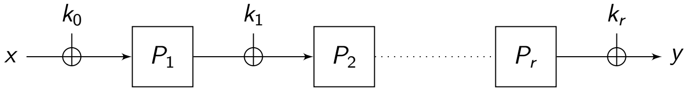
Security Analysis of Key-Alternating Feistel Ciphers

Rodolphe Lampe and Yannick Seurin

University of Versailles and ANSSI

4th March 2014 - FSE 2014

Key-Alternating Ciphers (*aka* iterated Even-Mansour)



- $P_1, \ldots, P_r$ are modeled as public random permutation oracles
- interpretation: gives a guarantee against any adversary which does not use particular properties of the P_i's

Results on the pseudorandomness of KA ciphers

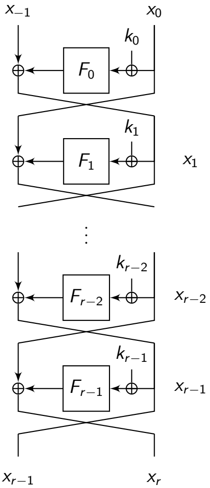
The following results have been successively obtained for the pseudorandomness of KA ciphers (notation: $N = 2^n$):

- for $r = 1$ round, security up to $\mathcal{O}(N^{\frac{1}{2}})$ queries [EM97]
- for $r \geq 2$, security up to $\mathcal{O}(N^{\frac{2}{3}})$ queries [BKL$^+$12]
- for $r \geq 3$, security up to $\mathcal{O}(N^{\frac{3}{4}})$ queries [Ste12]
- for any even r, security up to $\mathcal{O}(N^{\frac{r}{r+2}})$ queries [LPS12]
- tight result: for r rounds, security up to $\mathcal{O}(N^{\frac{r}{r+1}})$ queries [CS13]

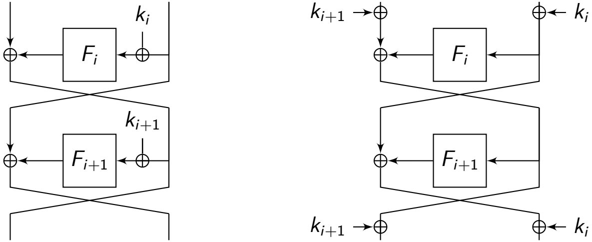
NB: Results for independent round keys $(k_0, k_1, \ldots, k_r)$

Key-Alternating Feistel Ciphers

- functions F_i are public random oracles
- different from the Luby-Rackoff setting (where the F_i's are pseudorandom)



KAF ciphers as a special type of Key-Alternating ciphers



Two rounds of a KAF cipher is equivalent to a 1-round KA cipher where the permutation is a two-round (un-keyed) Feistel cipher with public random functions

Results

- previous results: Gentry and Ramzan [GR04]: secure up to $N^{1/2}$ queries for $r = 4$ rounds
- our results: secure up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{3} \right\rfloor \quad \text{for NCPA attacks}$$

$$t = \left\lfloor \frac{r}{6} \right\rfloor \quad \text{for CCA attacks}$$

- improved results in the Luby-Rackoff setting: security up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{2} \right\rfloor \quad \text{for NCPA attacks}$$

$$t = \left\lfloor \frac{r}{4} \right\rfloor \quad \text{for CCA attacks}$$

Results

- previous results: Gentry and Ramzan [GR04]: secure up to $N^{1/2}$ queries for $r = 4$ rounds
- our results: secure up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{3} \right\rfloor \quad \text{for NCPA attacks}$$
$$t = \left\lfloor \frac{r}{6} \right\rfloor \quad \text{for CCA attacks}$$

- improved results in the Luby-Rackoff setting: security up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{2} \right\rfloor \quad \text{for NCPA attacks}$$
$$t = \left\lfloor \frac{r}{4} \right\rfloor \quad \text{for CCA attacks}$$

Results

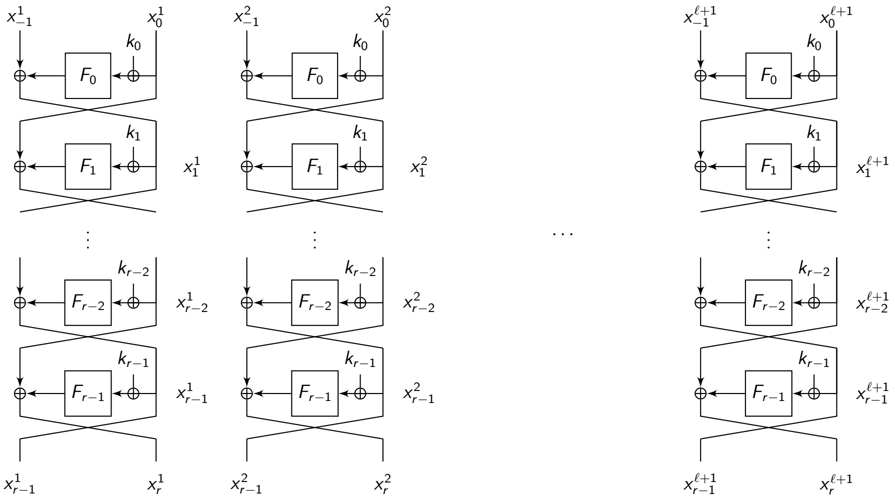
- previous results: Gentry and Ramzan [GR04]: secure up to $N^{1/2}$ queries for $r = 4$ rounds
- our results: secure up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{3} \right\rfloor \quad \text{for NCPA attacks}$$
$$t = \left\lfloor \frac{r}{6} \right\rfloor \quad \text{for CCA attacks}$$

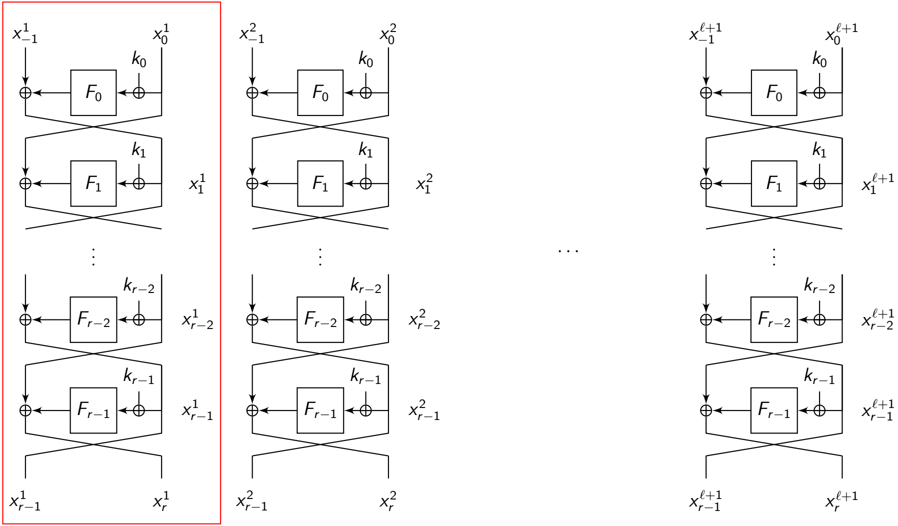
- improved results in the Luby-Rackoff setting: security up to $N^{\frac{t}{t+1}}$ queries where

$$t = \left\lfloor \frac{r}{2} \right\rfloor \quad \text{for NCPA attacks}$$
$$t = \left\lfloor \frac{r}{4} \right\rfloor \quad \text{for CCA attacks}$$

