Kryptoanalýza šifier v mobilných sieťach

Vedúci práce: RNDr. Rastislav Krivoš-Belluš, PhD.

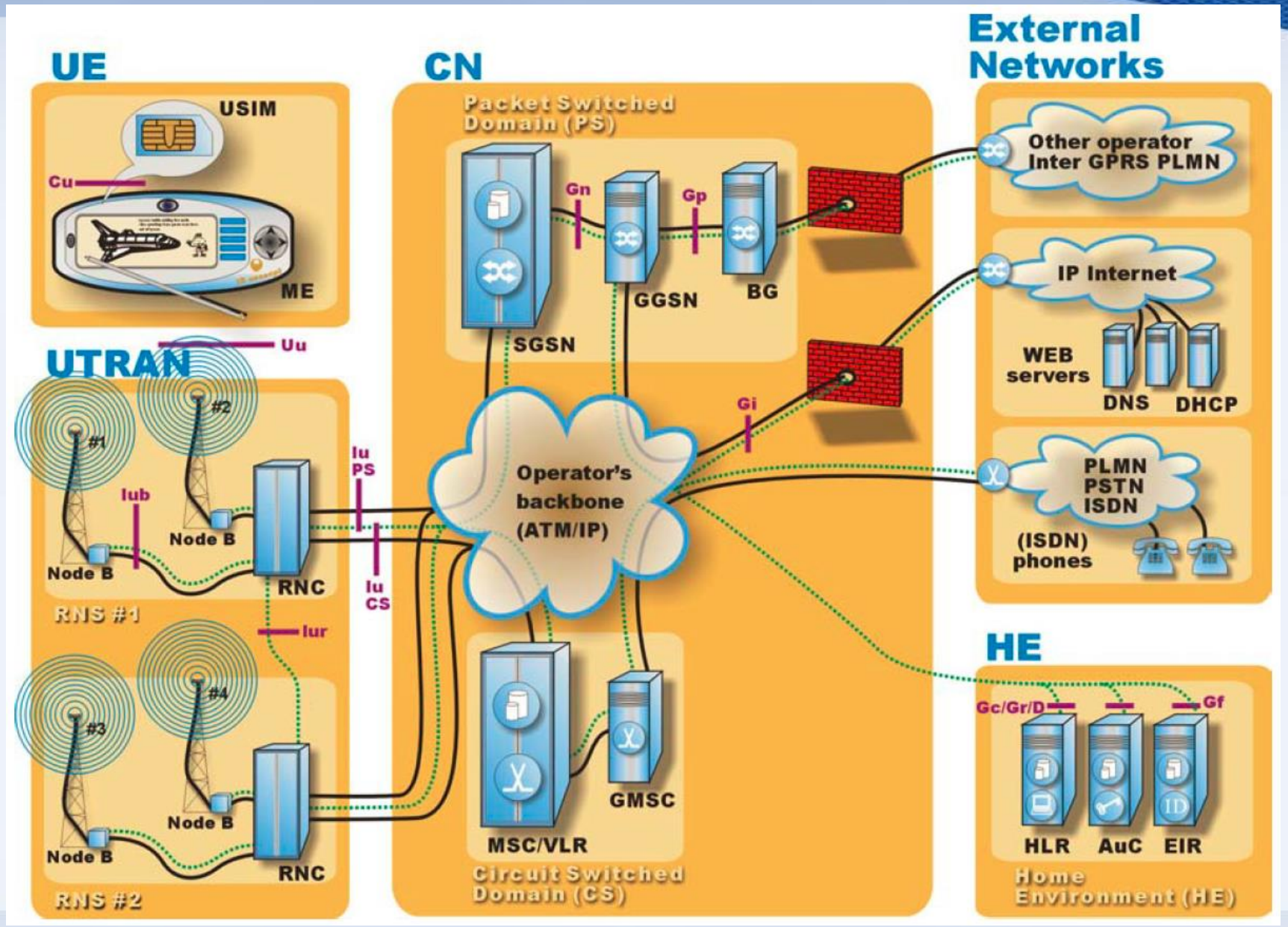
Autor: Bc. Ján Kotrady

Ciele

- 1. Analyzovať a porovnať publikované útoky na šifry používané v mobilných sieťach.
- 2. Preskúmať praktické implementácie analyzovaných útokov.
- 3. Navrhnúť nové metódy kryptoanalýzy týchto šifier.

