Aalto University
School of Science

AE in Radio Standards

Kaisa Nyberg

Aalto University, School of Science
Department of Information and Computer Science
and
Nokia Research Center
Finland

July 2012

Mobile Algorithms

- GSM
  - A5/1
  - A5/3 (Kasumi-based)
- UMTS
  - UEA1 and UIA1 both Kasumi-based
  - UEA2 Snow 3G and UIA2 Galois MAC
- LTE
  - EEA1 and EIA1 same as UEA2 and UIA2
  - EEA2 and EIA2 AES CTR and AES-CBC-MAC
  - EEA3 ZUC and EIA3 Universal hash-function

Specifications available at:

`http://www.gsma.com/technicalprojects/fraud-security/security-algorithms/`

Most Used AE Algorithm ?

- IEEE 802.11 WLAN: AES CCM
- IEEE 802.15.1 (Bluetooth): E0 encryption only
- IEEE 802.15.3: AES CCM
- IEEE 802.15.4: AES CCM
- ECMA-368 Wireless USB: AES CCM
- BTLE (Bluetooth Low Energy): AES CCM

Scope of AE

System	Unprotected	Authenticated	Encrypted	Encrypted and authenticated
GSM	Stealing flags		User data Ctrl data	
UMTS	MAC hdrs Flow ctrl		User data	RRC cmds
WLAN	MAC hdrs Flow ctrl MAC cmds	MAC hdrs of data PDUs		SDUs
Bluetooth	Packet hdrs Flow ctrl		User data LMP cmds L2CAP ctrl	
IEEE 802.15.3		MAC hdrs Flow ctrl MAC cmds		SDUs
IEEE 802.15.4		MAC hdrs Flow ctrl		SDUs MAC cmds Beacon pld

Table 6.4: Scope of encryption and authentication

Integrity of Signaling

- UMTS: RRC signaling encrypted and authenticated
  to protect against call hijacking.
  Recall that GSM has only encryption of call frames.
- IEEE 802.15 have integrity-protected secure frame counters.
  to prevent replay attacks

Threat of Repeating Nonce ?

System	Channel	Counter	Direction	Counter skew prevention	Other
GSM	Physical layer TDMA frame #		Split key-stream	—	—
UMTS	Bearer ID	Packet #	Input to *f8* & *f9*	FRESH (*f9* only)	—
WLAN	Priority	Packet #	Trnsmtr addr	—	—
Bluetooth	—	Master's clock		—	Master's addr
IEEE 802.15.3	—	Superfrm #, Packet #, Frag ctrl	Src ID, Dest ID	—	—
IEEE 802.15.4	—	Key #, Packet #	Src addr	—	—

Table 6.2: Additional inputs to data protection functions

Additonal Requirements

Pseudo-random Function

- PANs and WANs do link layer session key derivation

$\Rightarrow$ Pseudorandom function primitive

Error Correction

- How to combine error correction and integrity?

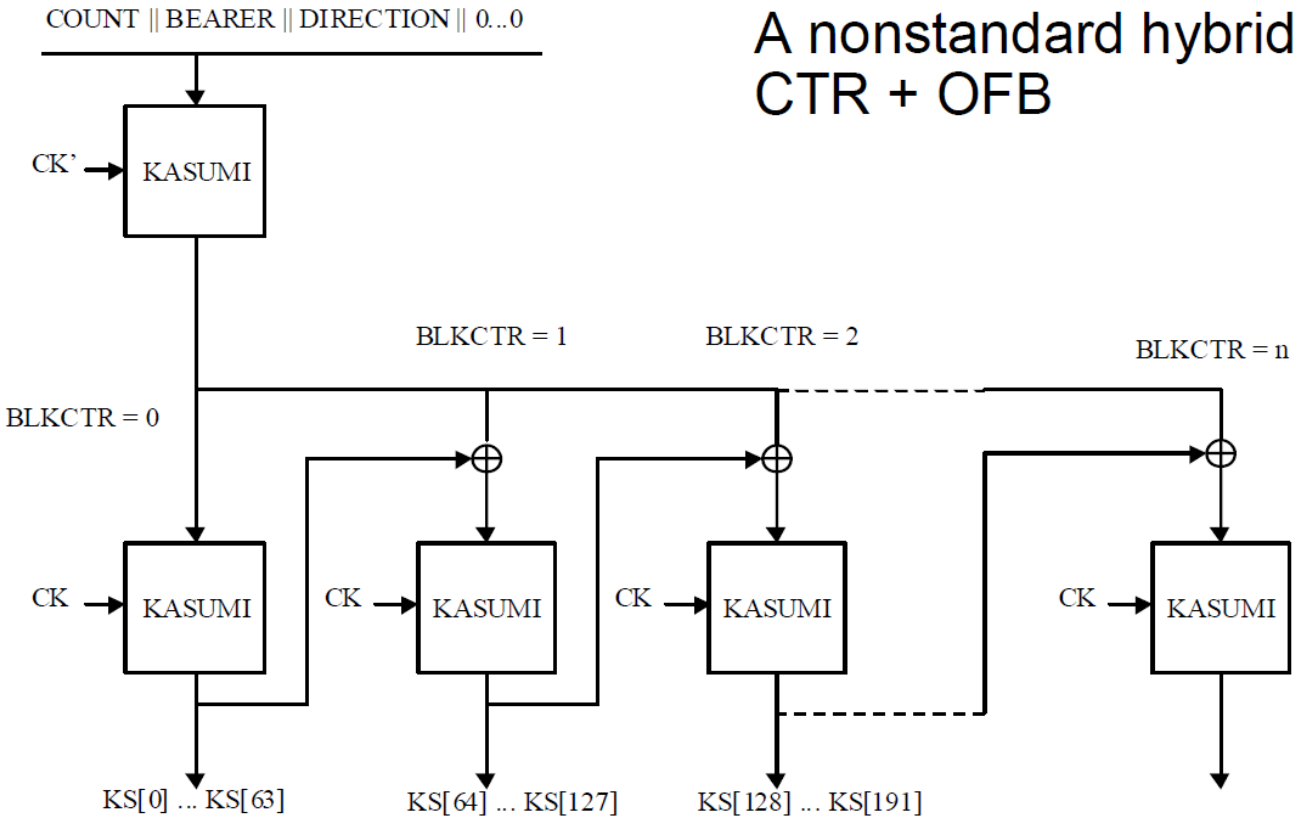
Design Strategies

CTR Mode

"We know more about ciphers in 2012 than we did in 1998. Can we obtain better speeds by replacing AES with another block cipher?"

- Adopted as the design strategy of the first UMTS f8: CTR mode enforced with CBC coupling and a special purpose block cipher
- But, beware of the Big Bad Cryptanalyst who wants to analyze the block cipher as a stand-alone primitive

UMTS Encryption algorithm f8



A nonstandard hybrid mode:
CTR + OFB

Dedicated Stream Cipher

"We know more about ciphers in 2012 than we did in 1998. Can we obtain better speeds by replacing AES-CTR with another stream cipher?"

- Adopted as the design strategy of the second UMTS f8: Snow 3G
- But, beware of the Big Bad Authority who wants the AES to be used everywhere
  $\Rightarrow$ LTE adopted AES CCM

Acknowledgements

The Master's thesis of my student Kaarle Ritvanen

Protection of Data Confidentiality and Integrity in Radio Communication Systems
Helsinki University of Technology (2004)

was very useful when preparing this presentation.

Also many thanks to Steve Babbage for useful discussions.