Improved Security Bounds for Generalized Feistel Networks

Yaobin Shen[1] Chun Guo[2] Lei Wang[1]

[1]Shanghai Jiao Tong University

[2]Shandong University

November 13, FSE 2020

Outline

Feistel Network

- Feistel network: iterate several times of Feistel permutation
  - $\Psi_{F_i}(A, B) = (B, A \oplus F_i(B))$, where $F_i : \{0,1\}^n \to \{0,1\}^n$ is called round function

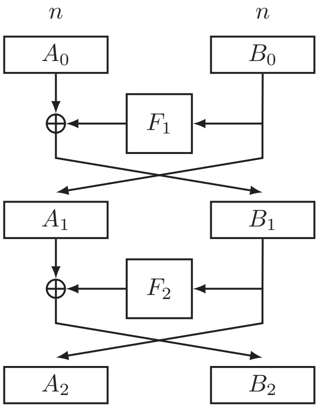
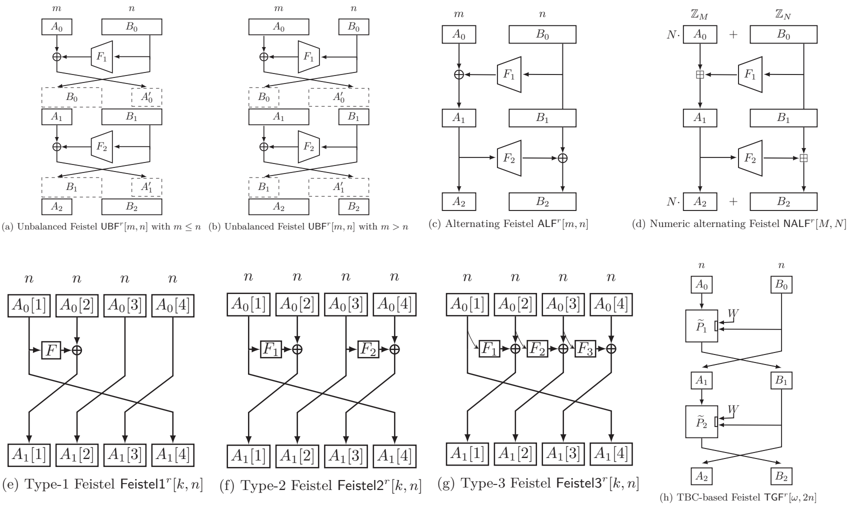


Figure: Classical Feistel

Generalized Feistel Networks

- Replace round functions with expanding or contracting ones
  - unbalanced Feistel
- Alternatively use expanding and contracting round functions
  - alternating Feistel
- Partition the input into more than two blocks
  - type-1, type-2, type-3 Feistel
- Use tweakable blockcipher
  - TBC-based Feistel

Generalized Feistel Networks



(a) Unbalanced Feistel $\mathsf{UBF}^r[m,n]$ with $m \le n$ (b) Unbalanced Feistel $\mathsf{UBF}^r[m,n]$ with $m > n$ (c) Alternating Feistel $\mathsf{ALF}^r[m,n]$ (d) Numeric alternating Feistel $\mathsf{NALF}^r[M,N]$

(e) Type-1 Feistel $\mathsf{Feistel1}^r[k,n]$ (f) Type-2 Feistel $\mathsf{Feistel2}^r[k,n]$ (g) Type-3 Feistel $\mathsf{Feistel3}^r[k,n]$ (h) TBC-based Feistel $\mathsf{TGF}^r[\omega,2n]$

Figure: Illustration of generalized Feistel networks

Applications of Feistel Networks

- DES (classical Feistel)
- Skipjack (unbalanced Feistel)
- BEAR/LION, Format-Preserving Encryption (alternating Feistel)
- CAST-256 (type-1), RC6 (type-2), MARS (type-3)
- Double-block length Tweakable blockcipher (TBC-based Feistel)