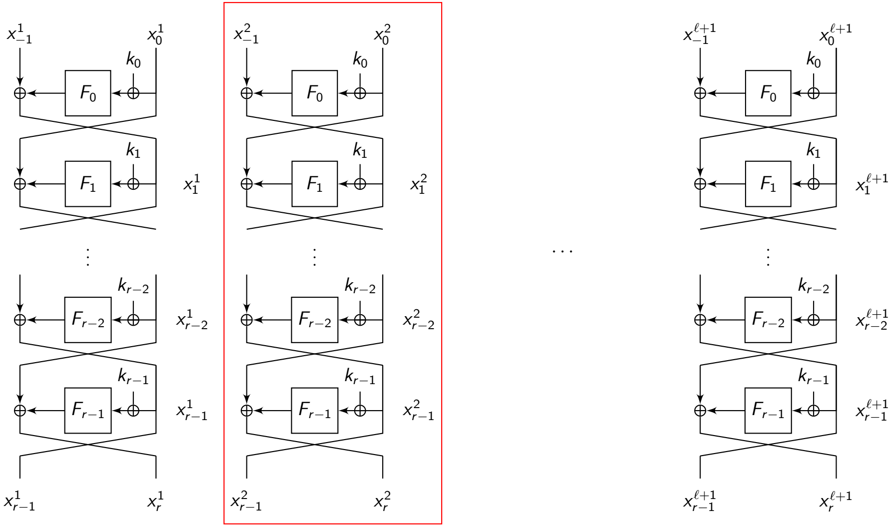
Intuition of the proof



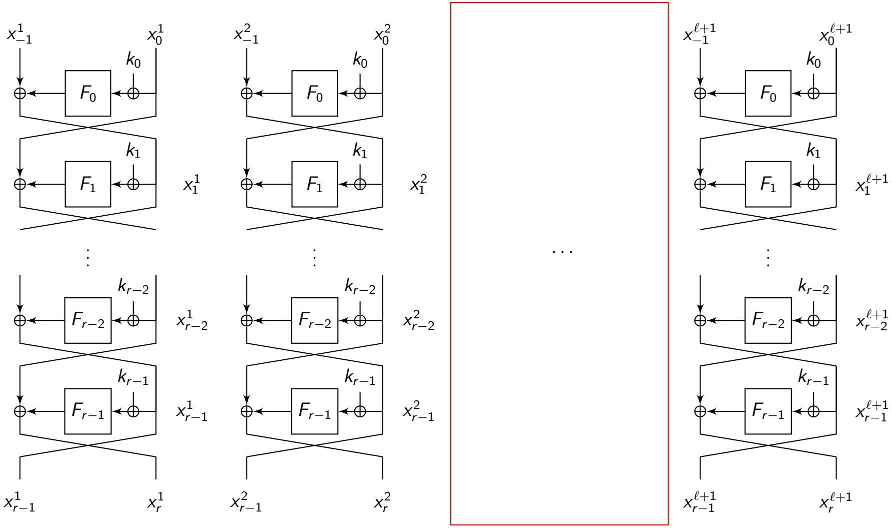
Intuition of the proof



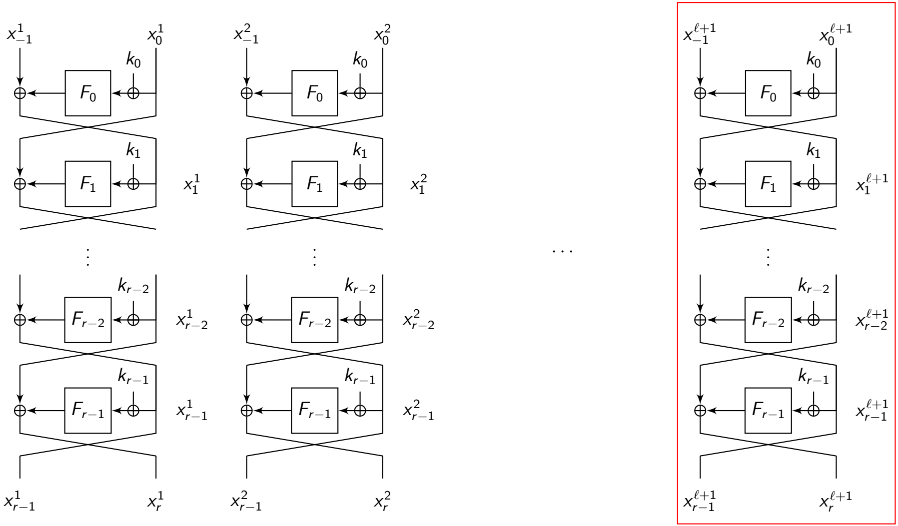
Intuition of the proof



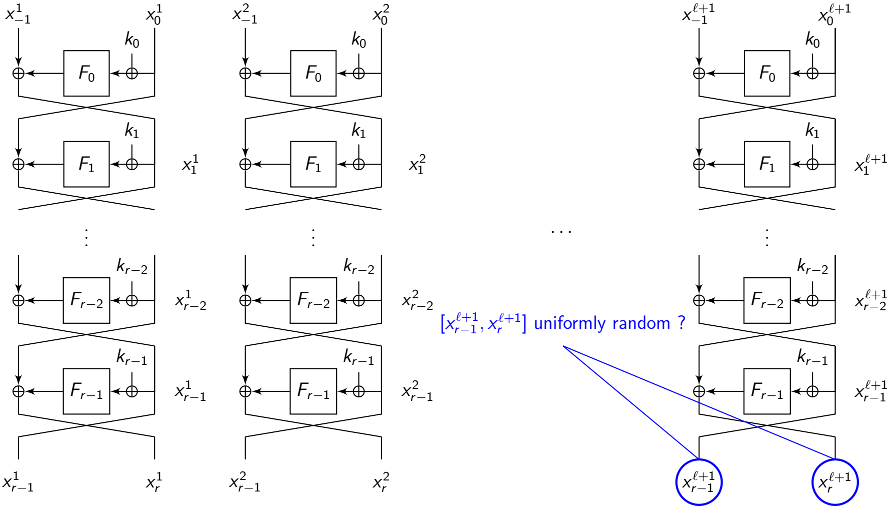
Intuition of the proof



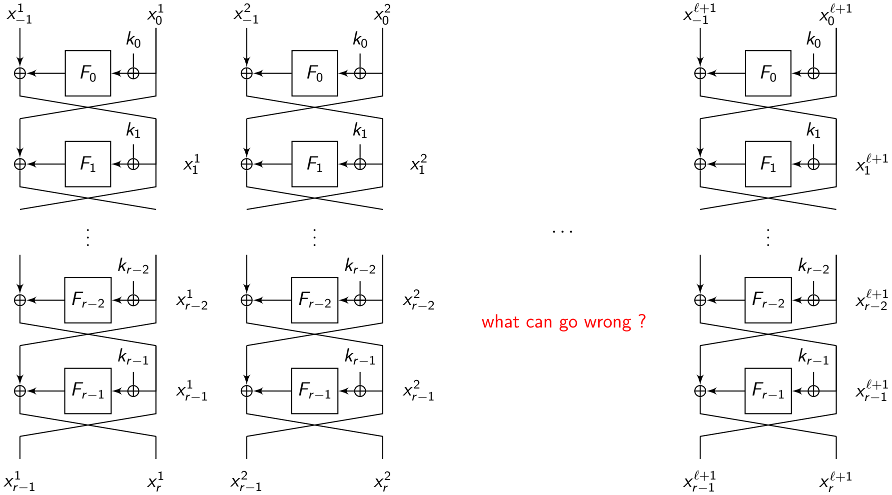
Intuition of the proof



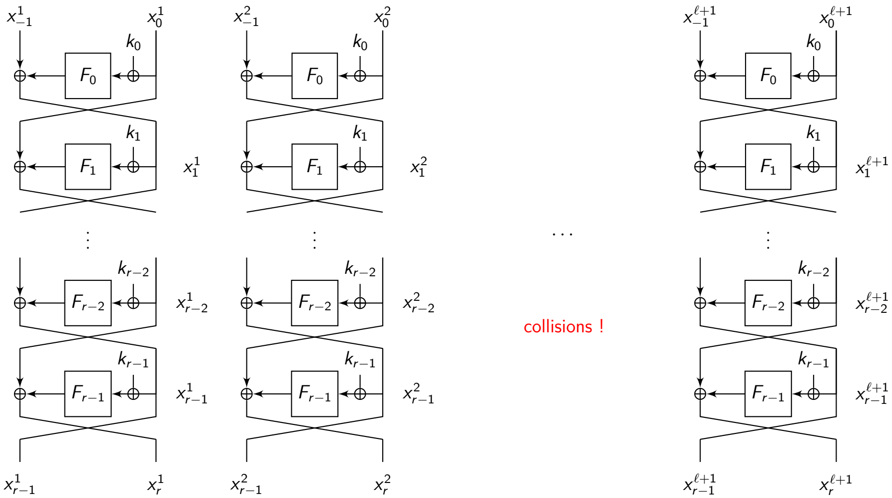
Intuition of the proof



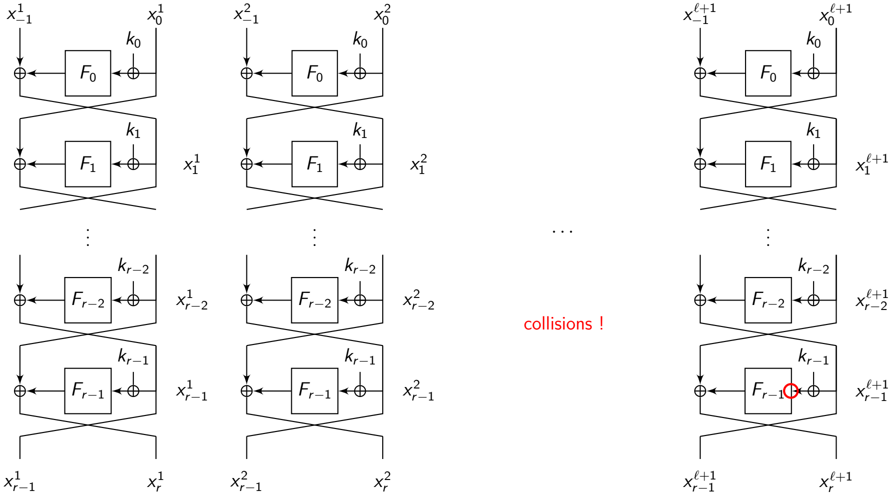
Intuition of the proof



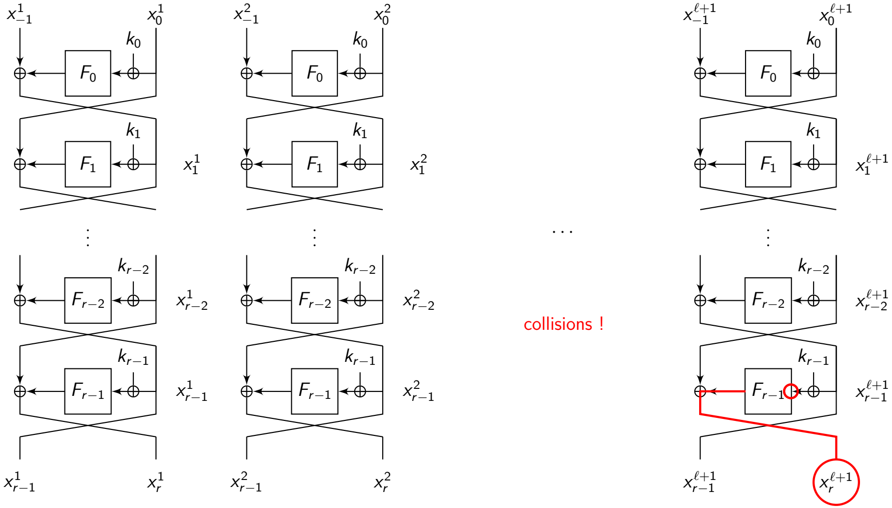
Intuition of the proof



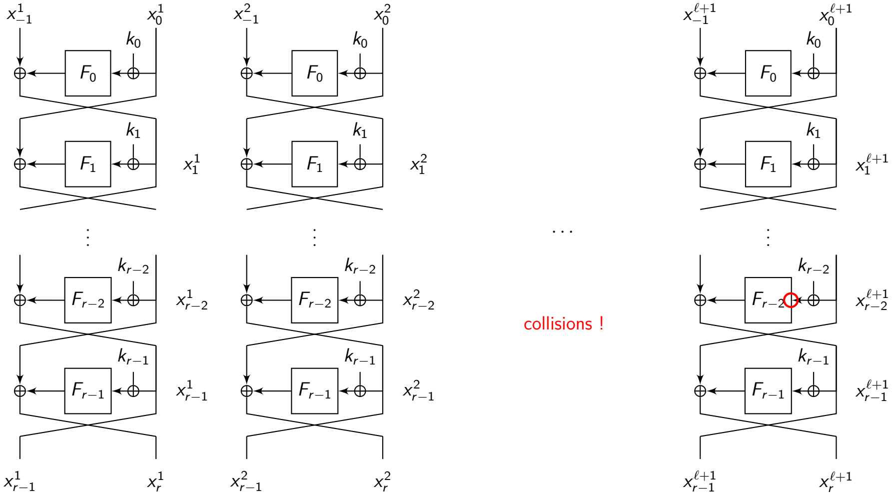
Intuition of the proof



