S3-000326

On the Security of 3GPP Networks

Michael Walker

Vodafone AirTouch & Royal Holloway,
University of London

Chairman 3GPP SA3 - Security

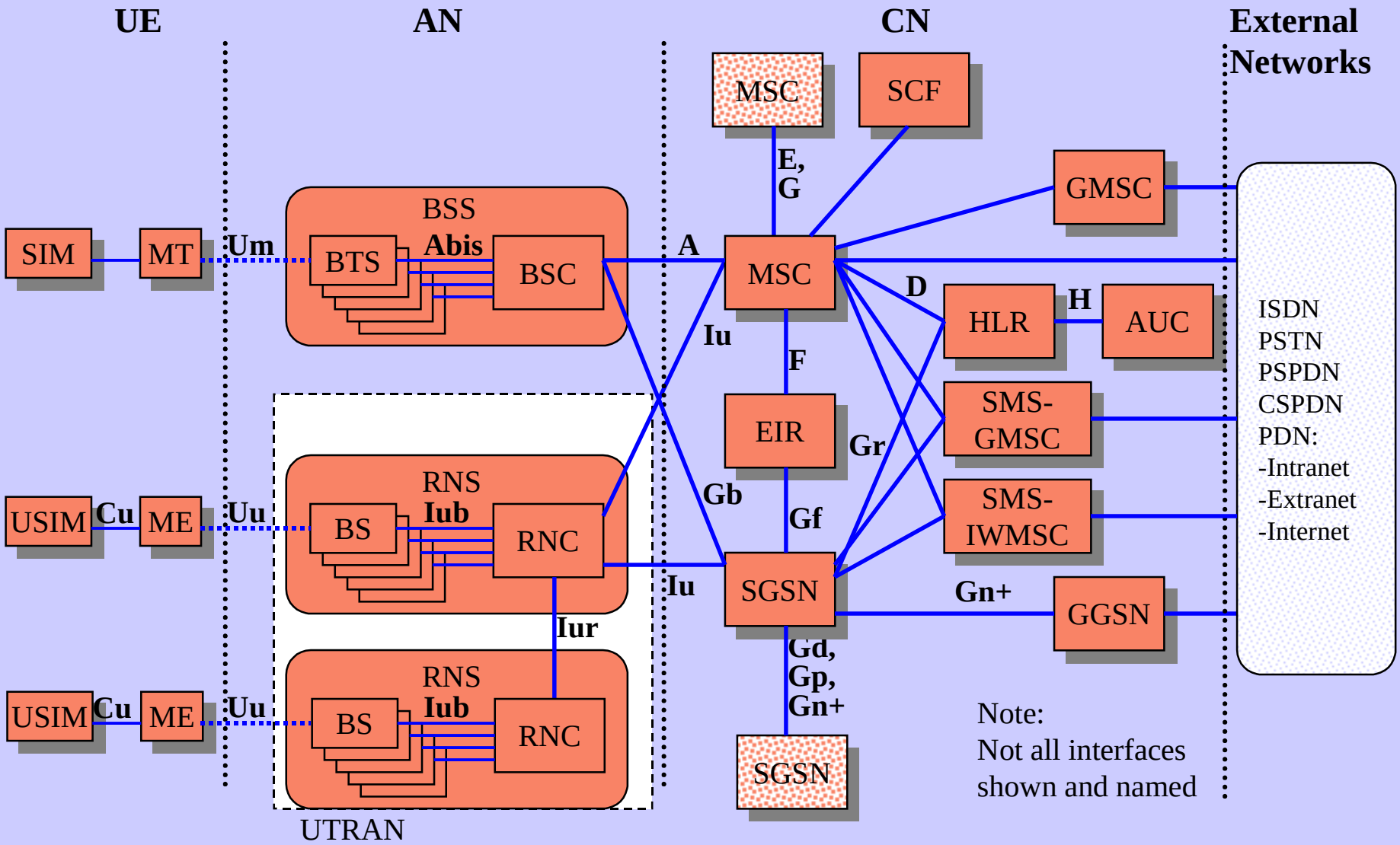
Acknowledgements

- This presentation is based on the technical specifications and reports produced by the members of 3GPP SA3 and ETSI SAGE
  - available from http://www.3gpp.org
- Much of the back ground work was done as part of the EU funded ACTS project USECA
  - the partners are Vodafone, G&D, Panasonic, Siemens Atea, Siemens AG & Katholieke Universiteit Leuven
  - http://www.useca.freeserve.co.uk

Principles for 3G Security

- Build on the security of GSM
  - adopt the security features from GSM that have proved to be needed and robust
  - try to ensure compatibility with GSM in order to ease inter-working and handover
- Correct the problems with GSM by addressing its real and perceived security weaknesses
- Add new security features
  - as are necessary to secure new services offered by 3G
  - to take account of changes in network architecture

Building on GSM Security - Architecture



Building on GSM Security, 2

- Remain compatible with GSM network architecture
- User authentication & radio interface encryption
- SIM used as security module
  - removable hardware
  - terminal independent
  - management of all customer parameters
- Operates without user assistance
- Requires minimal trust in serving network

Limitations of GSM Security

- Problems with GSM security stem by and large from design limitations on what is protected rather than on defects in the security mechanisms themselves
  - only provides *access security* - communications and signalling in the fixed network portion aren't protected
  - does not address *active attacks*, whereby network elements may be impersonated
  - designed to be only as secure as the fixed networks to which they connect
  - lawful interception only considered as an after thought

Limitations of GSM Security, 2

- Failure to acknowledge limitations
  - encryption needed to guard against radio channel hijack
  - the terminal is an unsecured environment - so trust in the terminal identity is misplaced
- Inadequate flexibility to upgrade and improve security functions over time
- Lack of visibility that the security is being applied
  - no indication to the user that encryption is on
  - no explicit confirmation to the home network that authentication is properly used when customers roam

Limitations of GSM Security, 3

- Lack of confidence in cryptographic algorithms
  - lack of openness in design and publication of A5/1
  - misplaced belief by regulators in the effectiveness of controls on the export or (in some countries) the use of cryptography
  - key length too short, but some implementation faults make increase of encryption key length difficult
  - need to replace A5/1, but poor design of support for simultaneous use of more than one encryption algorithm, is making replacement difficult
  - ill advised use of COMP 128

