

Kryptoanalýza šifrier v mobilných siet'ach

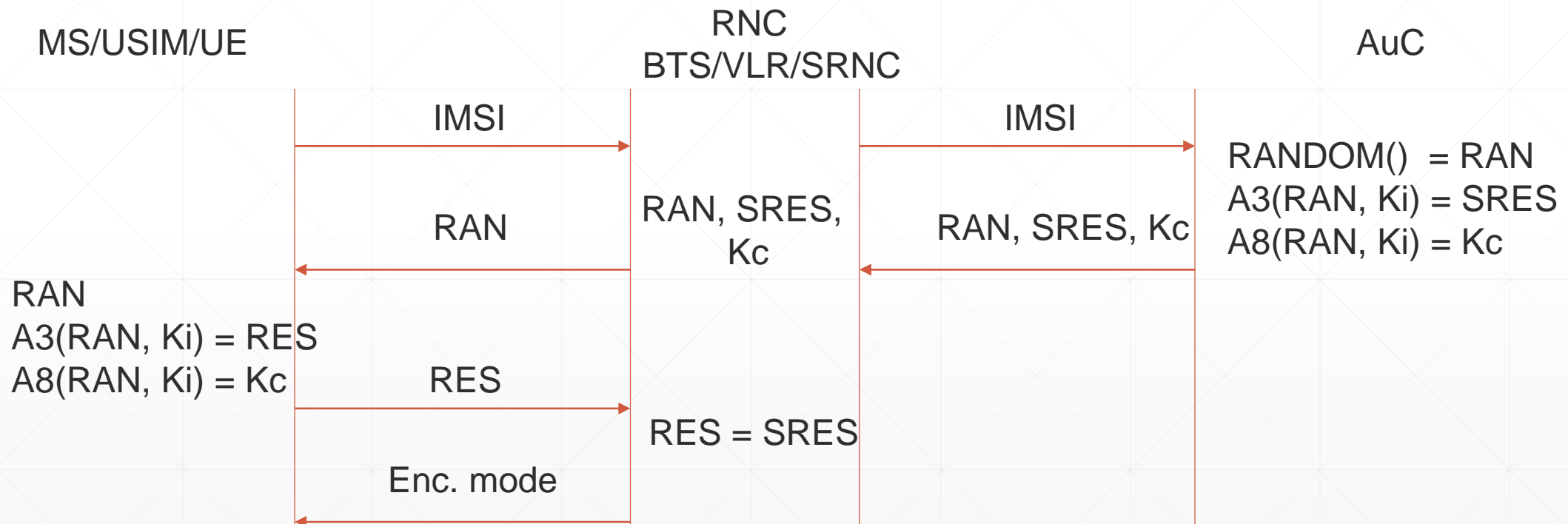
Ján Kotrady

Obsah

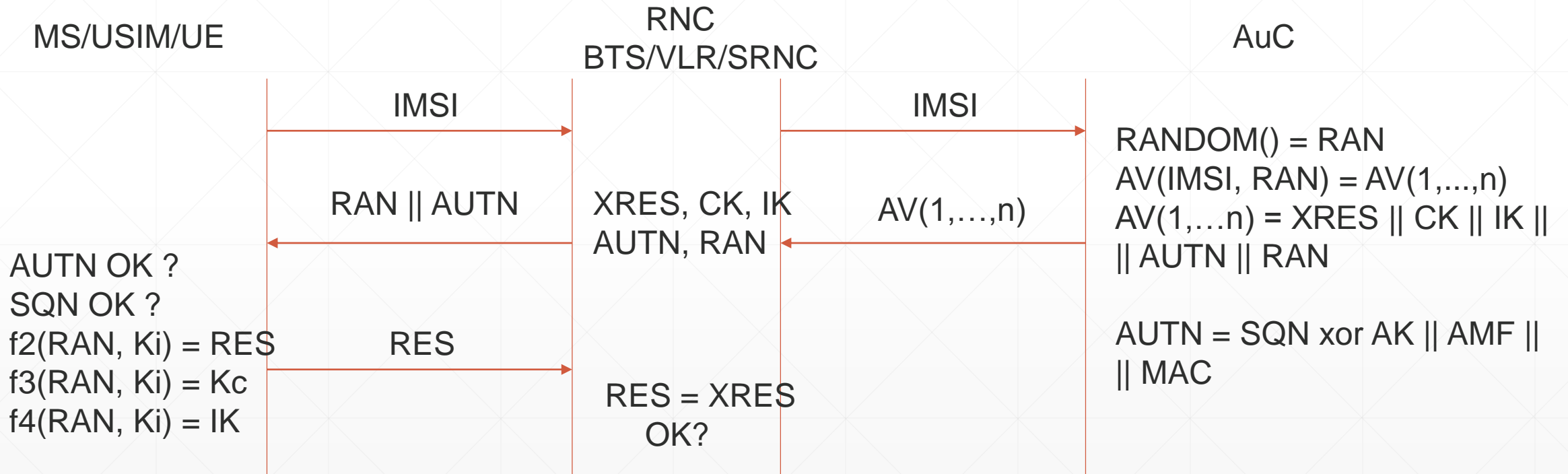
- Diferenčná kryptoanalýza
 - Pár algoritmov
 - KASUMI Related-Key Sandwich (Boomerang) Attack*
 - ...
-

Pripomenutie GSM a 3G protokolov

GSM autentifikácia



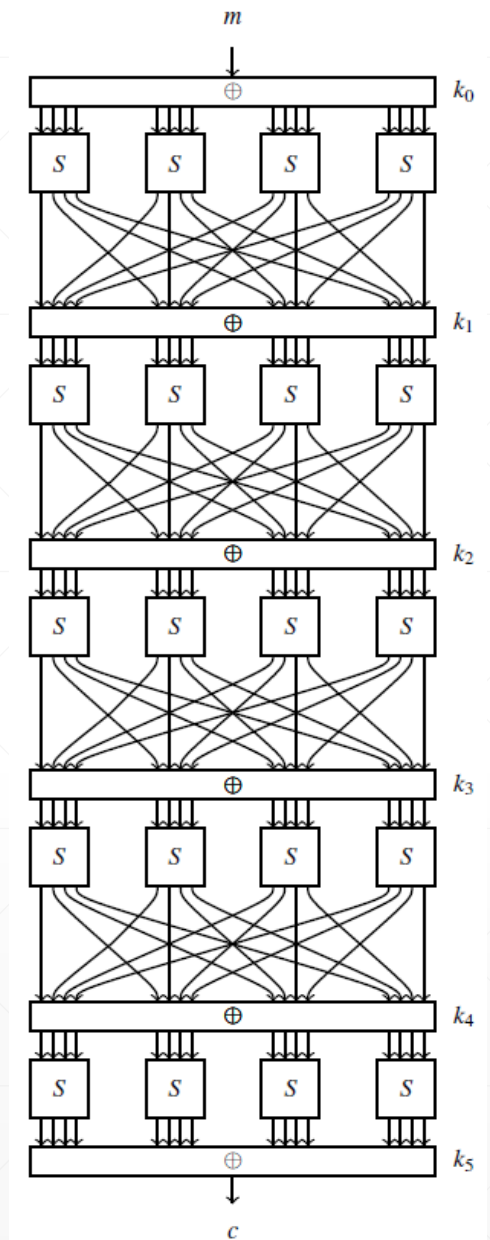
3G a LTE



Diferenčná kryptoanalýza „myšlienka“

Blokové šifry

- Najúčinnnejšia kryptoanalýza (\neg DES)
- Základ: „rundy“, Feistelovú sieť
- **CPA – Chosen plain-text attack**
- Ciele:
 - „Zbaviť sa kľúča“
 - Zistiť kľúč
 - Útok hrubou silou jednoduchší



XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1)$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1 = m_1 \oplus m_2 \oplus (k_1 \oplus k_1)$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$
 $= m_1 \oplus m_2 \oplus (k_1 \oplus k_1) = m_1 \oplus m_2 \oplus (0)$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

XOR – základný princíp

- \oplus
- XOR šifra: k_1 kľúč, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}(e_{k_1}(m)) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$
 $= m_1 \oplus m_2 \oplus (k_1 \oplus k_1) = m_1 \oplus m_2 \oplus (0) = m_1 \oplus m_2$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0

**Práve sme pochopili
diferenčnú kryptoanalýzu**

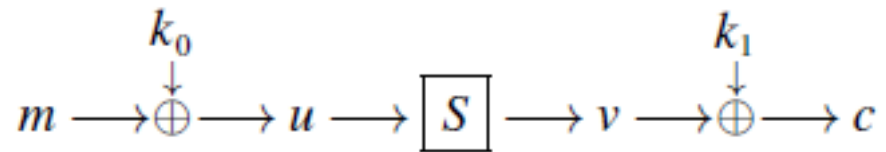
**Práve sme pochopili
diferenčnú kryptoanalýzu
nasleduje jej aplikácia 😞**

