KFC - The Krazy Feistel Cipher

Thomas Baignères    Matthieu Finiasz

ASIACRYPT 2006
Block Ciphers’ specialists are very good at designing extreme constructions

On the one hand: Feistel scheme with 3 perfectly random functions.
- **Provably** secure in the Luby-Rackoff model (computationally unbounded adversary with limited queries)
- **Unpractical** $\approx 2^{70}$ random bits are necessary to instantiate a 128-bit block scheme.

On the other hand: AES and friends.
- Incredibly fast
- Only **practically** secure: none of the smart cryptanalysts who attacked them was able to break them (yet).
- ↞ don’t miss today’s new cryptanalytic results on IDEA!
Block Ciphers’ specialists are very good at designing extreme constructions.

On the one hand: Feistel scheme with 3 perfectly random functions.

- Provably secure in the Luby-Rackoff model (computationally unbounded adversary with limited queries)
- Unpractical $\approx 2^{70}$ random bits are necessary to instantiate a 128-bit block scheme.

On the other hand: AES and friends.

- Incredibly fast
- Only practically secure: none of the smart cryptanalysts who attacked them was able to break them (yet).
- $\Rightarrow$ don’t miss today’s new cryptanalytic results on IDEA!
KFC lies in-between both extremes:

- It comes with security proofs in the Luby-Rackoff model,
- and is practical (we mean, it can be implemented in practice).

More precisely, depending on the parameters choice:

- KFC is provably secure against $d$-limited adversaries for values of $d$ ranging from 2 up to 70.
- This is enough to resist several statistical attacks.
- This includes Linear and Differential Cryptanalysis (taking hull/differentials effects in consideration), higher order differential cryptanalysis, etc.
- KFC's speed ranges from “not-very-fast” to “outrageously-slow”.

Yet another Block Cipher?

KFC lies in-between both extremes:

- It comes with security proofs in the Luby-Rackoff model,
- and is practical (we mean, it can be implemented in practice).

More precisely, depending on the parameters choice:

- KFC is provably secure against $d$-limited adversaries for values of $d$ ranging from 2 up to 70.
- This is enough to resist several statistical attacks.
- This includes Linear and Differential Cryptanalysis (taking hull/differentials effects in consideration), higher order differential cryptanalysis, etc.
- KFC’s speed ranges from “not-very-fast” to “outrageously-slow”.
Yet another Block Cipher?

KFC lies in-between both extremes:
- It comes with security proofs in the Luby-Rackoff model,
- and is practical (we mean, it can be implemented in practice).

More precisely, depending on the parameters choice:
- KFC is provably secure against $d$-limited adversaries for values of $d$ ranging from 2 up to 70.
- This is enough to resist several statistical attacks.
- This includes Linear and Differential Cryptanalysis (taking hull/differentials effects in consideration), higher order differential cryptanalysis, etc.
- KFC’s speed ranges from “not-very-fast” to “outrageously-slow”.

Outline

1. Security Model

2. From the SPN of C to the Feistel scheme of KFC

3. Overview of Security Proofs on KFC
Outline

1. Security Model

2. From the SPN of C to the Feistel scheme of KFC

3. Overview of Security Proofs on KFC
We consider a $d$-limited adversary $\mathcal{A}$ in the Luby-Rackoff model:

- computationally unbounded
- limited to $d$ queries to an oracle $\mathcal{O}$ implementing either
  - a random instance $C$ of the block cipher
  - or a random instance $C^*$ of the perfect cipher
- the objective of $\mathcal{A}$ being to guess which is the case.

\[
\text{Advantage of } \mathcal{A} = | \Pr[\mathcal{A}(C) = 0] - \Pr[\mathcal{A}(C^*) = 0]|.
\]
A block cipher $C$ is secure if $\text{Adv}_A(C, C^*)$ is negligible for all $A$'s. **Problem**: computing this advantage is not a trivial task in general.
Computing $\text{Adv}_A(C, C^*)$ using the Decorrelation Theory

A block cipher $C$ is secure if $\text{Adv}_A(C, C^*)$ is negligible for all $A$’s.

