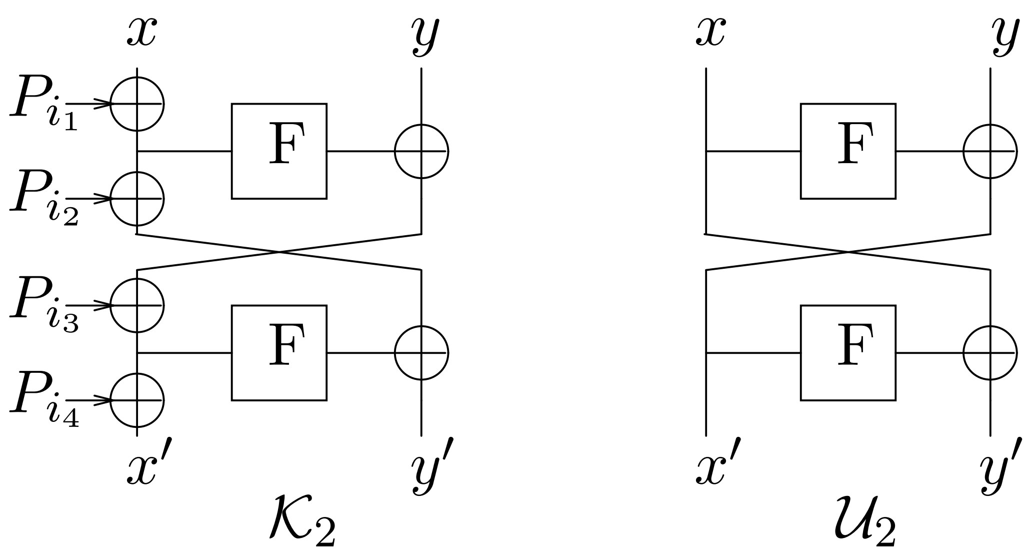
A New Class Of Weak Keys for Blowfish

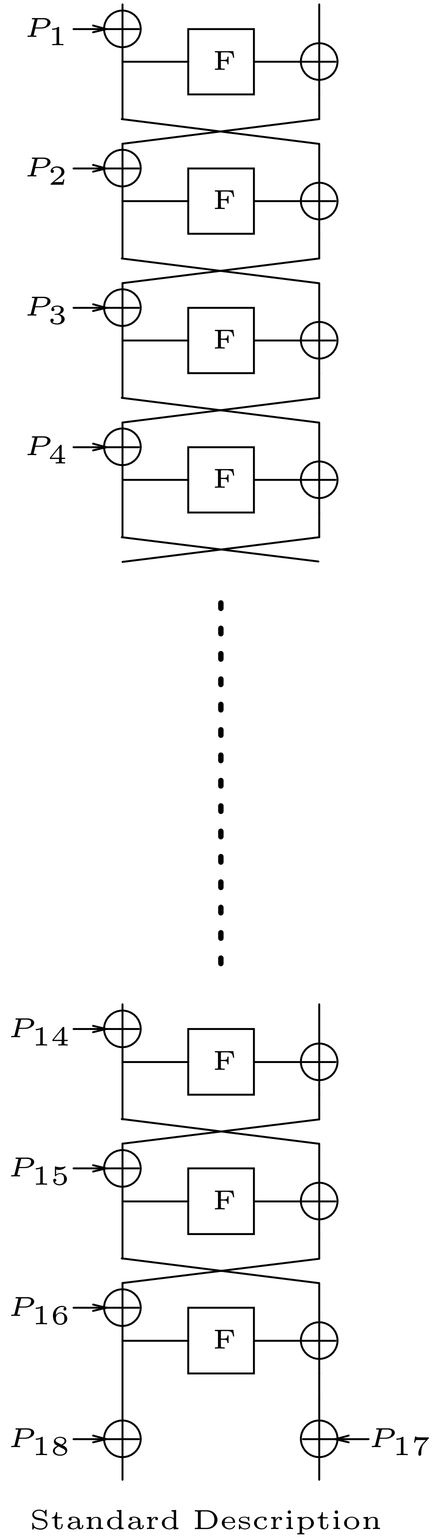
Orhun KARA and Cevat MANAP
TÜBİTAK - UEKAE
(National Research Institute of Electronics and Cryptology)

Redefining Blowfish

Key XORs in Blowfish can be moved around to generate two building blocks $\mathcal{K}_2$ and $\mathcal{U}_2$.



$\mathcal{U}_2$ is an involution and has 2^{32} fixed points of the form $(x, F(x) \oplus x)$.
$\mathcal{K}_2^{-1}$ is same as $\mathcal{K}_2$ with a different ordering of the subkeys.