História chýb algoritmov

- 1991 – GSM implementácia
- Apríl 1998 - The Smartcard Developer Association (SDA) spolu s U.C. Berkeley researches prelomili COMP128 algoritmus uložený v SIM karte a úspešne získali Ki v priebehu pár hodín. Zistili, že Kc používa iba 54 bitov.
- August 1999: Slabá A5/2 bola prelomená použitím PC v priebehu pár sekúnd.
- December 1999: Alex Biryukov, Adi Shamir a David Wagner publikovali schému útoku na algoritmus A5/1. Pri získaní dvoch minút rozhovoru boli schopný prelomiť A5/1 algoritmus v priebehu 1 sekundy.
- Máj 2002: IBM Research group objavila nový spôsob rýchleho získavania Kc z COMP128 použitím útokov side channels.


UE
USIM
Cu
ME
Uu
UTRAN
#1
#2
Node B
Node B
Iub
RNC
RNS #1
Iur
#3
#4
Node B
Node B
RNC
RNS #2
Iu PS
Iu CS
CN
Packet Switched Domain (PS)
Gn
Gp
SGSN
GGSN
BG
Gi
Operator's backbone (ATM/IP)
MSC/VLR
GMSC
Circuit Switched Domain (CS)
External Networks
Other operator Inter GPRS PLMN
IP Internet
WEB servers
DNS
DHCP
PLMN
PSTN
ISDN
(ISDN) phones
HE
Gc/Gr/D
Gf
HLR
AuC
EIR
Home Environment (HE)

Šifry v mobilných sieťach

- GSM:
  - ENC: A5/1 & A5/2
  - COMP128: A3 – 32 bit, A8 – 64 bit
    - Utajované, revernzé inžinierstvo ...
- 3G:
  - ENC: KASUMI (GEA0, GEA1) -> RNC CHOOSE ENC. -> MS
  - f9: Milenage
- 4G:
  - ENC: Snow 3G || AES 128b.
  - Možnosť dvojitého šifrovania

Útoky

- Pasívny útok – COA - BFA
- Pasívny útok – KPA
- CPA
- MITM
- ...

A5/1 a A5/2

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

KASUMI

- “Neprelomená” bloková šifra
- 3G, 4G
- MISTY1
- 2010 – 2h útok
- Nemožný v 3G systémoch