**Problem:** computing this advantage is not a trivial task in general.

**Possible Solution:** Use Vaudenay’s Decorrelation Theory as a toolbox.

For a given cipher $C : \mathcal{M} \rightarrow \mathcal{M}$, the distribution matrix at order $d$ is:

$$[C]^d = \left\{ \begin{array}{c}
\Pr \\
\Sigma \\
|\mathcal{M}|^d \\
\end{array} \right\}$$

$$\Pr = \Pr_{C}[C(x_1) = y_1, \ldots, C(x_d) = y_d]$$
Computing $\text{Adv}_A(C, C^*)$ using the Decorrelation Theory

A block cipher $C$ is secure if $\text{Adv}_A(C, C^*)$ is negligible for all $A$'s.

**Problem:** computing this advantage is not a trivial task in general.

**Possible Solution:** Use Vaudenay’s Decorrelation Theory as a toolbox.

For a given cipher $C : \mathcal{M} \rightarrow \mathcal{M}$, the distribution matrix at order $d$ is:

- $[C]^d = \begin{pmatrix} y_1, \ldots, y_d \\ x_1, \ldots, x_d \end{pmatrix}$
- $\Pr = \Pr[C(x_1) = y_1, \ldots, C(x_d) = y_d]$
- $= 1$
- $|\mathcal{M}|^d$

**Link between $\text{Adv}_A(C, C^*)$ and $[C]^d$**

$$\max_A \text{Adv}_A(C, C^*) = \frac{1}{2} \| [C]^d - [C^*]^d \|.$$ 

⚠️ $|\mathcal{M}|^d \approx 2^{128d}$ for a 128-bit block cipher! ⚠️
Computing $\text{Adv}_A(C, C^*)$ using the Decorrelation Theory

There are at least two ways to deal with distribution matrix size:

- Use decorrelation modules as building blocks (drawback: may lead to “algebraic” constructions)
- Exploit the symmetries of the cipher (as done in [Baignères, Finiasz SAC06] and here)
Computing $\text{Adv}_A(C, C^*)$ using the Decorrelation Theory

There are at least two ways to deal with distribution matrix size:

- **Use decorrelation modules** as building blocks (drawback: may lead to “algebraic” constructions)
- Exploit the symmetries of the cipher (as done in [Baignères, Finiasz SAC06] and here)
There are at least two ways to deal with distribution matrix size:

- Use **decorrelation modules** as building blocks (drawback: may lead to “algebraic” constructions)
- Exploit the **symmetries** of the cipher (as done in [Baignères, Finiasz SAC06] and here)
The security proofs we provide not only induce resistance against LC and DC but against a wider class of attacks. Most of statistical attacks (LC, DC, Higher order differentials, etc.) belong to the family of iterated attacks of order $d$.

For example:
- LC is an iterated attack of order 1, and
- DC is an iterated attack of order 2.

Provable security against $d$-limited adversaries $\Rightarrow$ Provable security against iterated attacks of order $\frac{d}{2}$ [Vaudenay JOC03].

$\Rightarrow$ one security proof leads to provable security against several attacks.
The security proofs we provide not only induce resistance against LC and DC but against a wider class of attacks. Most of statistical attacks (LC, DC, Higher order differentials, etc.) belong to the family of iterated attacks of order $d$.

For example:
- LC is an iterated attack of order 1, and
- DC is an iterated attack of order 2.

Provable security against $d$-limited adversaries $\Rightarrow$ Provable security against iterated attacks of order $\frac{d}{2}$ [Vaudenay JOC03].

$\Rightarrow$ one security proof leads to provable security against several attacks.
The security proofs we provide not only induce resistance against LC and DC but against a wider class of attacks. Most of statistical attacks (LC, DC, Higher order differentials, etc.) belong to the family of iterated attacks of order $d$.

For example:

- LC is an iterated attack of order 1, and
- DC is an iterated attack of order 2.

Provable security against $d$-limited adversaries $\Rightarrow$ Provable security against iterated attacks of order $\frac{d}{2}$ [Vaudenay JOC03].

$\Rightarrow$ one security proof leads to provable security against several attacks.
The security proofs we provide not only induce resistance against LC and DC but against a wider class of attacks. Most of statistical attacks (LC, DC, Higher order differentials, etc.) belong to the family of iterated attacks of order $d$.

For example:
- LC is an iterated attack of order 1, and
- DC is an iterated attack of order 2.

Provable security against $d$-limited adversaries $\Rightarrow$ Provable security against iterated attacks of order $\frac{d}{2}$ [Vaudenay JOC03].

