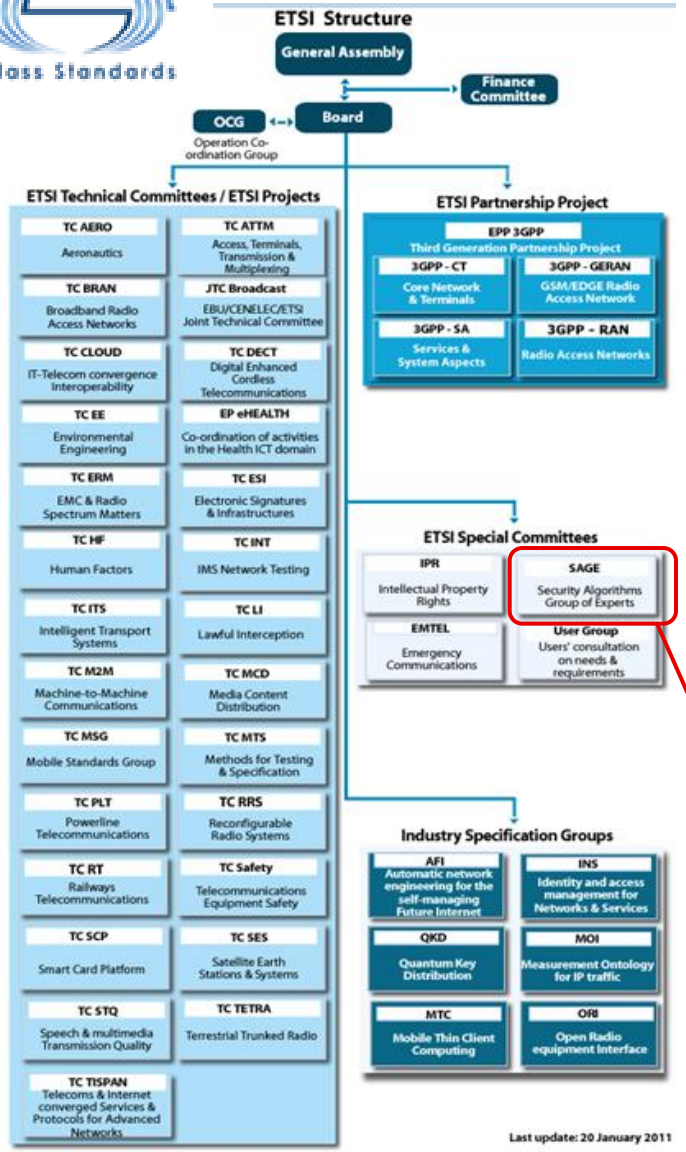
# New mobile phone algorithms – a real world story

Steve Babbage
Vodafone Group R&D

17 February 2011

# Standards groups

ETSI World Class Standards




3GPP™ A GLOBAL INITIATIVE

**TSG GERAN**
GSM EDGE Radio Access Network
- GERAN WG1 — Radio Aspects
- GERAN WG2 — Protocol Aspects
- GERAN WG3 — Terminal Testing

**TSG RAN**
Radio Access Network
- RAN WG1 — Radio Layer 1 spec
- RAN WG2 — Radio Layer 2 spec, Radio Layer 3 RR spec
- RAN WG3 — Iub spec, Iur spec, Iu spec, UTRAN O&M requirements
- RAN WG4 — Radio Performance, Protocol aspects
- RAN WG5 — Mobile Terminal Conformance Testing

**TSG SA**
Service & Systems Aspects
- SA WG1 — Services
- SA WG2 — Architecture
- SA WG3 — Security
- SA WG4 — Codec
- SA WG5 — Telecom Management

