ECRYPT

Design and Analysis of Cryptographic Algorithms for Mobile Communication Systems

Henri Gilbert
Orange Labs
{firstname.lastname@orange-ftgroup.com}

orange

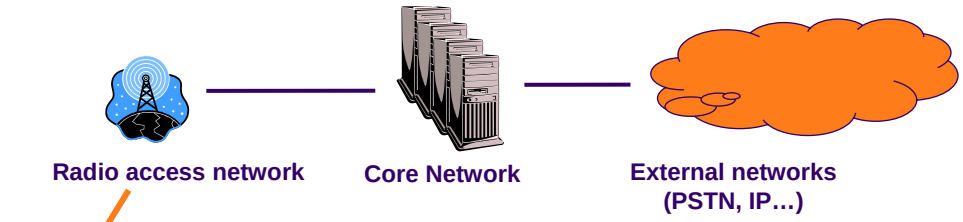
research & development

outline

development of cryptographic algorithms for a real life application

- **introduction**
  - cryptographic features of 2G and 3G systems
- **algorithms development process within ETSI/SAGE**
  - approach to design / specification / evaluation
  - links with academic research
- **case studies**
  - 1999: **KASUMI** block cipher + resulting encryption (**UEA1, A5/3**) and MAC (**UIA1**)
  - 2005: **SNOW 3G** stream cipher + resulting encryption (**UEA2**) and MAC (**UIA2**)

security in mobile systems



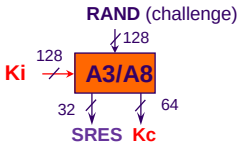
MS = ME + (U)SIM

security aspects:

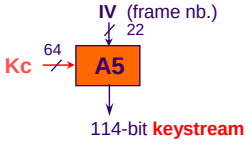
- **radio access**
- terminal
- core network
- e2e transactions

cryptographic algorithms of GSM

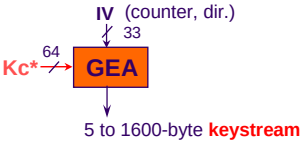
- **subscriber authentication**
  - authentication & key generation algorithms **A3/A8**
  - permanent subscriber key **Ki** (SIM & HLR)
  - **A3/A8 is not standardized** (operator dependent)