Previous Results

- For unbalanced, alternating, type-1, type-2, type-3 Feistel
  - Birthday-bound security [NR99,MRS09,AB96,BR02,BRRS09,Luc96,ZMI90]
  - Beyond-birthday-bound security for unbalanced Feistel [Pat10]
  - Asymptotically n-bit security [HR10] for all these Feistels
- Hoang and Rogaway's result [HR10]
  - CCA-secure up to $2^{(1-\varepsilon)n}$ queries for any $\varepsilon > 0$
  - requires a large number of rounds for asymptotically n-bit security
- For TBC-based Feistel by Coron et al. [CDMS10]
  - 3 rounds are proved to have n-bit security
  - the input size to underlying tweakable permutation is: $n + w$ (w is the size of tweak, $w > n$)
  - n-bit security is only birthday-type with respect to the input size [LL18]

Outline

1 Feistel Networks

2 Our Contributions

3 Security Proofs

4 Conclusion

Improved Security Bounds

- For unbalanced, alternating, type-1, type-2 and type-3 Feistel
  - improve the coupling analyzes of Hoang and Rogaway [HR10]
  - achieve almost the same security bound with a nearly half number of rounds

Scheme	Previous Bound	#rounds	Our Bound	#rounds
$\mathsf{UBF}^r[m,n]$				
$n \geq m$	$\frac{2q}{t+1}\left(\frac{(3\lceil\frac{n}{m}\rceil+3)q}{2^n}\right)^t$	$(4\lceil\frac{n}{m}\rceil+4)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{4\lceil\frac{n}{m}\rceil q+4q}{2^n}\right)^t$	$(2\lceil\frac{n}{m}\rceil+2)t+2\lceil\frac{n}{m}\rceil+1$
$n < m$	$\frac{2q}{t+1}\left(\frac{4\lceil\frac{m}{n}\rceil q}{2^n}\right)^t$	$(2\lceil\frac{m}{n}\rceil+4)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{4\lceil\frac{n}{m}\rceil q}{2^n}\right)^t$	$4t+2\lceil\frac{n}{m}\rceil+1$
$\mathsf{ALF}^r[m,n]$	$\frac{2q}{t+1}\left(\frac{(6\lceil\frac{n}{m}\rceil+3)q}{2^n}\right)^t$	$(12\lceil\frac{n}{m}\rceil+8)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{6\lceil\frac{n}{m}\rceil q+3q}{2^n}\right)^t$	$(12\lceil\frac{n}{m}\rceil+2)t+5$
$\mathsf{NALF}^r[M,N]$	$\frac{2q}{t+1}(\frac{(6\lceil\log_M N\rceil+3)q}{N})^t$	$(12\lceil\log_M N\rceil+8)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{6\lceil\log_M N\rceil q+3q}{N}\right)^t$	$(12\lceil\log_M N\rceil+2)t+5$
$\mathsf{Feistel1}^r[k,n]$	$\frac{2q}{t+1}\left(\frac{2k(k^2-k+1)q}{2^n}\right)^t$	$(2k^2+2k)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{2k(k-1)q}{2^n}\right)^t$	$(k^2+k-2)t+1$
$\mathsf{Feistel2}^r[k,n]$	$\frac{2q}{t+1}\left(\frac{2k(k-1)q}{2^n}\right)^t$	$(2k+2)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{2k(k-1)q}{2^n}\right)^t$	$2kt+1$
$\mathsf{Feistel3}^r[k,n]$	$\frac{2q}{t+1}\left(\frac{4(k-1)^2q}{2^n}\right)^t$	$(k+4)t$ [HR10]	$\frac{2q}{t+1}\left(\frac{4(k-1)^2q}{2^n}\right)^t$	$(k+2)t+1$

Table: Summary of improved bounds for generalized Feistel networks

Improved Security Bounds

- For TBC-based Feistel
  - give the first coupling analysis
  - achieves $2n$-bit security with enough rounds

Scheme	Previous Bound	#rounds	Our Bound	#rounds
$\mathrm{TGF}^r[\omega, 2n]$	$\frac{q^2}{2^{2n}}$	3 [CDMS10]	$2 \cdot \left(\frac{q}{t+1} \left(\frac{30q}{2^{2n}} \right)^t \right)^{1/2}$	$4t+2$

Table: Comparison between Coron et al.'s bound and our bound.

