Cryptanalysis of FROG

David Wagner
University of California, Berkeley

Niels Ferguson   Bruce Schneier
Counterpane Systems

Many details also independently discovered by Don Coppersmith.

Organization

- Description of FROG
- Observations
- Differential attacks
- Linear attacks

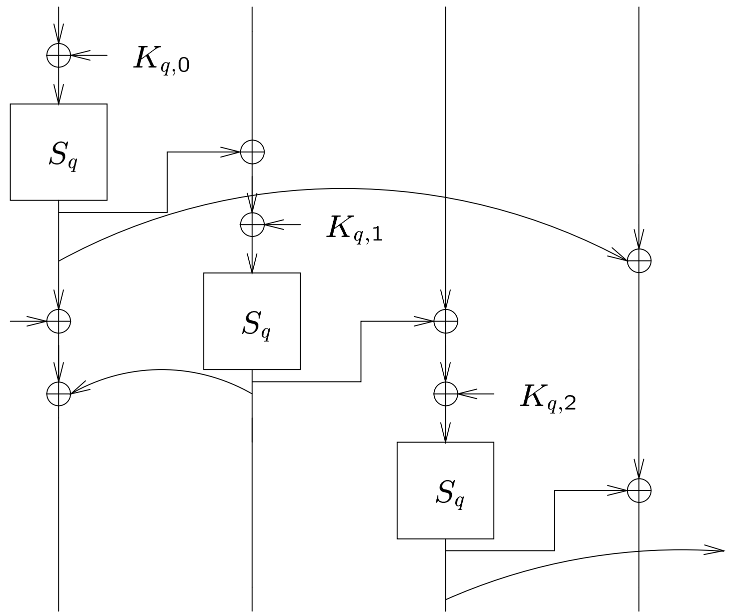
The cipher

- Novel byte-oriented structure.
- Key-dependent S-boxes and internal wiring.
- 8 “cycles”, each containing 16 rounds.
- Round r of cycle q operates as

$$\begin{aligned} X_r &\leftarrow S_q(X_r \oplus K_{q,r}) \\ X_{r+1} &\leftarrow X_{r+1} \oplus X_r \\ X_{\pi_q(r)} &\leftarrow X_{\pi_q(r)} \oplus X_r, \end{aligned}$$

See next slide for a pictorial illustration.

One cycle of FROG



Property: Key-dependent diffusion structure

The FROG diffusion structure is partly key-dependent. Thus,

THE QUALITY OF DIFFUSION IN FROG IS KEY-DEPENDENT.

Each setting for the internal wiring gives a different cipher, which must be analyzed separately.

Property: Asymmetrical round function

A FROG round looks different depending on whether you're running it forward or backward.

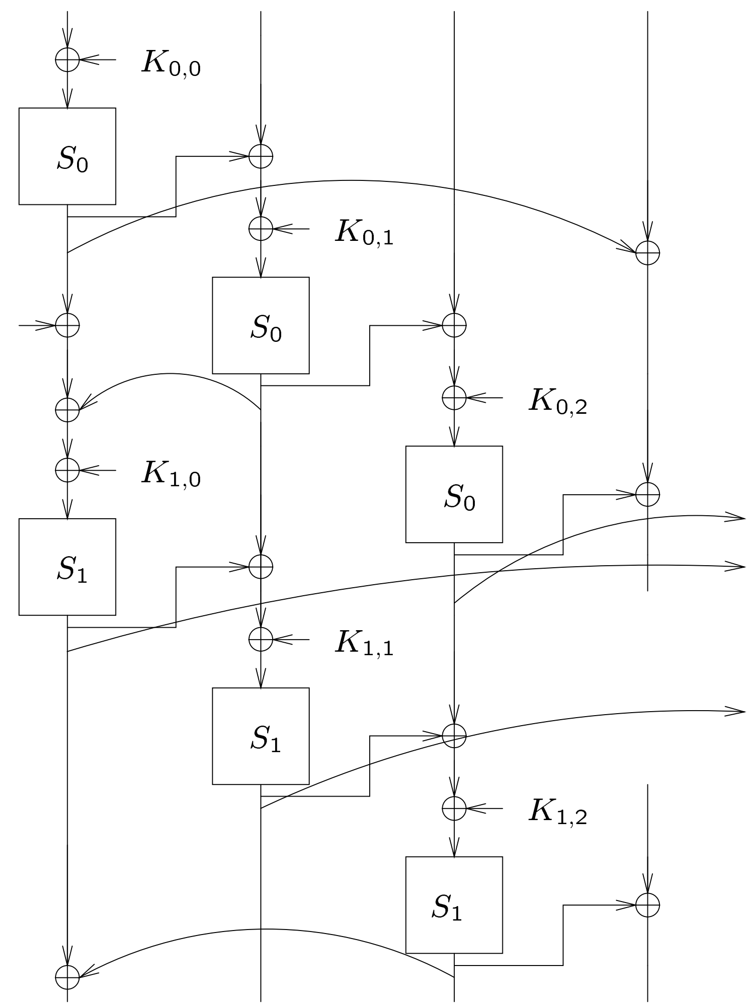
To use Skipjack terminology, FROG uses only A-rounds.