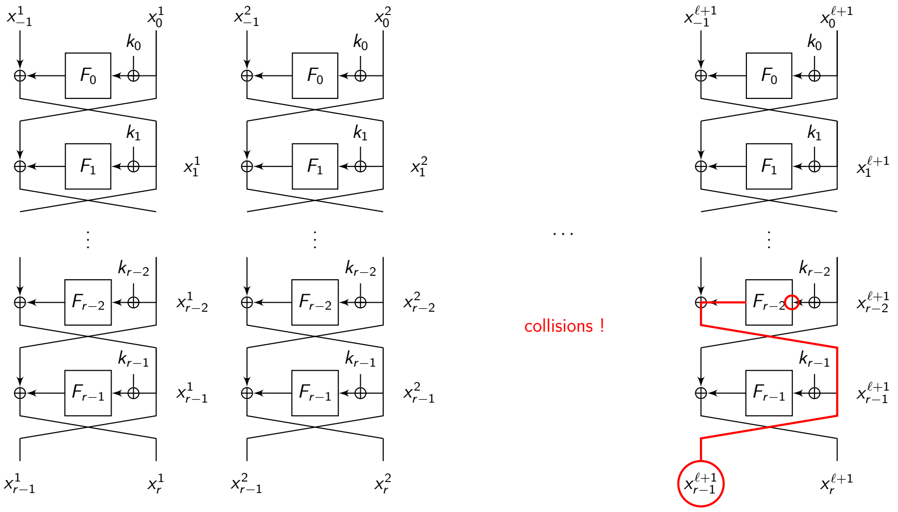
Intuition of the proof



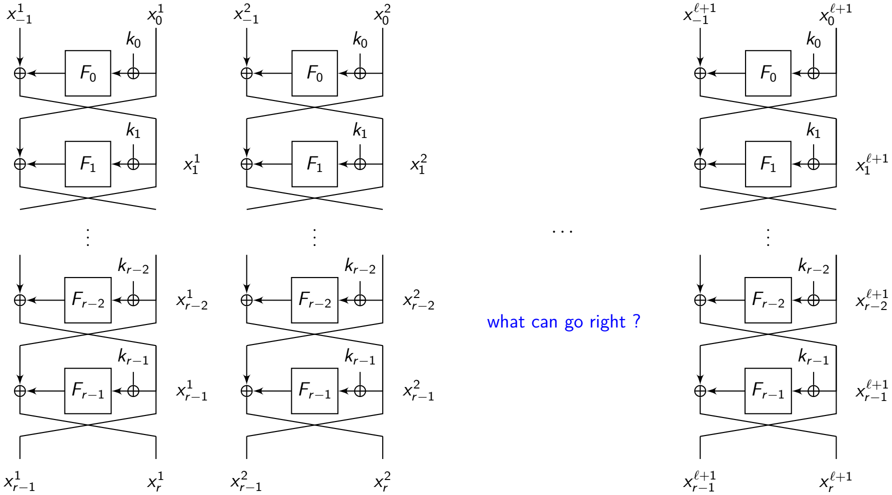
Intuition of the proof



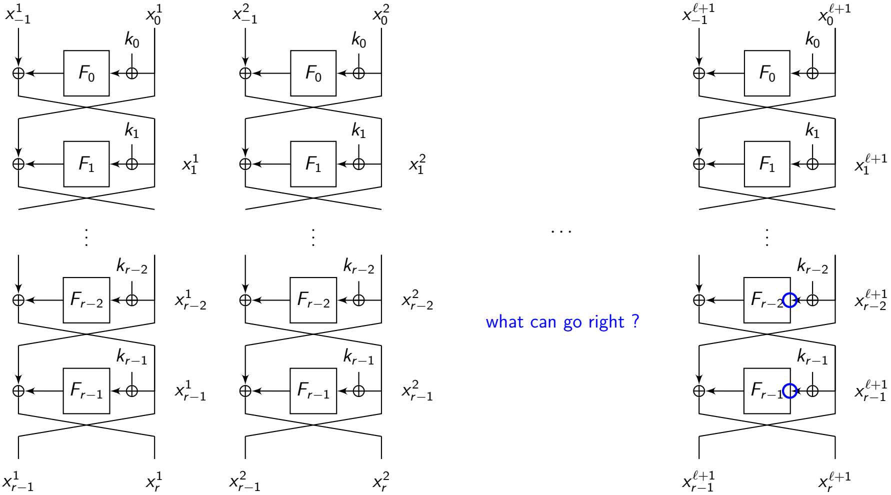
Intuition of the proof



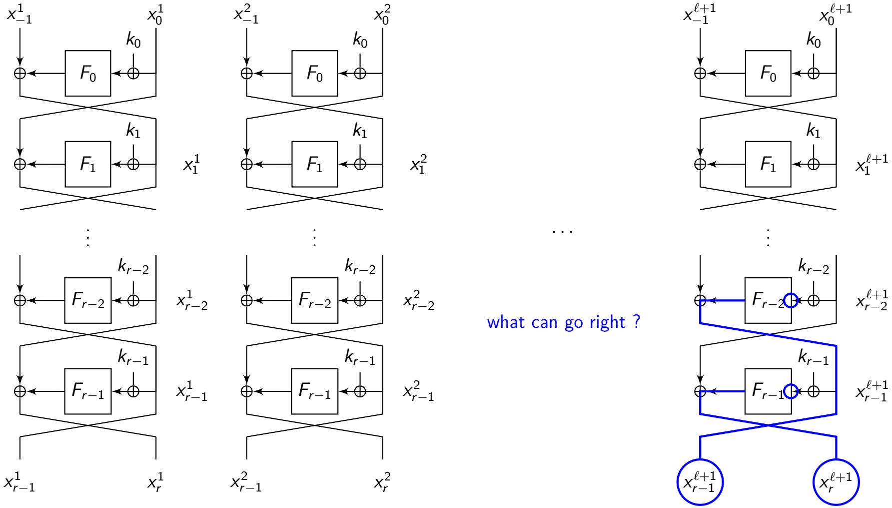
Intuition of the proof



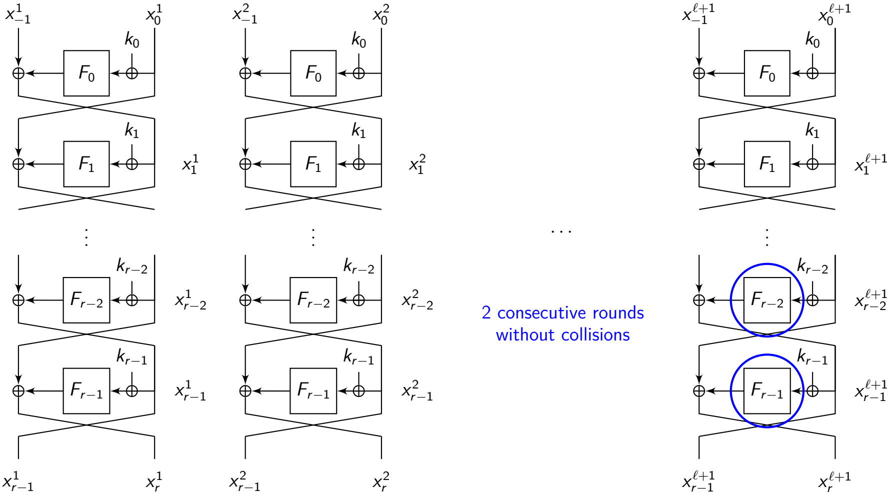
Intuition of the proof



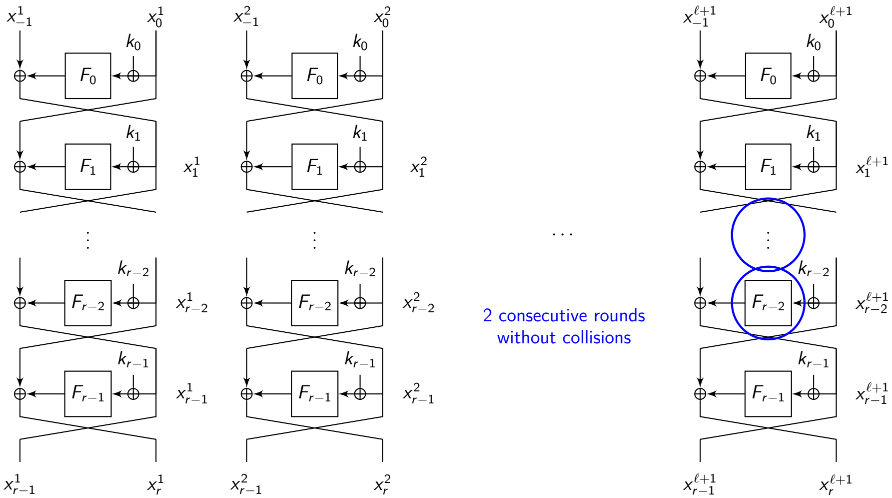
Intuition of the proof



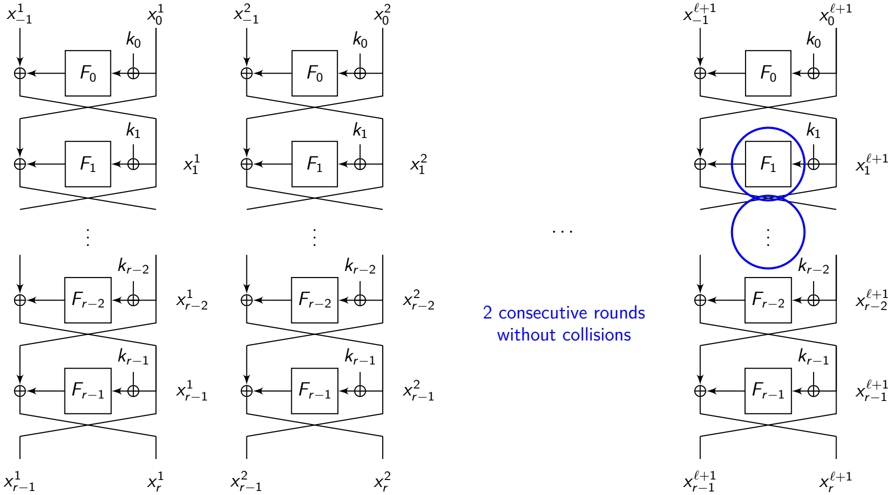
Intuition of the proof



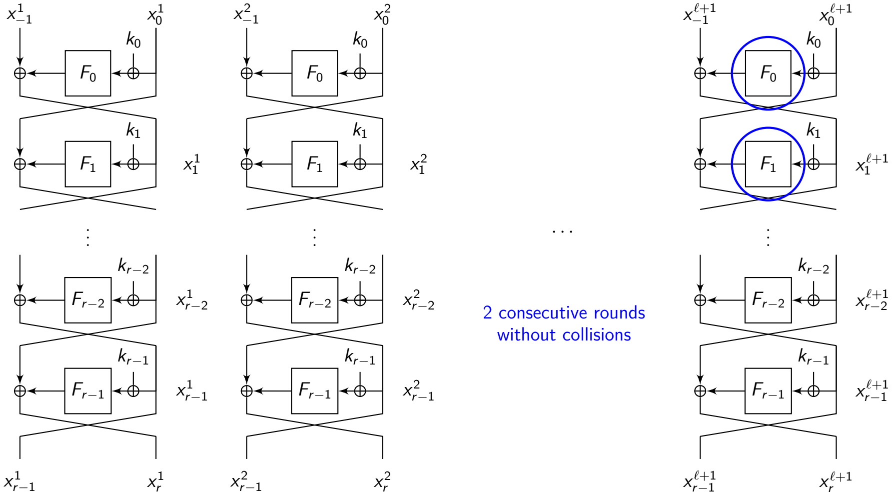
Intuition of the proof



Intuition of the proof



Intuition of the proof



Technique

- Proof using the coupling technique
- main problem: given ℓ queries, upper bound the probability that, for every two consecutive rounds, the $\ell+1$-th query collision in (at least) one of the two rounds.
- A_i = event that the ℓ-th query collisions with previous queries at round i; we want to upper bound

$$\Pr\left[(A_1 \cup A_2) \cap (A_2 \cup A_3) \cap \cdots \cap (A_{r-2} \cup A_{r-1}) \cap (A_{r-1} \cup A_r)\right]$$

Technique

- Proof using the coupling technique
- main problem: given ℓ queries, upper bound the probability that, for every two consecutive rounds, the $\ell+1$-th query collision in (at least) one of the two rounds.
- A_i = event that the ℓ-th query collisions with previous queries at round i; we want to upper bound

$$\Pr\left[(A_1 \cup A_2) \cap (A_2 \cup A_3) \cap \cdots \cap (A_{r-2} \cup A_{r-1}) \cap (A_{r-1} \cup A_r)\right]$$

Technique

- Proof using the coupling technique
- main problem: given ℓ queries, upper bound the probability that, for every two consecutive rounds, the $\ell + 1$-th query collision in (at least) one of the two rounds.
- A_i = event that the ℓ-th query collisions with previous queries at round i; we want to upper bound