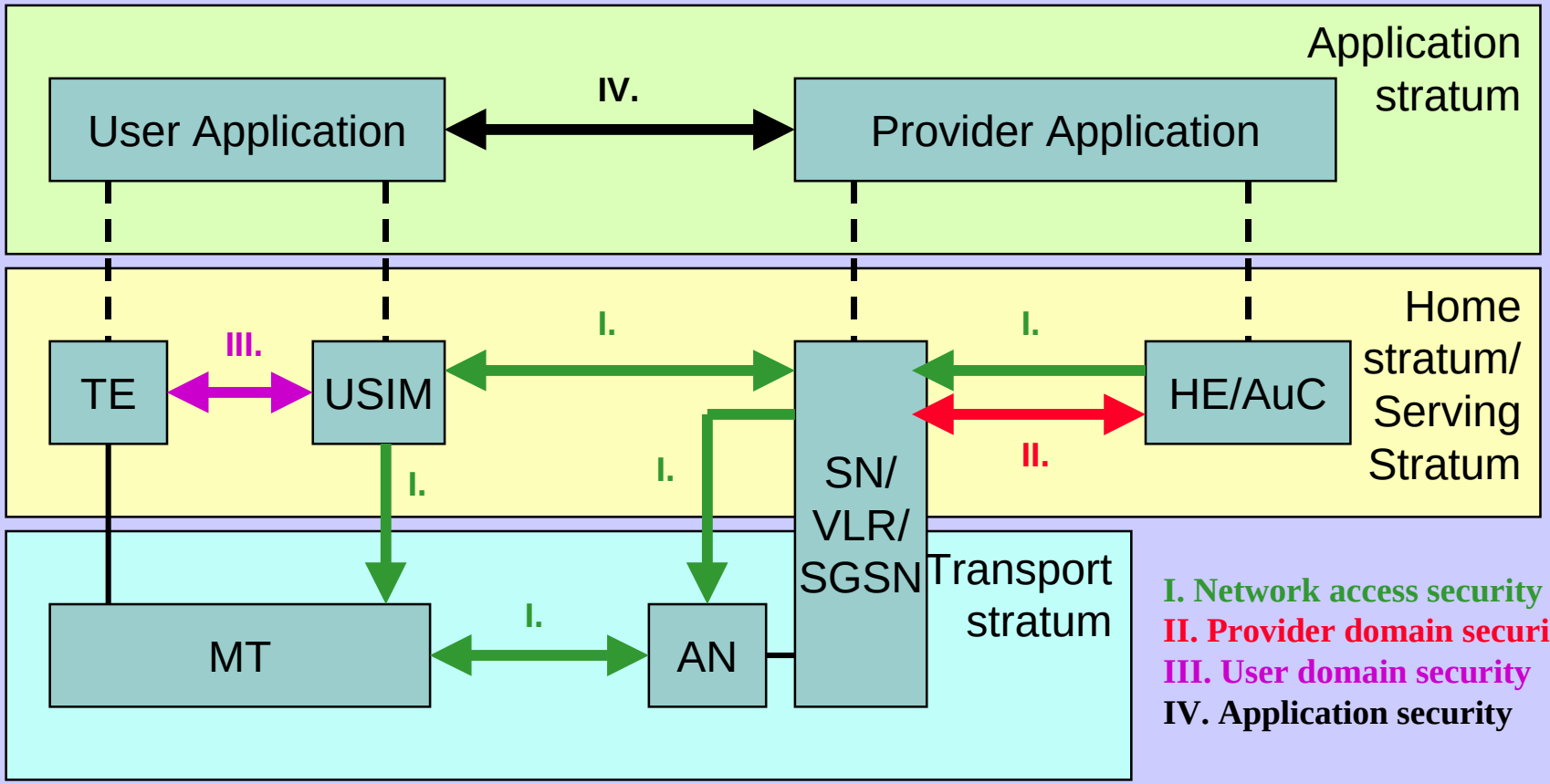
Specific GSM Security Problems

- Encryption terminated too soon
  - user traffic and signalling in clear on microwave links
- Clear transmission of cipher keys & authentication values within and between networks
  - signalling system vulnerable to interception and impersonation
- Confidence in strength of algorithms
  - failure to choose best authentication algorithms
  - improvements in cryptanalysis of A5/1
- Use of false base stations

False Base Stations

- Used as *IMSI Catcher* for law enforcement
- Used to intercept mobile originated calls
  - encryption controlled by network and user unaware if it is not on
- Dynamic cloning risk in networks where encryption is not used

3GPP Security Architecture Overview



Authentication & Key Agreement (AKA) Protocol Objectives

- Authenticate user to network & network to user
- Establish a cipher key CK (128 bit) & an integrity key IK (128 bit)
- Assure user and network that CK/IK have not been used before
- Authenticated management field HE $\rightarrow$ USIM
  - authentication key and algorithm identifiers
  - limit CK/IK usage before USIM triggers a new AKA

AKA Prerequisites

- AuC and USIM share
  - user specific secret key K
  - message authentication functions f1, f1*, f2
  - key generating functions f3, f4, f5
- AuC has a random number generator
- AuC has scheme to generate fresh sequence numbers
- USIM has scheme to verify freshness of received sequence numbers

