RSAConference2021
May 17 – 20 | Virtual Experience


SESSION ID: **CRYP-W06C**

# The Key-Dependent Message Security of Key-Alternating Feistel Ciphers

**By Pooya Farshim, Louiza Khati, Yannick Seurin and Damien Vergnaud.**

ANSSI and ENS

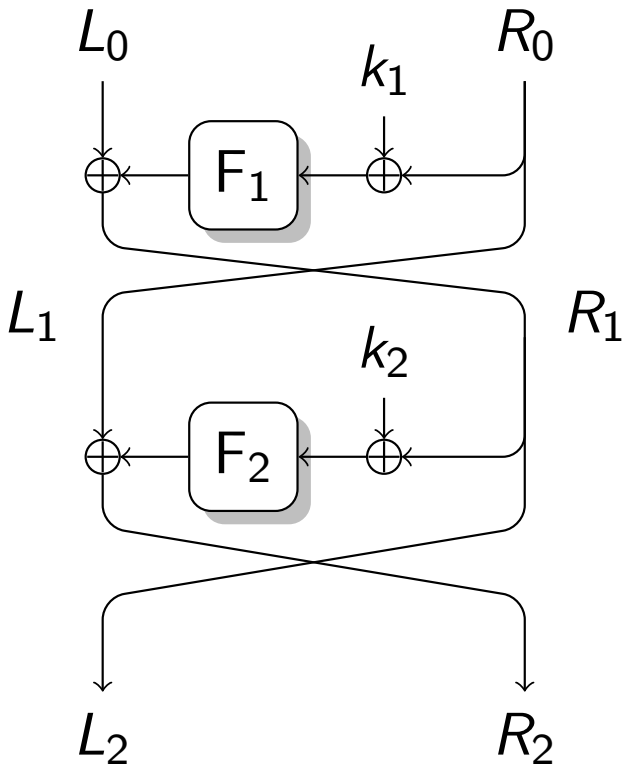
# KDM Security

- Key Dependent-Message Security
  - access to a ciphertext resulting from the encryption of **key-dependent message** [BRS03]

