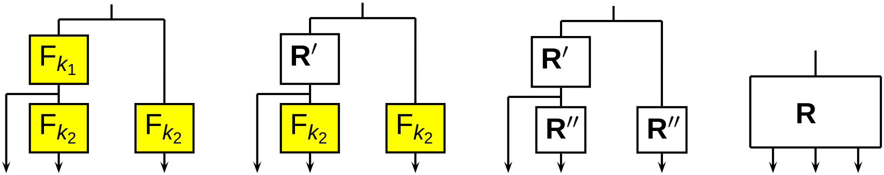
$$\mathbf{Adv}_{t,q}^{\mathrm{KPA}}(C, R) \leq ?$$

Proof (of the "Good" range extension for wPRFs)



$$\mathbf{Adv}^{\mathrm{KPA}}_{t,q}(C,R) \leq \alpha + \beta + \gamma$$

Proof (of the “Good” range extension for wPRFs)

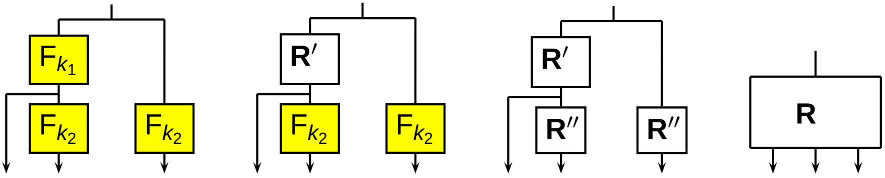


C H_1 H_2 R

$\leq \mathbf{Adv}^{\text{KPA}}_{t,q}(\mathsf{F},\mathbf{R}')$ $\leq \mathbf{Adv}^{\text{KPA}}_{t,2q}(\mathsf{F},\mathbf{R}'')+q^2/2^{n+1}$ $\leq q^2/2^{n+1}$

$$\mathbf{Adv}^{\text{KPA}}_{t,q}(C,R) \leq \alpha + \beta + \gamma$$

Proof (of the "Good" range extension for wPRFs)



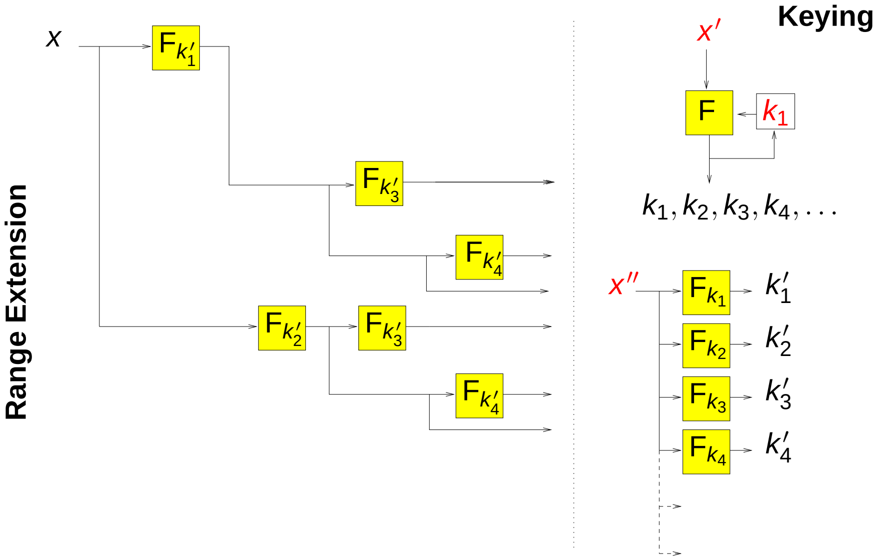
C $\quad H_1 \quad H_2 \quad R$

$\leq \mathbf{Adv}^{\text{KPA}}_{t,q}(\mathsf{F},\mathbf{R}')$ $\quad \leq \mathbf{Adv}^{\text{KPA}}_{t,2q}(\mathsf{F},\mathbf{R}'')+q^2/2^{n+1}$ $\quad \leq q^2/2^{n+1}$