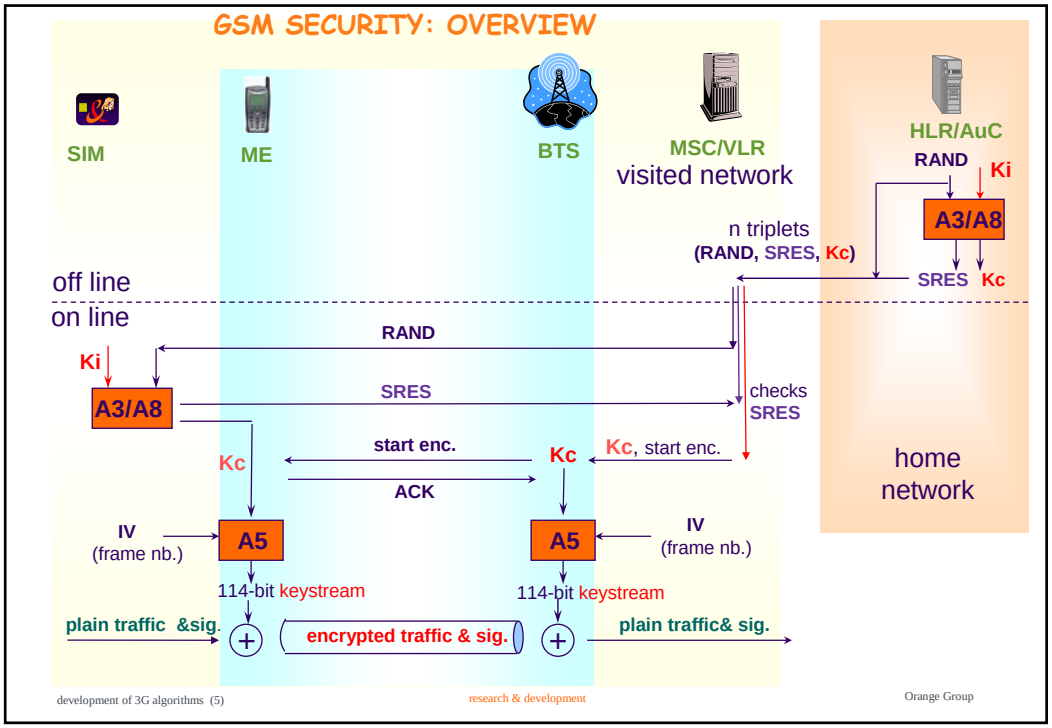


- **traffic and signalling encryption**
  - **circuit switched GSM:**
    standard **A5** algorithms **A5/1, A5/2, A5/3**



  - **packet oriented GSM (GPRS):**
    standard **GEA** algorithms **GEA1, GEA2, GEA3**





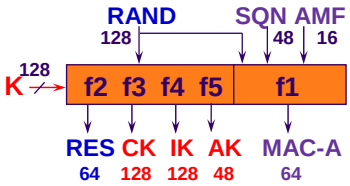
limitations of GSM security

- **no network authentication and no explicit integrity protection**
  - moreover encryption initiative is left up to the network
  - **eavesdropping attacks using false base stations** turned out to be a reality…
  - ⇒ UMTS: network authentication and signalling messages auth.
  - ⇒ GSM and UMTS: encryption indicator (in some mobiles)
- **limitations of GSM encryption**
  - encryption ends at the base station => **vulnerability of the BTS-BSC interface**
  - **efficient attack on A5/2, gradual erosion of the protection offered by A5/1** [Biham et al.]
  - ⇒ UMTS: strong encryption (128-bit key, hopefully full strength), ends at RNC
  - ⇒ GSM: move to A5/3 (derived from 3G algorithm KASUMI)

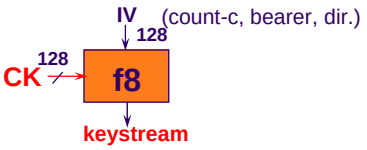
cryptographic features of UMTS

- **mutual authentication** (slightly simplified)
  - **subscriber auth.** ≈ GSM auth
  - **generation of session keys** CK and IK
  - **network auth.** ≈ MAC of sequence nb. SQN
  - SQN anonymization: mask AK

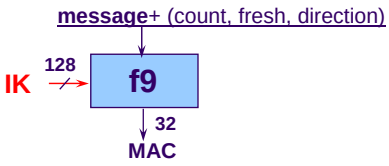
  f1-f5 also named AKA (auth. & key agreement)
  no standard AKA; example AKA: MILENAGE



