Lineare Kryptoanalyse

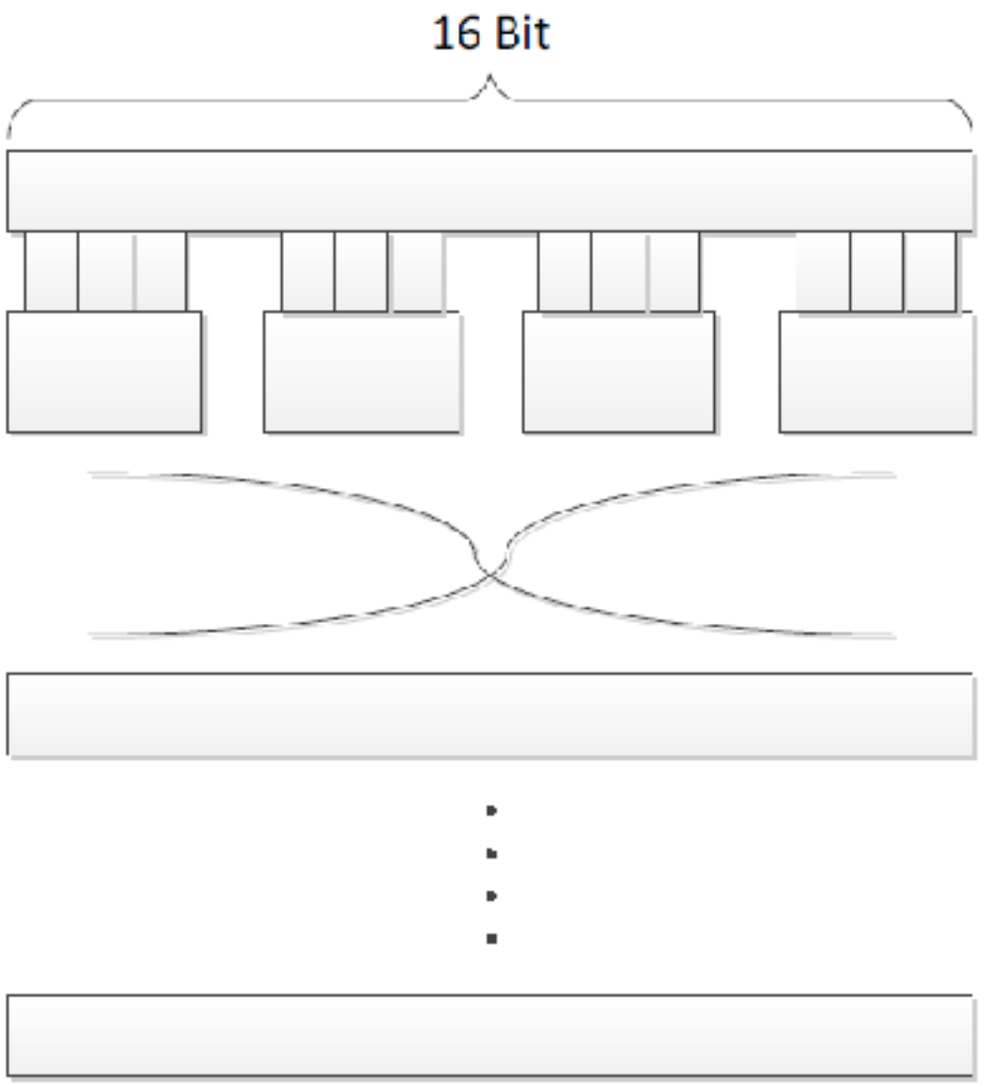
Kryptologie Projekt WS 2016/17

Simeon Ackermann & Tim Menapace

Aufgabenstellung

Implementieren Sie die Verschlüsselung in vier Runden, die in der Vorlesung als Beispiel zur Linearen Kryptoanalyse vorgestellt wurde. Die Rundenschlüssel seien in Form einer Tabelle fest vorgegeben. Erzeugen Sie 2_{16} gut gestreute Paare aus 16-Bit-Blöcken von Klartext und zugehörigem Geheimtext und führen Sie vor, wie Charlie daraus den Teilschlüssel ermittelt.