AKA Variables and Functions

RAND = random challenge generated by AuC

XRES = $f2_K$ (RAND) = expected user response computed by AuC

RES = $f2_K$ (RAND) = actual user response computed by USIM

CK = $f3_K$ (RAND) = cipher key

IK = $f4_K$ (RAND) = integrity key

AK = $f5_K$ (RAND) = anonymity key

SQN = sequence number

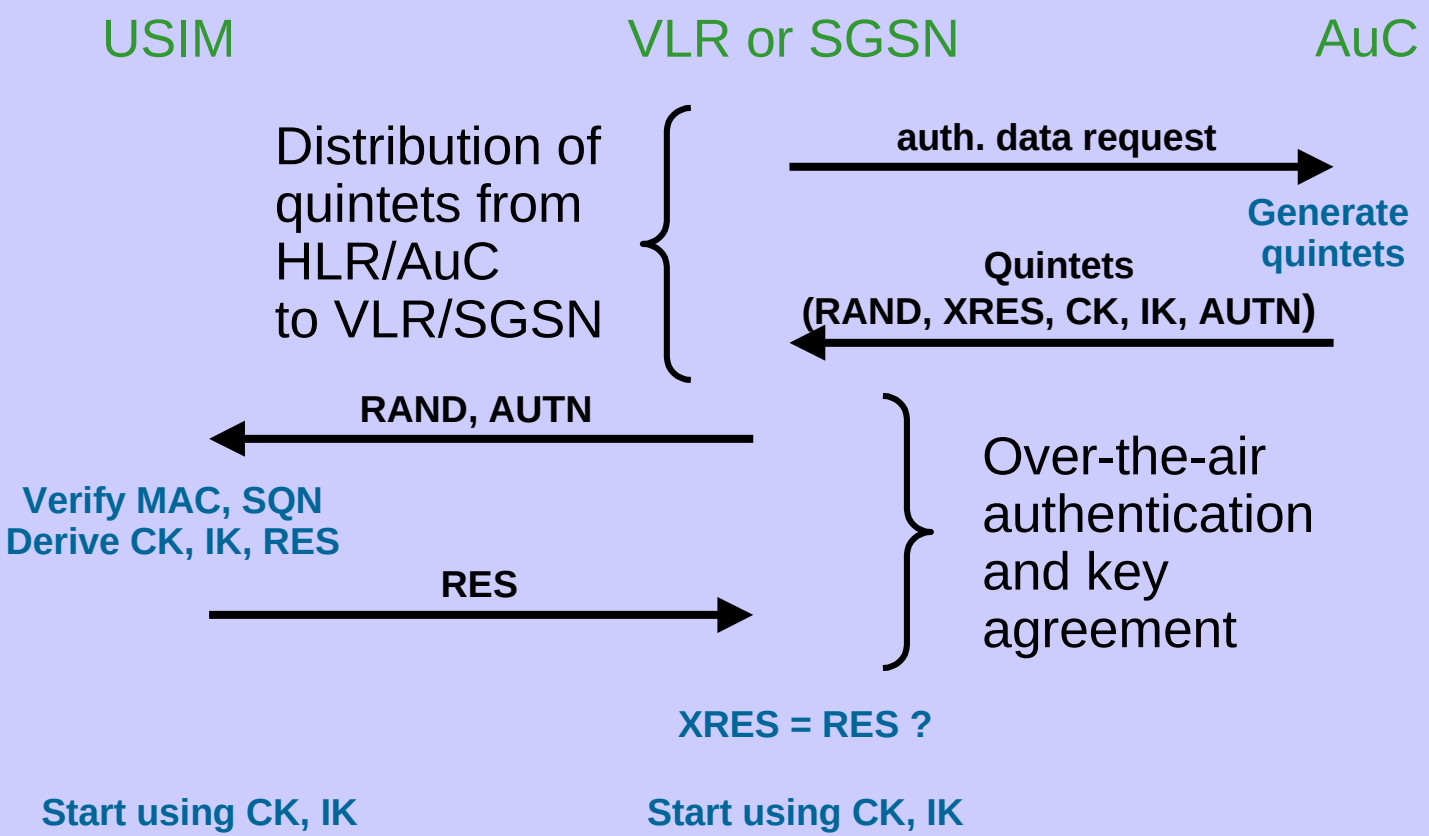
AMF = authentication management field

MAC = $f1_K$(SQN || RAND || AMF) = message authentication code computed over SQN, RAND and AMF

AUTN = SQN⊕AK || AMF || MAC = network authentication token, concealment of SQN with AK is optional

Quintet = (RAND, XRES, CK, IK, AUTN)