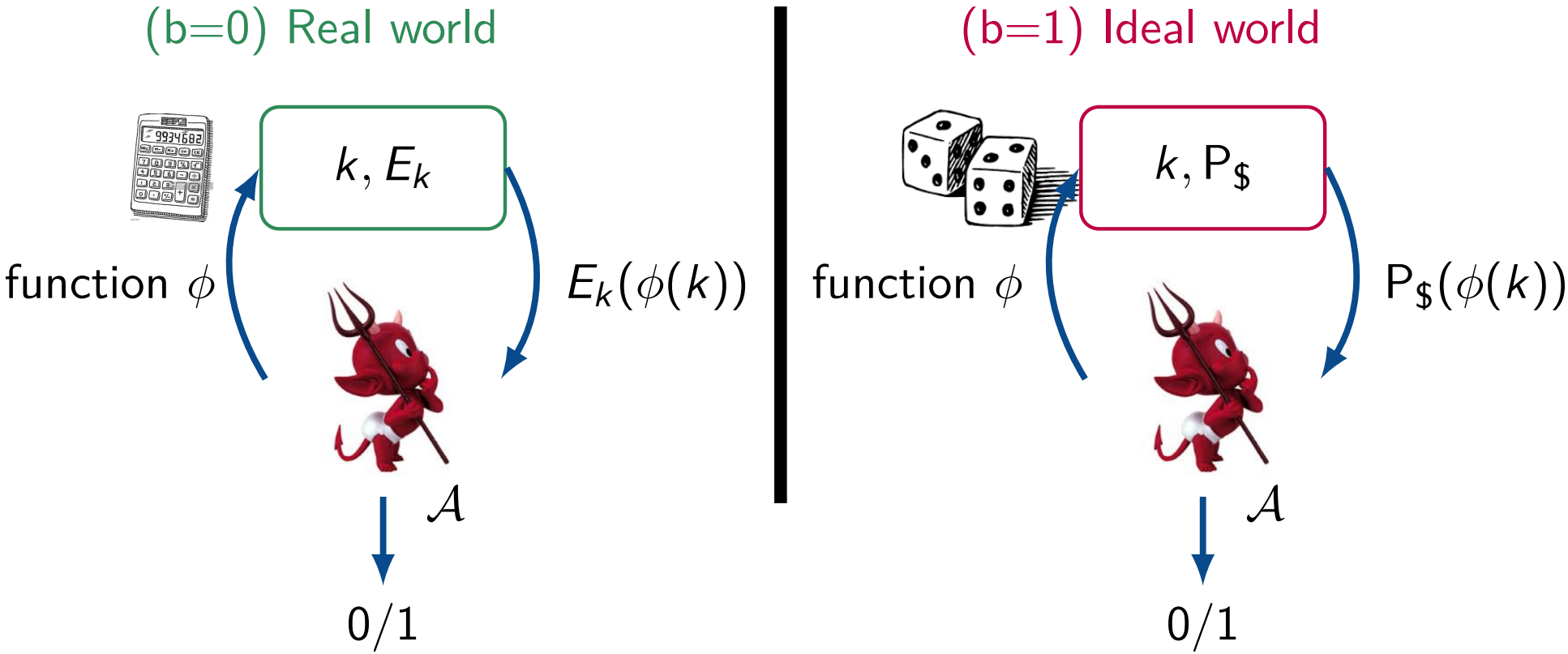
- Full disk encryption

# Key-Alternating Feistel (KAF)

- Configuration:
  - $r$ rounds
  - $r$ internal functions $\mathsf{F}_i$ ($=$ or $\neq$)
  - Key schedule:
    - $r$ keys ($=$ or $\neq$)
    - $r$ keys derivated from a master key
- Previous security analysis
  - Indistinguishability ([LS15])
  - (Indifferentiability KAF*[GL15])
- Examples:
  - DES, GOST etc.



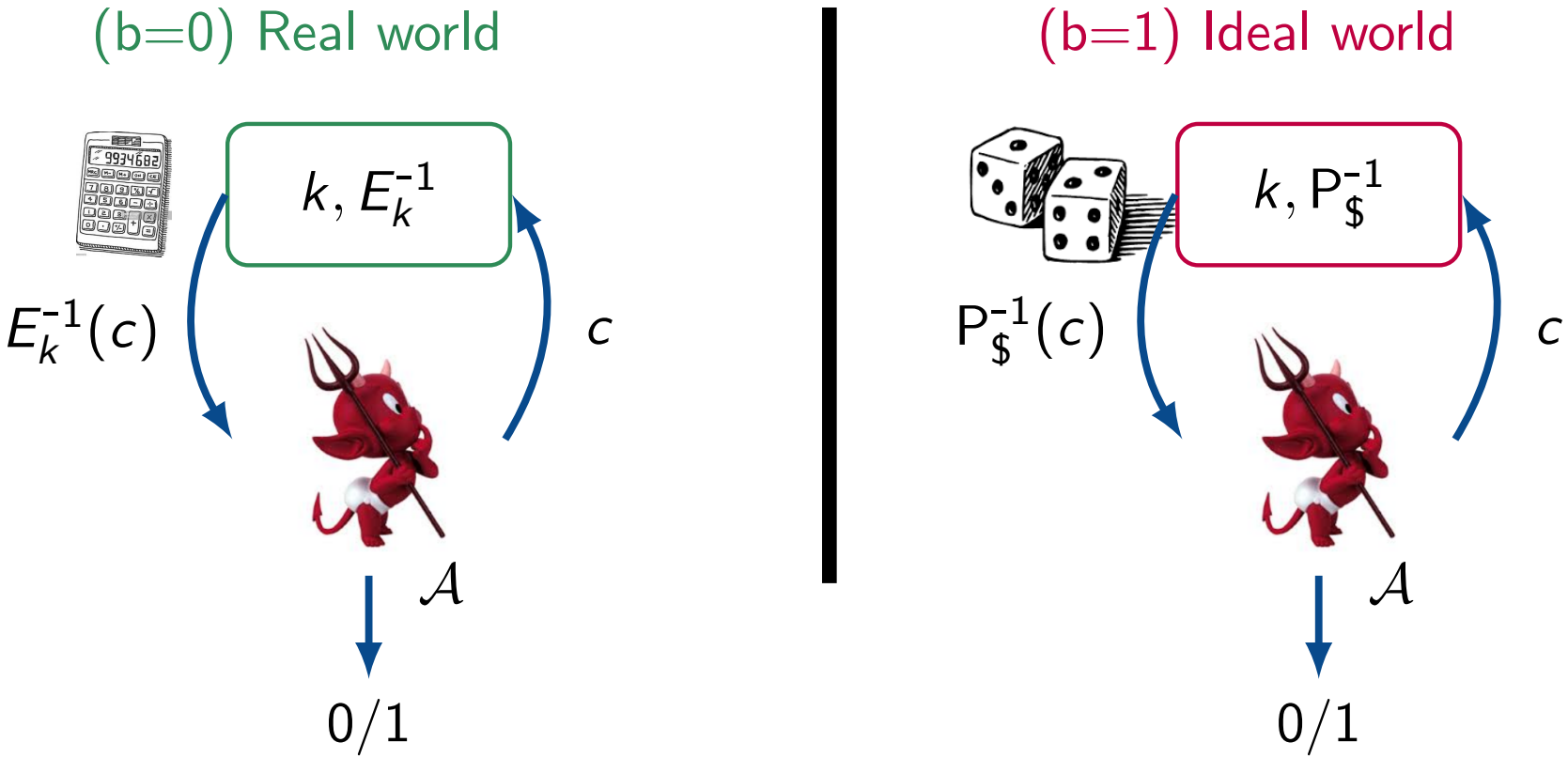
# KDM security: Indistinguishability game