P_1
P_2
P_3
P_4
P_{13}
P_{14}
P_{15}
P_{16}
P_{17}
P_{18}
P_5
0
F
$\mathcal{K}_2$
$\mathcal{U}_2$
Standard Description
Type II
Type III

Weak Keys

Type III definition can be summarised as:

$$\text{plaintext} \rightarrow initW \rightarrow F \rightarrow S$$

$$\rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow$$

$$S \rightarrow F \rightarrow finalW \rightarrow \text{ciphertext}$$

Weak Keys

Type III definition can be summarised as:

$$\text{plaintext} \rightarrow initW \rightarrow F \rightarrow S$$

$$\rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow S \stackrel{X_0}{\rightarrow} \mathcal{U}_2 \stackrel{X_0}{\rightarrow} S \rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow$$

$$S \rightarrow F \rightarrow finalW \rightarrow \text{ciphertext}$$

X_0 is a fixed point of $\mathcal{U}_2$.

Weak Keys

Type III definition can be summarised as:

$$\text{plaintext} \rightarrow initW \rightarrow F \rightarrow S$$

$$\rightarrow \mathcal{K}_2 \rightarrow S \rightarrow \mathcal{U}_2 \rightarrow S \xrightarrow{X_2} \mathcal{K}_2 \xrightarrow{X_1} S \xrightarrow{X_0} \mathcal{U}_2 \xrightarrow{X_0} S \xrightarrow{X_1} \mathcal{K}_2 \xrightarrow{X_2} S \rightarrow \mathcal{U}_2 \rightarrow S \rightarrow \mathcal{K}_2 \rightarrow$$

$$S \rightarrow F \rightarrow finalW \rightarrow \text{ciphertext}$$

X_0 is a fixed point of $\mathcal{U}_2$.

Conditions on subkeys used in $\mathcal{K}_2$.

Weak Keys

Type III definition can be summarised as:

$$\text{plaintext} \rightarrow initW \stackrel{X_8}{\rightarrow} F \stackrel{X_7}{\rightarrow} S$$

$$\stackrel{X_6}{\rightarrow} \mathcal{K}_2 \stackrel{X_5}{\rightarrow} S \stackrel{X_4}{\rightarrow} \mathcal{U}_2 \stackrel{X_3}{\rightarrow} S \stackrel{X_2}{\rightarrow} \mathcal{K}_2 \stackrel{X_1}{\rightarrow} S \stackrel{X_0}{\rightarrow} \mathcal{U}_2 \stackrel{X_0}{\rightarrow} S \stackrel{X_1}{\rightarrow} \mathcal{K}_2 \stackrel{X_2}{\rightarrow} S \stackrel{X_3}{\rightarrow} \mathcal{U}_2 \stackrel{X_4}{\rightarrow} S \stackrel{X_5}{\rightarrow} \mathcal{K}_2 \stackrel{X_6}{\rightarrow}$$

$$S \stackrel{X_7}{\rightarrow} F \stackrel{X_8}{\rightarrow} finalW \rightarrow \text{ciphertext}$$

X_0 is a fixed point of $\mathcal{U}_2$.

Conditions on subkeys used in $\mathcal{K}_2$.

Definition: A key is called weak if the encryption function has 2^{32} fixed points in the middle step.

Detecting Weak Keys

- Fixed points occur with probability $\frac{2^{32}}{2^{64}} = 2^{-32}$.
- For a fixed point

$$\text{plaintext} \oplus initW = X_8 = \text{ciphertext} \oplus finalW$$

$$initW \oplus finalW = \text{plaintext} \oplus \text{ciphertext}$$

- For 2^{34} known plaintexts, calculate plaintext $\oplus$ ciphertext.
  - on average 4 fixed points occur, giving $initW \oplus finalW$.
  - random 64 bit values for non-fixed points.

Detect weak keys by looking at "plaintext$\oplus$ciphertext."

First Attack

- Detecting a weak key gives $P_1 \oplus P_{18}$ and $P_2 \oplus P_{17}$ for free.
- Conditions on subkeys of $\mathcal{K}_2$ dictate $P_3 = P_{16}$, $P_4 = P_{15}$, $P_5 = P_{14}$, $P_6 = P_{13}$, $P_7 = P_{12}$,$P_8 = P_{11}$ and $P_9 = P_{10}$. (Hence, expected number of weak keys : $2^{k-7*32} = 2^{k-224}$)
- 9 equations in 18 variables.
- Guess 9 variables, determine remaining 9 variables. $2^{9*32} = 2^{288}$ guesses total.
- Check if a guess is valid by 9 encryptions. $9 * 2^{288}$ encryptions $\approx 2^{282.1}$ exhaustive search steps. (1 Exhaustive search step is 512+9 encryptions.)

Second Attack

- Exhaustively search and store all weak keys, sorting them w.r.t. $(P_1 \oplus P_{18}, P_2 \oplus P_{17})$.
- Pre-computation costs $\approx 2^{k-7}$ exhaustive search steps.
- Weak keys occupy 2^{k-224} spaces in memory.
- Online phase costs $2^{\frac{k-224}{64}}$ exhaustive search steps.

Attacks On Weak Keys

For some attack working on weak keys,

- W workload of identification, w total number of weak keys.
- Given a set of $\frac{2^k}{w}$ keys, expect one weak key on average,
- Run identification on the set, with complexity $W\frac{2^k}{w}$.
- Successful attack requires $W\frac{2^k}{w} < 2^k$,i.e. $W < w$.

Thanks.