As a result,

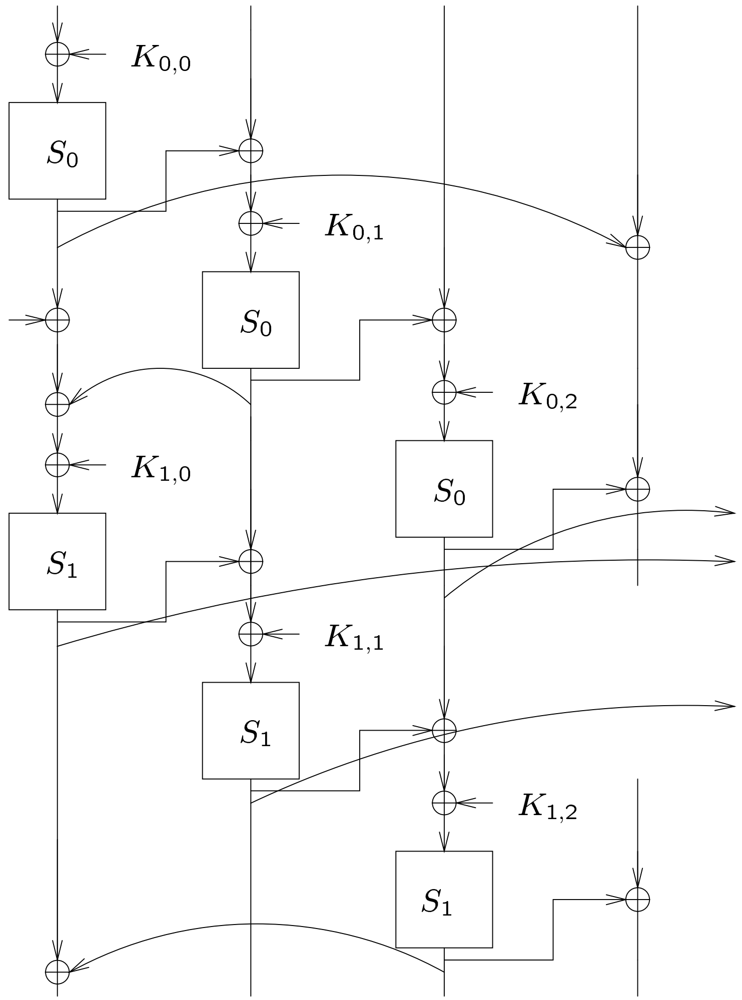
DIFFUSION IS MUCH WORSE IN THE REVERSE DIRECTION THAN IN THE FORWARD DIRECTION.

(Full avalanche requires 48–64 rounds when decrypting but only 16–24 rounds when encrypting.)