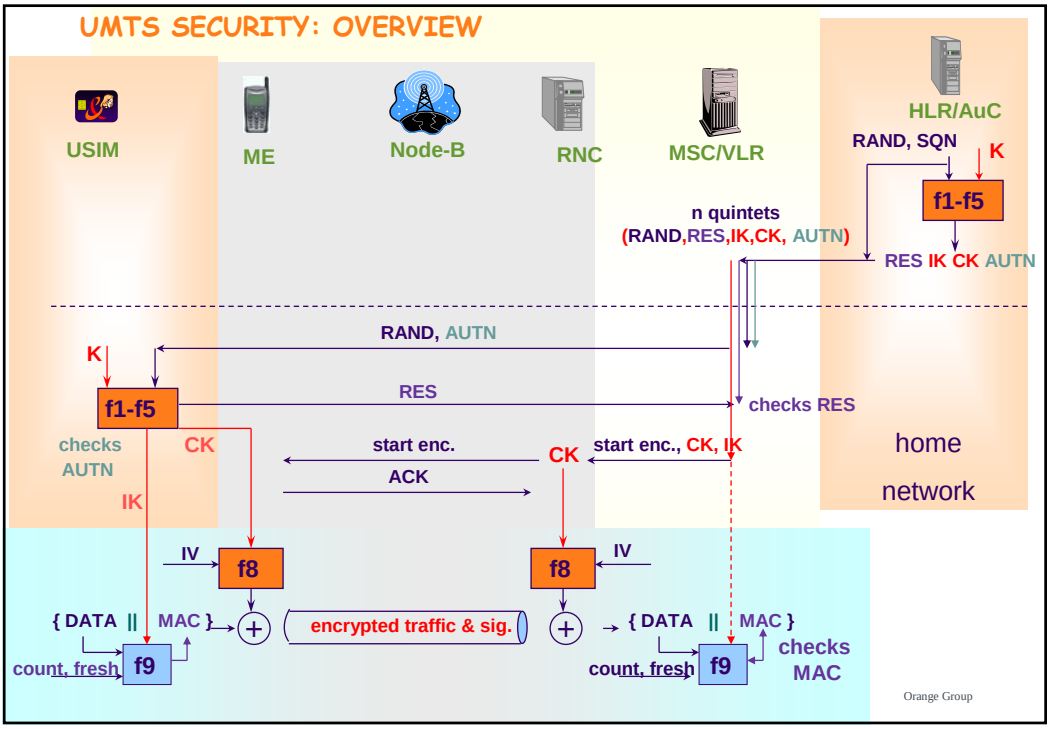
- **traffic and signalling encryption**
  - two standard **f8** algorithms
    - **UEA1** derived from **KASUMI**
    - **UEA2** derived from **SNOW 3G**



- **message authentication**
  - two standard **f9** algorithms
    - **UEA1** derived from **KASUMI**
    - **UEA2** derived from **SNOW 3G**



UMTS SECURITY: OVERVIEW



ETSI/SAGE

- **what's that?**
  - security algorithms group of experts of European Telecommunication Standard Institute
  - in charge of security algorithms standardisation for telecommunications
    - **mobile communication systems:** 2G (GSM/GPRS), 3G (UMTS) …
    - **other systems:** radio lans, teleconferencing, smart cards, inter-PNO exchanges, TETRA
  - created in the early 90's
  - initial mandate included liaison with national authorities to get export approval
- **membership**
  - **closed group:** no longer for secrecy reasons, for efficiency reasons
  - **∼ 10 telecom. operators or manufacturers** with strong cryptography expertise
  - **chaired by** Gert Roelofsen until he left KPN research
    and since then by Steve Babbage, Vodafone

export controls

- **before 98**
  - **strong export restrictions on encryption**, in particular for mobile systems
    - A5/1 was much stronger than ciphers that were freely exportable at that time
  - no transparent rules, case by case approval
  - **SAGE algorithms were not published**
    - this was needed to get export approval
    - however, for massively deployed algorithms, secrecy does not last long…
- **since 98 (Wassenaar agreements)**
  - **export controls** still exist…
    … but have been **considerably eased** and are no longer a real issue for mobiles
  - **SAGE moved to public algorithms soon after 98**
    - ☺ increase public confidence
    - ☺ take advantage from publicly available designs
    - other less decisive pros & cons:
      ☺ public evaluation after deployment, ☹ increased vulnerability to side channel attacks

SAGE approach to algorithms development

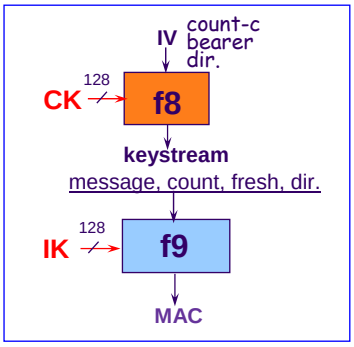
"balance the benefits of public evaluation against industry timescales" [S. Babbage]

