Revisiting Key-alternating Feistel Ciphers for Shorter Keys and Multi-user Security

Chun Guo and Lei Wang

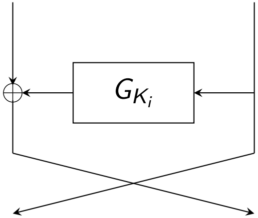
ICTEAM/ELEN/Crypto Group, Université catholique de Louvain
Shanghai Jiao Tong University

Presented by Yaobin Shen, Shanghai Jiao Tong University
December 3 AISACRYPT 2018

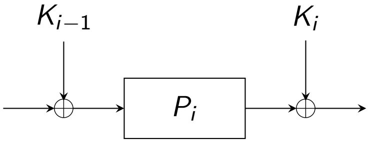
Outline

Block Ciphers

- Usually iterative designs
- Fall into two paradigms:



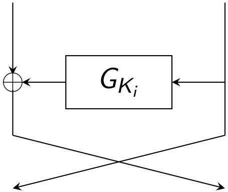
Feistel Cipher



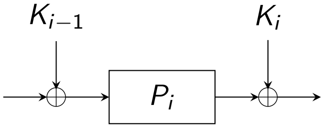
substitution-permutation networks
(Even-Mansour Cipher)

Feistel cipher v.s. Even-Mansour cipher

- Consider constructing a cipher with $2n$-bit blocks.
- Feistel: underlying primitives have
  - smaller size, *i.e.*, half block size; and
  - less construction properties, *i.e.* no need for invertibility



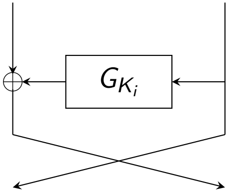
Feistel Cipher



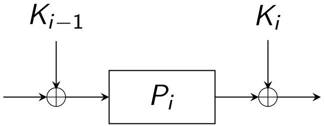
Even-Mansour Cipher

Feistel cipher v.s. Even-Mansour cipher

- Consider constructing a cipher with $2n$-bit blocks.
- Feistel: underlying primitives have
  - smaller size, *i.e.*, half block size; and
  - less construction properties, *i.e.* no need for invertibility
- Even-Mansour: larger primitives for higher provable (lower) bound.
  - $O(n)$ rounds for 2^{2n} security.
  - In comparison, for Feistel security is at most 2^n.



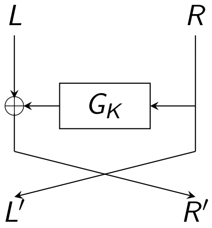
Feistel Cipher



Even-Mansour Cipher

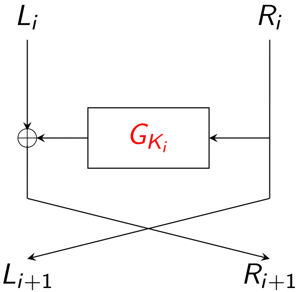
Luby-Rackoff Feistel Cipher

- Use a keyed PRF G_K for the round function: $(L, R) \mapsto (L \oplus G_K(R), L)$
- Long-term research since [Luby and Rackoff, 1988], consists of
  - provable security lower bound;
  - cryptanalytic: generic attacks;
  - bridge abstract model and dedicated ciphers, *e.g.* practical key size, less round functions;



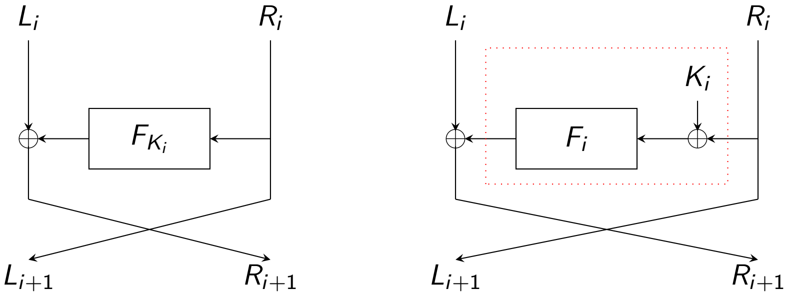
Gap between Generic Feistel and Dedicated Cipher

- (Recall) the general model: *independent* round-keys.
- In reality: round-keys are derived from a short main-key, thus *correlated*.
    - Using identical round-keys: 5 rounds [Pie91]
    - Using two independent round-keys: [NR99, PRG+99]
- Besides, how to design the keyed PRF G_K?



