Kryptoanalýza šifier v mobilných sieťach

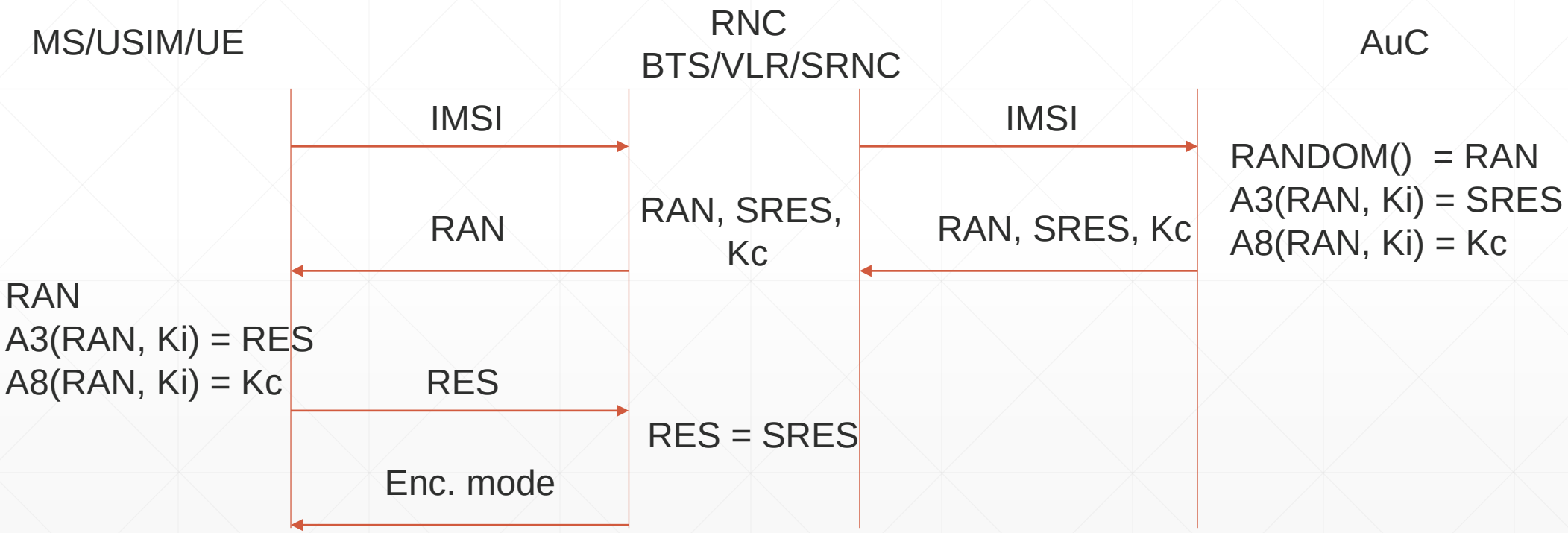
Ján Kotrady

Obsah

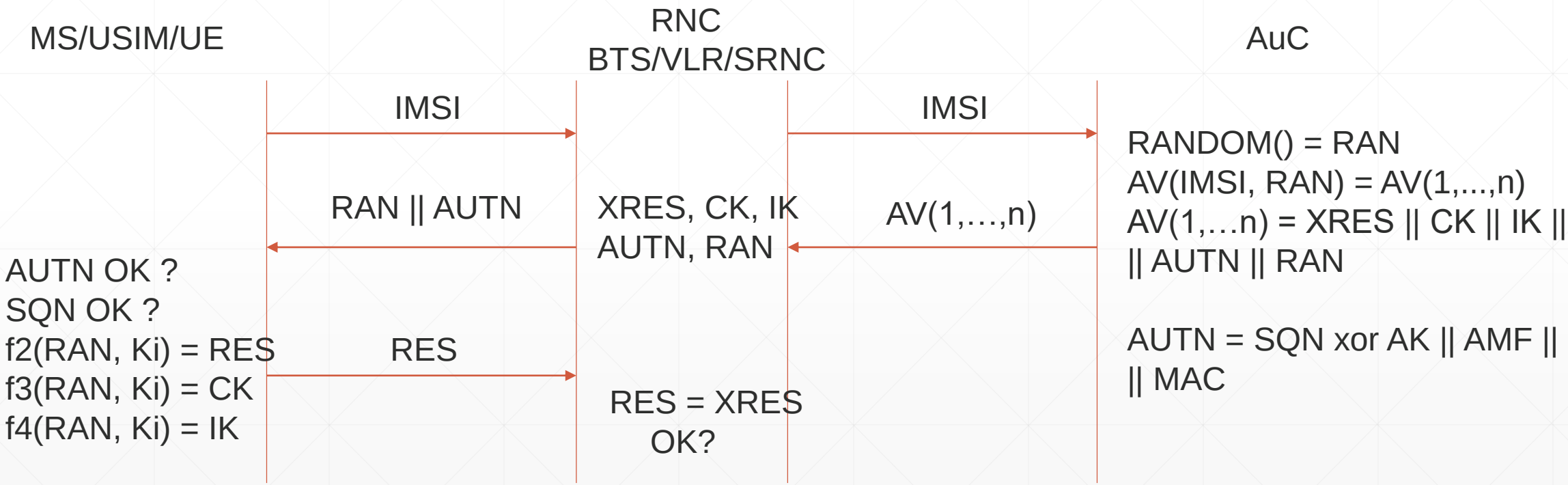
- Diferenčná kryptoanalýza
- Pár algoritmov
- KASUMI Related-Key Sandwich (Boomerang) Attack*
- ...

