Improved Analysis of Unbalanced Feistel Networks by Coupling

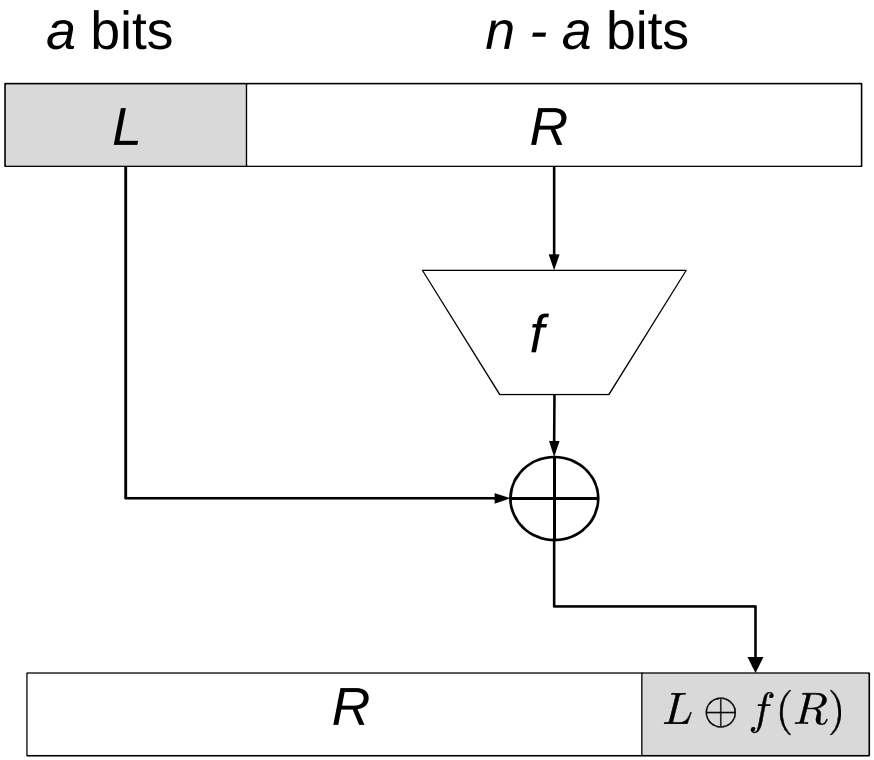
Viet Tung Hoang & Phillip Rogaway

University of California, Davis

Unbalanced Feistel networks

- By *[Schneier-Kelsey]*

Feistel (*n*, *a*)-network



CCA-security of unbalanced Feistel networks

a	Queries
a	about $2^{(n-a)/2}$ *[Naor - Reingold]*
$n/2$	about $2^{n/2}$ *[Patarin]*
1	about 2^{n-1} *[Morris et al.]*

Our results

- **Theorem**: If a Feistel (*n*, *a*)-network E has $\frac{4rn}{a}$ rounds then

$$\mathbf{Adv}^{cca}(E, q) \leq \frac{q}{r+1}\left(\frac{2nq}{a} \cdot 2^{a-n}\right)$$

Our results

- **Theorem**: If a Feistel (*n*, *a*)-network E has $\frac{4rn}{a}$ rounds then

$$\mathbf{Adv}^{cca}(E, q) \leq \frac{q}{r+1}\left(\frac{2nq}{a} \cdot 2^{a-n}\right)$$

- Interpretation: CCA-secure to nearly 2^{n-a} queries

Our results

- **Theorem**: If a Feistel (*n*, *a*)-network E has $\frac{4rn}{a}$ rounds then

$$\mathbf{Adv}^{cca}(E, q) \leq \frac{q}{r+1}\left(\frac{2nq}{a} \cdot 2^{a-n}\right)$$

- Interpretation: CCA-secure to nearly 2^{n-a} queries
- Attack: $r\,2^{n-a}$ queries to break a network of *r* rounds.