KDM-CPA adversary

$$\mathbf{Adv} = |\ \Pr[\mathcal{A} \to 1|\text{Real}] - \Pr[\mathcal{A} \to 1|\text{Ideal}]\ |$$

# KDM security: Indistinguishability game




KDM-CCA adversary ("Standard" decryption)

$$\mathbf{Adv} = |\ \Pr[\mathcal{A} \to 1|\text{Real}] - \Pr[\mathcal{A} \to 1|\text{Ideal}]\ |$$

# KDM set restriction: Claw-freeness

- Find the largest set $\Phi$ of functions $\phi$ such that Adv is small
  - Including constant functions
- The KDM set $\Phi$ has to be restricted $\rightarrow$ Key extraction [FKV17]

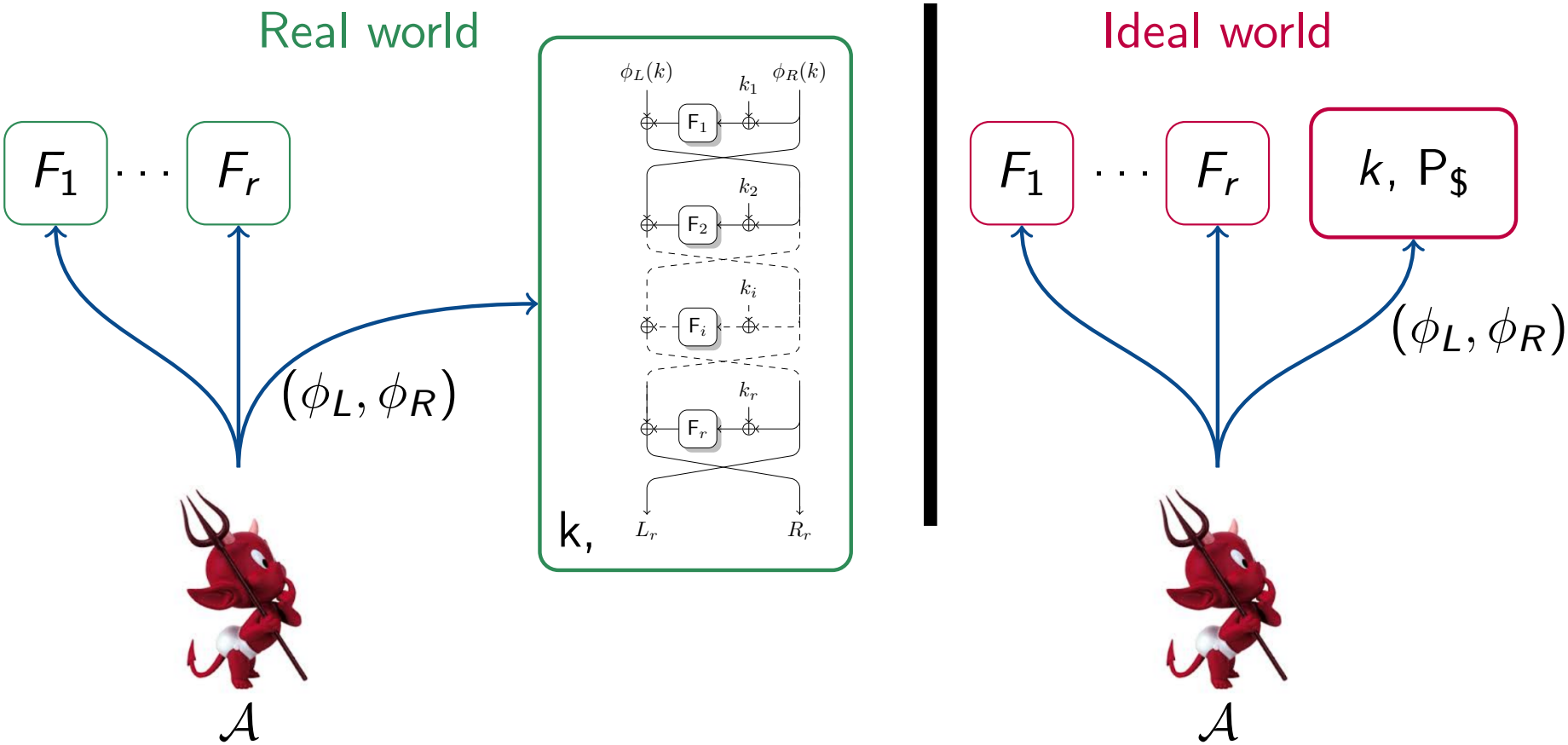
Claw-freeness of a set $\Phi$:

$$\mathbf{cf}(\Phi) := \max_{\phi_1 \neq \phi_2 \in \Phi} \Pr[k \twoheadleftarrow \mathcal{K} : \phi_1(k) = \phi_2(k)]$$

KDM security:

- Ideal-Cipher KDM-secure under claw-free sets [FKV17]
- What about Key-Alternating Feistels ?

# Securiy analysis: KDM Security game for KAF




$F_i$ uniformly random functions,
KDM set $\Phi = (\Phi_L, \Phi_R)$

# KDM attack

- A claw-free set $\Phi$ is not always enough...

# KDM attack

- A claw-free set $\Phi$ is not always enough...
- 4-round KAF
  - Same internal function
  - **Independent keys**
  - Attack 2 queries $\rightarrow$ $\Phi_R$ offset-free

Detailed in the paper

Offset-freeness of a set $\Phi$:

$$\mathbf{of}(\Phi) := \max_{\substack{i\in\{1,..,\ell\} \\ \phi\in\Phi,\, x\in\{0,1\}^n}} \Pr[(k_1,..,k_\ell) \twoheadleftarrow \mathcal{K} : \phi(k_1,..,k_\ell) = k_i \oplus x]$$

# KDM attack

- A claw-free set $\Phi$ is not always enough...
- 4-round KAF
  - Same internal function
  - **Independent keys**
  - Attack 2 queries $\rightarrow \Phi_R$ offset-free

Detailed in the paper

- Sliding attack (any number of rounds)
  - Same internal function and same key
  - not CPA-secure
  - Key extraction attack (1 query)
    - $\phi_L(k) = k \oplus \mathsf{F}^2(\Delta) \oplus \Delta \oplus \mathsf{F}[\mathsf{F}(\Delta) \oplus \mathsf{F}(\mathsf{F}^2(\Delta) \oplus \Delta)$
    - $\phi_R(k) = k \oplus \mathsf{F}(\Delta) \oplus \mathsf{F}[\mathsf{F}^2(\Delta) \oplus \Delta]$
    - $R_r = k$
    - $L_r \oplus R_r = \Delta$

# Generic Proof Methodology

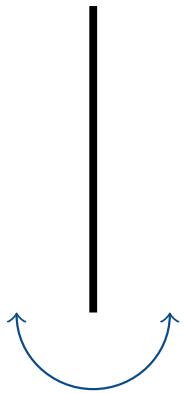
Ideal world (iw) Perfect world (pw) Real world (rw)

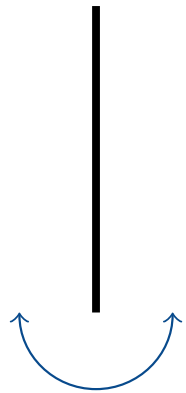
$\mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A})$ $\mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A})$

- Indistinguishability game with H-coefficient technique
- Triangular inequality: $\mathbf{Adv}_{\mathsf{iw},\mathsf{rw}}(\mathcal{A}) \leq \mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A}) + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A})$

# Generic Proof Methodology

Ideal world (iw) Perfect world (pw) Real world (rw)