CipherOne

CipherOne

$$c = S[m \oplus k_0] \oplus k_1$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



$\text{CIPHERONE}(m_0, k_0 k_1)$	$\text{CIPHERONE}(m_1, k_0 k_1)$
$u_0 = m_0 \oplus k_0$	$u_1 = m_1 \oplus k_0$
$v_0 = S[u_0]$	$v_1 = S[u_1]$
$c_0 = v_0 \oplus k_1$	$c_1 = v_1 \oplus k_1$

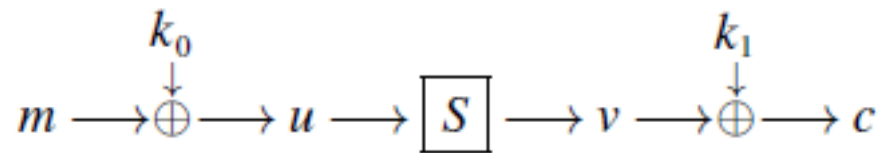
Aplikácia v praxi

- $m_0 \oplus m_1 = (m_0 \oplus k_0) \oplus (m_1 \oplus k_0) = u_0 \oplus u_1$

CipherOne

$$c = S[m \oplus k_0] \oplus k_1$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



$\text{CIPHERONE}(m_0, k_0 k_1)$	$\text{CIPHERONE}(m_1, k_0 k_1)$
$u_0 = m_0 \oplus k_0$	$u_1 = m_1 \oplus k_0$
$v_0 = S[u_0]$	$v_1 = S[u_1]$
$c_0 = v_0 \oplus k_1$	$c_1 = v_1 \oplus k_1$

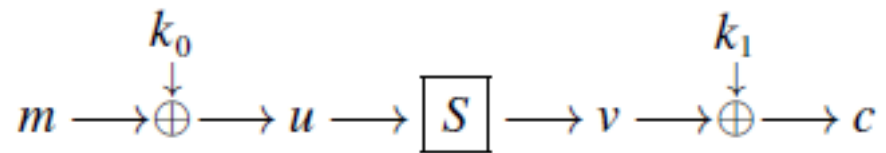
Aplikácia v praxi

- $m_0 \oplus m_1 = (m_0 \oplus k_0) \oplus (m_1 \oplus k_0) = u_0 \oplus u_1$
- $(m_0, c_0), (m_1, c_1)$ - pár

CipherOne

$$c = S[m \oplus k_0] \oplus k_1$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



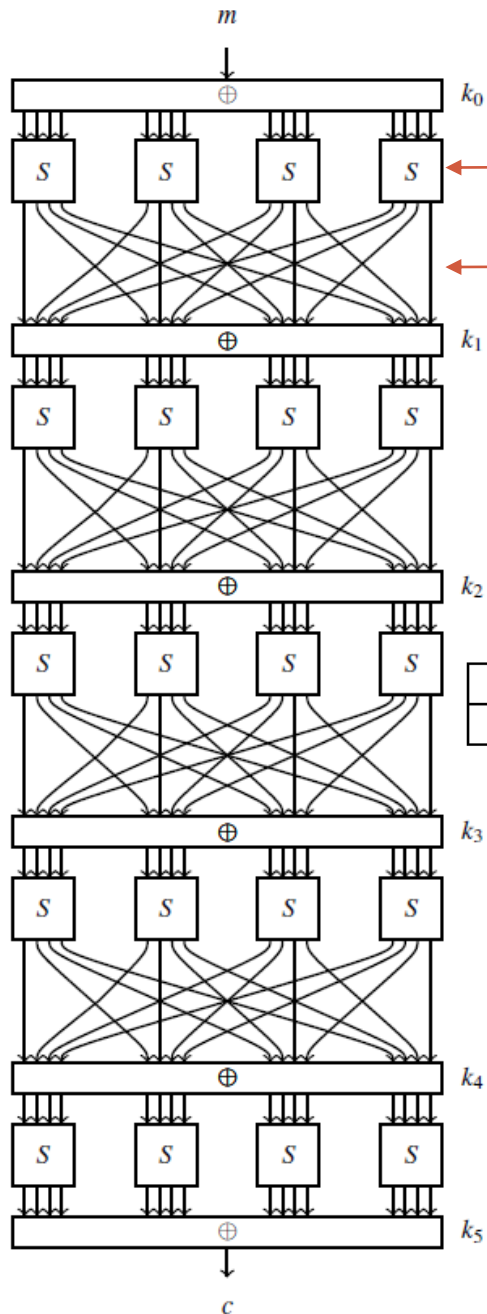
CIPHERONE($m_0, k_0 k_1$)	CIPHERONE($m_1, k_0 k_1$)
$u_0 = m_0 \oplus k_0$	$u_1 = m_1 \oplus k_0$
$v_0 = S[u_0]$	$v_1 = S[u_1]$
$c_0 = v_0 \oplus k_1$	$c_1 = v_1 \oplus k_1$

Aplikácia v praxi

- $m_0 \oplus m_1 = (m_0 \oplus k_0) \oplus (m_1 \oplus k_0) = u_0 \oplus u_1$
- $(m_0, c_0), (m_1, c_1)$ - pár
- $u_0 \oplus u_1 = S^{-1}[t \oplus c_0] \oplus S^{-1}[t \oplus c_1], \forall t$

CipherFour

CipherFour



S-box

P-box

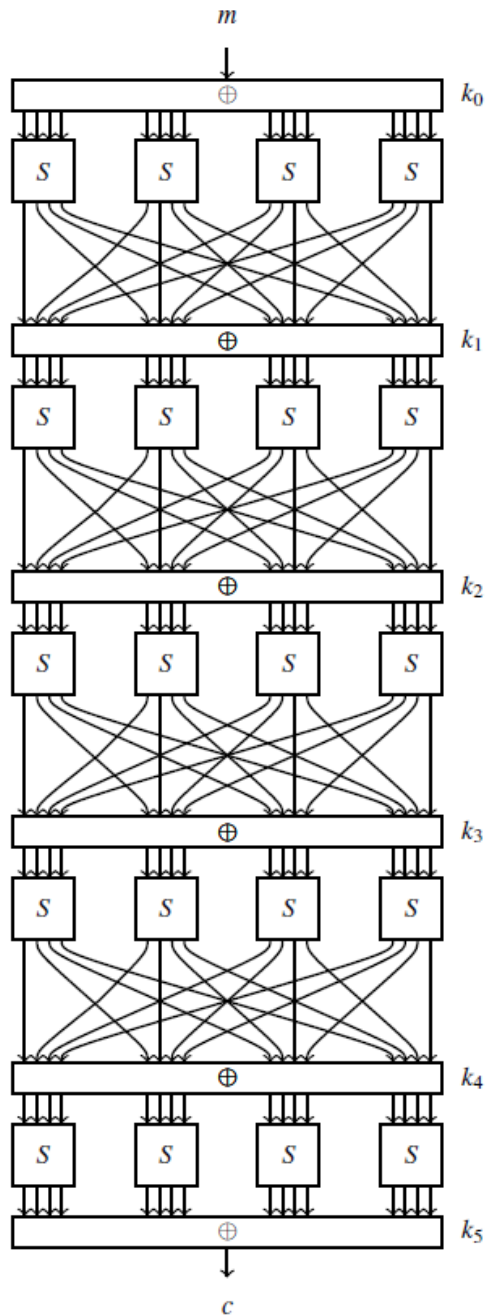
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b

i	0	1	2	3	4	5	6	7
$P[i]$	0	4	8	12	1	5	9	13
i	8	9	10	11	12	13	14	15
$P[i]$	2	6	10	14	3	7	11	15