Our results

- **Theorem**: If a Feistel (*n*, *a*)-network E has $\frac{4rn}{a}$ rounds then

$$\mathbf{Adv}^{cca}(E, q) \leq \frac{q}{r+1}\left(\frac{2nq}{a} \cdot 2^{a-n}\right)$$

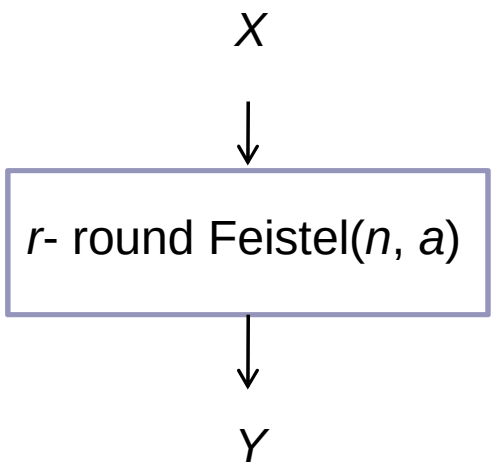
- Interpretation: CCA-secure to nearly 2^{n-a} queries
- Attack: $r\,2^{n-a}$ queries to break a network of *r* rounds.
- Simple proof by **coupling argument**.

Intuition of the proof

- Adversary asks nCPA queries $X_1, \ldots, X_q$

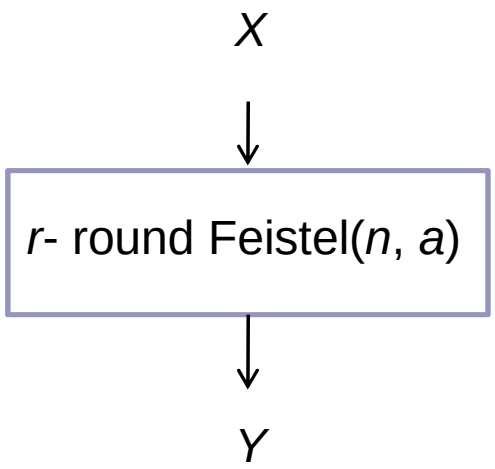
Intuition of the proof

- Adversary asks nCPA queries $X_1,\ldots, X_q$
- $X = (X_1, \ldots, X_q)$, and Y : the vector of outputs from X



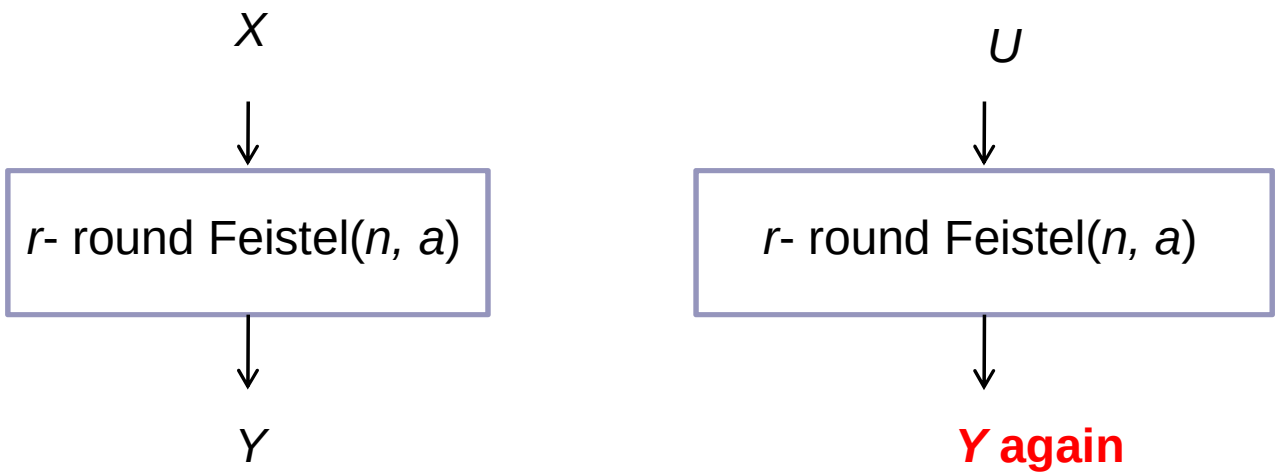
Intuition of the proof

- Adversary asks nCPA queries $X_1,\ldots, X_q$
- $X = (X_1, \ldots, X_q)$, and Y : the vector of outputs from X
- π: uniform distribution in the set of q-tuples of elements of $\{0, 1\}^n$



Intuition of the proof

- Pick random vector $U = (U_1, \ldots, U_q)$ with distribution π
- Design a new Feistel (n, a)-network that outputs ***Y*** on input U, with high probability.



Intuition of the proof