Keyed Functions from Keyless Functions

- Important and popular research direction: constructing the keyed function from public *keyless* random functions F_i
- This turns *Luby-Rackoff* into *key-alternating Feistel* [Lampe and Seurin, FSE 2014]



Luby-Rackoff Feistel $\Longrightarrow$ Key-Alternating Feistel

Key-Alternating Feistel: Provable Security

- General case

  using *independent* public round functions F_i
  independent round keys K_i.
- t rounds has $2^{\frac{rn}{r+1}}$ security with $r = \lfloor t/6 \rfloor$ [Lampe and Seurin, FSE 2014] (asymptotically optimal)

Security	#rounds	Reference
$2^{n/2}$	6	[Lampe and Seurin]
$2^{2n/3}$	12	
$2^{3n/4}$	18	

Key-Alternating Feistel: Generic Attacks

- Known as *Feistel-2* schemes in the cryptanalytic community [Isobe and Shibutani, ASIACRYPT 2013]

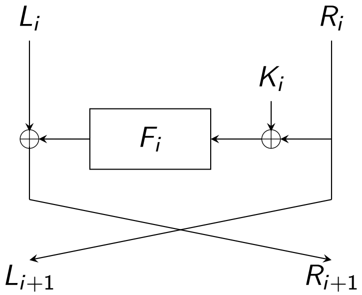
Attacks	# Rounds	Key size	Complexity	Reference
Key-Recovery	6	$2n$	$2^{3n/2}$	[Guo et al, ASIACRYPT 2014]
	8	$3n$	$2^{8n/3}$	
	10	$4n$	$2^{11n/3}$	

Outline

In Short

We revisit the information-theoretic security of key-alternating Feistel in the ideal model.

- We prove security for correlated round-keys.
- We prove non-degradating multi-user security.



Recapitulating Previous Result

- Assume independent round-keys K_i

  In reality: correlated round-keys.

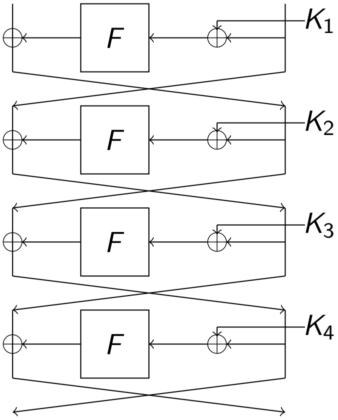
- Assume (mostly) independent public round functions F_i

  In reality: identical round functions.

Security	#rounds	Reference
$2^{n/2}$	4	[Gentry and Ramzan, ASIACRYPT 2004]
$2^{n/2}$	6	[Lampe and Seurin, FSE 2014]
$2^{2n/3}$	12	
$2^{3n/4}$	18	

Our First Result for Birthday $2^{n/2}$ Security

- Uses 4 rounds with single public round function
- Uses **Suitable Round Key Vectors** $\overrightarrow{K} = (K_1, K_2, K_3, K_4)$:
  - K_1 is uniformly distributed;
  - K_4 is uniformly distributed;
  - $K_1 \oplus K_4$ is uniformly distributed;



Our First Result for Birthday $2^{n/2}$ Security

- Denote q_e the number of cipher queries
- Denote q_f the number of function queries

Theorem

For the 4-round idealized Key-Alternating Feistel with a Single public round Function (SF) and a suitable round-key vector, in single-user (su) setting it holds