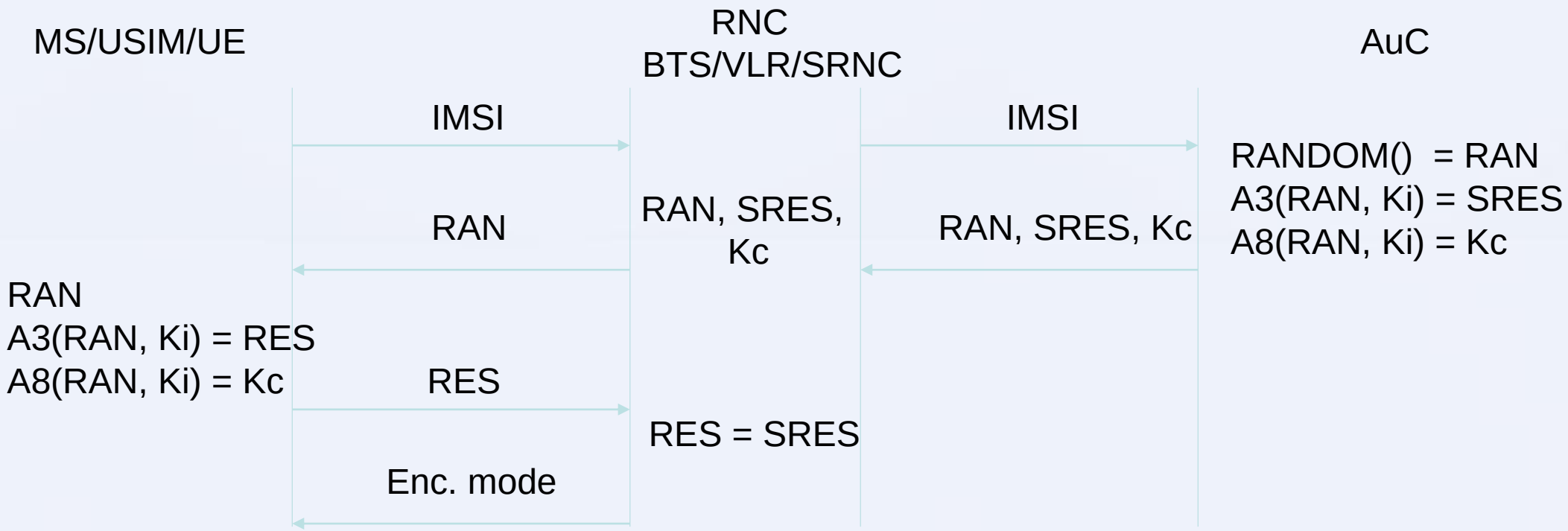
KASUMI

- Diferenčná kryptoanalýza + Related key attack
- Články:
  - The round functions of KASUMI generate the alternating group - Rüdiger Sparr & Ralph Wernsdorf, 2015, Journal of Mathematical Cryptology
  - Practical-time attacks against reduced variants of MISTY1 – Dunkleman, Keller, 2013, IACR
  - A practical-time related-key attack on the kasumi cryptosystem used in GSM and 3G telephony – Dunkleman, Keller, 2010, IACR

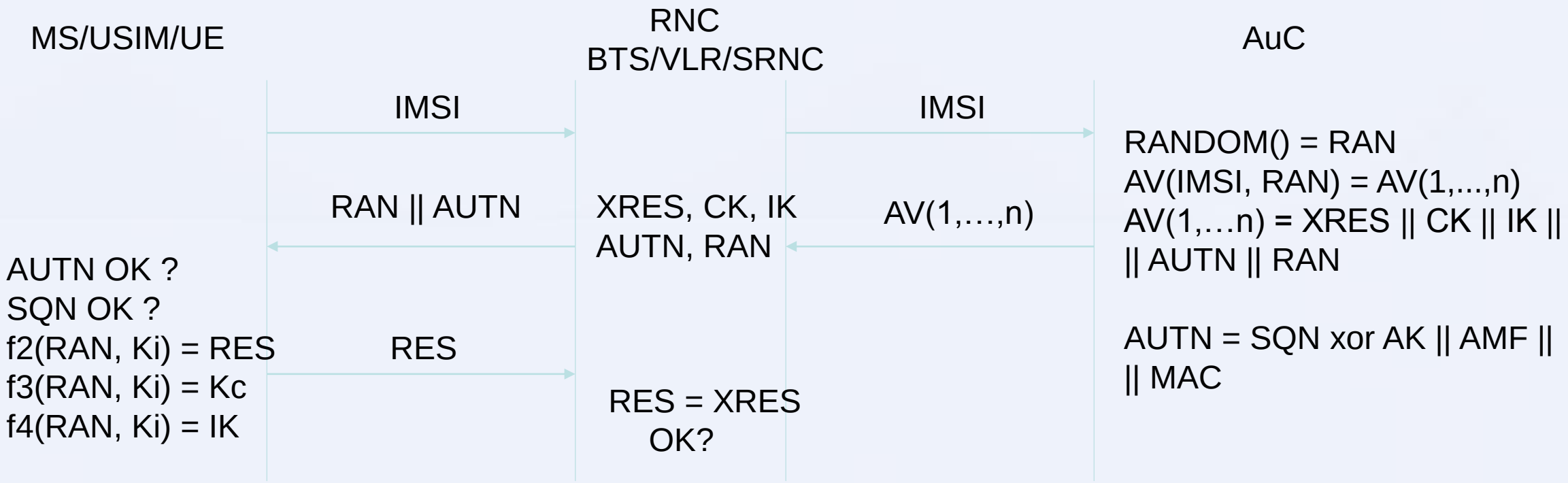
Progres

- Analýza protokolov, autentifikácia

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) = Kc
f4(RAN, Ki) = IK
RES
RES = XRES
OK?
AUTN = SQN xor AK || AMF ||
|| MAC