$\mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A})$

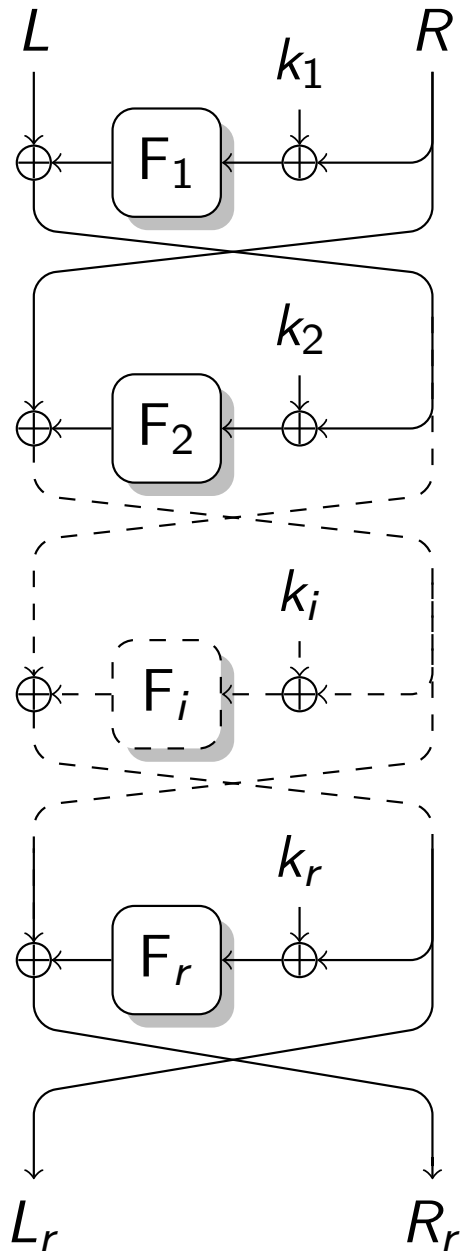
$\mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A})$

Detailed in the paper

- Indistinguishability game with H-coefficient technique
- Triangular inequality: $\mathbf{Adv}_{\mathsf{iw},\mathsf{rw}}(\mathcal{A}) \leq \mathbf{Adv}_{\mathsf{iw},\mathsf{pw}}(\mathcal{A}) + \mathbf{Adv}_{\mathsf{pw},\mathsf{rw}}(\mathcal{A})$

# Results: Key-Alternating Feistel

| Rounds | Functions | Keys schedule | KDM set |
|---|---|---|---|
| 4 | $\mathsf{F}_i =$ | $k_1, 0, 0, k_2$ | **cf** $\wedge$ **of** $\wedge$ **oxf** |
| 4 | $\mathsf{F}_i \neq$ | $k_i \neq$ | **cf** $\wedge$ **of**? |
| 5 | $\mathsf{F}_i =$ | $k_i \neq$ | **cf** $\wedge$ **of**? |
| ? | $\mathsf{F}_i =$ | $k_i \neq$ | **cf** |



# Results: Key-Alternating Feistel

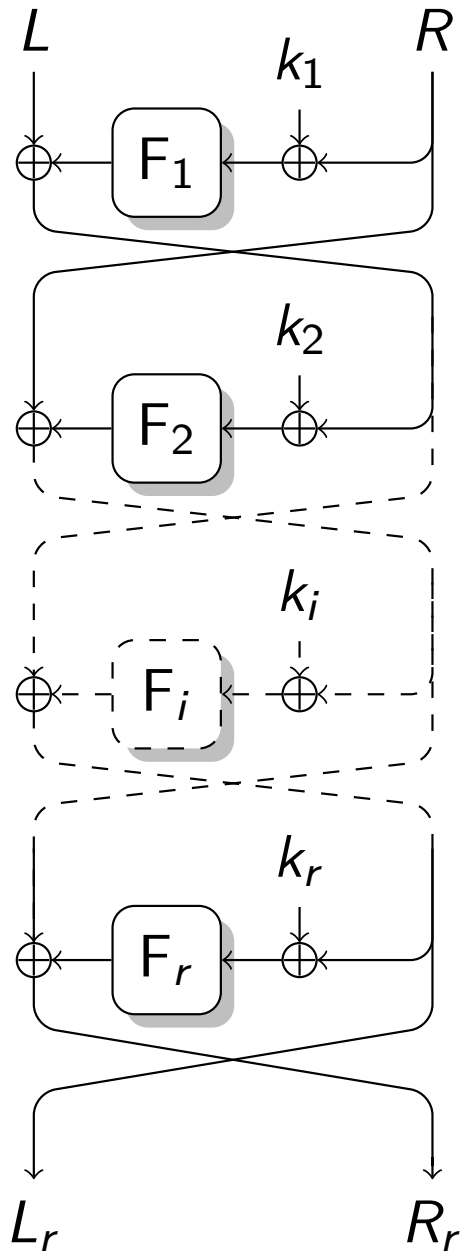
| Rounds | Functions | Keys schedule | KDM set |
|---|---|---|---|
| 4 | $\mathsf{F}_i =$ | $k_1, 0, 0, k_2$ | $\mathbf{cf} \wedge \mathbf{of} \wedge \mathbf{oxf}$ |
| 4 | $\mathsf{F}_i \neq$ | $k_i \neq$ | $\mathbf{cf} \wedge \mathbf{of}?$ |
| 5 | $\mathsf{F}_i =$ | $k_i \neq$ | $\mathbf{cf} \wedge \mathbf{of}?$ |
| ? | $\mathsf{F}_i =$ | $k_i \neq$ | $\mathbf{cf}$ |