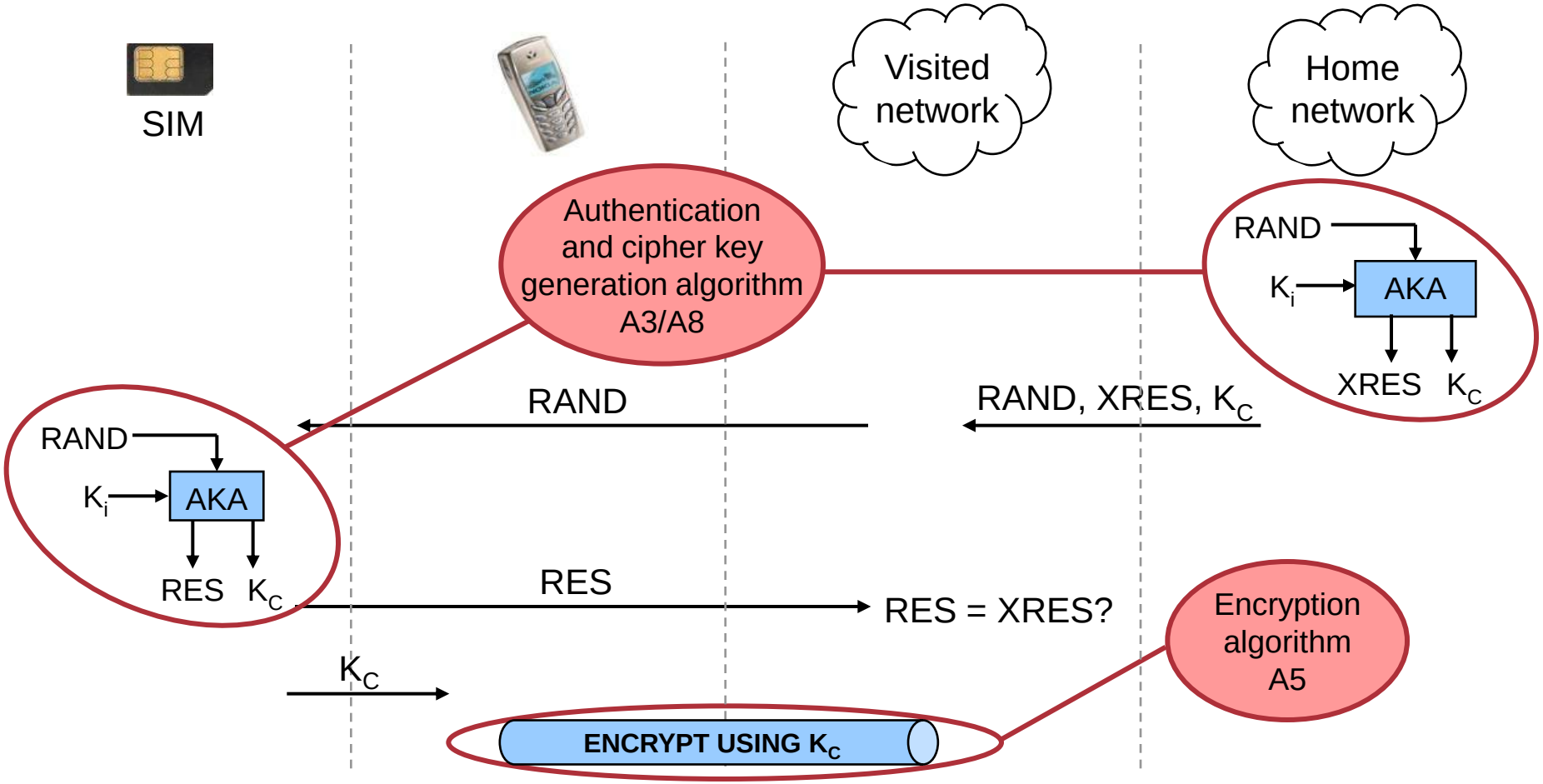
**TSG CT**
Core Network & Terminals
- CT WG1 — MM/CC/SM (Iu)
- CT WG3 — Interworking with external networks
- CT WG4 — MAP/GTP/BCH/SS
- CT WG6 — Smart Card Application Aspects