Spájanie charakteristík

- S-box – nelineárne
- P-box – permutácia

CipherFour



Δ_{out}

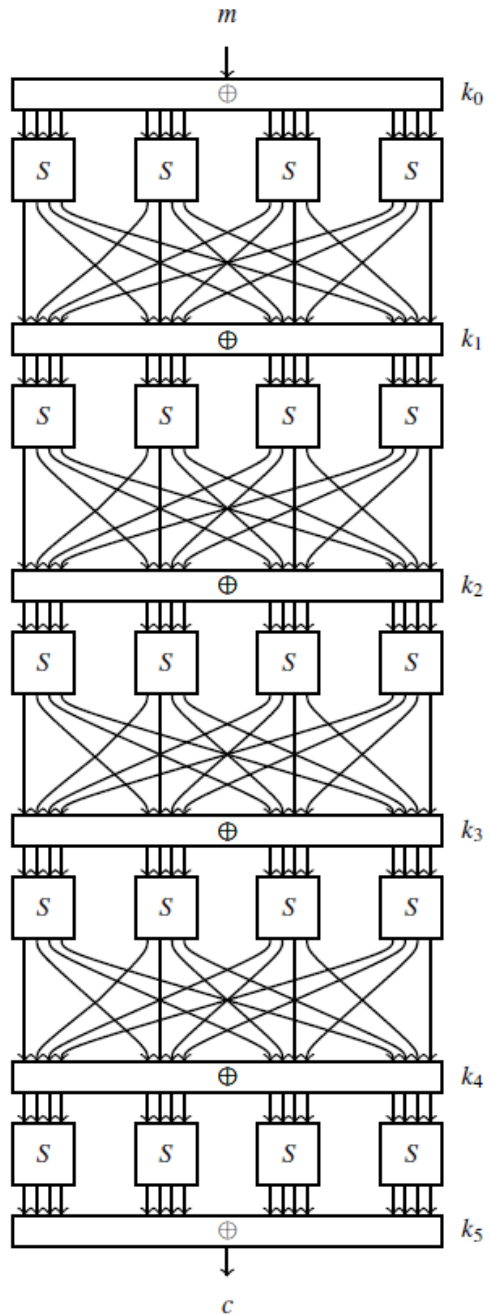
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

Spájanie charakteristík

- $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \xrightarrow{S} (\beta_1, \beta_2, \beta_3, \beta_4)$
- $(\beta_1, \beta_2, \beta_3, \beta_4) \xrightarrow{P} (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$
- $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \xrightarrow{R} (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$

CipherFour



Δ_{out}

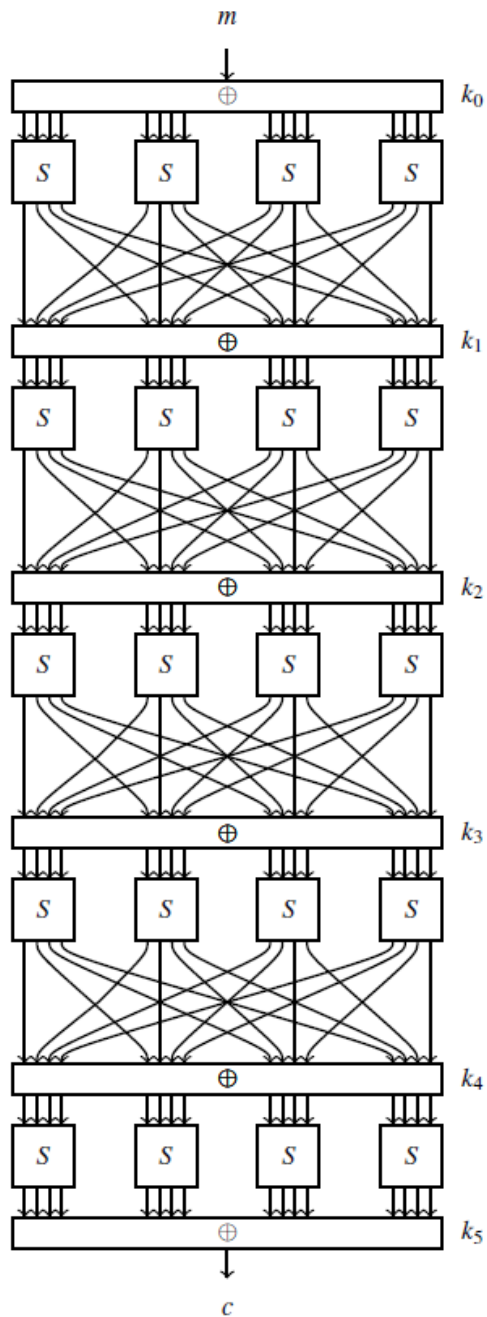
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

Spájanie charakteristík

- $(0,0,0,f) \xrightarrow{S} (0,0,0,d)$
- $(0,0,0,d) \xrightarrow{P} (1,1,0,1)$
- $P_1 = \frac{10}{16}$

CipherFour



Δ_{out}

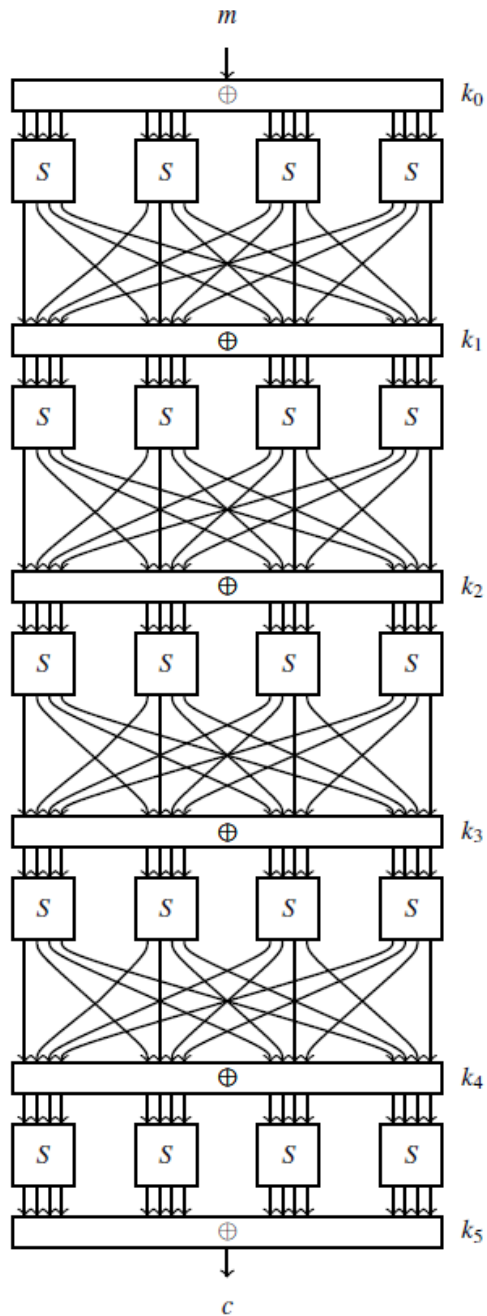
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

Spájanie charakteristík

- $(0,0,0,f) \xrightarrow{S} (0,0,0,d)$
- $(0,0,0,d) \xrightarrow{P} (1,1,0,1)$
- $P_1 = \frac{10}{16}$
- $(1,1,0,1) \xrightarrow{S} (2,2,0,2)$
- $(2,2,0,2) \xrightarrow{P} (0,0,d,0)$
- $P_2 = \left(\frac{6}{16}\right)^3$
- $P_1 \& P_2 = \frac{10}{16} \left(\frac{6}{16}\right)^3 = \frac{135}{4096}$

CipherFour



Δ_{out}

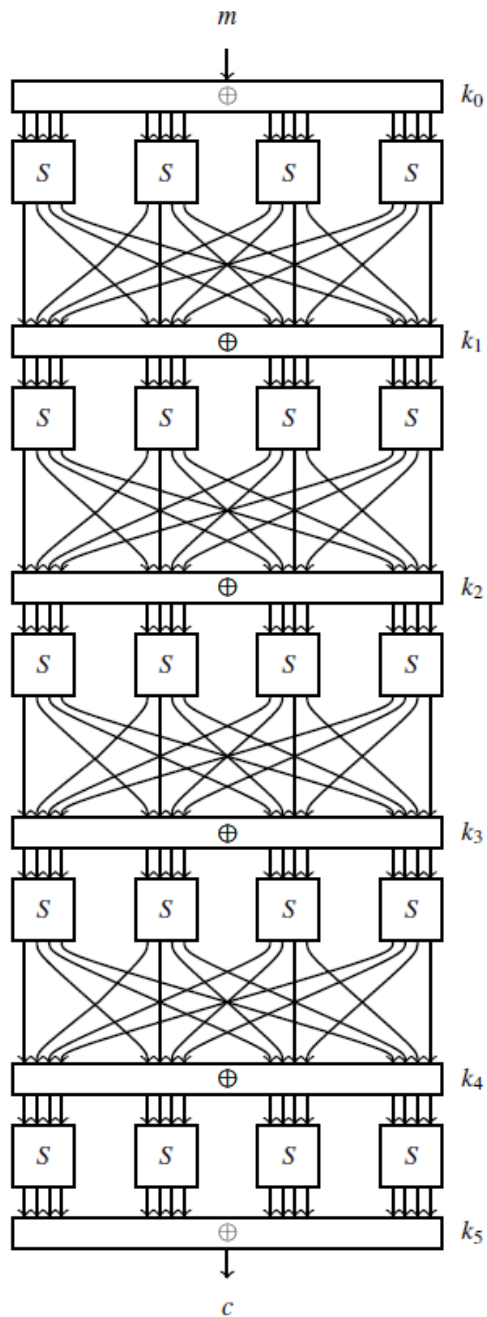
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