AKA Message Flow

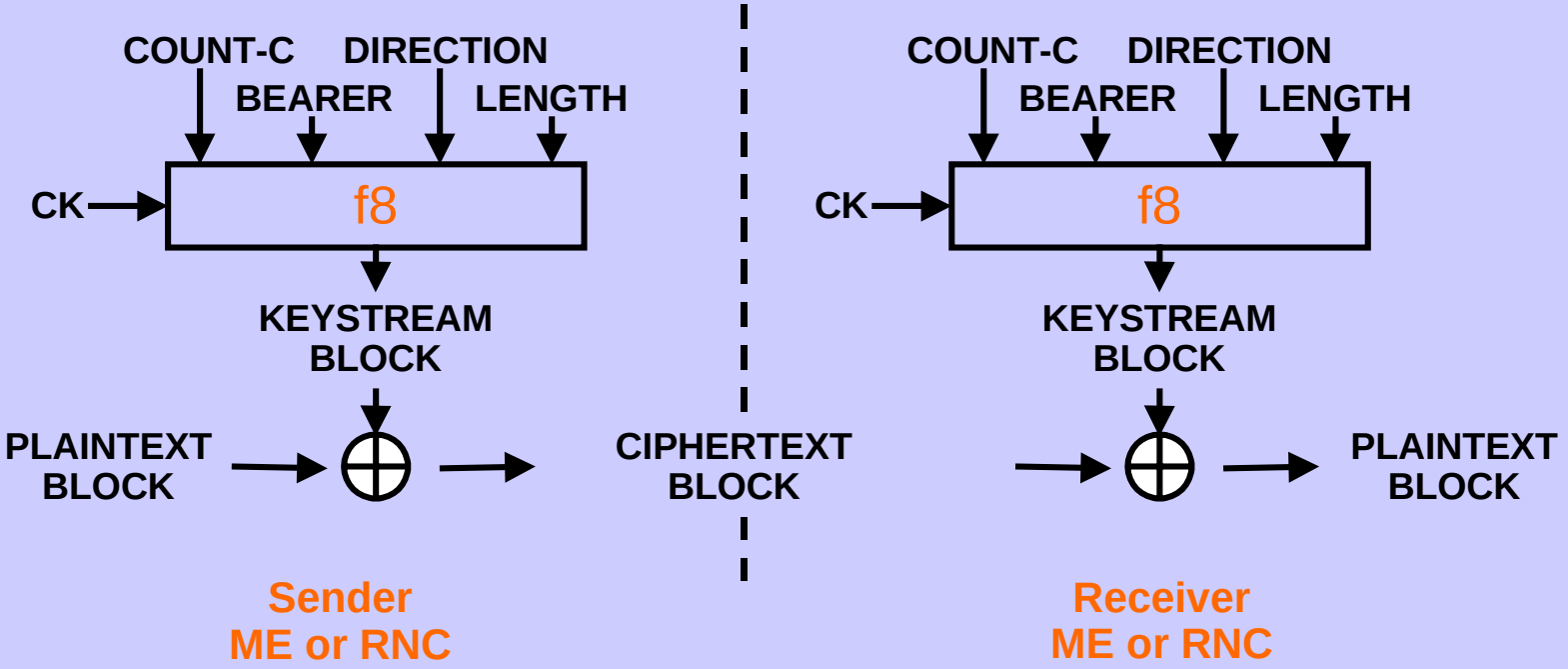


Length of AKA Cryptographic Parameters

- K 128 bits
- RAND 128 bits
- RES 32-128 bits
- CK 128 bits
- IK 128 bits
- AUTN 128 bits
  - SQN Sequence number 48 bits
  - AMF Authentication management field 16 bits
  - MAC Message authentication code 64 bits

Air-interface Encryption, 1

- Applies to all user traffic and signalling messages
- Uses stream ciphering function f8 - with provision for different algorithms: UEA1 = Kasumi; UEA0 = no encryption

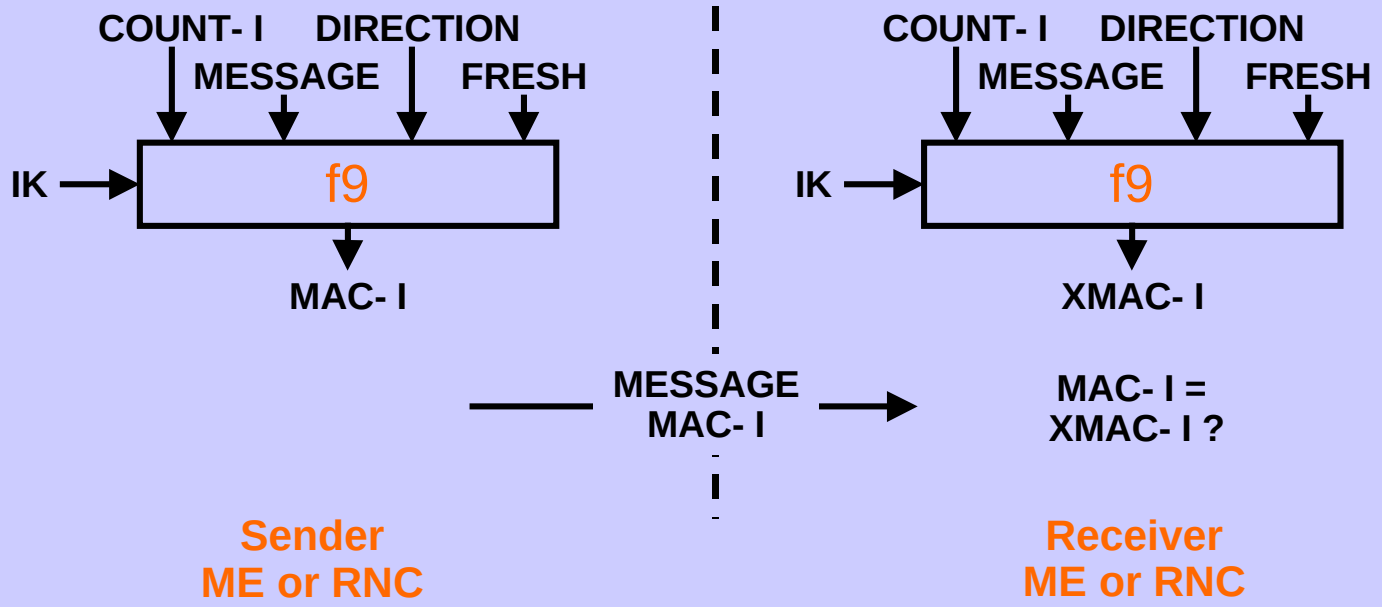


Air-interface Encryption, 2

- Termination points
  - user side: mobile equipment, network side: radio network controller
- Ciphering in layer 2
  - RLC sublayer — non-transparent RLC mode — (signalling, data)
  - MAC sublayer — transparent RLC mode — (voice)
- Key input values to algorithm
  - CK — 128 bits — Cipher key
  - COUNT-C — 32 bits — Ciphering sequence number
    - RLC sublayer — HFN_{RLC} (25/20)+ SN_{RLC} (7/12) — (SN_{RLC} is transmitted)
    - MAC sublayer — HFN_{MAC} (25) + CFN_{MAC} (7) — (CFN_{MAC} is transmitted)
- Further input values
  - BEARER — 5 bits — Bearer identity
  - DIRECTION — 1 bit — Uplink/downlink
  - LENGTH — 16 bits — Length of keystream block