**SAGE**
Security Algorithms Group of Experts

**SA WG3**
Security

# First generation

# GSM security architecture



# GSM security limitations

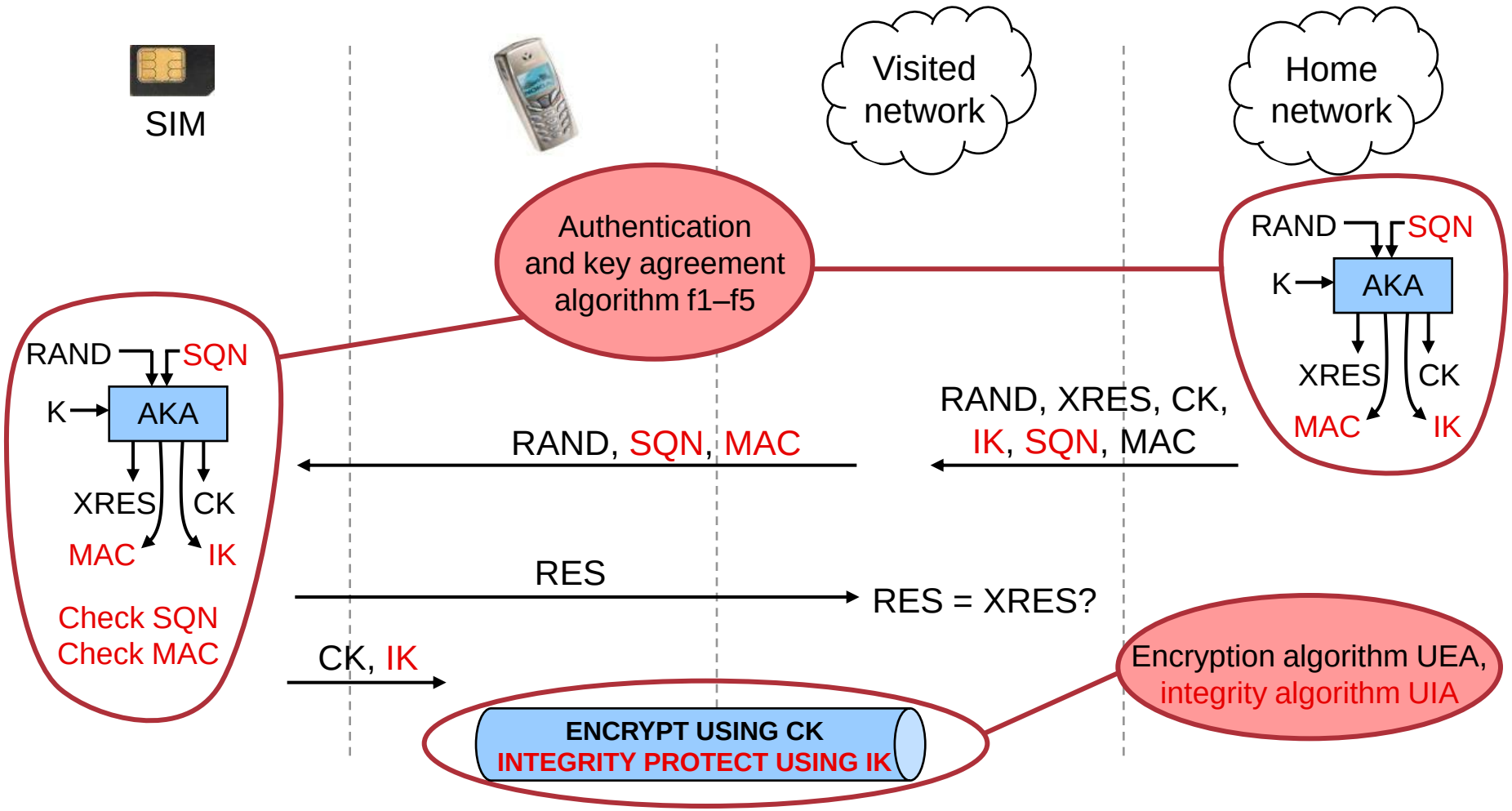
> Key length