Spájanie charakteristík

- $(0,0,2,0) \xrightarrow{S} (0,0,2,0)$
- $(0,0,2,0) \xrightarrow{P} (0,0,2,0)$
- $P_1 = \frac{6}{16}$
- $(0,0,2,0) \xrightarrow{S} (0,0,2,0)$
- $(0,0,2,0) \xrightarrow{P} (0,0,2,0)$
- $P_2 = \frac{6}{16}$
- $P_1 \& P_2 = \left(\frac{6}{16}\right)^2$

CipherFour



Δ_{out}

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

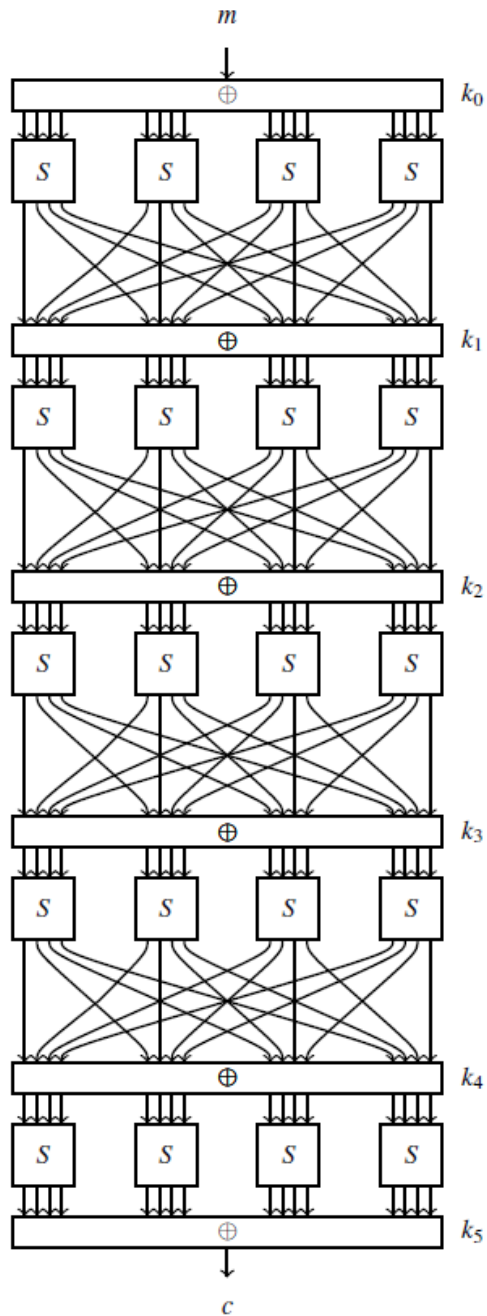
Spájanie charakteristík

- $(0,0,2,0) \xrightarrow{R} (0,0,2,0)$
- $(0,0,2,0) \xrightarrow{R} (0,0,2,0)$
- $(0,0,2,0) \xrightarrow{R} (0,0,2,0)$
- $(0,0,2,0) \xrightarrow{R} (0,0,2,0)$
- $P = \left(\frac{6}{16}\right)^4 = \frac{135}{4096}$

Zavedenie diferencií

- $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \xrightarrow{S} (\beta_1, \beta_2, \beta_3, \beta_4)$
 - $(\beta_1, \beta_2, \beta_3, \beta_4) \xrightarrow{P} (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$
 - $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \xrightarrow{R} (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$
 - $(0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0)$
 - $(0, 0, 2, 0) \xrightarrow{R} ? \xrightarrow{R} ? \xrightarrow{R} ? \xrightarrow{R} (0, 0, 2, 0)$
 - $(0, 0, 2, 0) \xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 0, 1) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0)$
 - $(0, 0, 2, 0) \xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0)$
 - $(0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0)$
-

CipherFour



Δ_{out}

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Δ_{in}

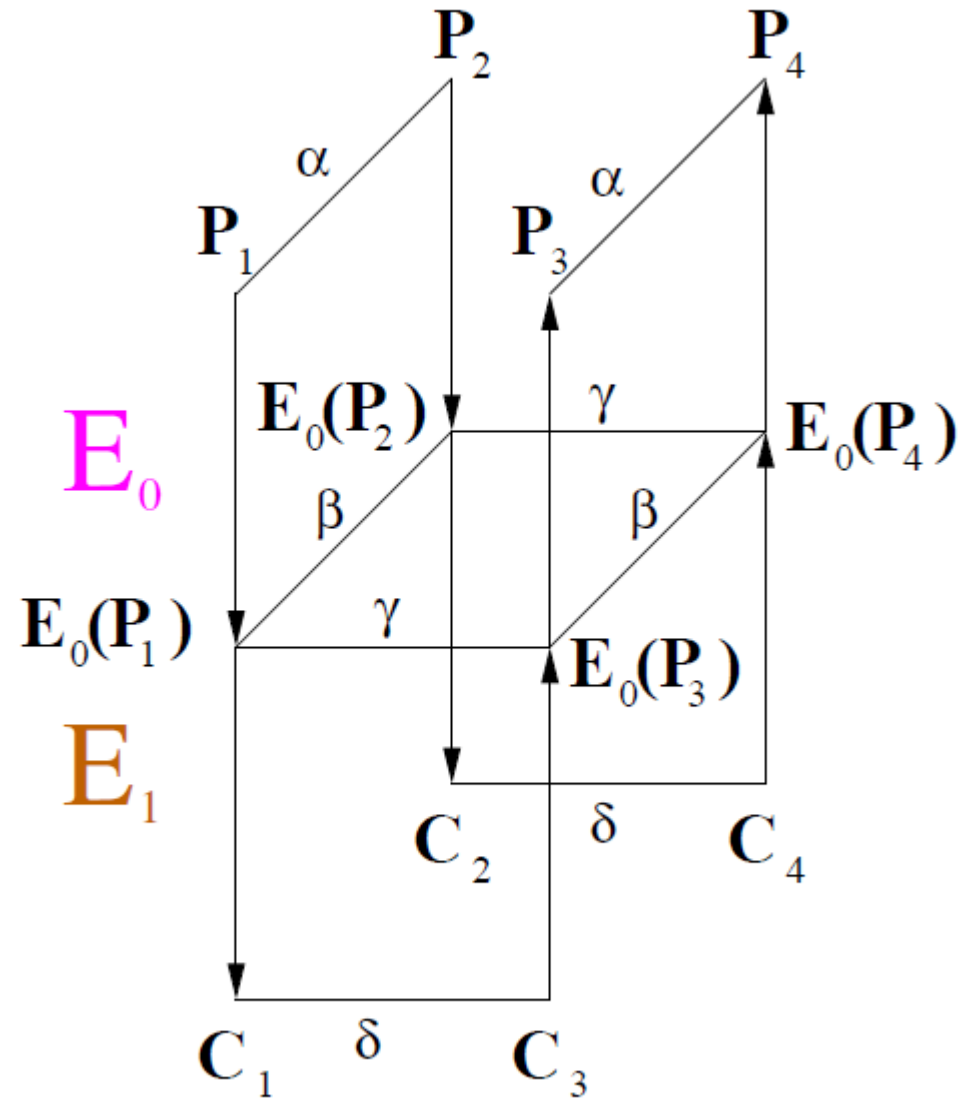
Filtrovanie

- $(0,0,2,0) \xrightarrow{S} (0,0,h,0)$
- $h \in \{1,2,9,a\}$
- $\frac{5310}{65536} \approx 0.08$ - diferencia
- $\frac{7387}{65536} \approx 0.11$ - filtrovanie
- $t \times 0.08$ - diferencia
- $t \times 0.11$ - filter
- $t \times (0.03)$ - chyba