Air-interface Integrity Mechanism, 1

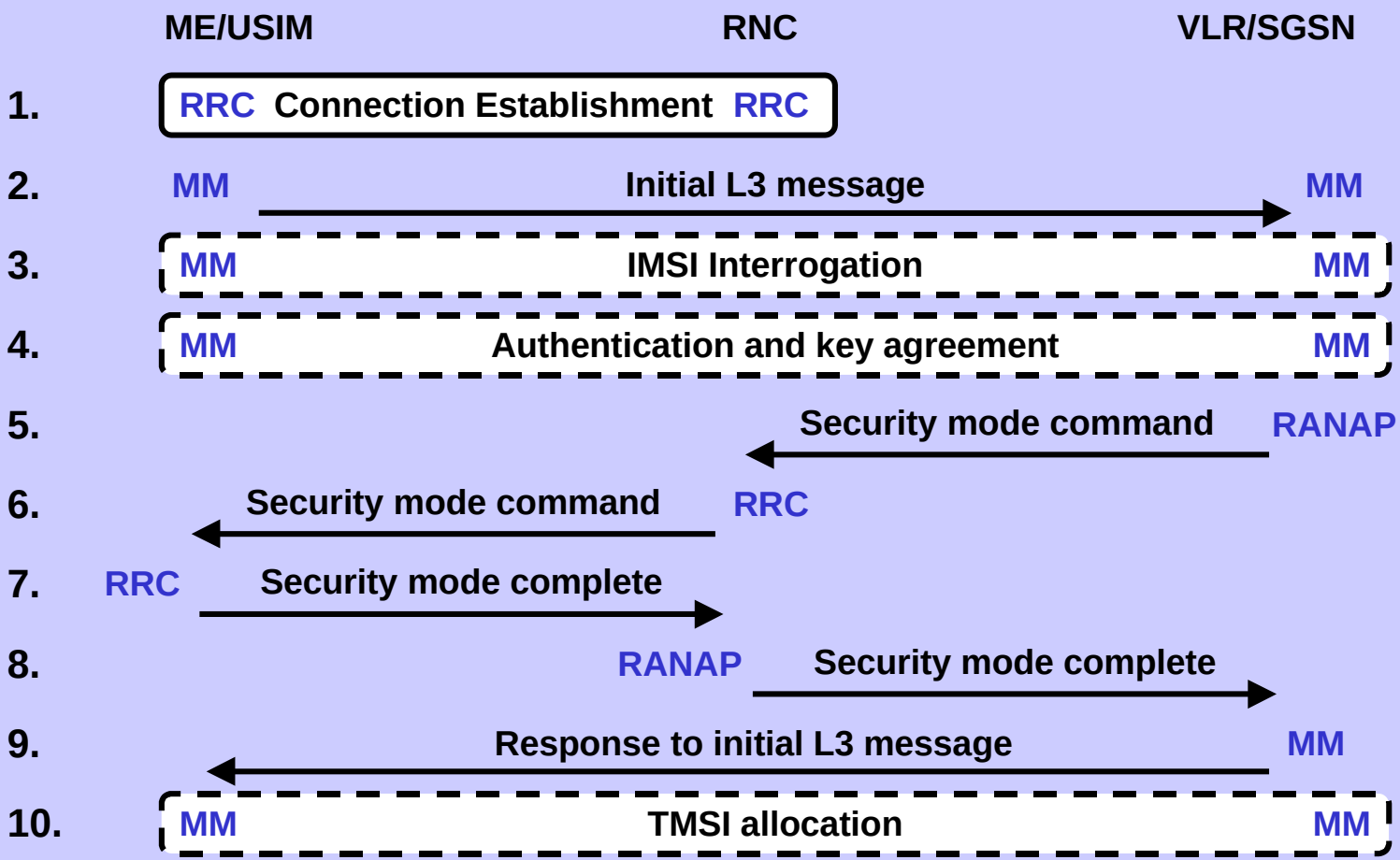
- Applies to all except a specifically excluded signalling messages after connection and security mode set-up
- MS supervises that it is started
- Uses integrity function f9 - with provision for different algorithms: UIA1 = Kasumi