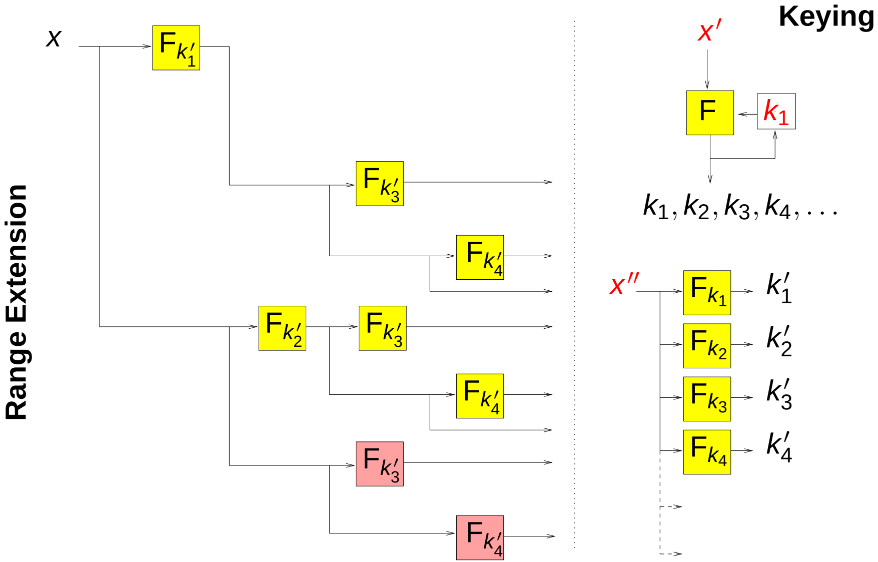
$$\mathbf{Adv}^{\text{KPA}}_{t,q}(C,R) \leq \alpha + \beta + \gamma$$

$\Rightarrow$ How can the range of F be extended even more?

Range Extension of wPRFs [DN02]

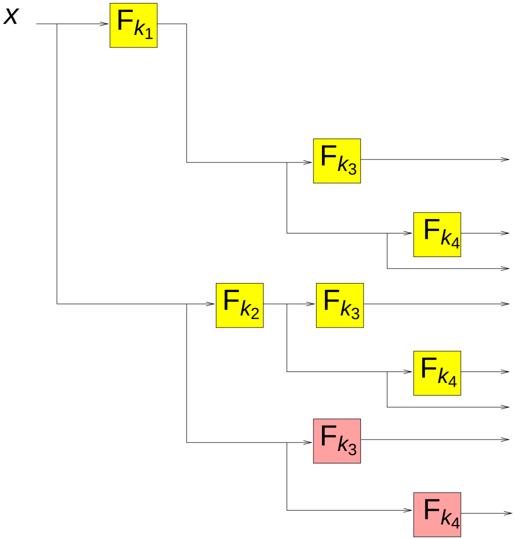


Range Extension of wPRFs [MT05]

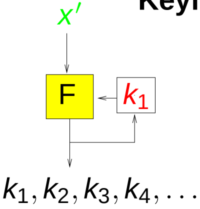


Range Extension of wPRFs [this paper]

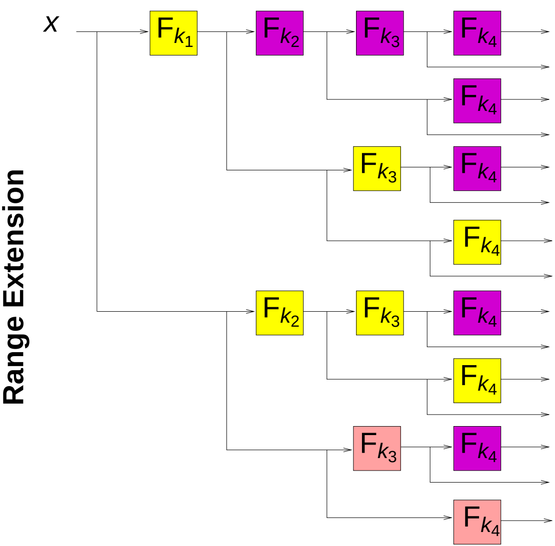
Range Extension



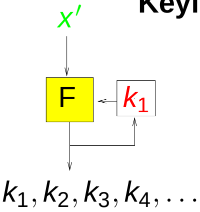
Keying



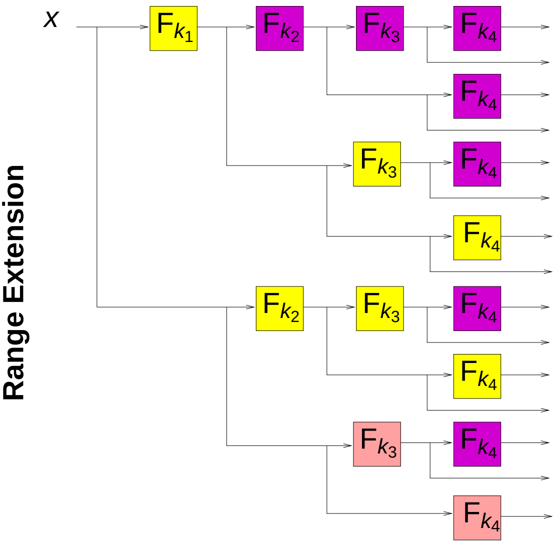
Range Extension of wPRFs [this paper]



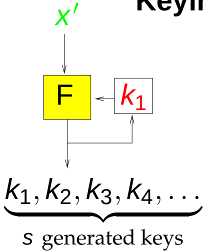
Keying



Range Extension of wPRFs [this paper]