1. **take the best from available research results**
   - investigate most promising **public designs**
   - adapt design to specific requirements of the intended application
   - taking most recent **advances in cryptanalysis** into account
2. **algorithm design /specification / evaluation work**
   - set-up a **project team** with clear timescales and allocation of tasks
   - split participants into **separate design and evaluation teams**
     - requirements capture (all)
     - design team: 1st design, 2nd design, final design
     - evaluation team: mathematical evaluation, statistical testing
   - **output:** specification, ref. implementation and spec.testing, design & eval. report
3. **Independent evaluation and follow-on research**
   - **evaluation reports by well known academic expert teams** (limited evaluation time)
   - monitoring of (and often contribution to) **follow-on public research**

Case study 1: KASUMI, UEA1, UIA1 (1999)

- **requirements (in brief)**
  - **stream cipher f8 and MAC f9**
    - security: full strength
    - low H/W complexity
    - good H/W and S/W performance
    - f8: good IV agility

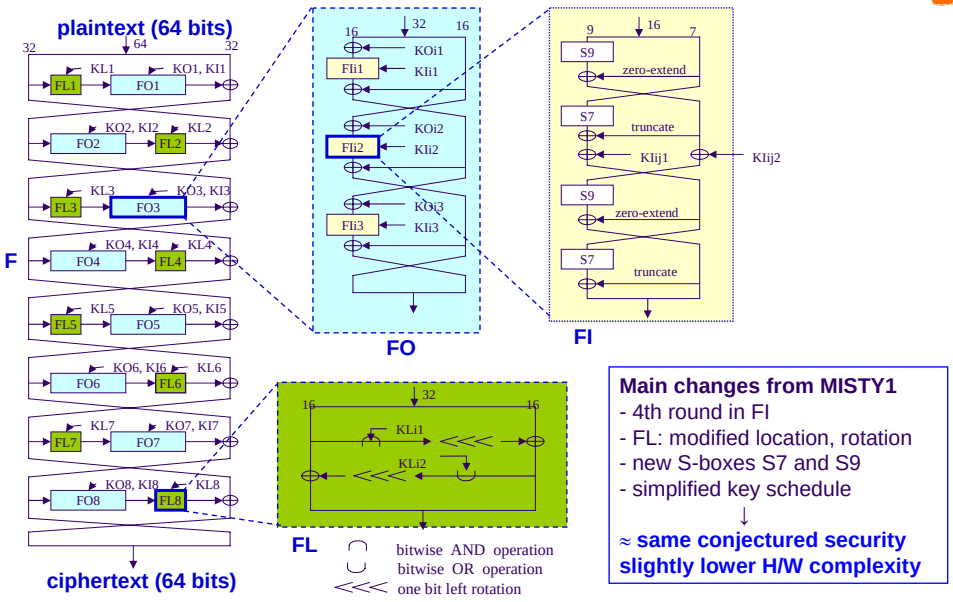
  ⇒ **block cipher** with stream cipher & MAC modes
    - for flexibility reasons



- **available research results to start from**
  - **strategies to thwart statistical attacks:**
    - [Daemen-Rijmen]: wide trail strategy
    - [Vaudenay]: decorrelation theory and resulting block ciphers
    - [Nyberg-Knudsen, Aoki]: differential & linear bounds on 3R-Feistel schemes
      [Matsui]: application to the embedded construction of MISTY block cipher

  ⇒ **MISTY (a 64-bit block cipher) was selected as the starting point for the design**
    - MISTY's designer, M. Matsui (Mitsubishi) joined SAGE
    - KASUMI (≈ "misty" in Japanese) was designed