Pripomenutie GMS a 3G protokolov

GSM autentifikácia



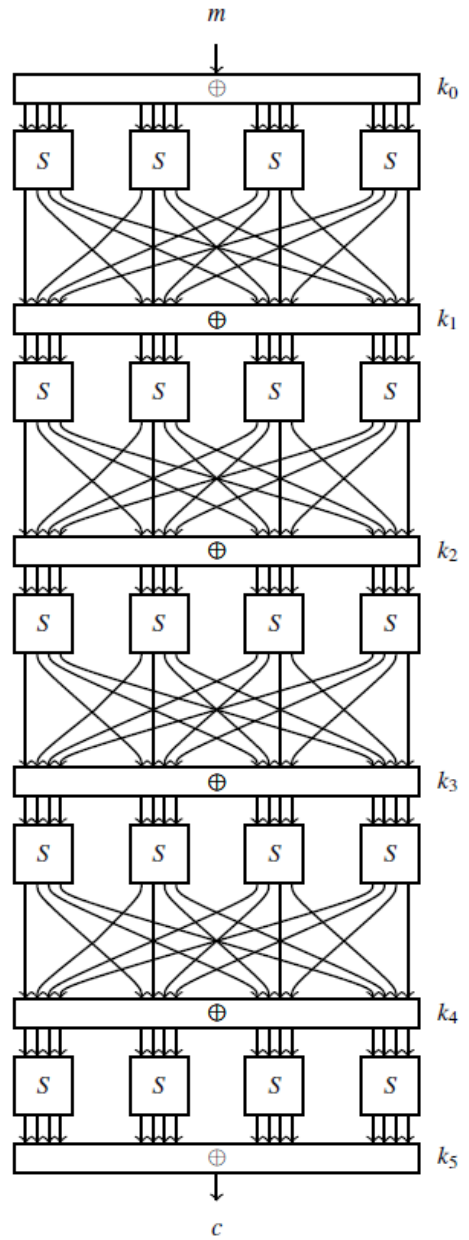
3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN OK ?
SQN OK ?
f2(RAN, Ki) = RES
f3(RAN, Ki) = CK
f4(RAN, Ki) = IK
RES
RES = XRES
OK?
AUTN = SQN xor AK || AMF ||
|| MAC

Diferenčná kryptoanalýza „myšlienka“

Blokové šifry

- Najúčinnejšia kryptoanalýza (¬DES)
- Základ: „rundy“, Feistelová sieť
- **CPA – Choosen plain-text attack**
- Ciele:
  - „Zbaviť sa kľúča“
  - Zistit kľúč
  - Útok hrubou silou jednoduchší



XOR – základný princíp

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

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1)$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$

$= m_1 \oplus m_2 \oplus (k_1 \oplus k_1)$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$

$= m_1 \oplus m_2 \oplus (k_1 \oplus k_1) = m_1 \oplus m_2 \oplus (0)$

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, $e_{k_1}(m) = m \oplus k_1$, $d_{k_1}(m) = m \oplus k_1$
- $d_{k_1}\left(e_{k_1}(m)\right) = m \oplus k_1 \oplus k_1 = m \oplus 0 = m$
- $(m_1 \oplus k_1) \oplus (m_2 \oplus k_1) = m_1 \oplus k_1 \oplus m_2 \oplus k_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_1$

$= m_1 \oplus m_2 \oplus (k_1 \oplus k_1) = m_1 \oplus m_2 \oplus (0) = m_1 \oplus m_2$

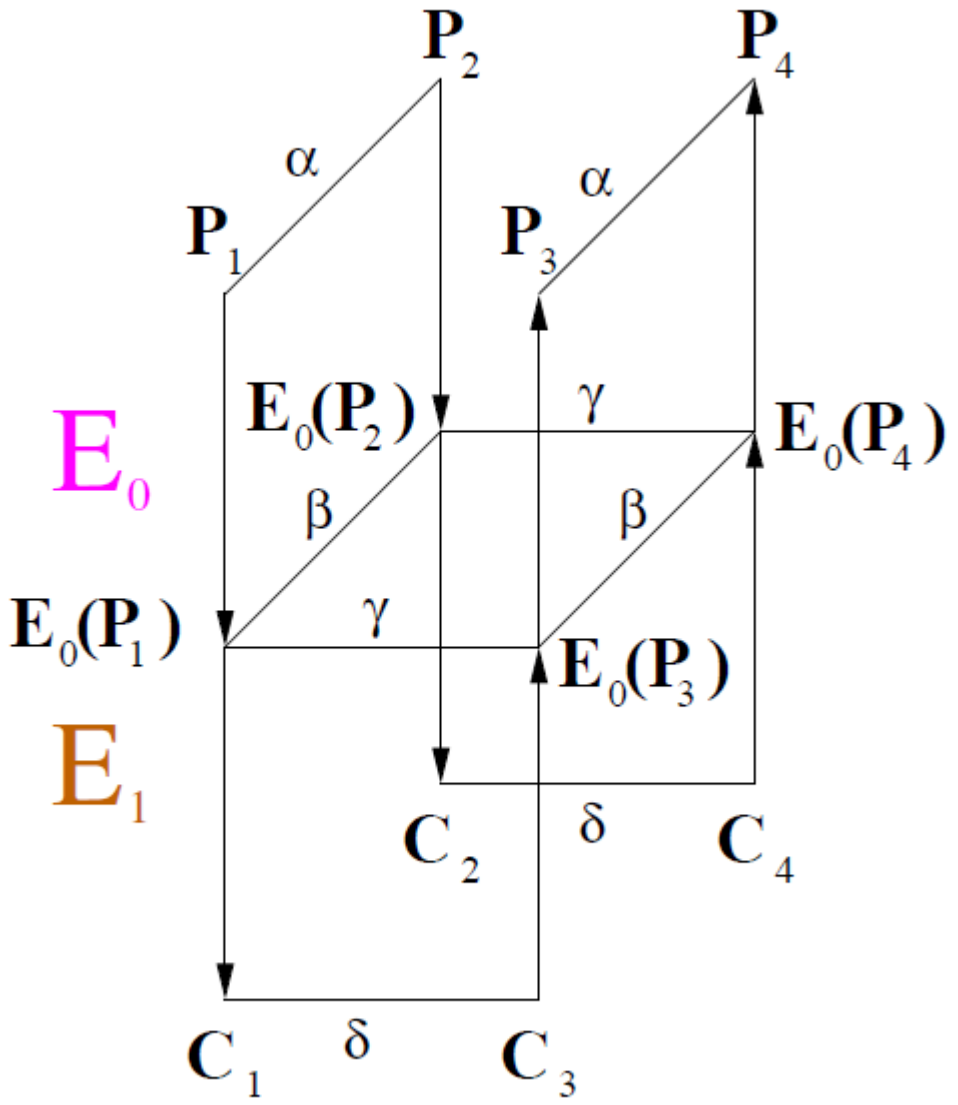
XOR operácie			
1	$\oplus$	1	0
1	$\oplus$	0	1
0	$\oplus$	1	1
0	$\oplus$	0	0