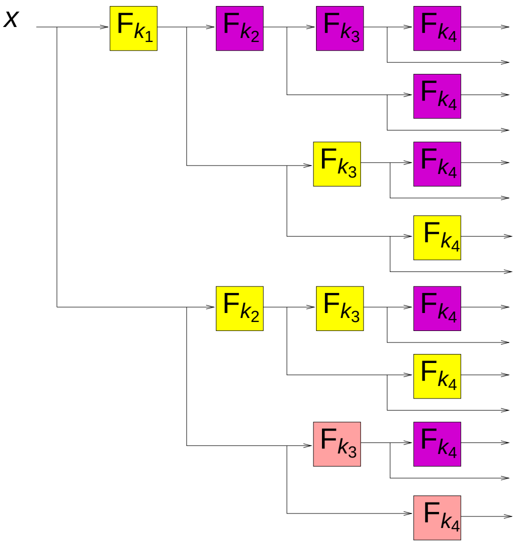
Keying



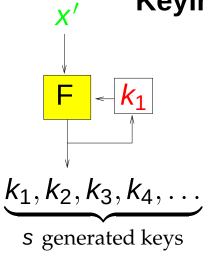
	# keys	out-puts	over-head
DN02	3	1.4^s	$2s$
MT05	3	1.7^s	$2s$
this	**1**	$\mathbf{2}^s$	**s**

Range Extension of wPRFs [this paper]

Range Extension

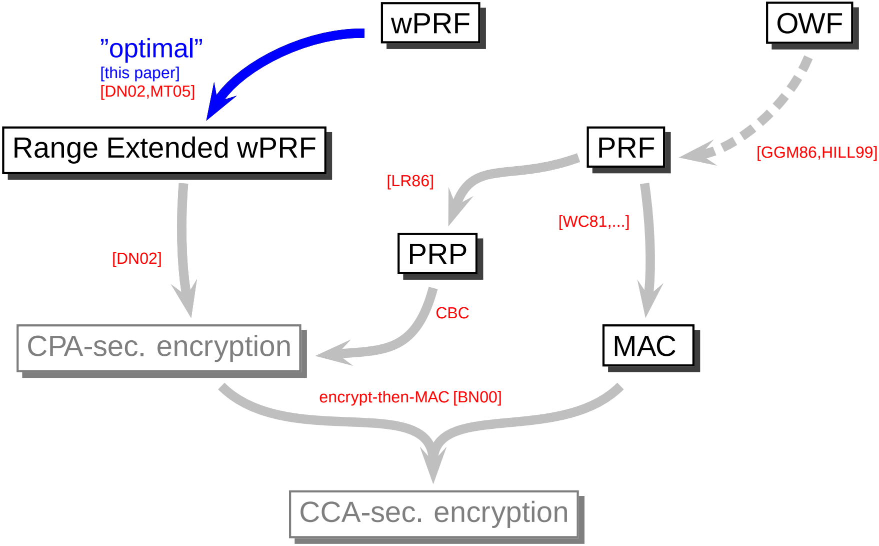


Keying



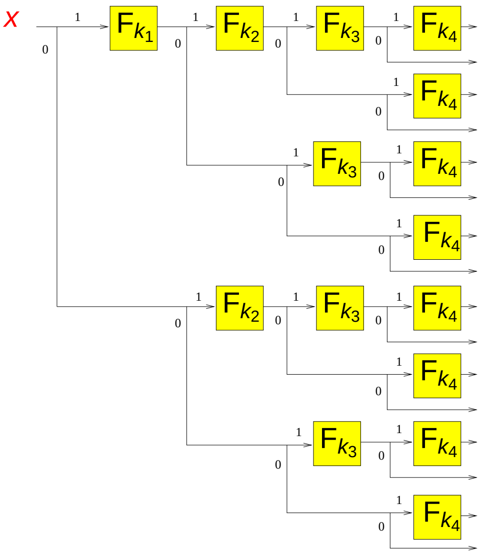
	# keys	out-puts	over-head
DN02	3	1.4^s	$2s$
MT05	3	1.7^s	$2s$
this	**1**	$\mathbf{2}^s$	**s**
better	no, this is “optimal”		

Overview

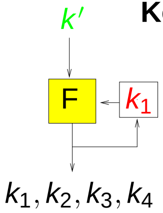

wPRF
OWF
"optimal"
[this paper]
[DN02,MT05]
Range Extended wPRF
PRF
[GGM86,HILL99]
[LR86]
[WC81,...]
PRP
[DN02]
CBC
CPA-sec. encryption
MAC
encrypt-then-MAC [BN00]
CCA-sec. encryption

wPRF ⇒ PRF [this paper]