Outline

The Coupling Technique

- Focus on NCPA security, then lift it to CCA security by a composition lemma [MP03]

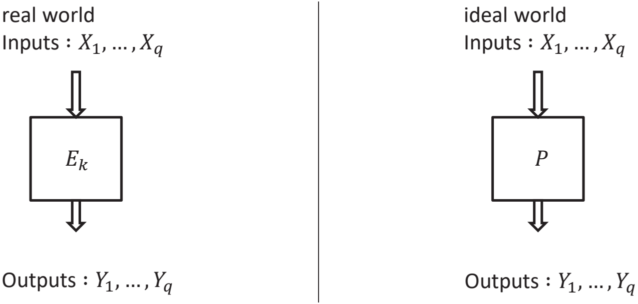


Figure: The NCPA indistinguishability game

The Coupling Technique

- Another ideal world
  - $U_1, \ldots, U_q$ are uniformly sampled at random without replacement from $\{0,1\}^n$
  - E_k is a permutation
  - So in the ideal world, $Y_1, \ldots, Y_q$ are also uniformly sampled at random without replacement from $\{0,1\}^n$

Figure: The NCPA indistinguishability game

The Coupling Technique

- Intermediate game

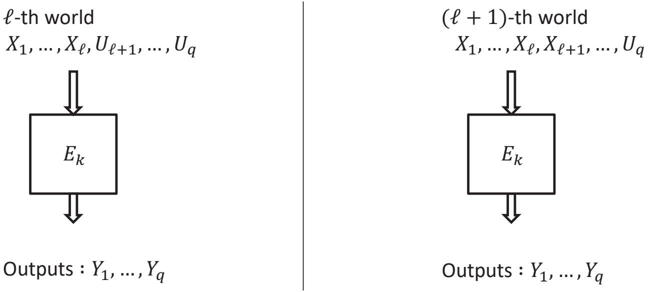


Figure: The NCPA indistinguishability game

- $\mathsf{Adv}^{\mathrm{ncpa}}_{E_k}(q) \leq \sum_{\ell=0}^{q-1} \|\mu_\ell - \mu_{\ell+1}\|$
  - μ_0 the distribution of outputs in the ideal world
  - μ_ℓ the distribution of outputs in the ℓ-th world
  - μ_q the distribution of outputs in the real world

The Coupling Technique

- A coupling of μ and ν is a distribution λ on $\Omega \times \Omega$ such that:

$$\begin{cases} \forall x \in \Omega, \sum_{y \in \Omega} \lambda(x,y) = \mu(x) \\ \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x,y) = \nu(y) \end{cases}$$

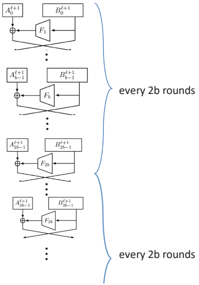
- Use coupling lemma to bound the distance between μ_ℓ and $\mu_{\ell+1}$

Lemma (Coupling Lemma)

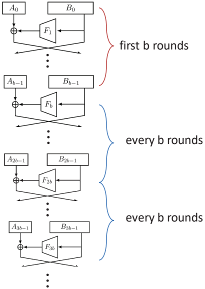
Let μ and ν be two probability distributions on a finite event space Ω. Let random variable (X, Y) be a coupling of μ and ν. Then $\|\mu - \nu\| \leq \Pr[X \neq Y]$.