$\Rightarrow$ one security proof leads to provable security against several attacks.
Outline

1 Security Model

2 From the SPN of C to the Feistel scheme of KFC

3 Overview of Security Proofs on KFC
The block cipher \( C \)

\( C \) is a block cipher based on a Substitution-Permutation Network (SPN) [Baignères, Finiasz SAC06].

Each round is made of:
- A layer of substitution boxes \( \leadsto \text{confusion} \)
- A linear layer \( \leadsto \text{diffusion} \)

- The \( C^* \)'s are mutually independent and perfectly random permutations on \( \{0, 1\}^8 \)
- The linear layer \( L \) is exactly the one used in AES
Security Results on the block cipher $C$

We showed that $C$ is provably secure against 2-limited adversaries:

- Instead of directly computing the $2^{256} \times 2^{256}$ distribution matrix $[C]^2$...
- We took advantage of the fact that symmetries of the cipher induce symmetries in the distribution matrix $[C]^2$.
- Computation on $625 \times 625$ matrices:

$$\max_{\mathcal{A}} \text{Adv}_{\mathcal{A}}(C, C^*) = 2^{-185.5}$$

**Problem:** we could not exhibit similar symmetries in $[C]^d$ for $d > 2$. 
The Main Idea that lead us to the KFC Construction

Instead of computing the advantage of the best $d$-limited adversary, we will bound it by a function of the advantage of the best $(d - 1)$-limited adversary.
The Main Idea that lead us to the KFC Construction

Instead of computing the advantage of the best $d$-limited adversary, we will bound it by a function of the advantage of the best $(d - 1)$-limited adversary.

This approach is problematic with layers of random permutations:

- two correlated inputs of a random permutation always lead to two correlated outputs,
- two different inputs of a random function lead to two independent outputs.
Idea: Replace the layers of mutually independent and perfectly random permutations by layers of mutually independent and perfectly random functions.
Problem #1

**Problem:** If two inputs are equal on all $F^*$ inputs but one $\Rightarrow$ non-negligible probability to obtain a full collision.
Problem #1

**Problem:** If two inputs are equal on all $F^*$ inputs but one $\leadsto$ non-negligible probability to obtain a full collision.

**Solution:** The Sandwich Technique
Problem #2

Problem: Our construction is not invertible.
Problem #2

Problem: Our construction is not invertible.
Trivial Solution: Plug it in a Feistel Scheme
KFC: The Big Picture

$F_{KFC} \equiv \begin{array}{c}
\begin{array}{c}
C^* C^* C^* C^* \\
\vdots \\
L \text{(multipermutation)}
\end{array}
\end{array}
\begin{array}{c}
F^* F^* F^* F^* \\
\vdots \\
L
\end{array}
\begin{array}{c}
C^* C^* C^* C^* \\
\vdots \\
\end{array}$

$F_{KFC} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ such that $\text{Adv}_A(F_{KFC}, F^*) \leq \epsilon$

$\text{Adv}_A(KFC, C^*) \leq 2\epsilon + \frac{d^2}{2^n}$

Objective: Prove that $\epsilon$ is negligible.
Outline

1. Security Model

2. From the SPN of C to the Feistel scheme of KFC

3. Overview of Security Proofs on KFC
Computing the Advantage of the Best 2-limited Adversary

We denote $F_{KFC} = S \circ (L \circ F)^{r_2} \circ (L \circ S)^{r_1}$ so that

$$[F_{KFC}]^2 = [S \circ (L \circ F)^{r_2} \circ (L \circ S)^{r_1}]^2 = ([S]^2 \times [L]^2)^{r_1} \times ([F]^2 \times [L]^2)^{r_2} \times [S]^2.$$  

⚠️ These are $2^{2n} \times 2^{2n}$ matrices... The shape of the confusion layers allows to write
Computing the Advantage of the Best 2-limited Adversary

Putting things together, we have (with $r_1 = r_2 = 1$):

\[
[F_{kfc}]^2 \times PS \times [L]^2 \times PS = \text{identity} \times SP
\]

Product of matrices indexed by weights of supports:

\[
P_{W} = \times \times F \times \times WP
\]
Computing the Advantage of the Best 2-limited Adversary

Putting things together, we have (with $r_1 = r_2 = 1$):

$$[F_{KFC}]^2 = PW \times (\mathbf{L})^{r_1} \times (\mathbf{F} \times \mathbf{L})^{r_2} \times WP$$
Computing the Advantage of the Best 2-limited Adversary
(at last)