Útok na šifru KASUMI POPIŠ ÚTOKU

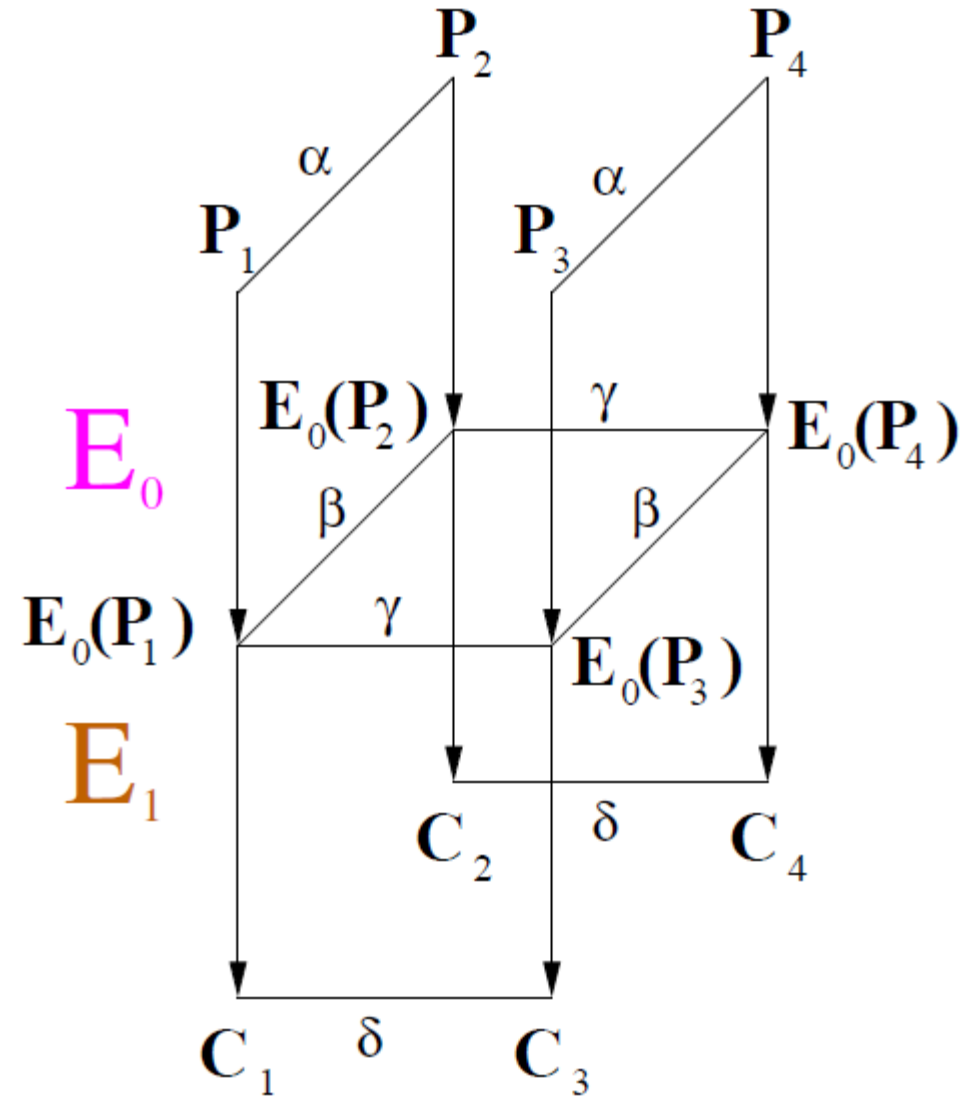
Boomerang Attack

- p^2q^2
- Dobré krátke diferencie
- Zlé dlhé diferencie



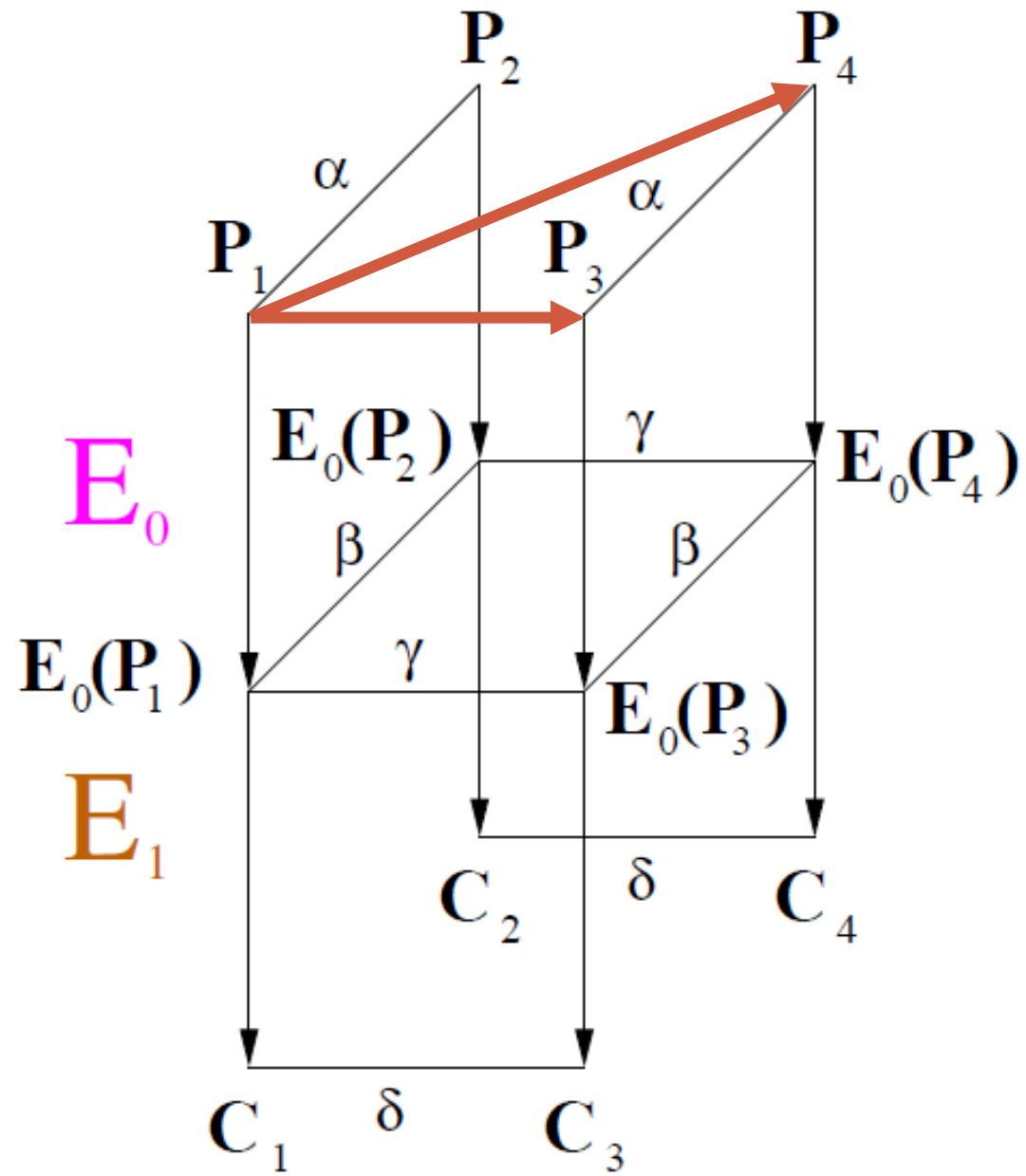
Amplified Boomerang Attack

- Zašifruj veľa textu a dúfaj v to, že nejaký bude spĺňať podmienku BA
- $2^{-n-1}p^2q^2$ - pravd. správneho páru
- $2^{-n-1}p^2q^2N^2$
- Aspoň $2^{\frac{n}{2}+1}$ plaintextov