> One-way authentication

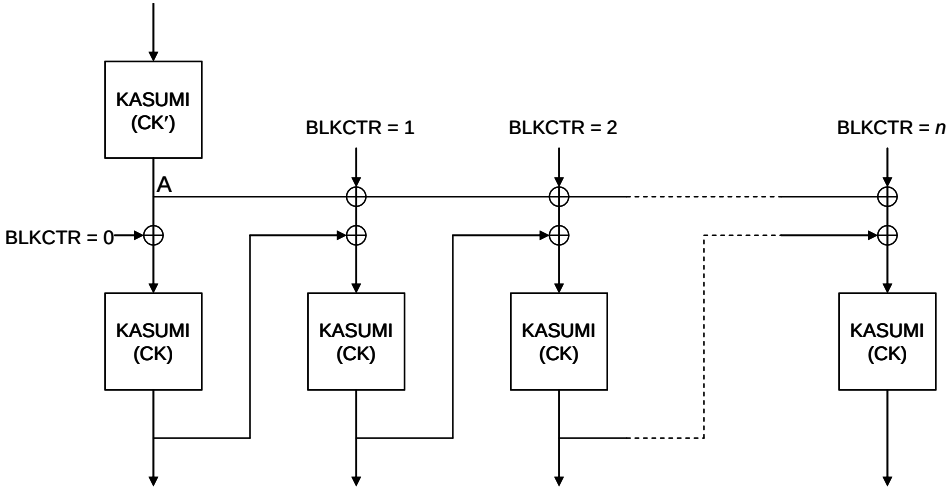
> Unprotected signalling

> A5/1, A5/2

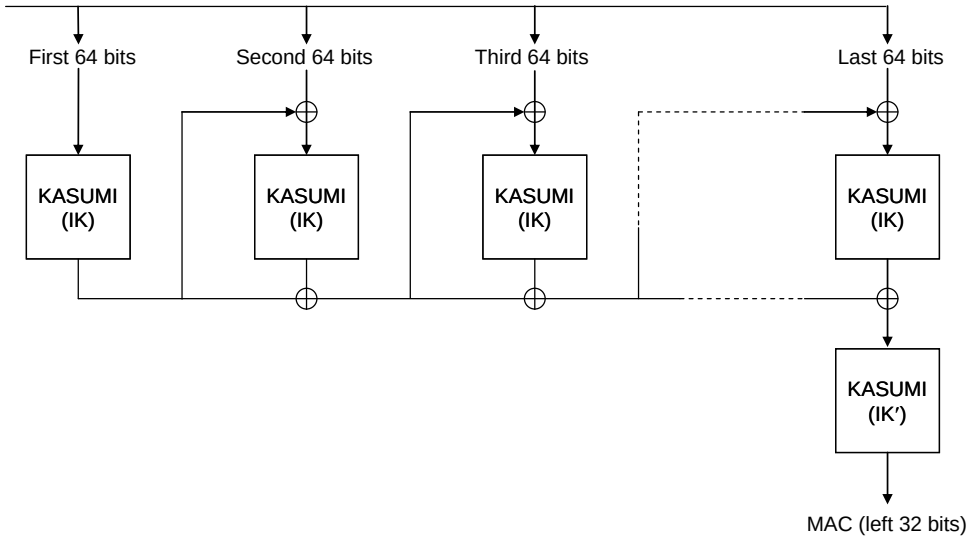
# UMTS security architecture (slightly simplified)