Verschlüsselung in 4 Runden



bitweises EXOR mit S_0

Substitution

Transposition

1. Runde

bitweises EXOR mit S_1

bitweises EXOR mit S_4

Initialisierung

- S-Box Tabelle für Substitution:

K	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
G	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

- Transpositions Tabelle:

K	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
G	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

- 16 Bit Schlüssel S_1 - S_5

- 2^{16} Known Plaintext Paare

Approximationstabelle

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Matsuis Algorithmus

Gleichungen mit Bias 1/4

$$X_1 \oplus X_3 \oplus X_4 \oplus Y_2 = 0$$

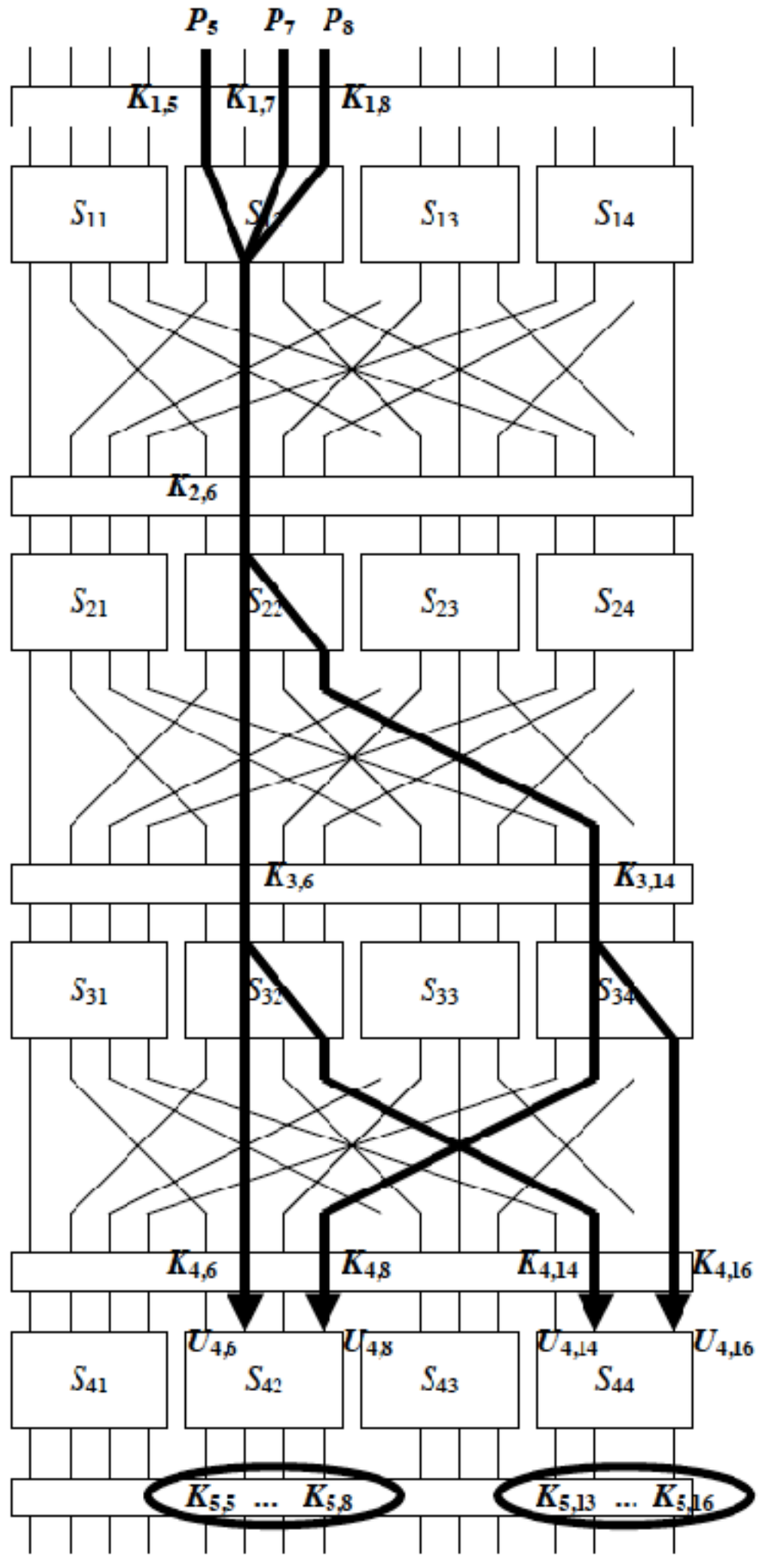
$$X_2 \oplus Y_2 \oplus Y_4 = 0$$

Piling-Up Lemma

$$P(X_1 \oplus X_2 = 0) = 2\varepsilon_1\varepsilon_2$$

Testen der Gleichung

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0$$



Resultat

Index	Teilschlüssel $K_{5,5}…K_{5,8}$; $K_{5,13}… K_{5,16}$	Schlüssel	Abweichung
000	0	0 0 0 0 0 0 0 0	0,0031
…		…	…
77	4D	0 1 0 0 1 1 0 1	0,0078
78	4E	0 1 0 0 1 1 1 0	0,0170
79	4F	0 1 0 0 1 1 1 1	0,0025
80	50	0 1 0 1 0 0 0 0	0,0211
81	**51**	**0 1 0 1 0 0 0 1**	**0,0336**
…		…	…
255	FF	1 1 1 1 1 1 1 1	0,0054