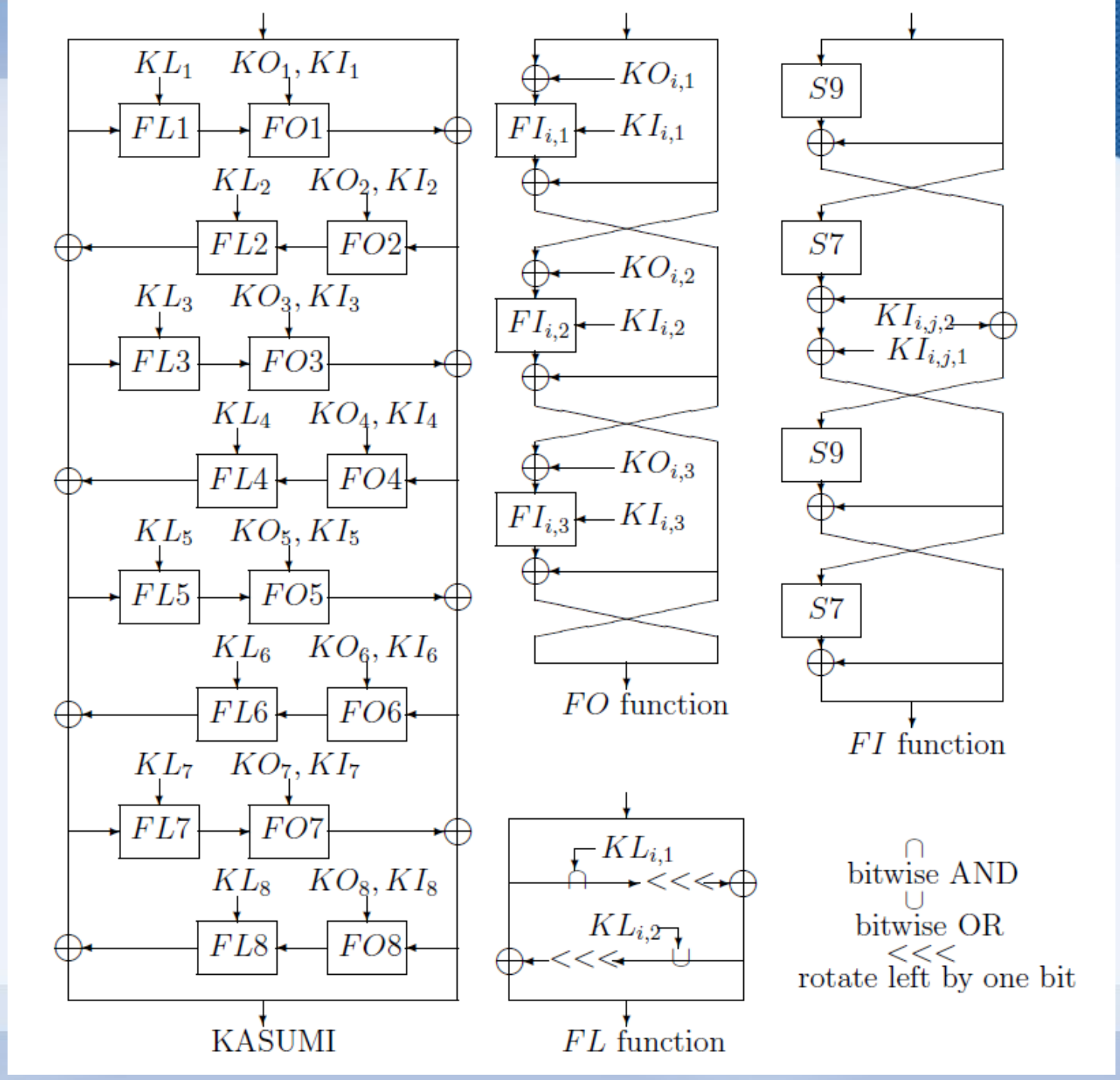
3G a LTE

Fukncia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	…	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na karte – zdieľaný	Žiadny	USIM, AuC		128