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

Útok na šifru KASUMI
POPIS ÚTOKU

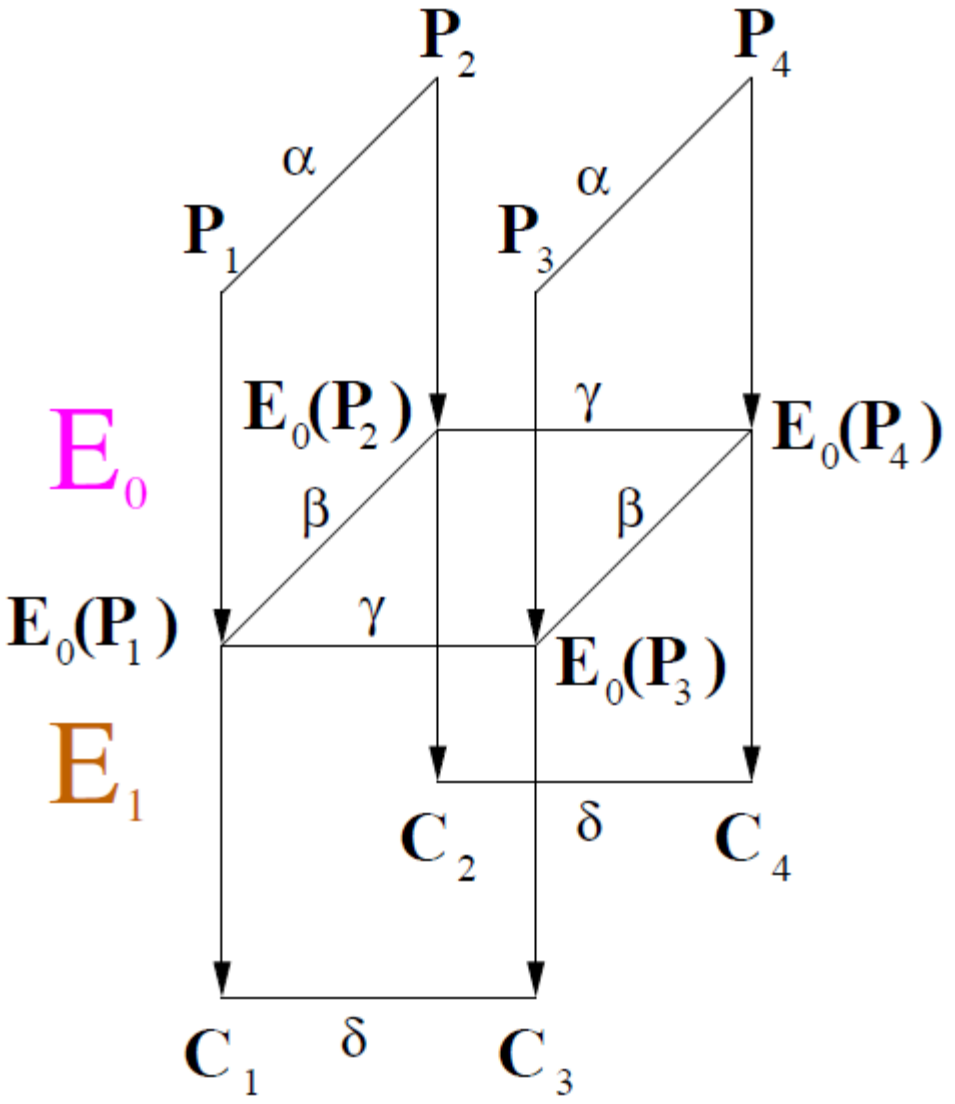
Boomerang Attack

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



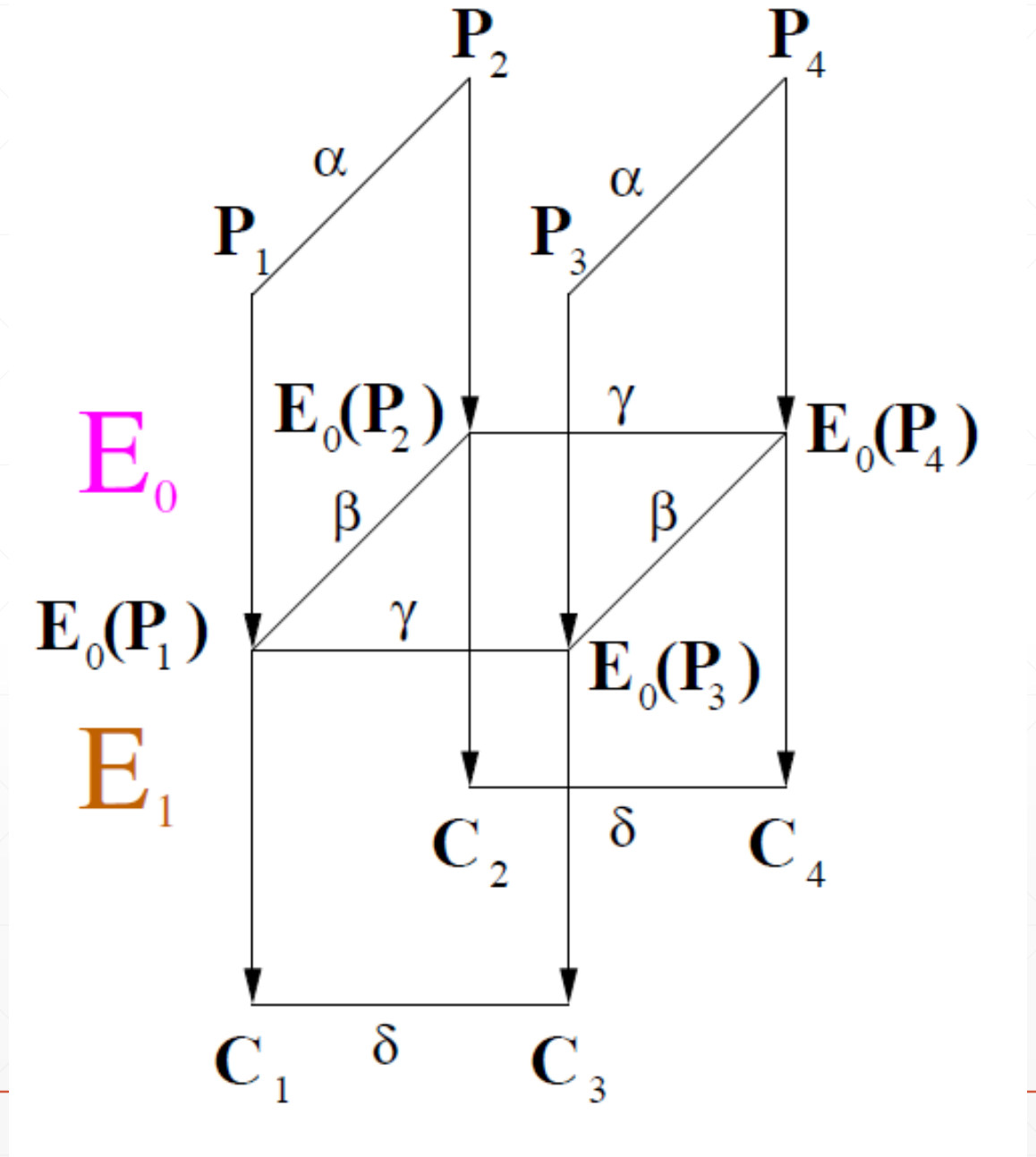
Amplified Boomerang Attack

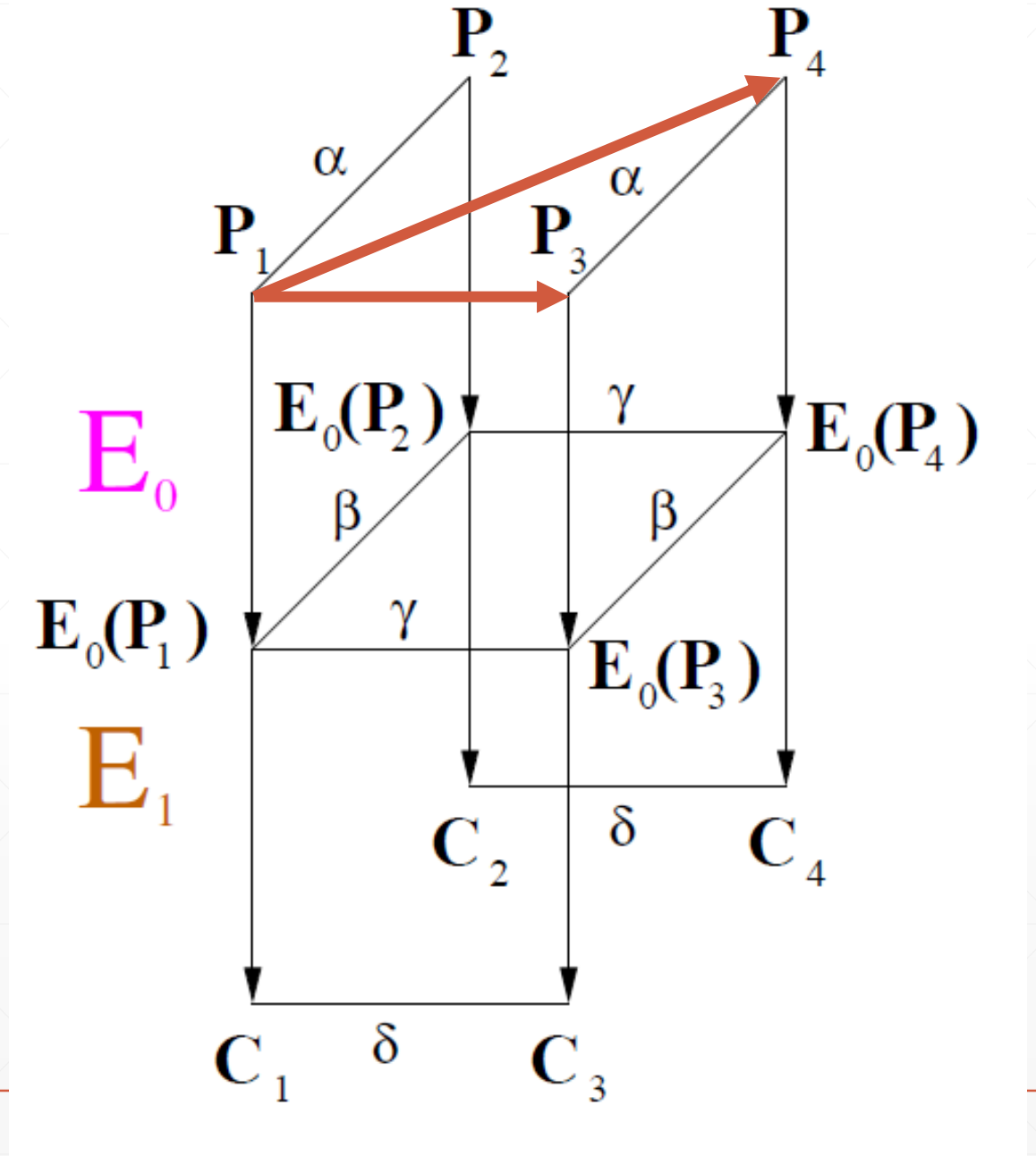
- Zašifruj veľa textu a dúfaj v to, že nejaký bude spĺňať podmienku BA
- $2^{-n-1}p^2q^2$ - pravd. správneho páru
- $2^{-n-1}p^2q^2N^2$
- Aspoň $2^{\frac{n}{2}+1}$ plaintextov



Rectangle Attack

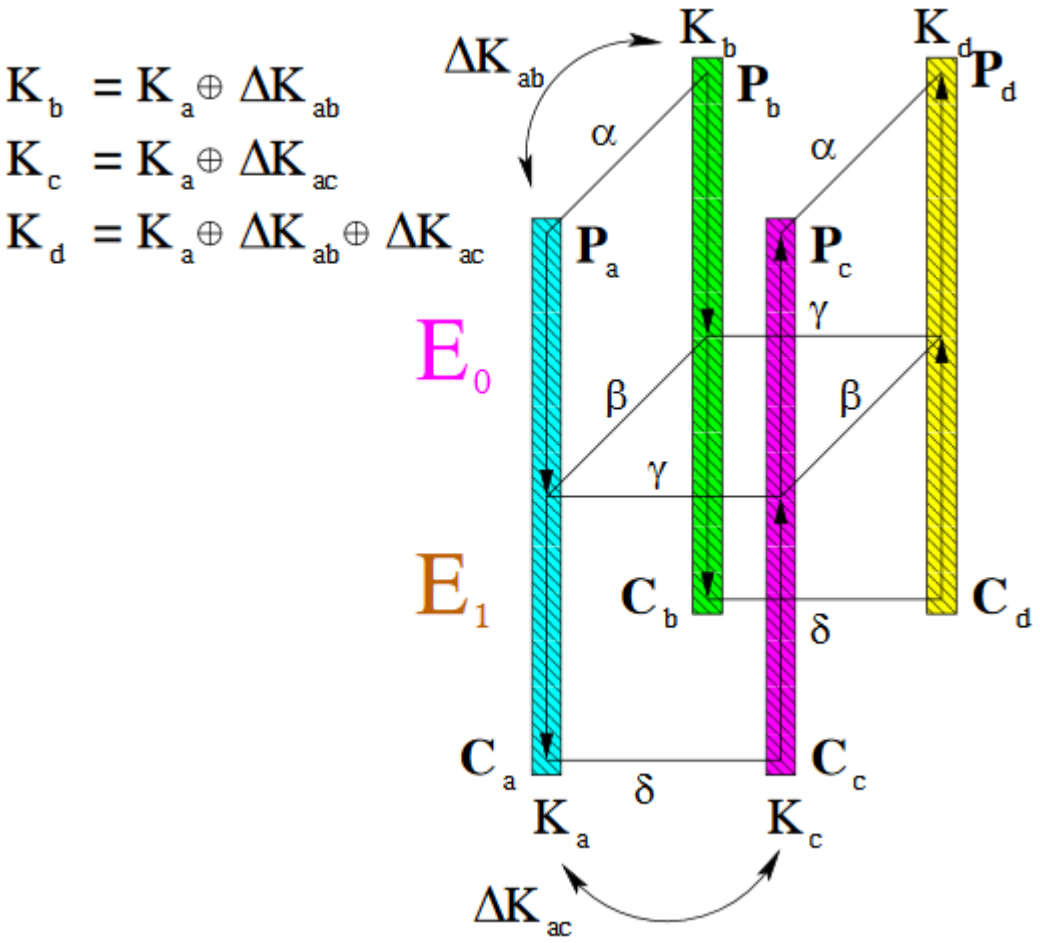
- Rozšírený Amplified Boomerang Attack – len analýzou $(\gamma \rightarrow \delta)$ v E_1;
- Štvorica$\big((P_1, P_2), (P_3, P_4)\big)$ a k tomu príslušný šifrovaný text $\big((C_1, C_2), (C_3, C_4)\big)$ také, že $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ a $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$, kde α je vstupná diferencia do E_0 a δ je výstupná diferencia 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“ $\big((P_1, P_2), (P_4, P_3)\big)$ a $\big((P_1, P_2), (P_3, P_4)\big)$