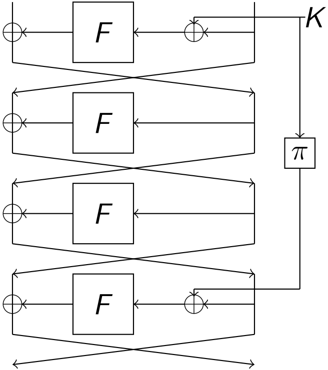
$$\mathbf{Adv}^{su}_{KAFSF}(q_f, q_e) \leq \frac{9q_e^2 + 4q_e q_f}{N}.$$

In the multi-user (mu) setting it holds

$$\mathbf{Adv}^{mu}_{KAFSF}(q_f, q_e) \leq \frac{50q_e^2 + 8q_e q_f}{N}.$$

Minimalism

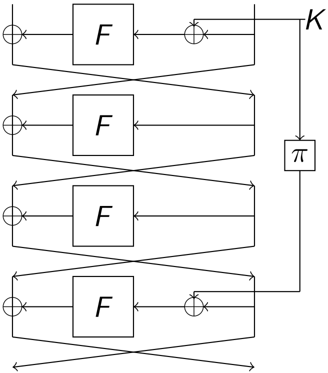
- Derive round-keys from an n-bit main-key K
- Key-schedule function π is a public and fixed orthomorphism of F_2^n, e.g., $\pi(K_L \| K_R) = K_L \oplus K_R \| K_L$



Minimalism

No round-key in middle rounds.

- But of course you can add any round-keys, they won't reduce security.
- On the other hand, the "unprotected" middle two rounds match Ramzan and Reyzin (CRYPTO 2000), who showed that the middle two round functions of 4-round *Luby-Rackoff* scheme can be public.



Our Second Result for Beyond-Birthday Security

- We consider *independent* round functions for simplicity.
- We prove 6 rounds have $2^{(2n-r)/3}$ security, when using **Suitable Round Key Vectors** $\overrightarrow{K} = (K_1, K_2, K_3, K_4, K_5, K_6)$ such that
  - K_1, K_3, K_5 are uniform in $\{0,1\}^n$, K_2, K_4, K_6 are uniform in 2^{n-r} possibilities
  - for $(i,j) \in \{(1,2),(2,3),(4,5),(5,6),(1,6)\}$, K_i and K_j are independent

    This means "adjacent" round-keys are independent. This is easily ensured by the common FSR-based key-schedules.

Our Second Result for Beyond-Birthday Security

Theorem

For the 6-round idealized Key-Alternating Feistel with a suitable round-key vector, in single-user (su) setting it holds

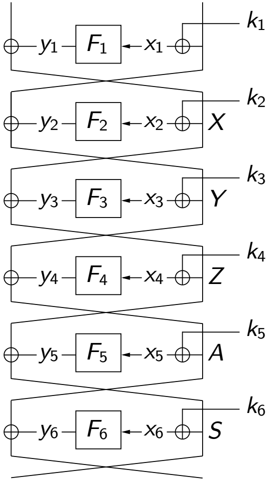
$$\mathbf{Adv}^{su}_{KAF}(q_f, q_e) \le \frac{7q_e^3 + 13q_e q_f^2 + 22q_e^2 q_f}{N^2} + \frac{2^r(8q_e q_f^2 + 2q_e^2 q_f)}{N^2}.$$

In multi-user (mu) setting it holds

$$\mathbf{Adv}^{mu}_{KAF}(q_f, q_e) \le \frac{1214q_e^3 + 26q_e q_f^2 + 356q_e^2 q_f}{N^2} + \frac{2^r(600q_e^3 + 16q_e q_f^2 + 196q_e^2 q_f)}{N^2}.$$