# First UMTS algorithms, UEA1 / UIA1




**A5/3 ≈ UEA1**
**(but 64-bit key)**



# So now we can replace A5/1 with A5/3 …

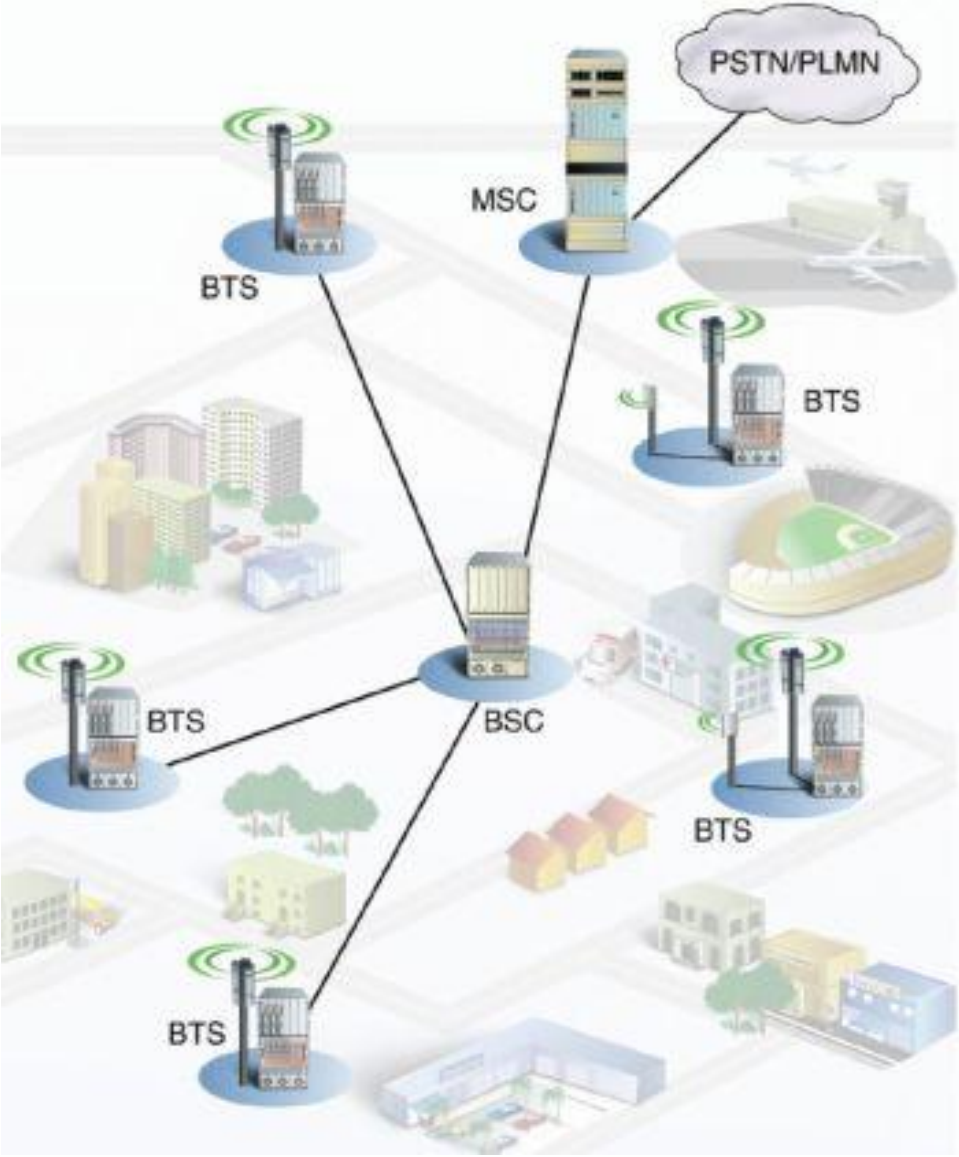