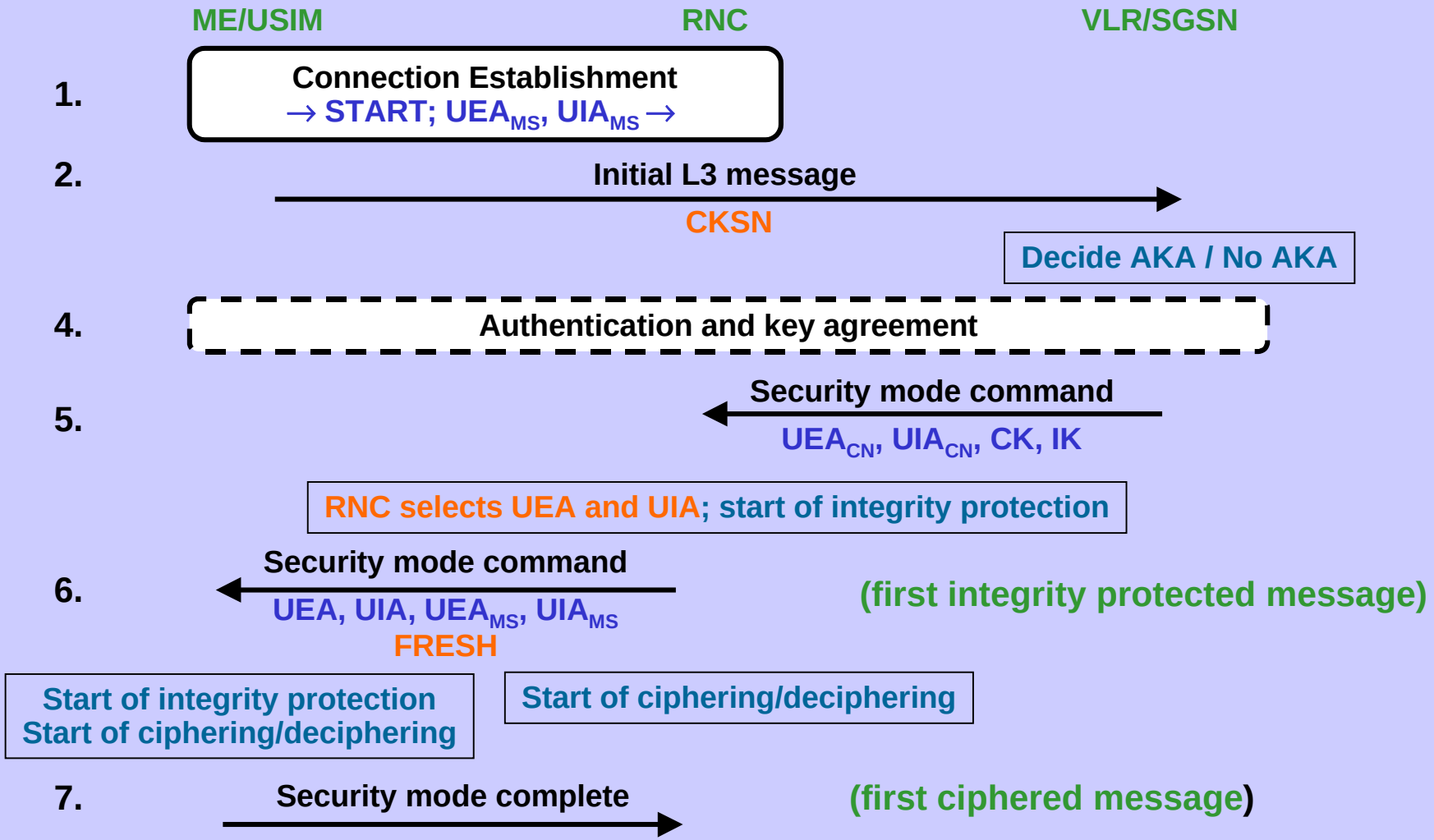
Air-interface Integrity Mechanism, 2

- Termination points
  - user side: mobile equipment, network side: radio network controller
- Integrity protection: layer 2
  - RRC sublayer
- Key input values
  - IK — 128 bits — Integrity key
  - COUNT-I — 32 bits — Integrity sequence number
    - consists of HFN_{RRC} (28) + SN_{RRC}(4) — (SN_{RRC} is transmitted)
  - FRESH — 32 bits — Connection nonce
  - MESSAGE — Signalling message
- Further input values
  - DIRECTION — 1 bit — Uplink/downlink
- Output values
  - MAC-I/XMAC-I — 32 bits — message authentication code

Connection Establishment Overview



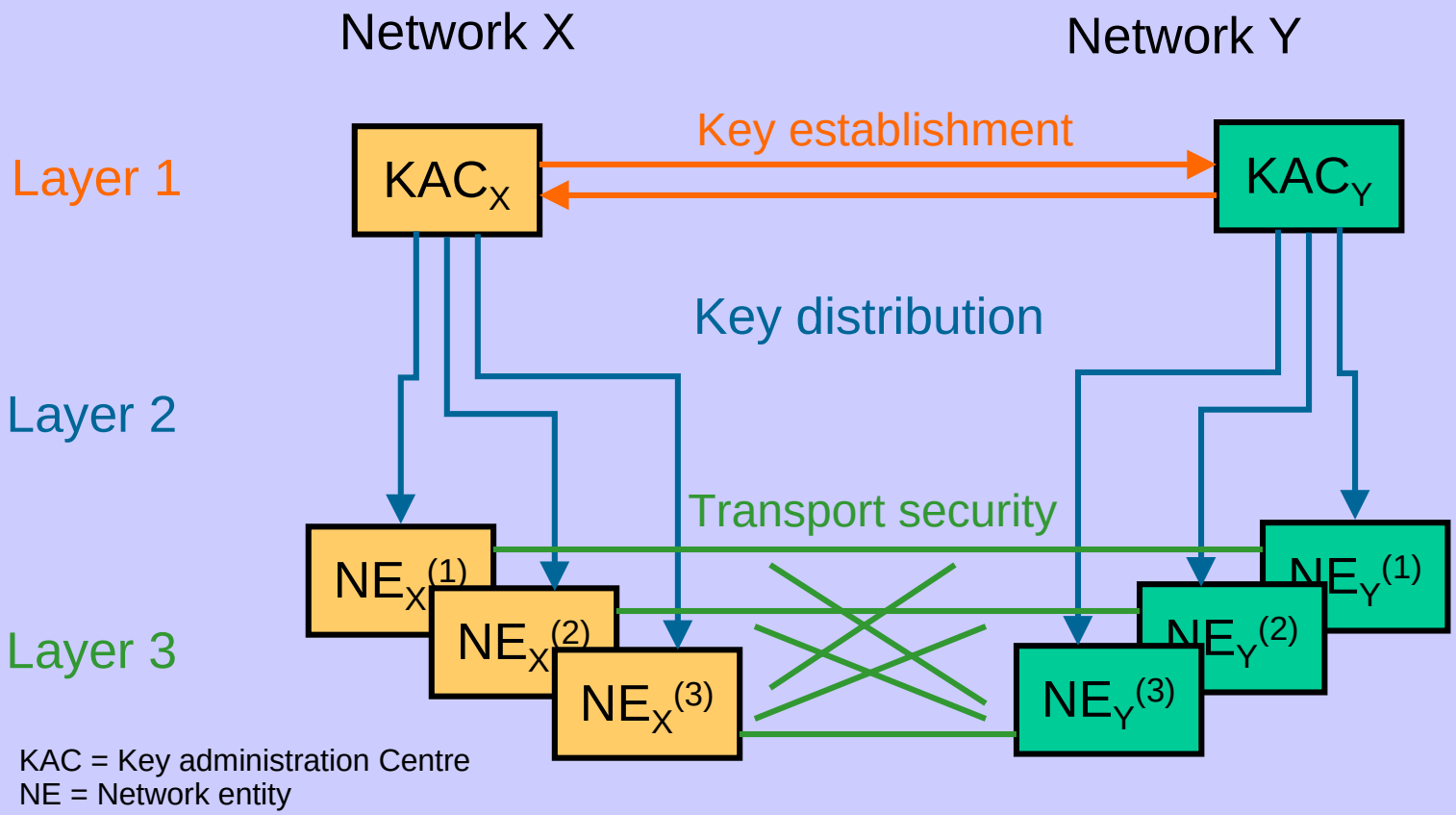
Starting Ciphering & Integrity



Security Parameters & Choices

- START(32bits) initial hyperframe number
  - used to initialise COUNT-C/I
  - assures user MAC-I is fresh
  - START stored/updated USIM
- CKSN(3 bits) cipher key sequence number
  - indicates the key set that is stored in USIM
  - when START exceeds a certain threshold, CKSN can be used to trigger a new AKA
- FRESH(32 bits) network nonce
  - assures network MAC-I fresh
- AKA is performed when
  - the user enters a new SN
  - the user indicates that a new AKA is required when the amount of data ciphered with CK has reached a threshold
  - the serving network decides
- Otherwise integrity-key based authentication
- Selection of UEA and UIA by user/user's home environment