All Outputs



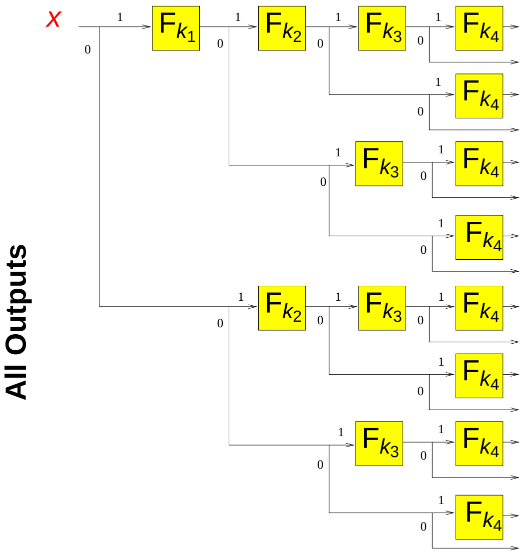
Keying



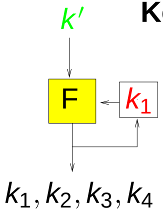
Input: 4-bits $b_1b_2b_3b_4$

Output: block $b_1b_2b_3b_4$

wPRF ⇒ PRF [this paper]



Keying



Input: 4-bits $b_1 b_2 b_3 b_4$

Output: block $b_1 b_2 b_3 b_4$

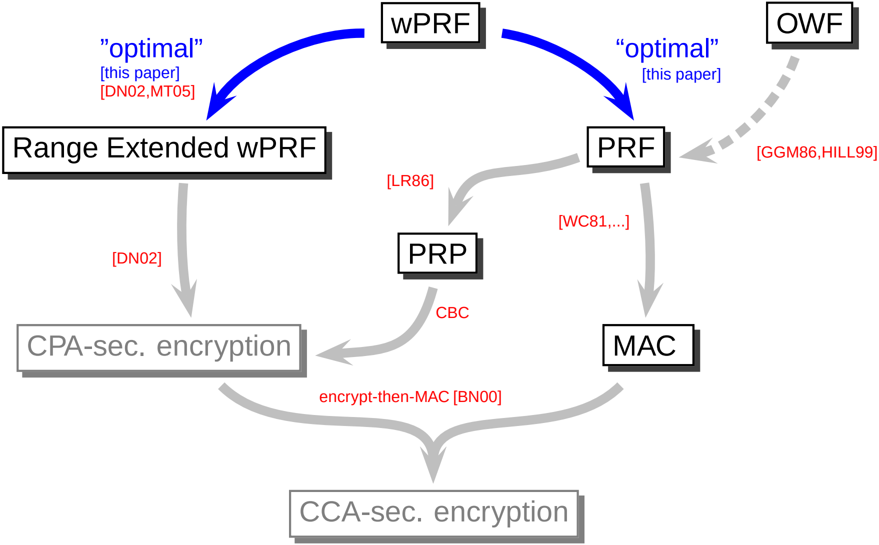
DDH-based wPRF: $x \mapsto x^k$

$\Rightarrow$

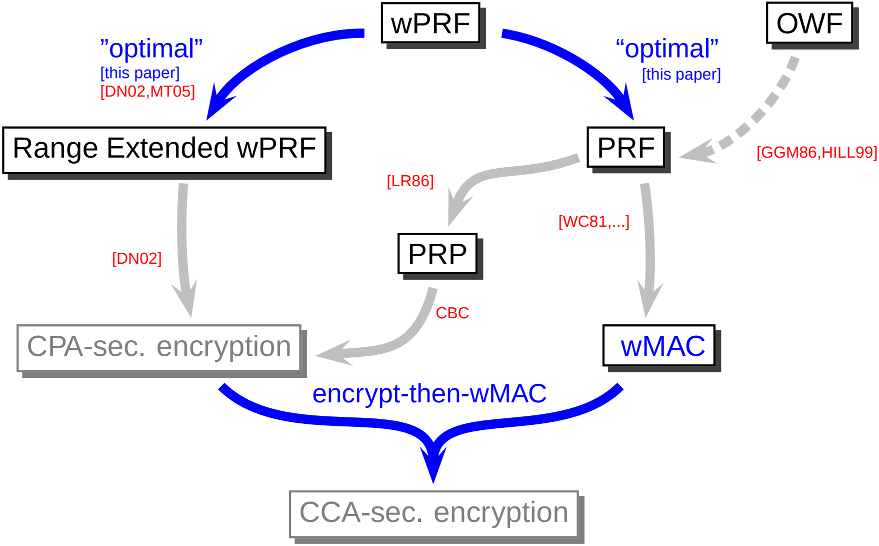
DDH-based PRF [NaoRei97]:

$(b_1, b_2, b_3, b_4) \mapsto x^{\prod_{b_i=1} k_i}$

Conclusions



Conclusions



Conclusions