Avalanche in forward direction



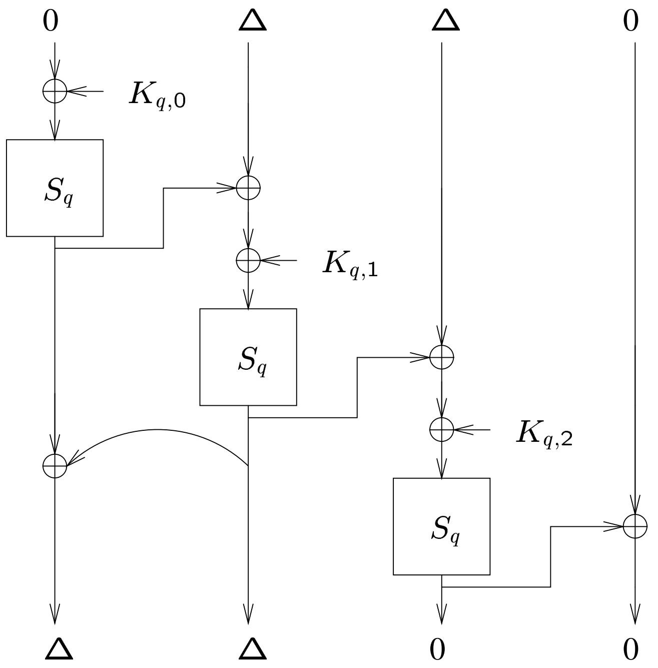
Avalanche in reverse direction



The differential attack: main ideas

- Exploit the key-dependence in the diffusion structure, by finding weak keys where diffusion is especially poor.
- Exploit the asymmetry, by using chosen ciphertexts.
- Use an iterative characteristic of prob. 2^{-7} for one cycle (16 rounds) (see next slide).
- Cover 5 cycles (80 rounds) with characteristic, use a 3-C (48-R) attack.
- Use structures, other tricks for incremental improvements (see paper).

The iterative characteristic



The differential attack: results

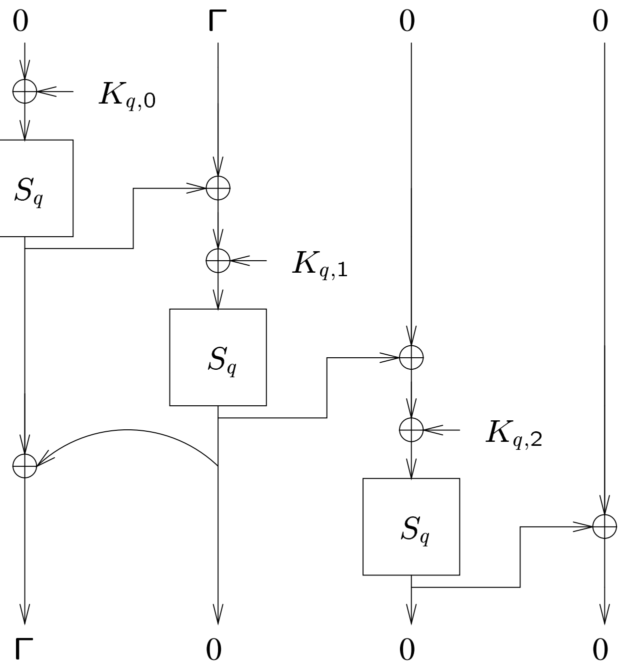
Our best differential attack:

- Needs 2^{36} chosen ciphertexts, and works on $2^{-29.3}$ of the keyspace.
- With enough cryptanalytic targets, the attacker can expect to recover (part of) his first key after $2^{56.7}$ texts.
- Results of preliminary investigation; more looking might find better attacks.

Linear attack

- There is a dual attack using linear approximations; very similar ideas.
- Again, there is a one-cycle (16-round) iterative approximation (see next slide).
- Best attack uses 2^{56} known texts and works for $2^{-31.8}$ of the keyspace.
- Can be converted to ciphertext-only attack, with 2^{64} ciphertexts.
- Results of preliminary investigation; more looking might find better attacks.

The iterative approximation



Conclusions

- A lesson? Key-dependent diffusion structures are tricky, since each setting of the internal wiring gives a new cipher to analyze.
- A lesson? Asymmetrical round functions require care.