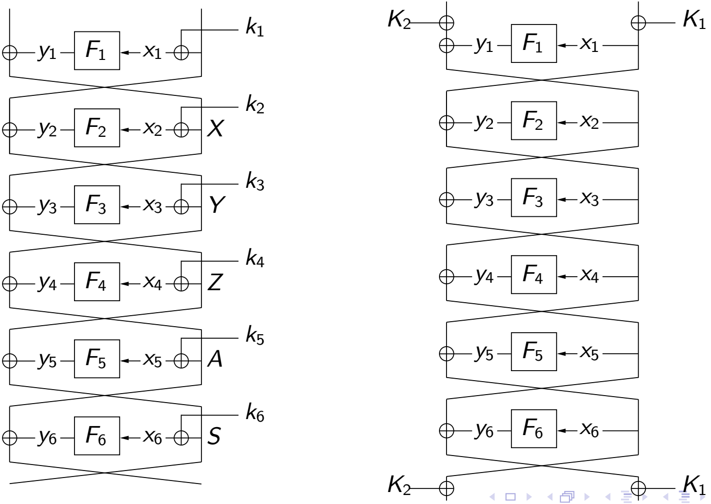
The Simplest Example

Alternating two main-keys $|K_1| = n$, $|K_2| = n - r$.



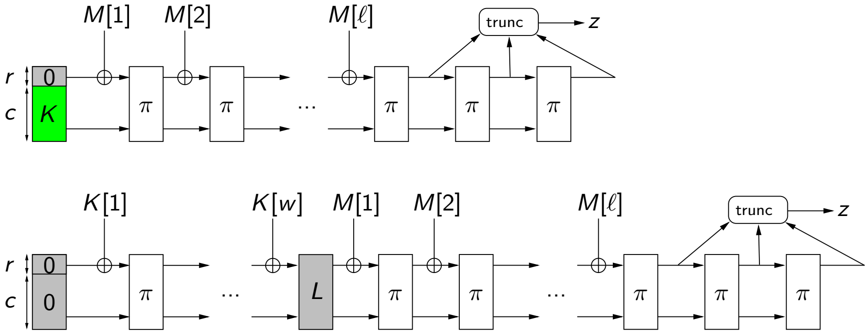
Collapses to Partial-key Even-Mansour (PKEM)

This means the permutation in PKEM can be instantiated with a 6-round keyless Feistel for beyond-birthday security.



Application: Instantiating Keyed Sponges

Keyed sponges can be used for MACs and authenticated encryption.

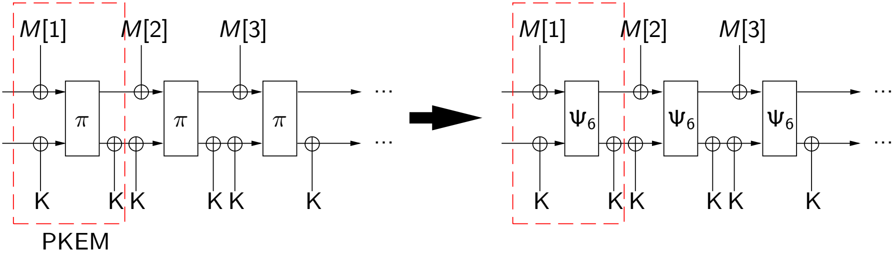


Application: Instantiating Keyed Sponges

Many (inner and outer) keyed sponges have their security reduce to the PKEM cipher.

We show PKEM can be instantiated with the 6-round keyless Feistel Ψ_6.

So (inner and outer) keyed sponges can also be instantiated with the 6-round keyless Feistel Ψ_6.