P2
P4
α
α
P1
P3
E0(P2)
γ
E0(P4)
E0
β
β
E0(P1)
γ
E0(P3)
E1
C2
δ
C4
C1
δ
C3


P2
P4
α
α
P1
P3
E0
E0(P2)
γ
E0(P4)
β
β
E0(P1)
γ
E0(P3)
E1
C2
δ
C4
C1
δ
C3

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 $P_c \oplus P_d = \alpha$



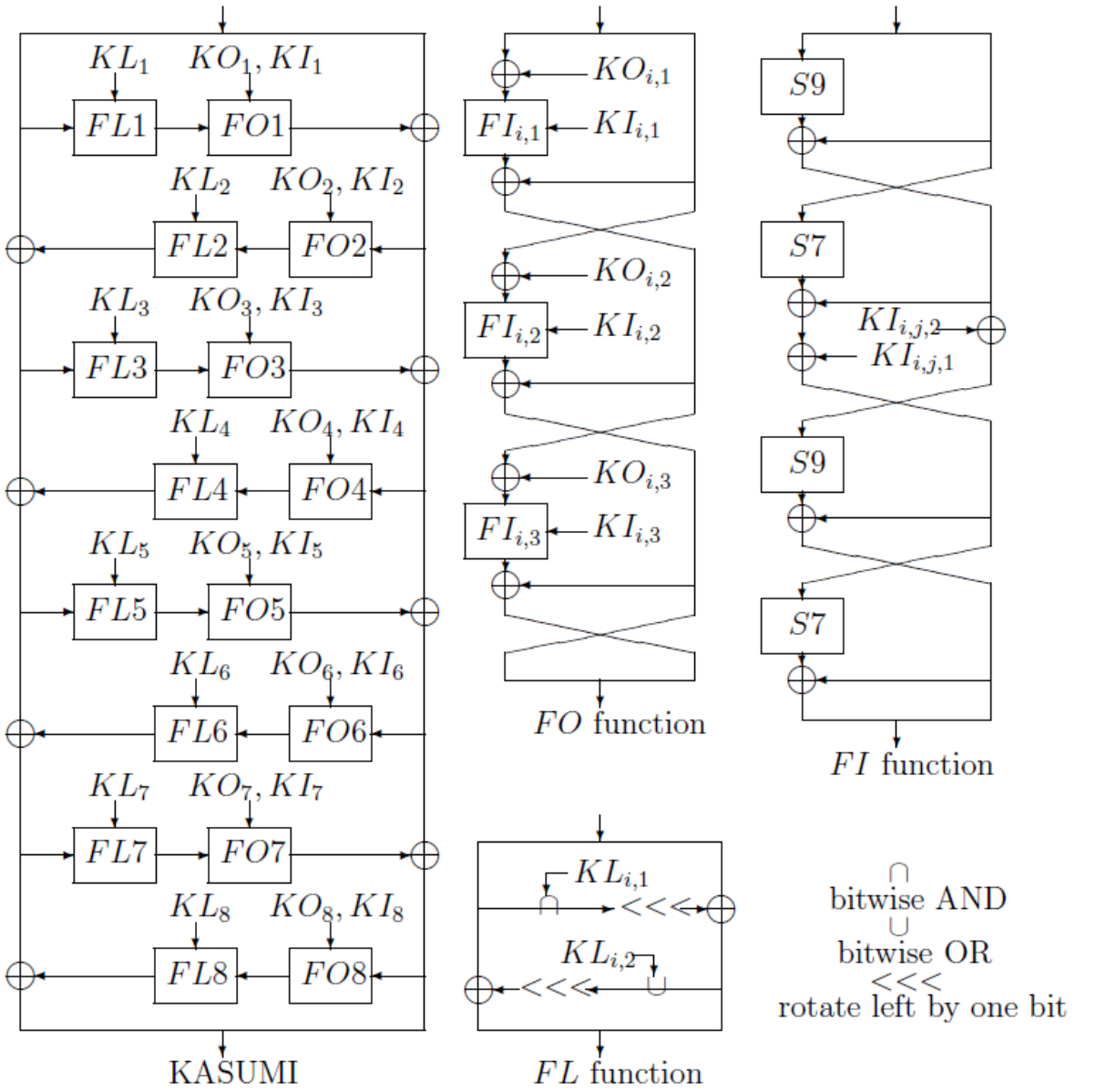
Related-Key Rectangle Attack

- $K_a, K_b = K_a \oplus K_{ab}$, $K_c = K_a \oplus K_{ac}$, $K_d = K_a \oplus K_{ad}$
- 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 štvorice (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:

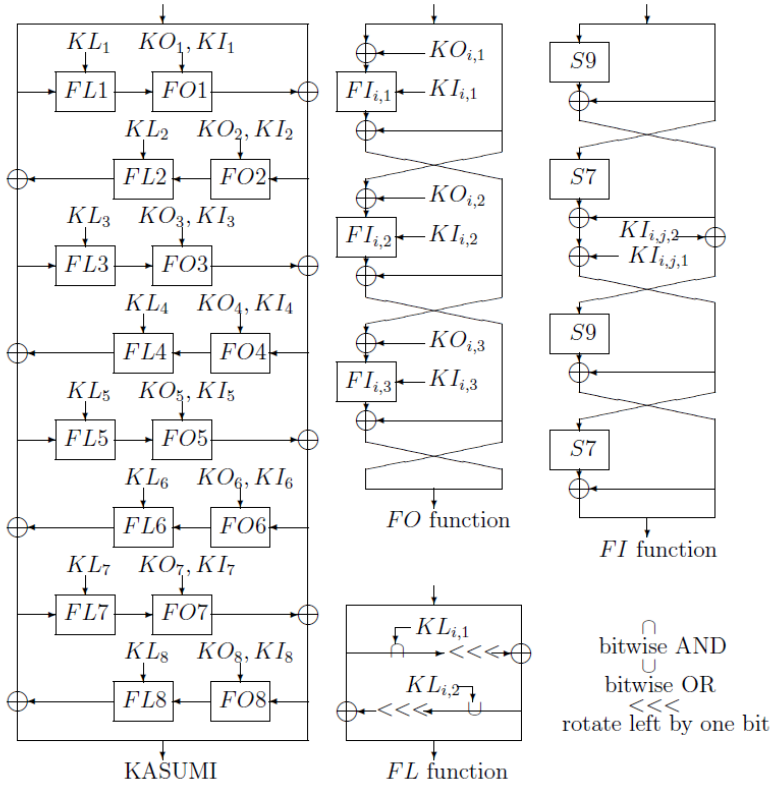
Related-Key Boomerang and Rectangle Attacks on the Full KASUMI

KASUMI


KL_1 KO_1, KI_1
$FL1$ $FO1$
KL_2 KO_2, KI_2
$FL2$ $FO2$
KL_3 KO_3, KI_3
$FL3$ $FO3$
KL_4 KO_4, KI_4
$FL4$ $FO4$
KL_5 KO_5, KI_5
$FL5$ $FO5$
KL_6 KO_6, KI_6
$FL6$ $FO6$
KL_7 KO_7, KI_7
$FL7$ $FO7$
KL_8 KO_8, KI_8
$FL8$ $FO8$
KASUMI
$KO_{i,1}$
$FI_{i,1}$ $KI_{i,1}$
$KO_{i,2}$
$FI_{i,2}$ $KI_{i,2}$
$KO_{i,3}$
$FI_{i,3}$ $KI_{i,3}$
FO function
$KL_{i,1}$
$KL_{i,2}$
FL function
S9
S7
$KI_{i,j,2}$
$KI_{i,j,1}$
S9
S7
FI function
bitwise AND
bitwise OR
rotate left by one bit

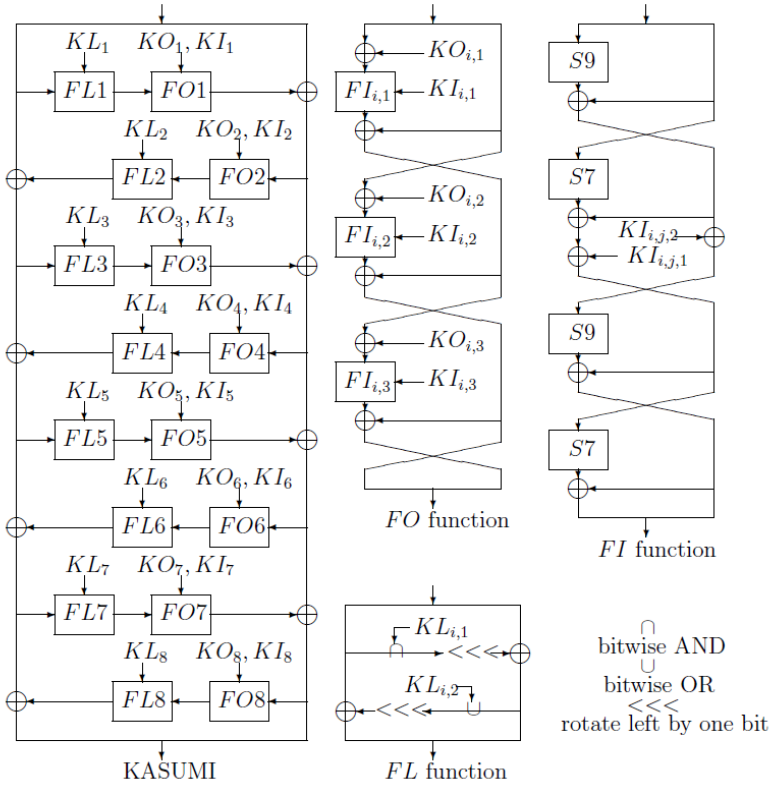
KASUMI 1-4

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



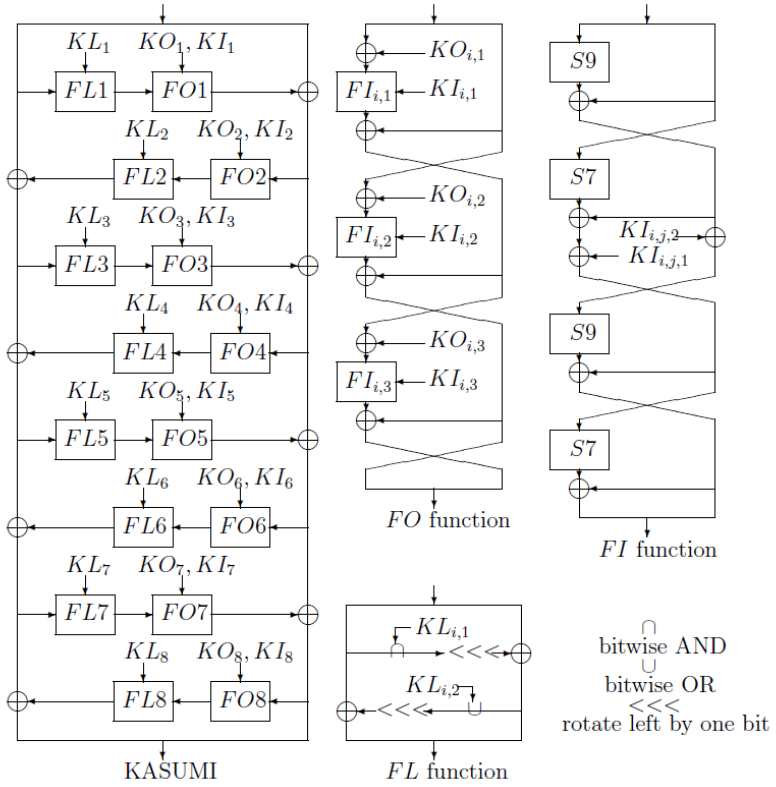
KASUMI 5-7

- $\Delta K_{ac} = (0,0,0,0,0,0,1,0)$
- 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 $\frac{1}{4}$