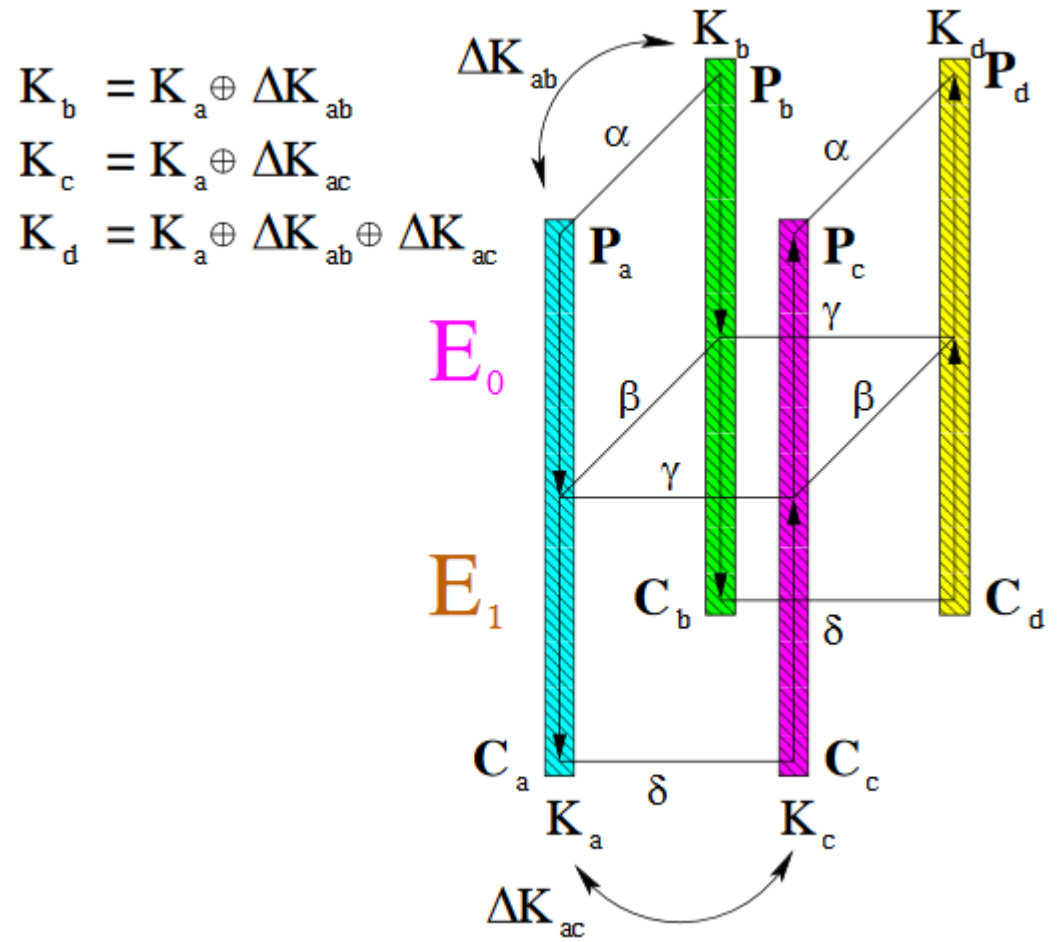
Rectangle Attack

- Rozšířený Amplified Boomerang Attack – len analýzou $(\gamma \rightarrow \delta) \text{ v } E_1$;
 - Štvorica $((P_1, P_2), (P_3, P_4))$ a k tomu príslušný šifrovaný text $((C_1, C_2), (C_3, C_4))$ také, že $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ a $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$, kde α je vstupná diferenciacia do E_0 a δ je výstupná diferenciacia z E_1
 - Využijeme všetky možné γ keď platí $Z_1 \oplus Z_3 = Z_2 \oplus Z_4 = \gamma$ a $Z_1 \oplus Z_2 = \beta$, kde $Z_i = E_0(P_i)$ ($\gamma \rightarrow \beta$) v E_1
 - Využijeme všetky možné β keď platí $Z_1 \oplus Z_2 = Z_3 \oplus Z_4$ a $Z_1 \oplus Z_3 = \gamma$
 - „Pre každý pár je k dispozícii viac párov“
 $((P_1, P_2), (P_4, P_3))$ a $((P_1, P_2), (P_3, P_4))$
-



Related-Key Boomerang Attack

- Vyber náhodne P_a ,
a spočítaj $P_b = P_a \oplus \alpha$
- Požiadaj o šifrovanie $C_a = E_{K_a}(P_a)$
a $C_b = E_{K_b}(P_b)$
- Spočítaj $C_c = C_a \oplus \delta$ a $C_d = C_b \oplus \delta$
- Požiadaj dešifrovať $P_c = E_{K_c}^{-1}(C_c)$
a $P_d = E_{K_d}^{-1}(C_d)$
- Skontroluj, či $P_c \oplus P_d = \alpha$



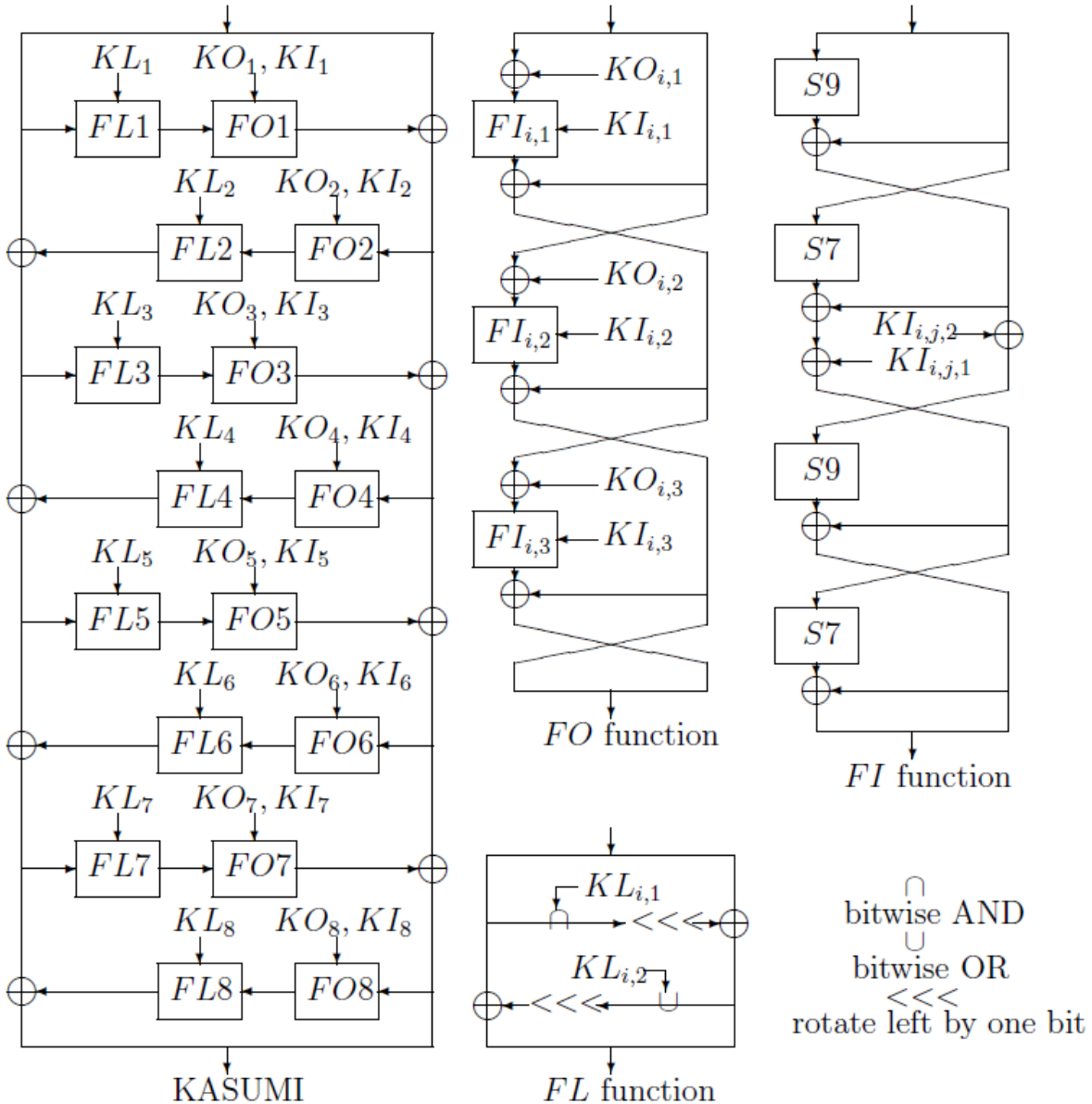
Related-Key Rectangle Attack

- $K_a, K_b = K_a \oplus K_{ab}, K_c = K_a \oplus K_{ac}, K_d = K_a \oplus K_{ad}$
 - Vyber N otvorených párov $(P_a, P_b = P_a \oplus \alpha)$ a požiadaj zašifrovanie P_a kľúčom K_a a P_b kľúčom K_b
 - Vyber N otvorených párov $(P_c, P_d = P_c \oplus \alpha)$ a požiadaj zašifrovanie P_c kľúčom K_c a P_d kľúčom K_d
 - Najdi štvorce (P_a, P_b, P_c, P_d) a odpovedajúce (C_a, C_b, C_c, C_d) splňujúce $C_a \oplus C_c = C_b \oplus C_d = \delta$
 - Lepšie pravdepodobnosti útokov
 - $N^2 2^{-n} (pq)^2$ - správnych štvoríc
-

Útok na šifru KASUMI sekcia:

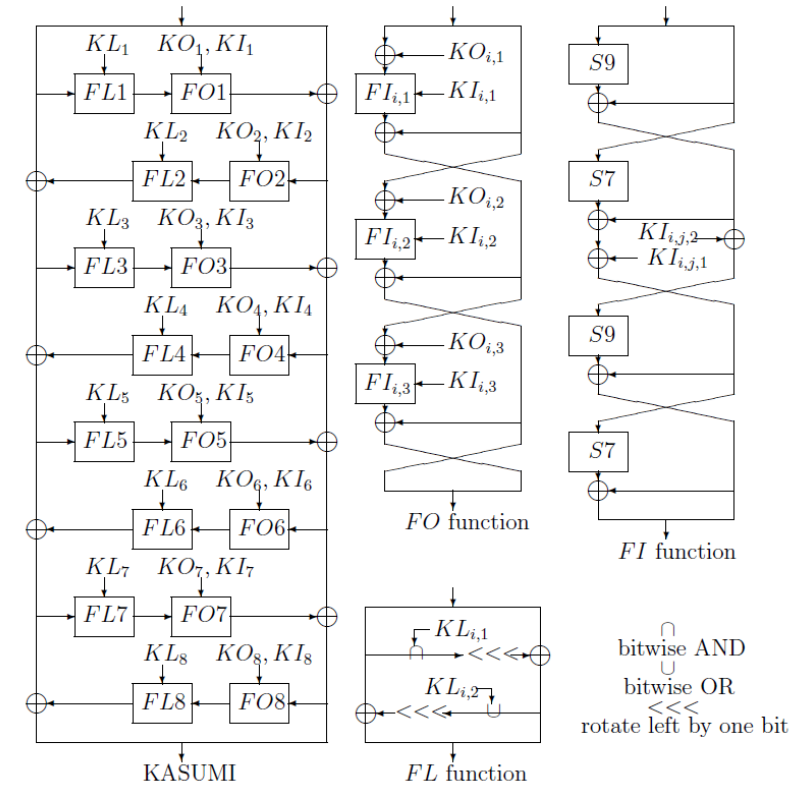
Related-Key Boomerang and Rectangle Attacks
on the Full KASUMI

KASUMI



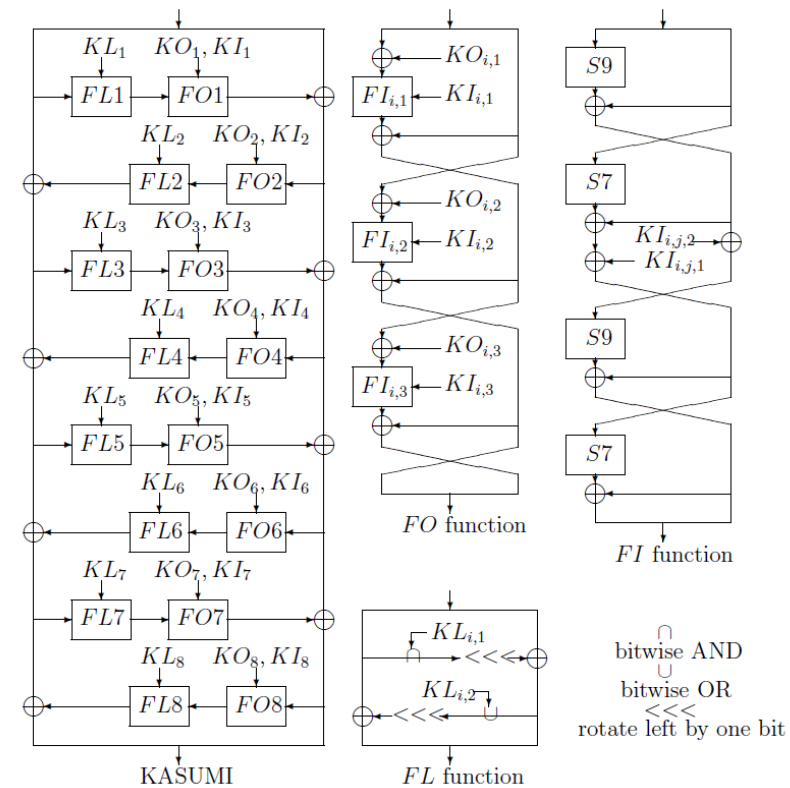
KASUMI 1-4

- $\Delta K_{ab} = (0,0,1,0,0,0,0,0)$
- Vstupná diferencia $\alpha = (0_X, (0020\ 0000)_X)$
- $\alpha = (0_X, (0020\ 0000)_X) \rightarrow (y_X, (0020\ 0000)_X)$
- $2^{-34} = \frac{1}{4} \frac{1}{2^{32}}$
- $P = (P_{LL}P_{LR}P_{RL}P_{RR})$
- $P_{LL}^0 = 0, P_{LR}^1 = 1$ – zlepšime charakteristiku
- $\frac{1}{2^{33}}$, efektívna pravdepodobnosť $\frac{1}{2^{17}}$



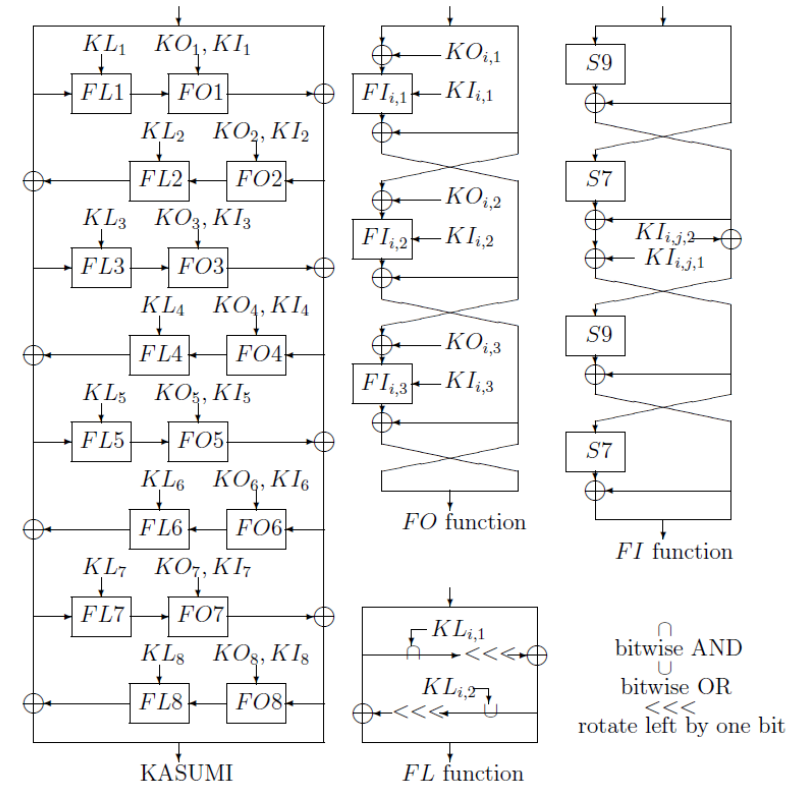
KASUMI 5-7

- $\Delta K_{ac} = (0,0,0,0,0,0,1,0)$
- Vstupná diferencia $\gamma = (0_X, (0020\ 0000)_X)$
- $\gamma = (0_X, (0020\ 0000)_X) \rightarrow (0_X, (0020\ 0000)_X)$
- $\frac{1}{4}$, efektívna je $\frac{1}{4}$