Another Application: A Key-schedule Proposal

By the derived conditions on 6 rounds, we propose a concrete key-schedule motivated by the complexity community [Luby and Wigderson, 2005]:

$$
\begin{aligned}
k_1 &= K_1 + 2 \otimes K_2, & k_2 &= 2 \otimes K_1 + 3 \otimes K_2, \\
k_3 &= 3 \otimes K_1 + 5 \otimes K_2, & k_4 &= 5 \otimes K_1 + 7 \otimes K_2, \\
&\ldots, & k_t &= a_t \otimes K_1 + a_{t+1} \otimes K_2,
\end{aligned}
$$

where:

- $2n$-bit main-key $K = K_1 \| K_2$
- $a \otimes b$ is the multiplication of two field elements $a, b \in \mathbb{F}_2^n$
- for $1 \leq t \ll 2^n$, let the constants a_t and a_{t+1} be the t and $(t+1)^{\text{th}}$ values in the prime sequence $1, 2, 3, 5, 7, 11, 13, \ldots$ resp.

The complicated sequence of constants eliminate obvious weak keys, see the full version of this paper.

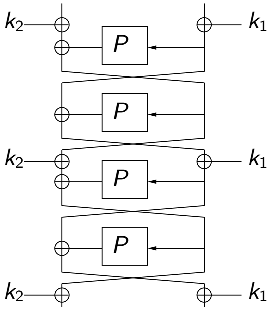
A Comparison with Previous KAF Results

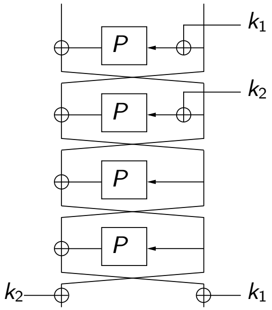
Security	#Rounds	#Indepedent Functions	Minimum key Size	Reference
$2^{n/2}$	4	2	$4n$	[Gentry and Ramzan]
	4	**1**	**n**	**Ours**
$2^{2n/3}$	12	12	$12n$	[Lampe and Seurin]
	6	**6**	**2n**	**Ours**

- For birthday security we improve upon Gentry and Ramzan.
- For beyond-birthday security we improve upon Lampe and Seurin.

Remark on a Recent Result

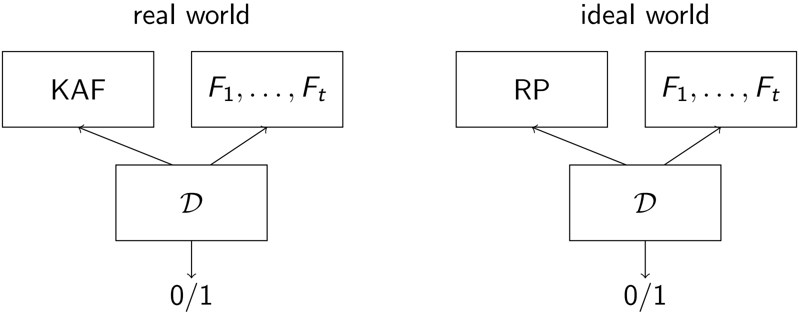
- Gilboa, Gueron, and Nandi (2016) proved the 2-round Even-Mansour with $2n$-bit keys and 2-round keyless Feistel $\Psi_2^{\mathbf{P}}$ ($\mathbf{P}$ a random permutation) as the round permutations is secure up to $2^{n/2}$ queries.
- This transits into a KAF variant *with whitening keys*, which may be quite different and incomparable to KAF without whitening keys, the focus of the presented work (see https://arxiv.org/abs/1810.07428).





Outline

Security Definition

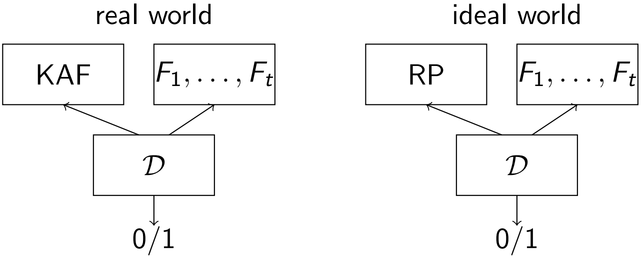


- real world: KAF with random master key
- ideal world: random permutation (RP)
- $\mathcal{D}$ has access to $F_1, F_2, \dots, F_t$ in both worlds