In the end...

\[ \| [F_{KFC}]^2 - [F^*]^2 \| = \| (\overline{L})^{r_1} \times (\overline{F} \times \overline{L})^{r_2} - U \| \]

so that one can easily compute

\[
\text{Adv}_A(F_{KFC}) = \frac{1}{2} \| (\overline{L})^{r_1} \times (\overline{F} \times \overline{L})^{r_2} - U \|
\]
Computing the Advantage of the Best 2-limited Adversary (at last)

In the end...

\[ \| [F_{KFC}]^2 - [F^*]^2 \| = \| (L)^{r_1} \times (F \times L)^{r_2} - U \| \]

\[ 2^{256} \times 2^{256} \text{ matrices} \]

\[ 9 \times 9 \text{ matrices} \]

so that one can easily compute

\[ \text{Adv}_A(F_{KFC}) = \frac{1}{2} \| (L)^{r_1} \times (F \times L)^{r_2} - U \| \]
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)

Assume one of the $d$ box inputs is different from all the others.

Then one of the $d$ box outputs is independent from all the others.
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)

Assume one of the $d$ box inputs is different from all the others on all boxes.

Then one of the $d$ box outputs is independent from all the others.
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)

\[
\text{Adv}_{\mathcal{A}_d}(F, F^*) \leq \text{Adv}_{\mathcal{A}_{d-1}}(F, F^*) + \Pr[\bar{\alpha}]
\]
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)

Considering several $\alpha$ events on $t$ successive rounds, one can bound the probability that *none* of them occurs:

$$\Pr[\overline{\alpha_1}, \ldots, \overline{\alpha_t}] \leq \left(1 - \left(1 - \frac{d - 1}{q}\right)^N\right)^t$$
Bounding the Advantage of the Best $d$-limited Adversary ($d > 2$)

Considering several $\alpha$ events on $t$ successive rounds, one can bound the probability that none of them occurs:

$$\Pr[\alpha_1, \ldots, \alpha_t] \leq \left(1 - \left(1 - \frac{d-1}{q}\right)^N\right)^t$$

**Theorem**

Assume $\text{Adv}_{A_2}(F_{KFC}, F^*) \leq \epsilon$. For any $d$ and set of integers $\{t_3, \ldots, t_d\}$ s.t. $\sum_{i=3}^{d} t_i \leq r_2$, we have

$$\text{Adv}_{A_d}(F_{KFC}, F^*) \leq \epsilon + \sum_{i=3}^{d} \left(1 - \left(1 - \frac{i-1}{q}\right)^N\right)^{t_i}$$
Regular KFC: $N = 8, q = 2^8, r_1 = 3, r_2 = 100$

- Provable security against 8-limited adaptive adversaries
- Thus against iterated attacks of order 4
- (Estimated) Speed of 15-25 Mbits/s
Regular KFC: $N = 8, q = 2^8, r_1 = 3, r_2 = 100$
- Provable security against 8-limited adaptive adversaries
- Thus against iterated attacks of order 4
- (Estimated) Speed of 15-25 Mbits/s

Extra Crispy KFC: $N = 8, q = 2^{16}, r_1 = 3, r_2 = 1000$
- Provable security against 70-limited adaptive adversaries
- Thus against iterated attacks of order 35
- (Estimated) Speed $< (\ll ?) 1$ Mbit/s
- 4 GB of memory are required
Conclusion and Further Improvements

- KFC is the first “practical” block cipher with security proofs up to a large order.

- Bounds can be improved: the same security level can be achieved with fewer rounds (hint: improve the bound on $\alpha$).

- It is possible to weaken the assumptions on the round functions of the Feistel scheme and obtain the same security level (see [Lucks FSE96] or [Maurer, Oswald, Pietrzak, Sjödin Eurocrypt06]).

- Use a faster diffusion layer (ShiftRows+Mixcolumns): increase $r_1$ but improve global speed.
KFC is the first “practical” block cipher with security proofs up to a large order.

Bounds can be improved: the same security level can be achieved with fewer rounds (hint: improve the bound on $\alpha$).

It is possible to weaken the assumptions on the round functions of the Feistel scheme and obtain the same security level (see [Lucks FSE96] or [Maurer, Oswald, Pietrzak, Sjödin Eurocrypt06]).

Use a faster diffusion layer (ShiftRows+Mixcolumns): increase $r_1$ but improve global speed.