Network Domain Security Overview



Network Security Features, 1

- Layer 1 - Key Establishment
  - KAC_X generates and stores asymmetric key pair for X, and stores public keys from other networks - exchanged as part of roaming agreement
  - generates, stores and distributes symmetric session keys for securing information sent from entities in X
  - receives and distributes symmetric session keys for securing information sent from other networks
- Session key transport to ISO/IEC 11770-3: *Key Management - mechanisms using symmetric techniques*

Network Security Features, 2

- Layer 2 - Key Distribution
  - KAC_X distributes session keys to nodes in X
- Layer 3 - Transport Security
  - MAP signalling provided with encryption, origin authentication and integrity using standard symmetric techniques
  - Protection limited to *new messages* in R'99 - includes authentication quintets
  - Block cipher BEANO designed by ETSI SAGE for public network operators may be used

Encryption & Integrity Algorithm Requirements

- Stream cipher f8 and integrity function f9 - parameters already described
- Low power, low gate-count hardware, as well as software
- No practical attack significantly more efficient than exhaustive key search
- No export restrictions on terminals (or SIMs); network equipment exportable under licence in accordance with Wassenaar
- Time for development - six months!

General Approach to Design

- Robust approach to exportability - full strength algorithm and expect agencies to fall into line
- ETSI SAGE appointed as design authority
- Take existing algorithm as starting point
- Use block cipher as building block for both algorithms - MISTY1 chosen:
  - fairly well studied, some provable security aspects
  - parameter sizes suitable
  - designed to be efficient in hardware and software
  - offered by Mitsubishi free from royalty payments

Design and Analysis

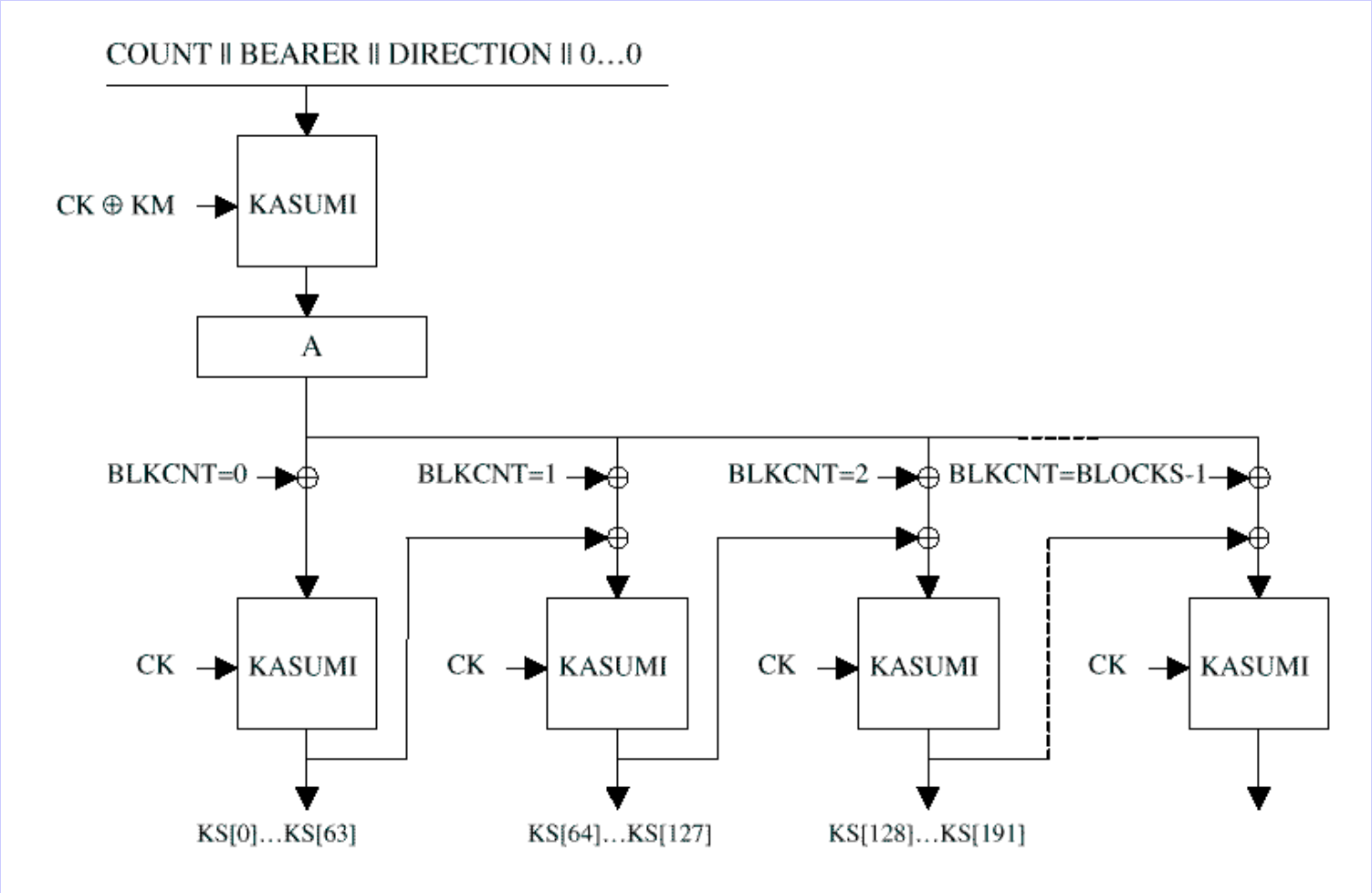
- Designed by SAGE team, led by Gert Roelofsen with external experts:
  - SAGE design and evaluation teams
  - joined by Mitsuru Matsui from Mitsubishi - designer of MISTY
  - additional evaluators from Nokia, Ericsson and Motorola led by Kaisa Nyberg
- External evaluation by three teams:
  - Leuven: Lars Knudsen, Bart Preneel, Vincent Rijmen, Johan Borst, Matt Robshaw
  - Ecole Normale Superiere: Jacques Stern, Serge Vaudenay
  - Royal Holloway: Fred Piper, Sean Murphy, Peter Wild, Simon Blackburn
- Open Publication - back on ETSI web site again in June?