KASUMI

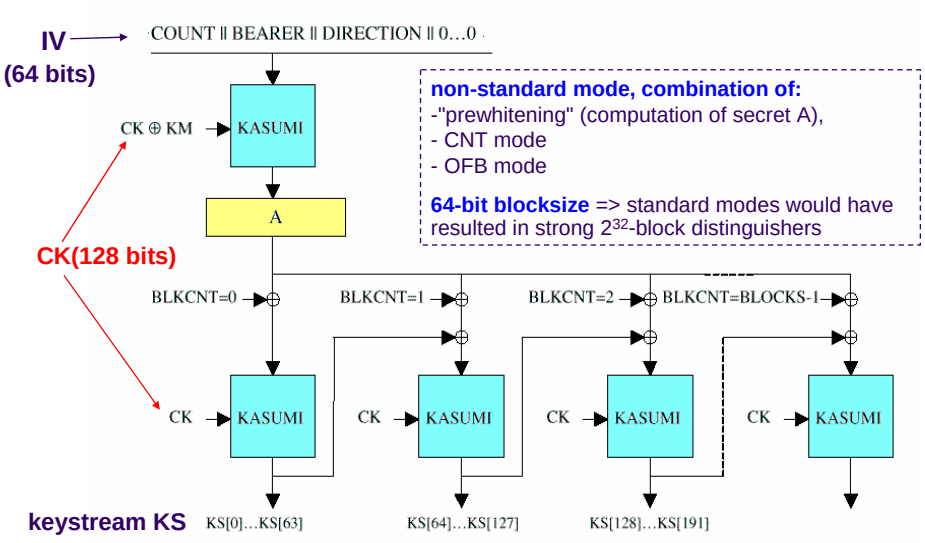


Main changes from MISTY1
- 4th round in FI
- FL: modified location, rotation
- new S-boxes S7 and S9
- simplified key schedule

↓

≈ same conjectured security
slightly lower H/W complexity

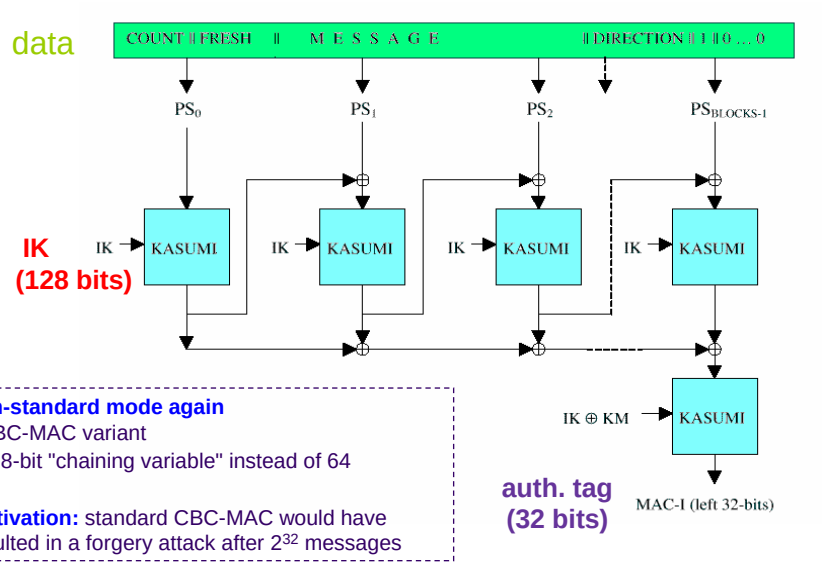
KASUMI-based f8: UEA1



non-standard mode, combination of:
-"prewhitening" (computation of secret A),
- CNT mode
- OFB mode

64-bit blocksize => standard modes would have resulted in strong 2^{32}-block distinguishers

KASUMI-based f9: UIA1



non-standard mode again
- CBC-MAC variant
- 128-bit "chaining variable" instead of 64

motivation: standard CBC-MAC would have resulted in a forgery attack after 2^{32} messages