Security Definition

- the F_i's are modeled as public random functions (adversary can only make black-box queries)
- adversary cannot exploit any weakness of round functions (generic attacks)
- complexity measure of the adversary
  - q_e: #construction queries (Data);
  - q_f: #function queries to each function (Time)
  - computationally unbounded

Security Definition



- advantage of $\mathcal{D}$ is defined as

$$\mathbf{Adv}(\mathcal{D}) = \Pr\left[\mathcal{D}^{\text{real}} \Rightarrow 1\right] - \Pr\left[\mathcal{D}^{\text{ideal}} \Rightarrow 1\right]$$

- security is defined via upper bounding $\mathbf{Adv}(\mathcal{D})$:

$$\mathbf{Adv}(q_e, q_f) = \max_{\mathcal{D}} \mathbf{Adv}(\mathcal{D})$$

Proof Framework

- H-coefficients Techniques [Pat09]
- transcript of distinguisher $\tau = (\mathcal{Q}_E, \mathcal{Q}_{F_1}, \ldots, \mathcal{Q}_{F_t})$:
  - $\mathcal{Q}_E$: q_e query-responses of cipher;
  - $\mathcal{Q}_{F_i}$: q_f query-responses of function F_i;
- $\Pr_{re}[\tau]$: the probability of $\mathcal{D}$ receiving τ in real world;
- $\Pr_{id}[\tau]$: the probability of $\mathcal{D}$ receiving τ in ideal world;

Theorem

Let $\varepsilon(q_f, q_e) > 0$. Assume that for any transcript τ with $\Pr_{id}[\tau] > 0$, we have

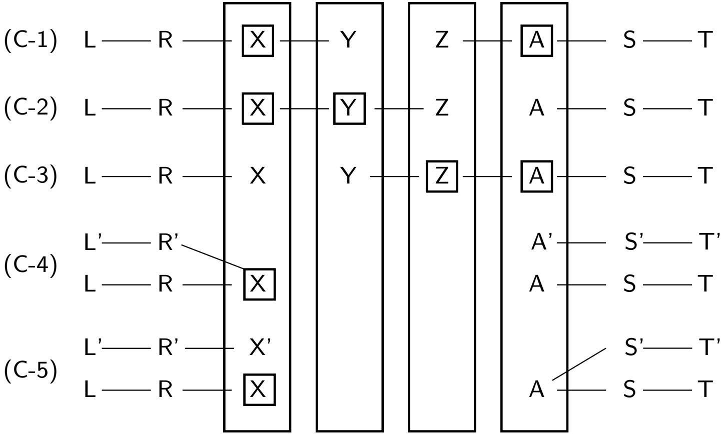
$$\Pr_{re}(\tau) \geq (1 - \varepsilon(q_f, q_e))\Pr_{id}(\tau),$$

then it holds

$$\mathbf{Adv}(q_f, q_e) \leq \varepsilon(q_f, q_e).$$

Proof Sketch

- peel off the first and the last rounds
- internal states are "random" and just "known" to adversary



Outline

Conclusion

- information-theoretic security of Key-Alternating Feistel
- towards minimizing sufficient conditions to guarantee certain bound
  - define suitable round key vectors
  - $2^{n/2}$ bound: 4 rounds with single function
  - $2^{2n/3}$ bound: 6 rounds
- in both single-user and multi-user settings

Conclusion

- information-theoretic security of Key-Alternating Feistel
- towards minimizing sufficient conditions to guarantee certain bound
  - define suitable round key vectors
  - $2^{n/2}$ bound: 4 rounds with single function
  - $2^{2n/3}$ bound: 6 rounds
- in both single-user and multi-user settings

Open Problem

- prove 6-round KAF with less public functions
- improve security bound of 6-round KAF
- improve security bound for t-round KAF with generic t

Thanks for your attention!