Kasumi

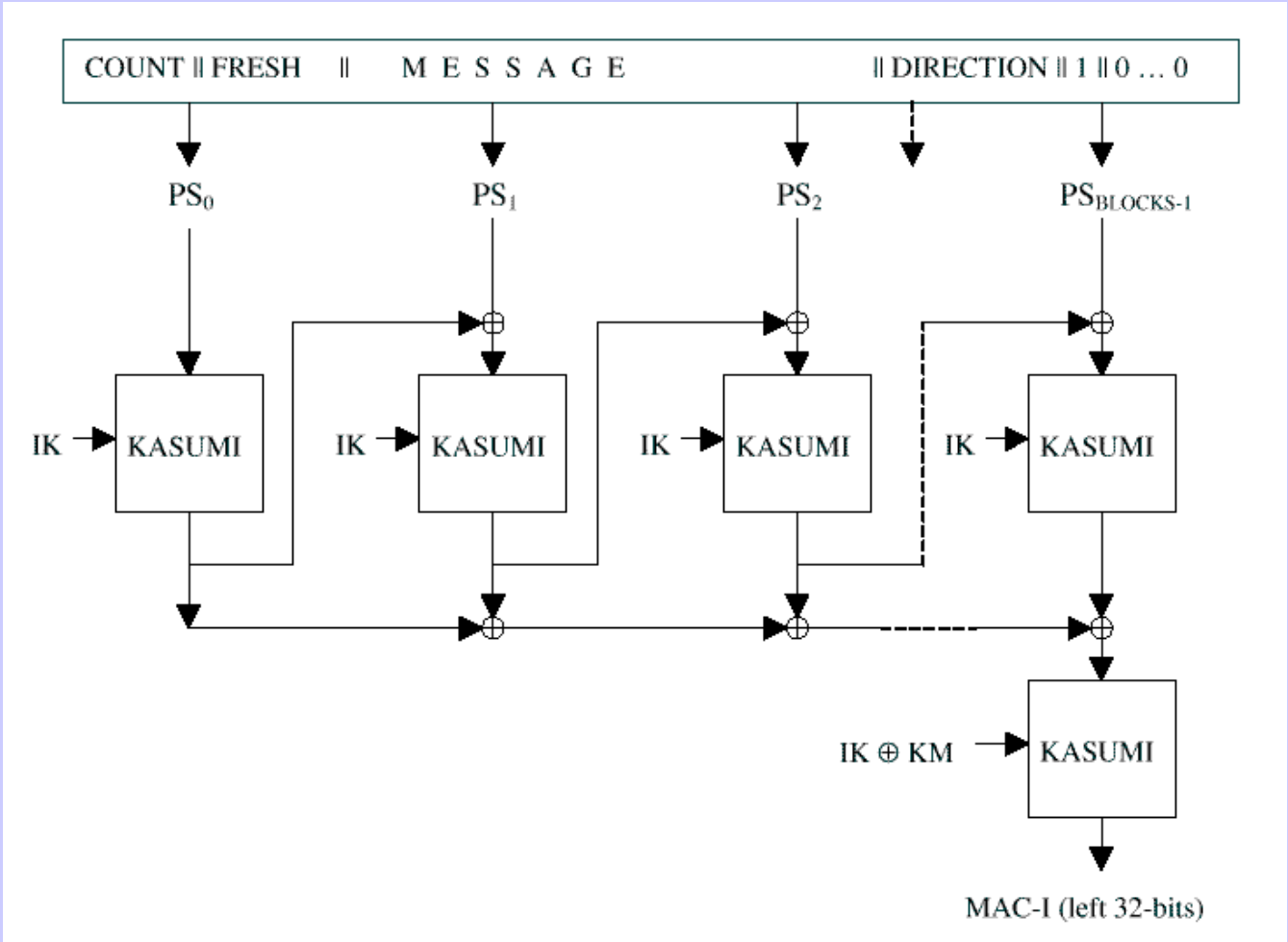
- Simpler key schedule than MISTY
- Additional functions to *complicate* cryptanalysis without affecting provable security aspects
- Changes to improve statistical properties
- Minor changes to speed up or simplify hardware

- Stream ciphering f8 uses Kasumi in a form of output feedback, but with:
  - BLKCNT added to prevent cycling
  - initial extra encryption added to protect against chosen plaintext attack and collisions
- Integrity f9 uses Kasumi to form CBC MAC with:
  - non-standard addition of 2nd feedforward

3GPP Stream Cipher f8



3GPP Integrity Function f9



Other Aspects of 3GPP Security

- Options in AKA for sequence management
- Re-authentication during a connection and periodic in-call
- Failure procedures
- Interoperation with GSM
- AKA+ and interoperation with 3GPP2 standards
- Formal analysis of AKA
- User identity confidentiality and enhanced user identity confidentiality (R00)
- User configurability and visibility of security features
- User-USIM, USIM-terminal & USIM - network (SAT)
- Terminal (identity) security
- Lawful interception
- Fraud information gathering
- Network wide encryption (R00)
- Location services security
- Access to user profiles
- Mobile IP security (R00+)
- Provision of a standard authentication and key generation algorithm for operators who do not wish to produce their own

References to 3GPP Security

Principles, objectives and requirements

- TS 33.120 Security principles and objectives
- TS 21.133 Security threats and requirements

Architecture, mechanisms and algorithms

- TS 33.102 Security architecture
- TS 33.103 Integration guidelines
- TS 33.105 Cryptographic algorithm requirements
- TS 22.022 Personalisation of mobile equipment

Lawful interception

- TS 33.106 Lawful interception requirements
- TS 33.107 Lawful interception architecture and functions

Technical reports

- TR 33.900 A guide to 3G security
- TR 33.901 Criteria for cryptographic algorithm design process
- TR 33.902 Formal analysis of the 3G authentication protocol
- TR 33.908 General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms

Algorithm specifications

- Specification of the 3GPP confidentiality and integrity algorithms
  - Document 1: f8 & f9
  - Document 2: KASUMI
  - Document 3: implementors' test data
  - Document 4: design conformance test data