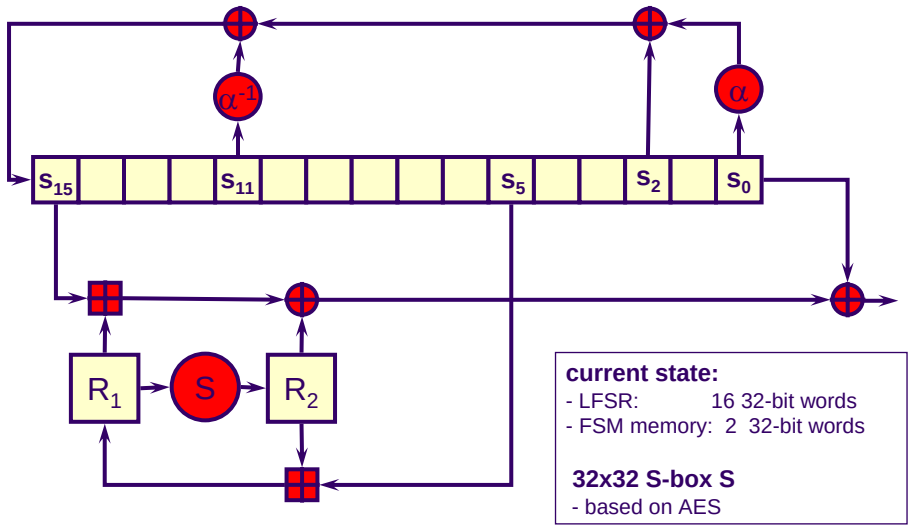
KASUMI, UEA1, UIA1 (end)

- **independent evaluation**
  - from three well known academic teams coordinated by leading ECRYPT partners…
  - in overall, confirmed soundness of proposed algorithms
    (some suggested variations not supported by strong cryptanalytic arguments against the evaluated specification were not retained)
- **follow on research**
  - f9 forgery from 2^{48} chosen message MACs [Knudsen-Mitchell]
    whether forgery from 2^{32} chosen message MACs feasible as for standard modes is still open
  - super-pseudo-randomness of 5-round MISTY [2 ind. papers at FSE 00]
  - pseudo-randomness of expanding functions inspired from f8 and MILENAGE [Gilbert]
  - algebraic interpretation of higher order differential properties of MISTY [Babbage-Frisch]
  - research on modes of operation…

Case study 2: SNOW 3G, UEA2, UIA2 (2005)

- **requirements (in brief)**
  - same as UEA1, UIA1, but **fallback algorithms** set
    - maximize "cryptographic distance" from KASUMI
    - minimize potential vulnerability to algebraic attacks
  - ⇒ **stream cipher + UH MAC approach** seemed worth being investigated
- **available research results to start from (stream ciphers)**
  - **NESSIE** had failed selecting a stream cipher, but:
    - had stimulated the design of **IV-dependent stream ciphers**
    - had resulted in cryptanalytic advances, e.g. **linear masking attacks** [Coppersmith et al.]
  - **ECRYPT / eSTREAM** stream ciphers project had just started
    - SASC workshop gave an accurate picture of the state of the art
  - ⇒ **SNOW 2.0** [Ekdahl-Johansson] was retained as a starting point for the design with permission of its authors.
    - its resistance to linear masking & algebraic attacks had been analysed [Watanabe et al., Billet-Gilbert]

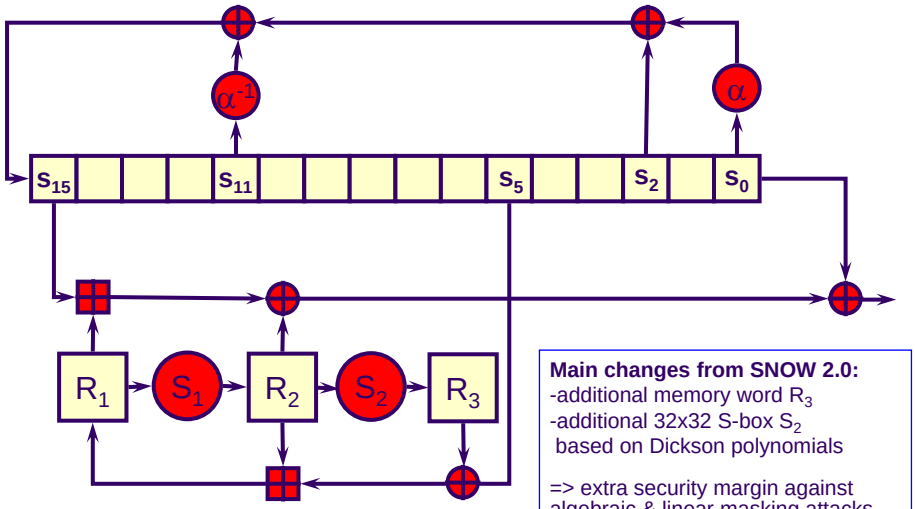
from SNOW 2.0 ...