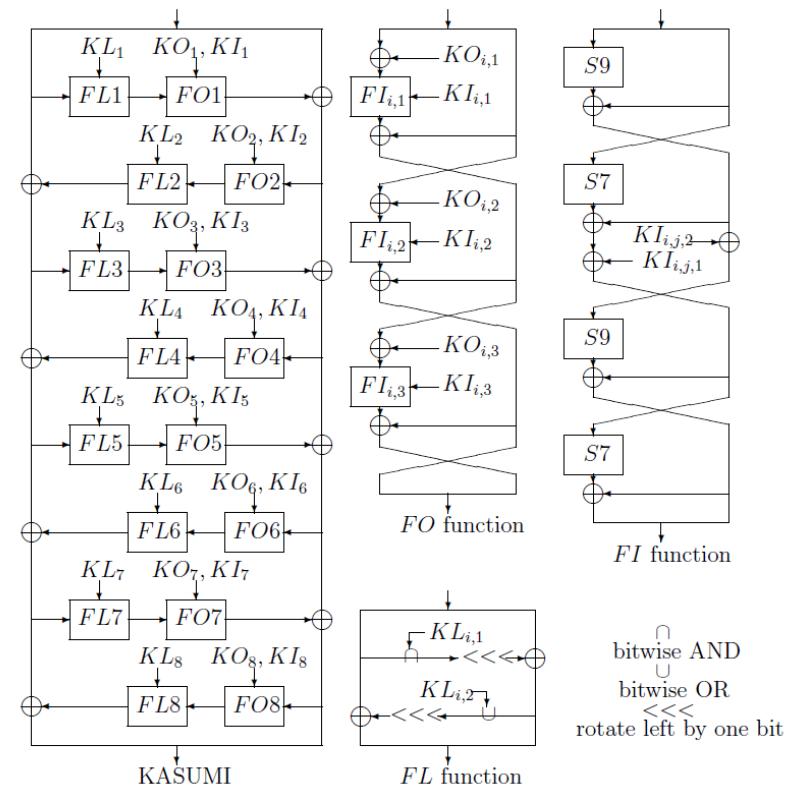
KASUMI ÚTOK

- $K_a, K_b = K_a \oplus K_{ab}, K_c = K_a \oplus K_{ac}, K_d = K_a \oplus K_{ad}$
- Potrebujeme 2^{51} - otvorených textov
- Celkovo štvoríc máme 2^{102} , potom dostávame 1 správny „obdĺžnik“
- Algoritmus:
 - 2^{51} šifrovaní: $(P_a, P_b = P_a \oplus \alpha), P_{aLL}^0 = 0, P_{aLR}^1 = 1, E(P_a, K_a), E(P_b, K_b)$
Index: $(C_{aRL} C_{aRR} C_{bRL} C_{bRR})$
 - 2^{51} šifrovaní: $(P_c, P_d = P_c \oplus \alpha), P_{cLL}^0 = 0, P_{cLR}^1 = 1, E(P_c, K_c), E(P_d, K_d)$
Index: $(C_{cRL} \oplus 0020_X, C_{cRR} C_{dRL} \oplus 0020_X, C_{dRR})$ (zhoduje sa diferencia?)



KASUMI ÚTOK

- $(C_{CRL} \oplus 0020_X, C_{CRR} C_{dRL} \oplus 0020_X, C_{dRR})$
 - Nájdeme (P_a, P_b) , pokračujeme štvoricou (P_a, P_b, P_c, P_d)
- 2^{38} približne bude vyhovovať
- Tipneme si kľúč $(KO_{8,1}, KI_{8,1})$ a vydedukujeme $KL_{8,2}$ - je možné vypočítať vstupné a výstupné diferencie do OR funkcie (spor)
- Tipneme si kľúč $(KO_{8,3}, KI_{8,3})$ a vydedukujeme $KL_{8,2}$ - spočítame diferencie vstupu a výstupu
- Pre všetky vyhovujúce kombinácie urob šifrovanie a over výsledok



KASUMI ÚTOK – ANALÝZA

- Ohadovanie $KL_{8,2}$ – 2^{-16} - zlých kľúčov

OR — $KL_{8,2}$

(X'_1, Y'_1)	(X'_2, Y'_2)			
	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	{0,1}	—	1	0
(0,1)	—	—	—	—
(1,0)	1	—	1	—
(1,1)	0	—	—	0

AND — $KL_{8,1}$

(X'_1, Y'_1)	(X'_2, Y'_2)			
	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	{0,1}	—	0	1
(0,1)	—	—	—	—
(1,0)	0	—	0	—
(1,1)	1	—	—	1

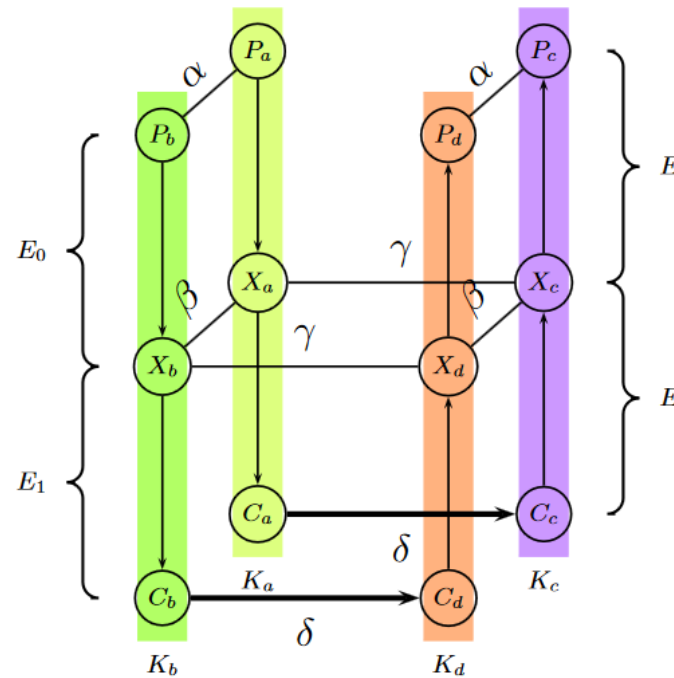
* The two bits of the differences are denoted by (input difference, output difference): (X'_1, Y'_1) for one pair and (X'_2, Y'_2) for the other.

KASUMI ÚTOK – ANALÝZA

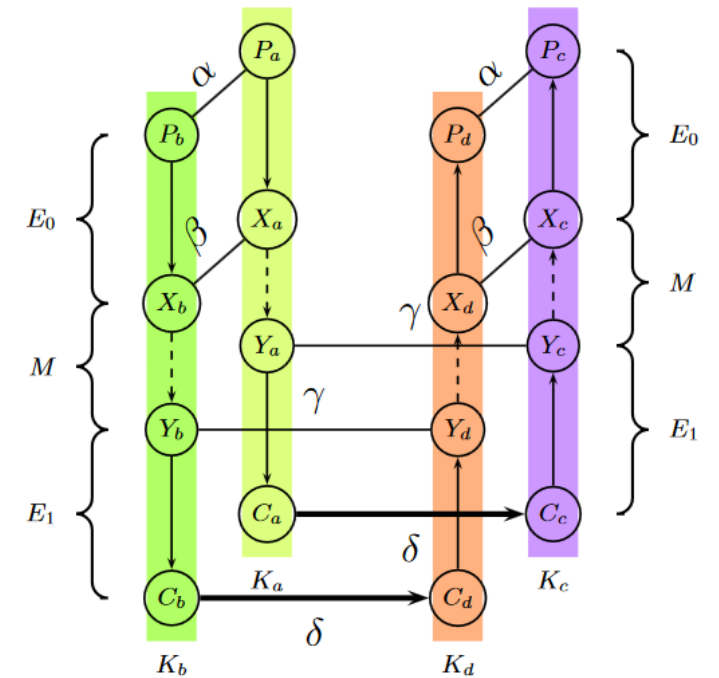
- Ohodadovanie $KL_{8,2}$ – 2^{-16} - zlých kľúčov
 - $2^{38}2^{32} = 2^{70}$; $2^{70}2^{-16} = 2^{54}$
 - $2^{54}2^{32} = 2^{86}$; $2^{86}2^{-16} = 2^{70}$ - pre 96 bitový kľúč ☺
 - Dokončiť zvyšných 32 bitov
 - 2^{102} operácii pri 128 bitovom kľúči
 - Vylepšenia:
 - Pri šifrovaní $2^{52,6}$ vstupných textov = $2^{86,6}$
 - Analýzov vieme dostať $2^{76,1}$ - viac informácií v mojej práci ☺
-

KASUMI ÚTOK 2

- Sandwich attack
- 2^{32} časová zložitost'
- 2^{30} paměťová zložitost'
- 2^{25} šifrových textov



A Related-Key Boomerang Quartet



A Related-Key Sandwich Quartet

Útoky na jiné šifry

A5/1, A5/2

A5/1

- Chris Paget a Karsten Nohl
 - 2 TB predpočítaných dát
 - Zdielané známou P2P sieťou
 - Pár sekúnd = prelomená A5/1
-

A5/2

- Nezaujímavé, všeobecne sa prestala používať
- Skript-kiddies 😊

SNOW 3G

- Side-channel attack
 - Možno sa na ňu pozriem 😊
-

Zdroj

- E. Biham, O. Dunkelman: *Techniques for Cryptanalysis of Block Ciphers* (Information Security and Cryptography), Springer, 2017, ISBN 978-3642172311
 - DUNKELMAN, Orr; KELLER, Nathan; SHAMIR, Adi. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: *Annual Cryptology Conference*. Springer Berlin Heidelberg, 2010. p. 393-410.
 - BRUMLEY, Billy Bob, et al. Consecutive S-box lookups: A Timing Attack on SNOW 3G. In: *International Conference on Information and Communications Security*. Springer Berlin Heidelberg, 2010. p. 171-185.
 - GSM: Srsly ? – Príspevok na konferencii, 26th Chaos Communication Congress, Paget Ch., Nohl K.
-

Ďakujem za pozornosť.