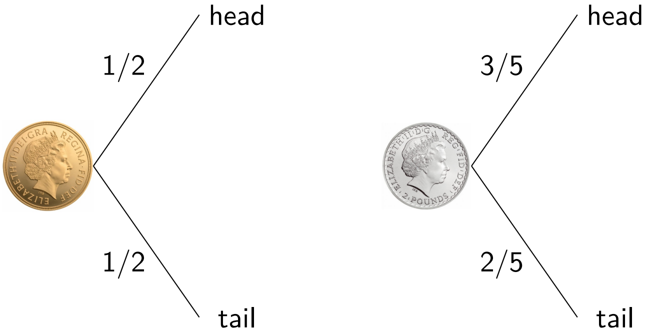
$$\Pr\left[(A_1 \cup A_2) \cap (A_2 \cup A_3) \cap \cdots \cap (A_{r-2} \cup A_{r-1}) \cap (A_{r-1} \cup A_r)\right]$$

Technique

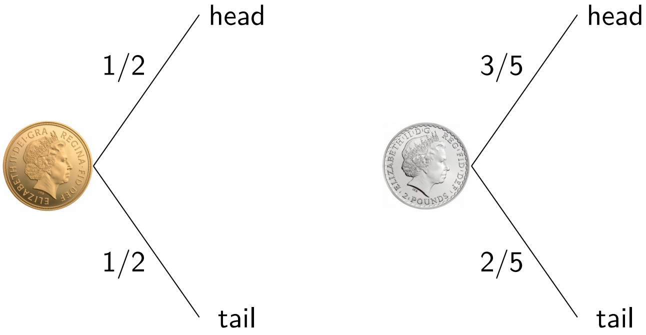
- Proof using the coupling technique
- main problem: given ℓ queries, upper bound the probability that, for every two consecutive rounds, the $\ell + 1$-th query collision in (at least) one of the two rounds.
- A_i = event that the ℓ-th query collisions with previous queries at round i; we want to upper bound

$$\Pr\left[(A_1 \cup A_2) \cap (A_2 \cup A_3) \cap \cdots \cap (A_{r-2} \cup A_{r-1}) \cap (A_{r-1} \cup A_r)\right]$$

The Coupling technique

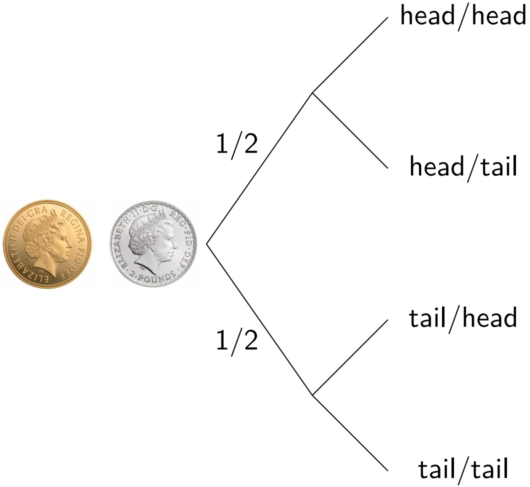


The Coupling technique

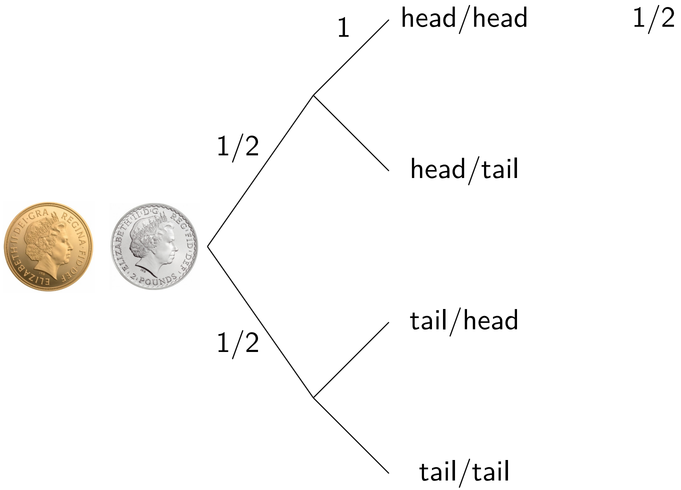


$$\text{Adv} = \text{Statistical distance} = \left|\frac{3}{5} - \frac{1}{2}\right| = \frac{1}{10}$$

