Differential Cryptanalysis of KHF

David Wagner
University of California, Berkeley
daw@cs.berkeley.edu

Organization

- The algorithm.
- A differential characteristic.
- Forging the MAC.
- Lessons.

KHF

- KHF is a fast MAC.
- Message is split into 32-bit blocks $M_{1\dots n}$.
- Two 128-bit chaining buffers $X_{1\dots 4}, Y_{1\dots 4}$.
- A 512-bit redundancy buffer $B_{1\dots 16}$.
- Round function f_i is a strong Boolean function, extended to 32-bit blocks by bitwise evaluation.
  - The underlying Boolean function has all sorts of nice theoretically provable security properties.
- Run for i rounds, using each message block exactly once.

Round function:

1. $T = f_i(Y_1, Y_2, Y_3, Y_4, M_i)$.
2. Modify X using T.
3. Xor M_i into B_{a_i}, $a_i = g(T)$.
4. Modify Y using T and B_i.

Differential analysis of f_i

f_i operates on each bit position independently; so use a one-bit input difference.

Can easily insert any chosen difference into M_i.

Therefore we get high-probability characteristics for f_i: e.g. $(0, 0, 0, 0, 2^j) \mapsto 0$ with probability $\approx 1/2$.

Analyzing the round

Flip a bit in M_i. We want $\Delta T = 0$.

To extend this to a full characteristic, we need the invariant $\Delta X = \Delta Y = \Delta B = 0$.

Problem: $\Delta B_{a_i} = \Delta M_i \neq 0$, so the redundancy buffer will change. This will eventually affect some later round, causing the characteristic to get derailed.

(Specifically, it affects the first round $j \geq i$ such that $j \equiv a_i \bmod 16$).

A full characteristic

Solution: Cancel out the difference in B before it gets used by flipping a bit in M_{i+1} too.

For this, we need $a_i = a_{i+1}$, so that

$$\Delta B_{a_{i+1}} = \Delta M_{i+1} \oplus \Delta M_i = 0.$$

Also need $a_i \neq i$.

This causes an internal collision, which is recognizable by the difference 0 at the MAC output.

Can get a full n-round characteristic with probability $\approx 1/36$**.**

Forgery

Problem: To predict KHF(M) for arbitrary M.

Solution: Generate internal collisions.

1. Let $M = X \mid\mid Y$. Pick Z.
2. Find X, X' so that KHF($X \mid\mid Z$) = KHF($X' \mid\mid Z$), by using the differential characteristic.
3. Find $d =$ KHF($X' \mid\mid Y$).
4. Guess that KHF($X \mid\mid Y$) $= d$ too.

Can forge the MAC with 37 chosen message queries.

What went wrong?

- Each message word used only once.
- Position where diffusion enters B was data-dependent, so it was easy to control.
- Ad-hoc internal structure.
- Spectacular failure of the f_i construction.

Lessons

Building strong f functions requires more than just knowing how to construct strong Boolean functions.

Watch what the theorems actually prove very carefully. . .