Xor-offset-freeness of a set $\Phi$:

$$\mathbf{oxf}(\Phi) := \max_{\substack{i \neq j \in \{1,..,\ell\} \\ \phi \in \Phi,\, x \in \{0,1\}^n}} \Pr[(k_1, .., k_\ell) \twoheadleftarrow \mathcal{K} : \phi(k_1, .., k_\ell) = k_i \oplus k_j \oplus x]$$

# Results: Key-Alternating Feistel

| Rounds | Functions | Keys schedule | KDM set |
|---|---|---|---|
| 4 | $\mathsf{F}_i =$ | $k_1, 0, 0, k_2$ | **cf** $\wedge$ **of** $\wedge$ **oxf** |
| 4 | $\mathsf{F}_i \neq$ | $k_i \neq$ | **cf** $\wedge$ **of**? |
| 5 | $\mathsf{F}_i =$ | $k_i \neq$ | **cf** $\wedge$ **of**? |
| ? | $\mathsf{F}_i =$ | $k_i \neq$ | **cf** |



RSAConference2021

# Thank you for your attention.

## Questions ?


Manuel Barbosa and Pooya Farshim.
The related-key analysis of Feistel constructions.
In Carlos Cid and Christian Rechberger, editors, FSE 2014, volume 8540 of LNCS, pages 265–284, London, UK, March 3–5, 2015. Springer, Heidelberg, Germany.


John Black, Phillip Rogaway, and Thomas Shrimpton.
Encryption-scheme security in the presence of key-dependent messages.
In Kaisa Nyberg and Howard M. Heys, editors, SAC 2002, volume 2595 of LNCS, pages 62–75, St. John's, Newfoundland, Canada, August 15–16, 2003. Springer, Heidelberg, Germany.


Yuanxi Dai and John P. Steinberger.

Indifferentiability of 8-round Feistel networks.
In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 95–120, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

Pooya Farshim, Louiza Khati, and Damien Vergnaud.
Security of even–mansour ciphers under key-dependent messages.
IACR Trans. Symm. Cryptol., 2017(2):84–104, 2017.

Chun Guo and Dongdai Lin.
On the indifferentiability of key-alternating Feistel ciphers with no key derivation.

In Yevgeniy Dodis and Jesper Buus Nielsen, editors, TCC 2015, Part I, volume 9014 of LNCS, pages 110–133, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany.

Michael Luby and Charles Rackoff.
How to construct pseudo-random permutations from pseudo-random functions (abstract).
In Hugh C. Williams, editor, CRYPTO'85, volume 218 of LNCS, page 447, Santa Barbara, CA, USA, August 18–22, 1986. Springer, Heidelberg, Germany.

Rodolphe Lampe and Yannick Seurin.
Security analysis of key-alternating Feistel ciphers.

In Carlos Cid and Christian Rechberger, editors, FSE 2014, volume 8540 of LNCS, pages 243–264, London, UK, March 3–5, 2015. Springer, Heidelberg, Germany.

Jacques Patarin.
Pseudorandom permutations based on the D.E.S. scheme.
In ESORICS'90, LNCS, pages 185–187, Toulouse, France, October 24–26, 1990. AFCET.