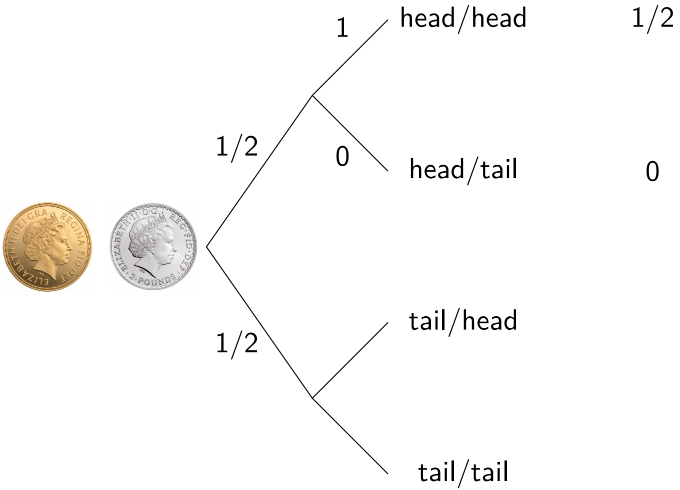
The Coupling technique



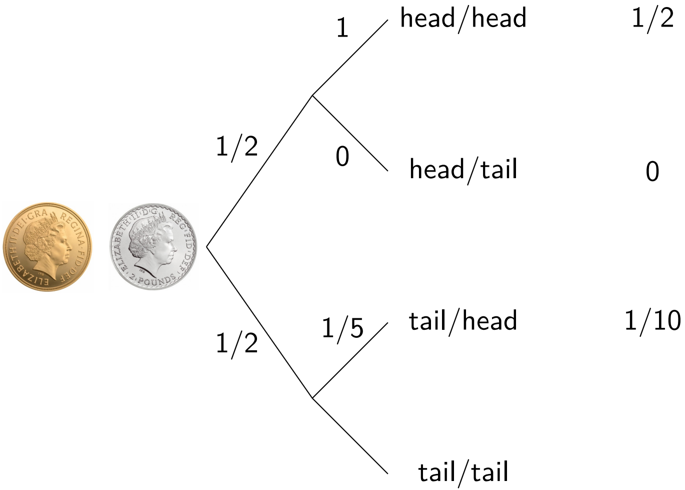
The Coupling technique



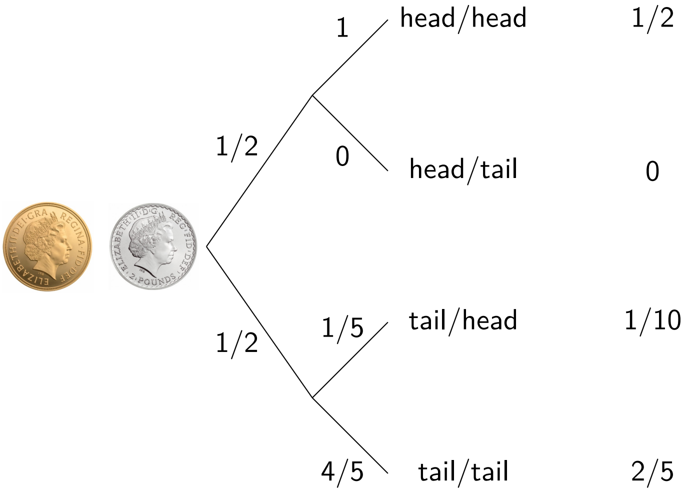
The Coupling technique



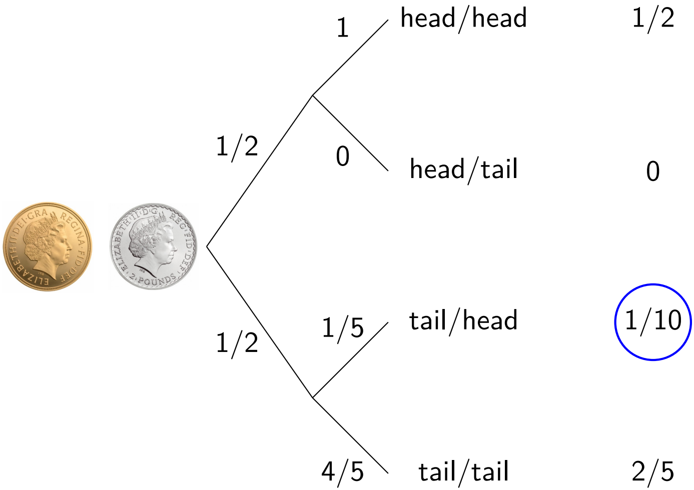
The Coupling technique



The Coupling technique



The Coupling technique



The Coupling technique

random variables	X	Y
probability distributions	μ	ν

The Coupling lemma

$$\|\mu - \nu\| \leq \Pr[X \neq Y]$$

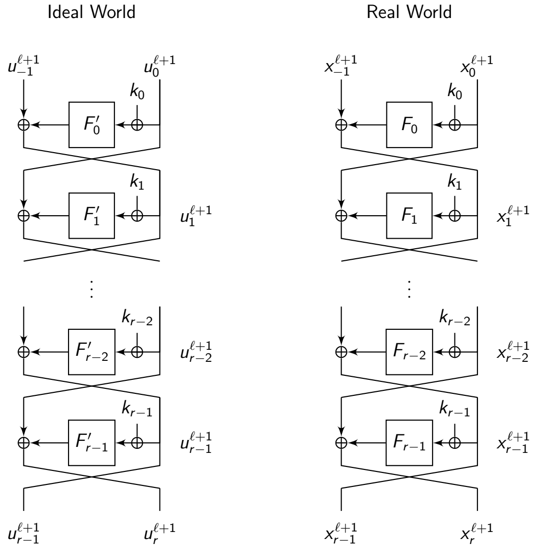
The Coupling technique

random variables	X	Y
probability distributions	μ	ν

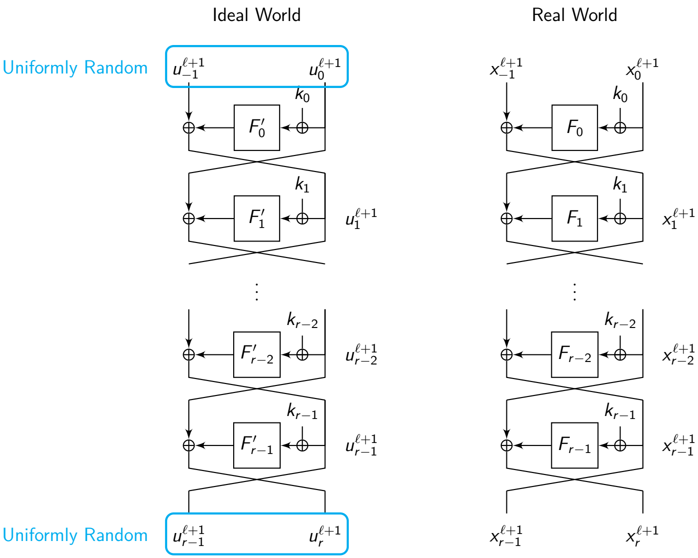
The Coupling lemma

$$\|\mu - \nu\| \leq \Pr[X \neq Y]$$

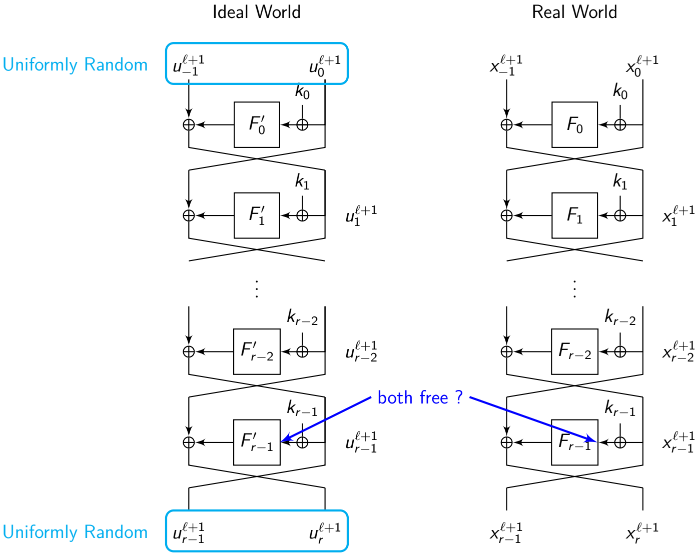
The Coupling Technique for the KAF



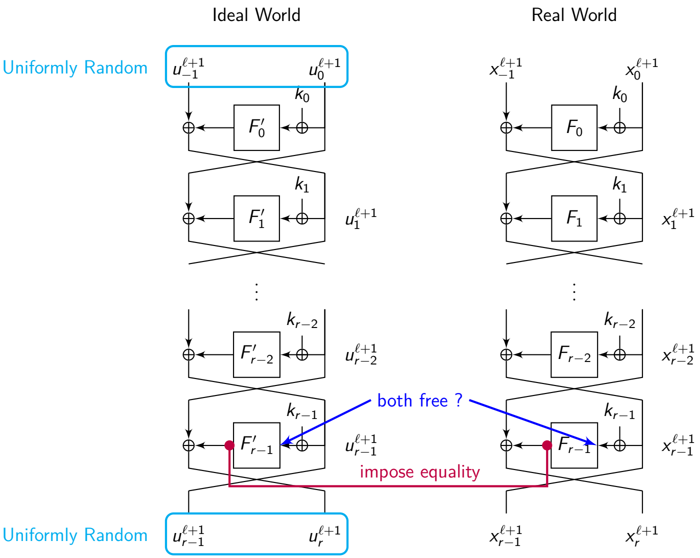
The Coupling Technique for the KAF



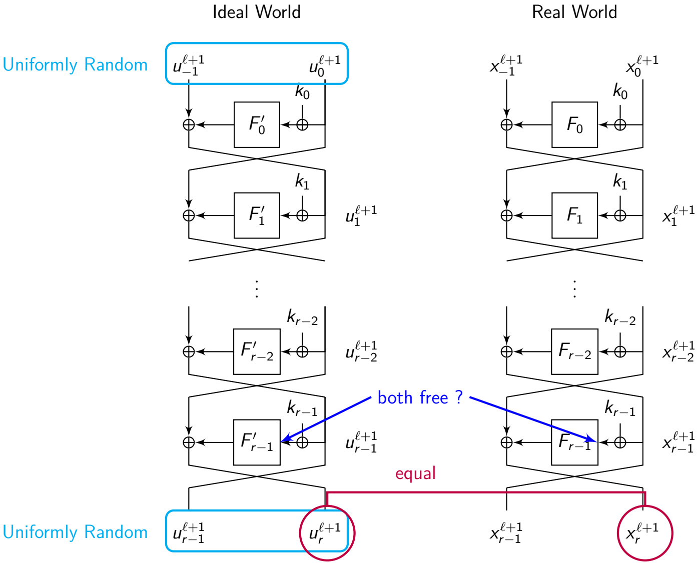
The Coupling Technique for the KAF



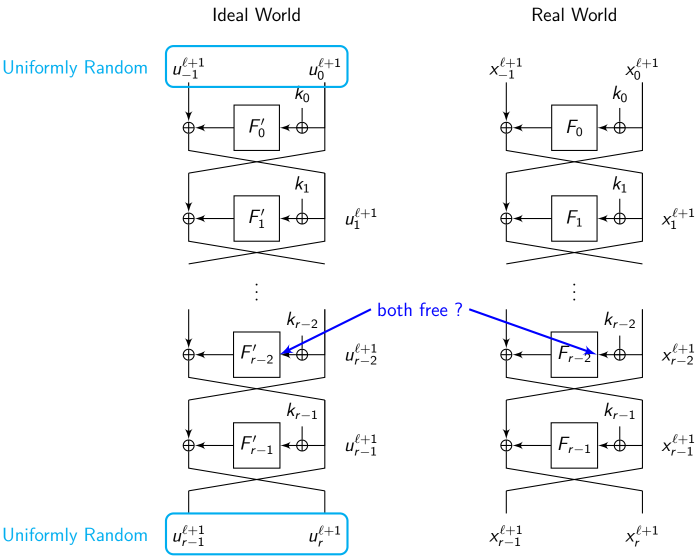
The Coupling Technique for the KAF



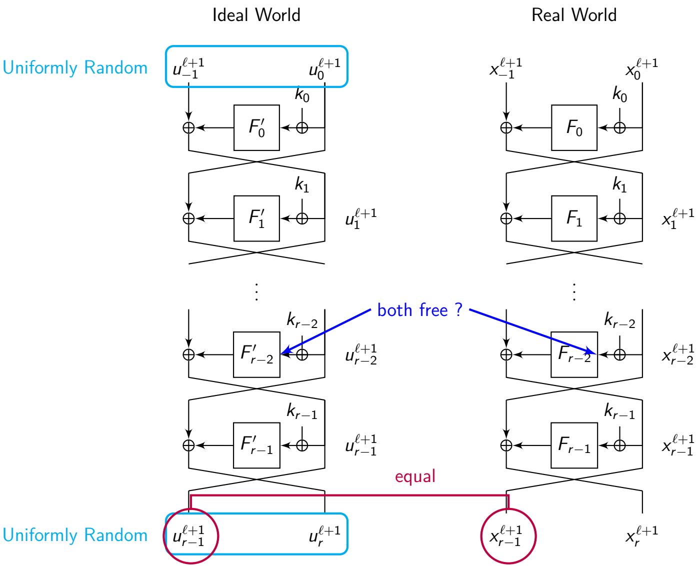
The Coupling Technique for the KAF



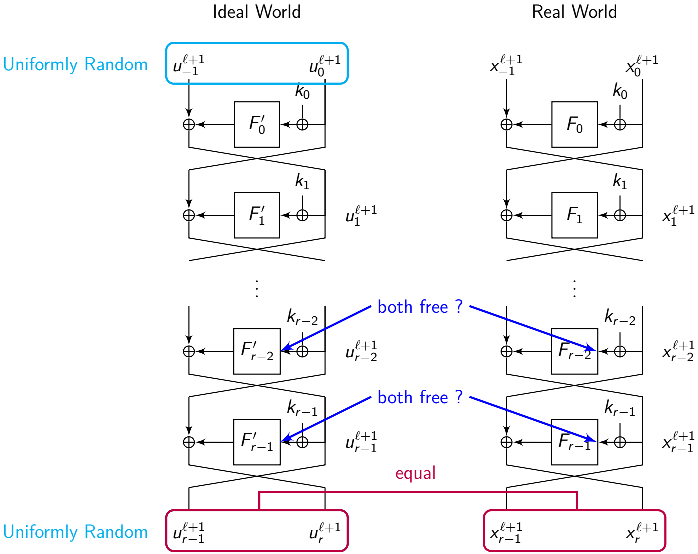
The Coupling Technique for the KAF



The Coupling Technique for the KAF



The Coupling Technique for the KAF



Advantage

q_e :number of queries to the cipher

q_f :number of queries to the round functions