current state:
- LFSR: 16 32-bit words
- FSM memory: 2 32-bit words

32x32 S-box S
- based on AES

to SNOW 3G



Main changes from SNOW 2.0:
-additional memory word R_3
-additional 32x32 S-box S_2
based on Dickson polynomials

=> extra security margin against algebraic & linear masking attacks

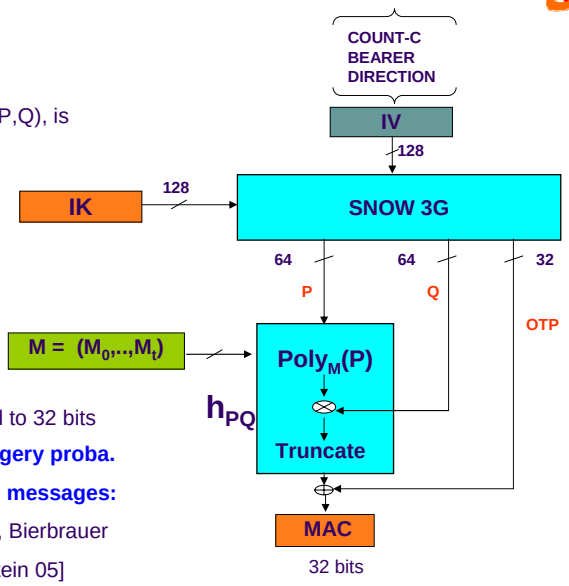
SNOW 3G, UEA2, UIA2 (cont.)

- **available research results to start from: UH function-based MACs**
  - Wegman-Carter paradigm: **$MAC(M) = h_k(M) \oplus OTP$**, **where $\{h_k\}$ is an almost 2-universal family of hash functions**
  - many efficient UH MACs based on polynomials had been recently proposed **$h_k(M) = Poly_M(k)$,** typically over GF(2^n)
  - how to best **derive k and OTP from IK using a streamcipher** was unclear

message authentication f9: UIA2

- computations are done over GF(2^{64})

• 32–bit OTP, but also 128-bit hash key (P,Q), is derived fom IK using SNOW 3G **(conservative choice)**



- MAC = $h_{PQ}(M) \oplus$ OTP
  where $h_{PQ}(M) = (Poly_M(P) \bullet Q)$ truncated to 32 bits

multiplication by Q allows to keep forgery proba. close to ideal value 2^{-32}, even for long messages: 2-stage MAC construction [Stinson 92, Bierbrauer et al. 93, Neversteen-Preneel 99, Bernstein 05]

SNOW 3G, UEA2, and UIA2 (end)

independent evaluation

- two well known academic teams (coordinated by leading ECRYPT partners…)
- various potential lines of attack were investigated
- in overall, confirmed SAGE confidence in proposed design

follow on research

- improved linear masking on SNOW 2.0 [Nyberg-Wallen]
- note about how to improve truncated G-MAC [Nyberg-Gilbert-Robshaw]
- warning about key recovery attacks on some polynomial based UH MACs when unlike in UIA2 hash key is not renewed [Handschuh-Preneel, Crypto 08]

conclusion

- **cryptographic research and standardisation are distinct processes…**
  - distinct objectives, distinct timescales
  - research must not be entirely driven by the requirements of applications
  - standardisation may have to deal with problems research did not / cannot solve
- **…but they must interact closely**
  - standardisation groups and the research community must not be disjoint
  - the research and scientific exchanges promoted by ECRYPT and ECRYPT II in the future are quite useful to achieve this kind of interaction
- **next cryptography standardization challenges in mobiles?**
  - other security aspects (underway)
  - massively deployed public key cryptography in (U)SIMs?