Improved Related-key Attacks on DESX and DESX+

Raphael C.-W. Phan

Swinburne University of Technology (Sarawak Campus), Malaysia

Adi Shamir

Weizmann Institute of Science, Israel

Asiacrypt 2004 rump session

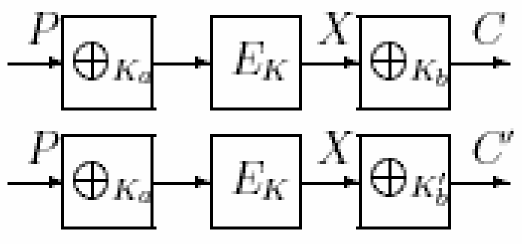
Outline: DESX Variants

- DESX $$C = K_b \oplus E_K(P \oplus K_a)$$

- DESX+ $$C = K_b + E_K(P + K_a)$$

Attacking DESX

- Get C of P under K_b, C' of P under $K_b' = (K_b \pm D) \bmod 2^n$
- $C \oplus C' = K_b \oplus (K_b \pm D) \bmod 2^n$



- Try all K_b : 1 XOR, 1 +

  $\Rightarrow$ remaining values significantly reduced
- Repeat 3 times

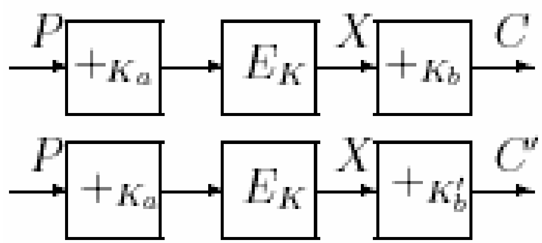
  $\Rightarrow$ 3 pairs (6) of *RK-KP*s

Attacking DESX

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX	$2^{32} CP$	-	2^{88}	D'91
DESX	$2\ KP$	-	2^{120}	D'91
DESX	$2^{32} KP$	-	2^{113}	KR'96
DESX	$2^{6}\ RK\text{-}KP$	-	2^{120}	KSW'97
DESX	$2^{32.5} KP$	$2^{32.5}$	$2^{87.5}$	BW'00
DESX	$2^{3.5}\ RK\text{-}KP$	-	2^{56}	This paper

DESX+: Attack 1

- Get C of P under K_b, C' of P under $K_b' = K_b \oplus D$



- Closer analysis of carries into C, C' bits

$\Rightarrow \uparrow$ texts, $\downarrow$ encs, $\times$ memory

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX+	2 RK-KP	-	2^{120}	P'04
DESX+	2 RK-KP	2^{56}	2^{56}	P'04
DESX+	2^7 RK-KP	-	2^{56}	This paper

DESX+: Attack 2

- Intuition:
  - $K_b' = (K_b \pm D) \bmod 2^n \Rightarrow C' = (C \pm D) \bmod 2^n$
  - $K_b' = (K_b \oplus D) = (K_b \oplus \varepsilon[i]) \Rightarrow K_b[i] = \overline{K_b[i]}$
    - $C' = C + 2^i$ if $K_b[i] = 0 \rightarrow 1$ (+)

      $= C - 2^i$ if $K_b[i] = 1 \rightarrow 0$ (–)
- Get C of P under K_b, C' of P under $K_b' = K_b \oplus D = \overline{K_b}$

  $\Rightarrow C + D \bmod 2^n$ where

$$D = \sum_{i=0}^{n-1} \pm 2^i = \pm\{1, 3, 5, \ldots, 2^n - 1\}$$

Example

- $D_{mod} = 15$,

  $LSB_3(K_b) = 000$

- $D_{mod} = 3$,

  $LSB_3(K_b) = 110$

± 8	± 4	± 2	± 1	$D = \sum_{i=0}^{n-1} \pm 2^i$	$D_{mod} = D \mod 2^4$
-	-	-	-	-15	1
-	-	-	+	-13	3
-	-	+	-	-11	5
-	-	+	+	-9	7
-	+	-	-	-7	9
-	+	-	+	-5	11
-	+	+	-	-3	13
-	+	+	+	-1	15
+	-	-	-	+1	1
+	-	-	+	+3	3
+	-	+	-	+5	5
+	-	+	+	+7	7
+	+	-	-	+9	9
+	+	-	+	+11	11
+	+	+	-	+13	13
+	+	+	+	+15	15

DESX+: Attack 2

- $\Rightarrow$ 1 pair (2) *RK-KP*s: 1 complementation

  $\Rightarrow$ DESX+ extremely weak against RK attack

Block Cipher	Texts	Memory	DES Encryptions	Source
DESX+	2 $RK\text{-}KP$	-	2^{120}	P'04
DESX+	2 $RK\text{-}KP$	2^{56}	2^{56}	P'04
DESX+	2^7 $RK\text{-}KP$	-	2^{56}	This paper
DESX+	2 $RK\text{-}KP$	-	2^{56}	This paper