Proof for Unbalanced Feistel

- Intuition of the improvement
  - the output after b rounds is somewhat random and collision-free
  - reduce the number of rounds in each of following trials in coupling analysis



HR's idea



our improvement

Proof for Unbalanced Feistel

- A more fine-grained analysis of the internal collision

Lemma

Consider an unbalanced Feistel cipher $\mathsf{UBF}^r[m,n]$ *with* $m \le n$. *Let* $b = \lceil n/m \rceil$. *For any* $i \in [b+1; r]$ *and any subset* $S \subseteq [b+1; i-1]$, *one has*

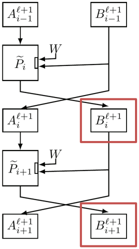
$$\Pr[\mathsf{COLL}_i \mid \cap_{s \in S} \mathsf{COLL}_s] \le \frac{4\ell}{2^n},$$

where ℓ *is the number of queries that has made to the cipher before the coupling.*

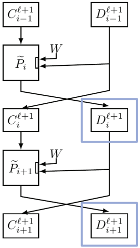
- Similar improvement idea for alternating, type-1, type-2, type-3 Feistels

Proof for TBC-based Feistel

- Define two bad events
  - coll_i: $D_i^{\ell+1} = B_i^j \wedge B_{i+1}^{\ell+1} = B_{i+1}^j$ for $j \leq \ell$
  - coll'_i: $B_i^{\ell+1} = B_i^j \wedge D_{i+1}^{\ell+1} = B_{i+1}^j$ for $j \leq \ell$

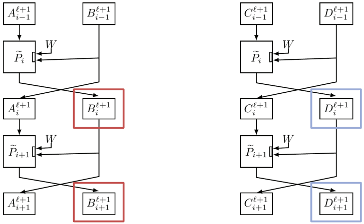


first cipher



second cipher

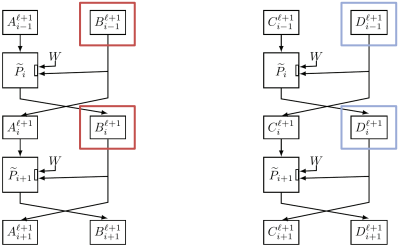
Proof for TBC-based Feistel



- coupling according to four sub-cases
  - $B_i^{\ell+1} \neq B_i^j \wedge D_i^{\ell+1} \neq B_i^j : D_{i+1}^{\ell+1} = B_{i+1}^{\ell+1} \leftarrow\$ \{0,1\}^n$
  - $B_i^{\ell+1} = B_i^j \wedge D_i^{\ell+1} \neq B_i^j : D_{i+1}^{\ell+1} = B_{i+1}^{\ell+1} \leftarrow\$ \{0,1\}^n \setminus \mathrm{Rng}(\widetilde{P}_{i+1}(W \parallel B_i^j,))$
  - $B_i^{\ell+1} \neq B_i^j \wedge D_i^{\ell+1} = B_i^j : D_{i+1}^{\ell+1} = B_{i+1}^{\ell+1} \leftarrow\$ \{0,1\}^n \setminus \mathrm{Rng}(\widetilde{P}_{i+1}(W \parallel B_i^j,))$
  - $B_i^{\ell+1} = B_i^j \wedge D_i^{\ell+1} = B_i^{j'} :$
    $D_{i+1}^{\ell+1} = B_{i+1}^{\ell+1} \leftarrow\$ \{0,1\}^n \setminus (\mathrm{Rng}(\widetilde{P}_{i+1}(W \parallel B_i^j,)) \cup \mathrm{Rng}(\widetilde{P}_{i+1}(W \parallel B_i^{j'},)))$

Proof for TBC-based Feistel

- Bound the probability of two bad events:



first cipher second cipher

  - analyze the probability that the number of repeated tweaks is greater than a threshold c
  - when the number of repeated tweaks $\leq c$

$$\Pr[\text{coll}_i] \leq \frac{2e^c \cdot \ell^c}{c^c \cdot 2^{nc}} + \frac{\ell}{(2^n - c)^2}$$

Outline

Conclusion

- For unbalanced, alternating, type-1, type-2, and type-3 Feistel
  - improve the coupling analysis of Hoang and Rogaway
  - achieve the asymptotically optimal security with nearly half number of rounds
- For TBC-based Feistel
  - prove that it can achieve $2n$-bit security with enough rounds
- Future works
  - give a tighter analysis via the coupling technique
  - analyze the security for a smaller number of rounds (χ^2 method, H-coefficient technique)