Progres

- Analýza protokolov, autentifikácia
- Prvotná analýza KASUMI

Zdroj:
Orr Dunkleman:
Techniques for Cryptanalysis of Block Ciphers
Zatiaľ nepublikované, PhD. práca



Zdroj:
Orr Dunkleman:
Techniques for Cryptanalysis of Block Ciphers
Zatiaľ nepublikované, PhD. práca

Round	$KL_{i,1}$	$KL_{i,2}$	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$
1	$K_1 \lll 1$	K'_3	$K_2 \lll 5$	$K_6 \lll 8$	$K_7 \lll 13$	K'_5	K'_4	K'_8
2	$K_2 \lll 1$	K'_4	$K_3 \lll 5$	$K_7 \lll 8$	$K_8 \lll 13$	K'_6	K'_5	K'_1
3	$K_3 \lll 1$	K'_5	$K_4 \lll 5$	$K_8 \lll 8$	$K_1 \lll 13$	K'_7	K'_6	K'_2
4	$K_4 \lll 1$	K'_6	$K_5 \lll 5$	$K_1 \lll 8$	$K_2 \lll 13$	K'_8	K'_7	K'_3
5	$K_5 \lll 1$	K'_7	$K_6 \lll 5$	$K_2 \lll 8$	$K_3 \lll 13$	K'_1	K'_8	K'_4
6	$K_6 \lll 1$	K'_8	$K_7 \lll 5$	$K_3 \lll 8$	$K_4 \lll 13$	K'_2	K'_1	K'_5
7	$K_7 \lll 1$	K'_1	$K_8 \lll 5$	$K_4 \lll 8$	$K_5 \lll 13$	K'_3	K'_2	K'_6
8	$K_8 \lll 1$	K'_2	$K_1 \lll 5$	$K_5 \lll 8$	$K_6 \lll 13$	K'_4	K'_3	K'_7

$X \lll i$ — X rotated to the left by i bits

Table C.3: KASUMI's Key Schedule Algorithm
KASUMI ly zegztnd izz aeyig mzixebl‘

Round	1	2	3	4	5	6	7	8
Constant	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
Value	0123_x	4567_x	$89AB_x$	$CDEF_x$	$FEDC_x$	$BA98_x$	7654_x	3210_x

Table C.4: KASUMI's Key Schedule Constants
KASUMI ly zegztnd izz aeyig mzixebl‘ yeniyay mireawd

Progres

- Analýza protokolov, autentifikácia
- Prvotná analýza KASUMI
- Štúdium útoku: 50 %

Plány do budúcnosti

- Predviesť útok na šifru používanú v A5/1 a A5/2
  - Menšie implementačné problémy
- Preskúmať útoky na šifru SNOW3G (a šifru samotnú)
- Štatistické útoky

Literatúra

- E. Biham, O. Dunkelman: Techniques for Cryptanalysis of Block Ciphers (Information Security and Cryptography), Springer, 2017, ISBN 978-3642172311
- W. Stallings: Cryptography and Network Security: Principles and Practice, 7th edition, Pearson, 2016, ISBN 978-0134444284
- A. G. H. Naim: Cryptanalysis of Some Block Ciphers, PhD. thesis, University of London, 2014

Literatúra

- O. Dunkelman, N. Keller: Practical-time attacks against reduced variants of MISTY1. Designs, Codes and Cryptography, 2015, 76.3: 601-627, ISSN: 0925-1022
- YI. Wentan, S. Chen: Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI. arXiv preprint arXiv:1404.6100, 2014.
- O. Dunkelman, N. Keller, A. Shamir: A practical-time related-key attack on the kasumi cryptosystem used in GSM and 3G telephony. Journal of Cryptology, 2014, 27.4: 824-849. ISSN: 0933-2790

Ďakujem za pozornosť.