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathtt{KAF}[n,r]}(q_e, q_f) \leq \frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \quad \text{with} \quad t = \left\lfloor \frac{r}{3} \right\rfloor.$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathtt{KAF}[n,2r']}(q_e, q_f) \leq 4 \left(\frac{4^t}{t+1} \frac{(q_e + 2q_f)^{t+1}}{2^{tn}} \right)^{1/2} \quad \text{with} \quad t = \left\lfloor \frac{r'}{3} \right\rfloor.$$

The end...

Thanks for your attention!
Comments or questions?

References I

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser.

Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract).

In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012.

Shan Chen and John P. Steinberger.

Tight security bounds for key-alternating ciphers.

IACR Cryptology ePrint Archive, 2013:222, 2013.

Shimon Even and Yishay Mansour.

A Construction of a Cipher from a Single Pseudorandom Permutation.

Journal of Cryptology, 10(3):151–162, 1997.

References II

Craig Gentry and Zulfikar Ramzan.

Eliminating Random Permutation Oracles in the Even-Mansour Cipher.

In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2004.

Rodolphe Lampe, Jacques Patarin, and Yannick Seurin.

An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher.

In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012.

John Steinberger.

Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance.

IACR Cryptology ePrint Archive, Report 2012/481, 2012.

Available at `http://eprint.iacr.org/2012/481`.