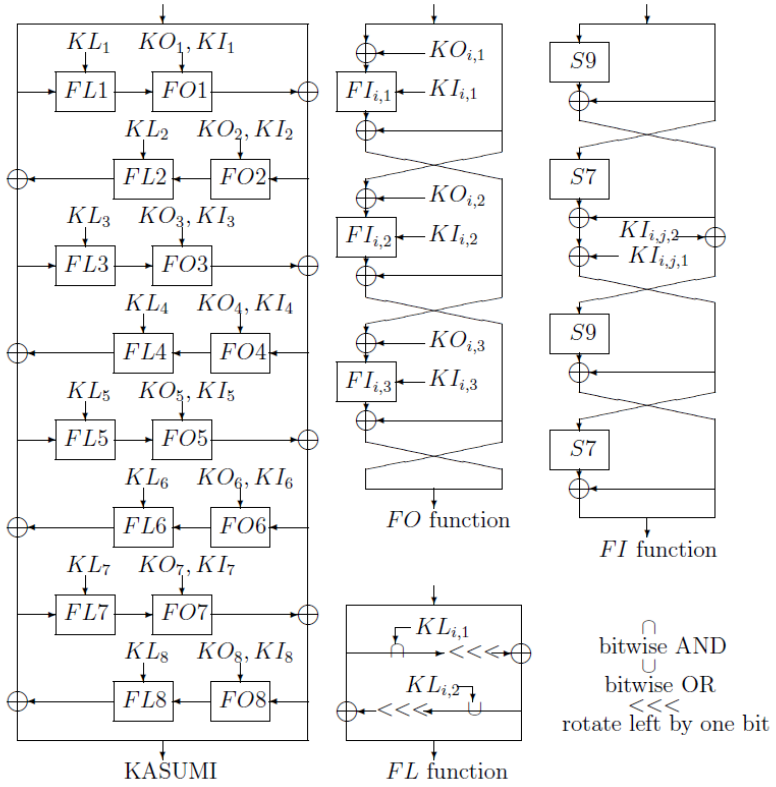
KASUMI ÚTOK

- $K_a, K_b = K_a \oplus K_{ab}$, $K_c = K_a \oplus K_{ac}$, $K_d = K_a \oplus K_{ad}$
- Potrebujeme 2^{51} - otvorených textov
- Celkovo štvoríc máme 2^{102}, potom dostávame 1 správny „obdĺžnik“
- Algoritmus:
  - 2^{51} šifrovaní: $(P_a, P_b = P_a \oplus \alpha)$, $P^0_{a_{LL}} = 0$, $P^1_{a_{LR}} = 1$, $\mathrm{E}(P_a, K_a)$, $\mathrm{E}(P_b, K_b)$
    Index: $\left(C_{a_{RL}} C_{a_{RR}} C_{b_{RL}} C_{b_{RR}}\right)$
  - 2^{51} šifrovaní: $(P_c, P_d = P_c \oplus \alpha)$, $P^0_{c_{LL}} = 0$, $P^1_{c_{LR}} = 1$, $\mathrm{E}(P_c, K_c)$, $\mathrm{E}(P_d, K_d)$
    Index: $\left(C_{c_{RL}} \oplus 0020_X, C_{c_{RR}} C_{d_{RL}} \oplus 0020_X, C_{d_{RR}}\right)$ (zhoduje sa diferencia?)



KASUMI ÚTOK

- $(C_{c_{RL}} \oplus 0020_X, C_{c_{RR}} C_{d_{RL}} \oplus 0020_X, C_{d_{RR}})$
  - 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 výstupne 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

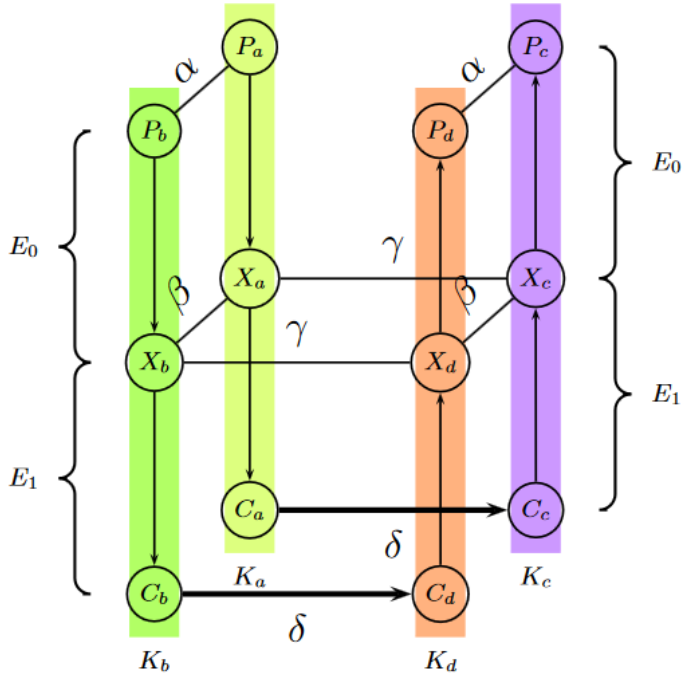
* The two bits of the differences are denotes by (input difference, output difference): (X'_1, Y'_1) for one pair and (X'_2, Y'_2) for the other.

KASUMI ÚTOK – ANALÝZA

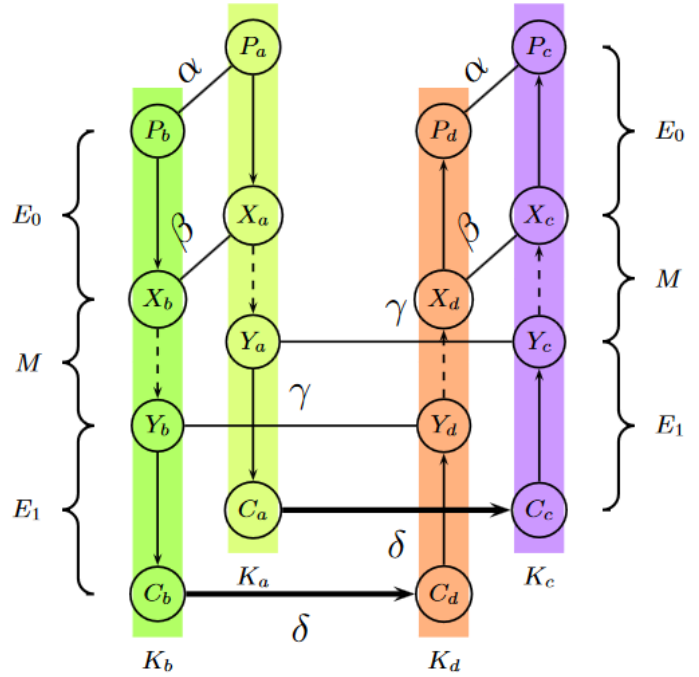
- Odhadovanie $KL_{8,2} - 2^{-16}$ - zlých kľúčov
- $\mathbf{2^{38}2^{32} = 2^{70}; 2^{70}2^{-16} = 2^{54}}$
- $\mathbf{2^{54}2^{32} = 2^{86}; 2^{86}2^{-16} = 2^{70}}$ - pre 96 bitový kľúč ☺
- Dokončiť zvyšných 32 bitov
  - $\mathbf{2^{102}}$ operácii pri 128 bitovom kľúči
- Vylepšenia:
  - Pri šifrovaní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

KASUMI ÚTOK - Sandwich

- Sandwich attack
- 2^{32} časová zlozitosť
- 2^{30} pamäťová zlozitosť
- 2^{25} šifrových textov



A Related-Key Boomerang Quartet

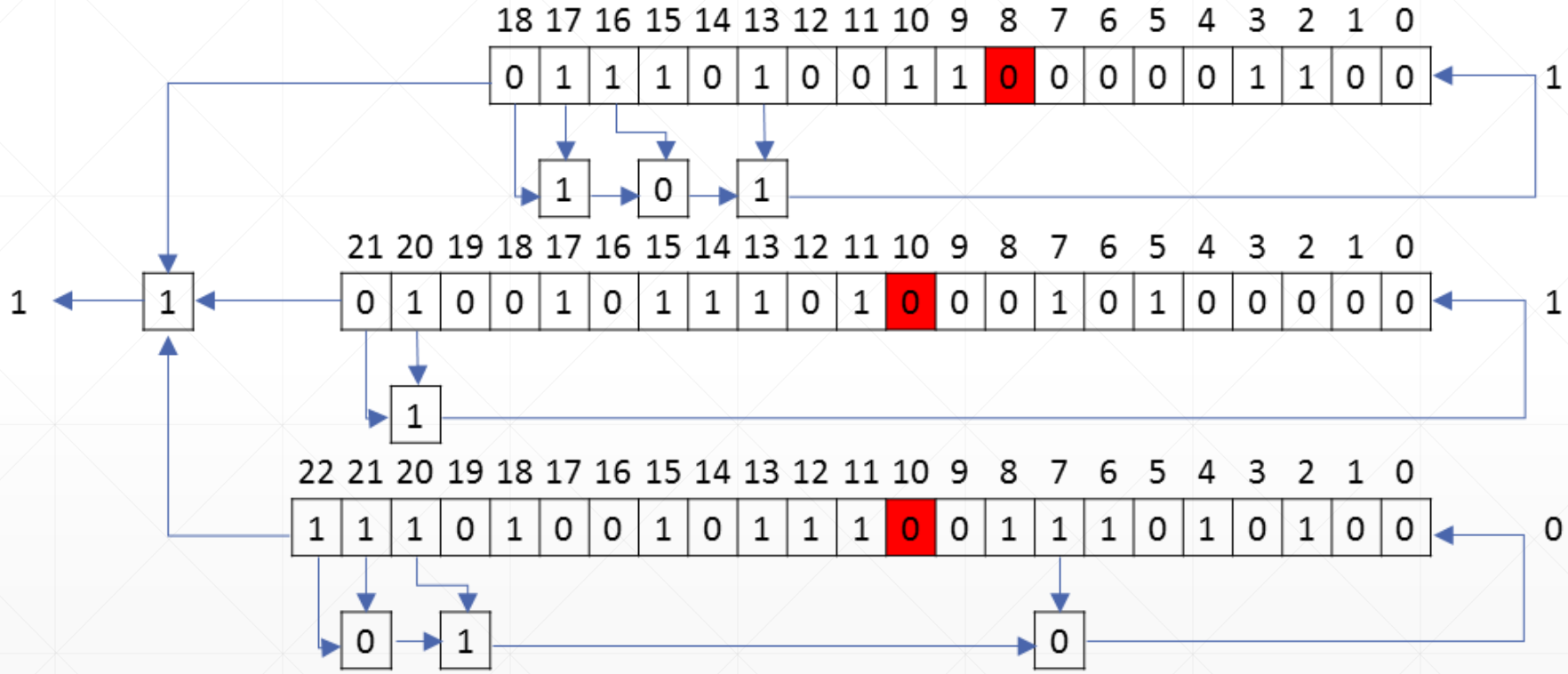


A Related-Key Sandwich Quartet

Útoky na iné šifry

A5/1, A5/2

A5/1


18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
0 1 1 1 0 1 0 0 1 1 0 0 0 0 0 1 1 0 0
1
1 0 1
21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
1
1
0 1 0 0 1 0 1 1 1 0 1 0 0 0 1 0 1 0 0 0 0 0
1
1
22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 1 1 0 1 0 1 0 0
0
0 1 0

A5/1

- Prúdové šifry
- Kryptoanalýza v reálnom čase
- BTS simulácia
  - Náročná implementácia
  - bb.osmocom.org
  - 5x Motorola C155 15$ || bladeRF x40 420$
- RTL-SDR

A5/1

- Chris Paget a Karsten Nohl
  - 2 TB predpočítaných dát
  - Zdielané známou P2P sieťou
  - Pár sekúnd = prelomená A5/1
- time memory trade off
  - S určitou pravdepodobnosťou
  - Rainbow table
- NOP správy
- Detekovanie kľúča

A5/2

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

SNOW 3G

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

Aktuálny stav

- Analýza KASUMI
  - Zefektívnenie Sandwich attack ?
  - KPA attack analýza – dokončujem
- A5/1
  - Tabuľky
  - Odchytávanie signálu
  - Pár technických problémov a kryptoanalýza bude fungovať
  - Dokončujem analýzu – možnosti zrýchlenia
- Odhadovaný termín dokončenia výskumu – december

Ďalšie problémy – [Orr Dunkleman]

- Článok:

  Dunkelman, O., Keller, N. & Shamir, A. J Cryptol (2014) 27: 824. https://doi.org/10.1007/s00145-013-9154-9

- Problem 1. Nájsť iné generické štruktúry, v ktorých sa dá sandwich útok použiť.
- Problem 2. Nájdite nutné a postačujúce podmienky, za ktorých sa dá predpokladať podmienka nezávislosti, ktorá sa využíva v Sandwich related key rectangle attack
- Problem 3. Overte ako prvý správnosť rectangle-like sandwich attack na šifru Kasumi.

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 konferencií, 26th Chaos Communication Congress, Paget Ch., Nohl K.

Ďakujem za pozornosť.