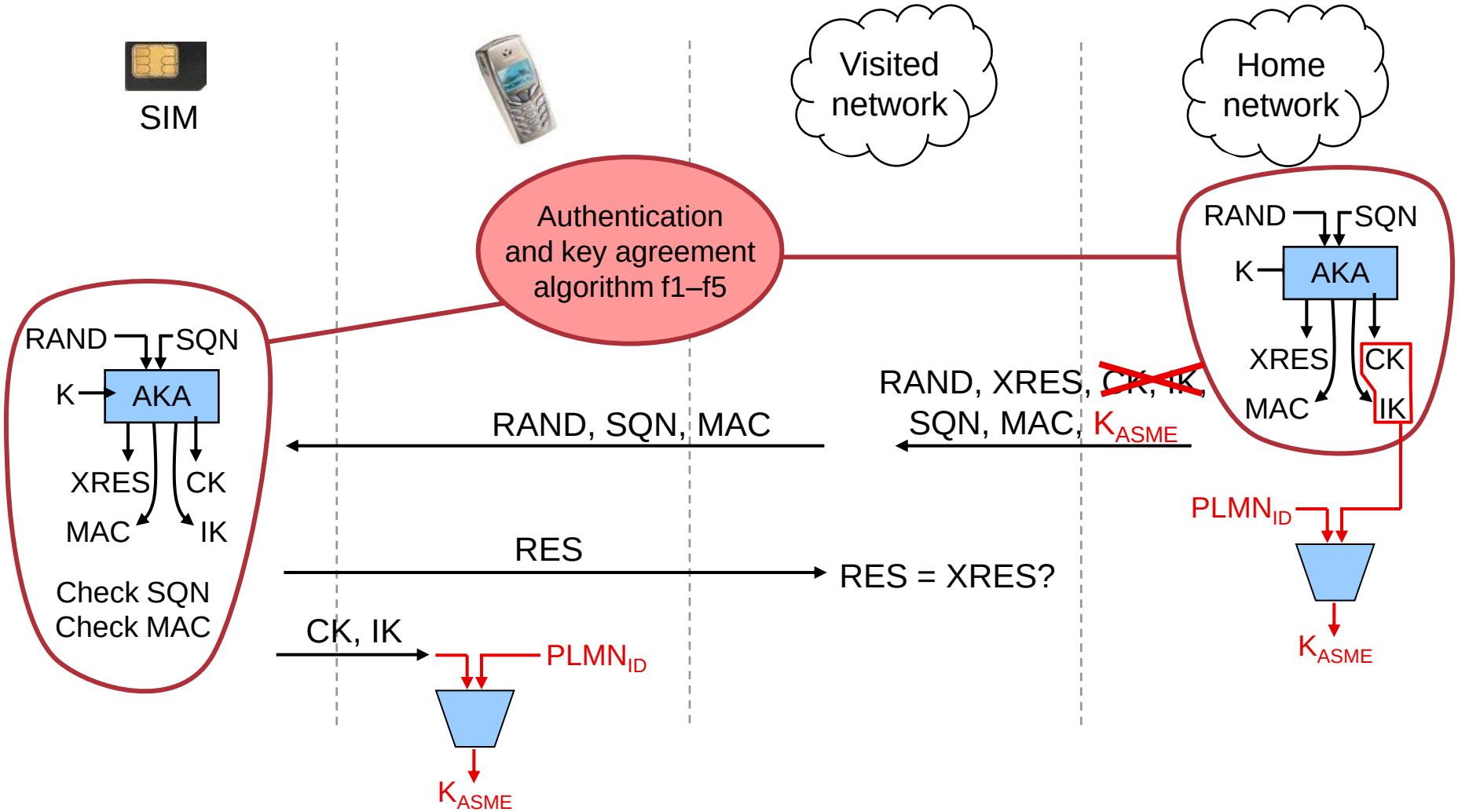

Image from http://www.elkomas.lt/

# Second UMTS algorithms, UEA2 / UIA2

> SNOW 3G

- Why not AES?
- Why not SNOW 2.0?

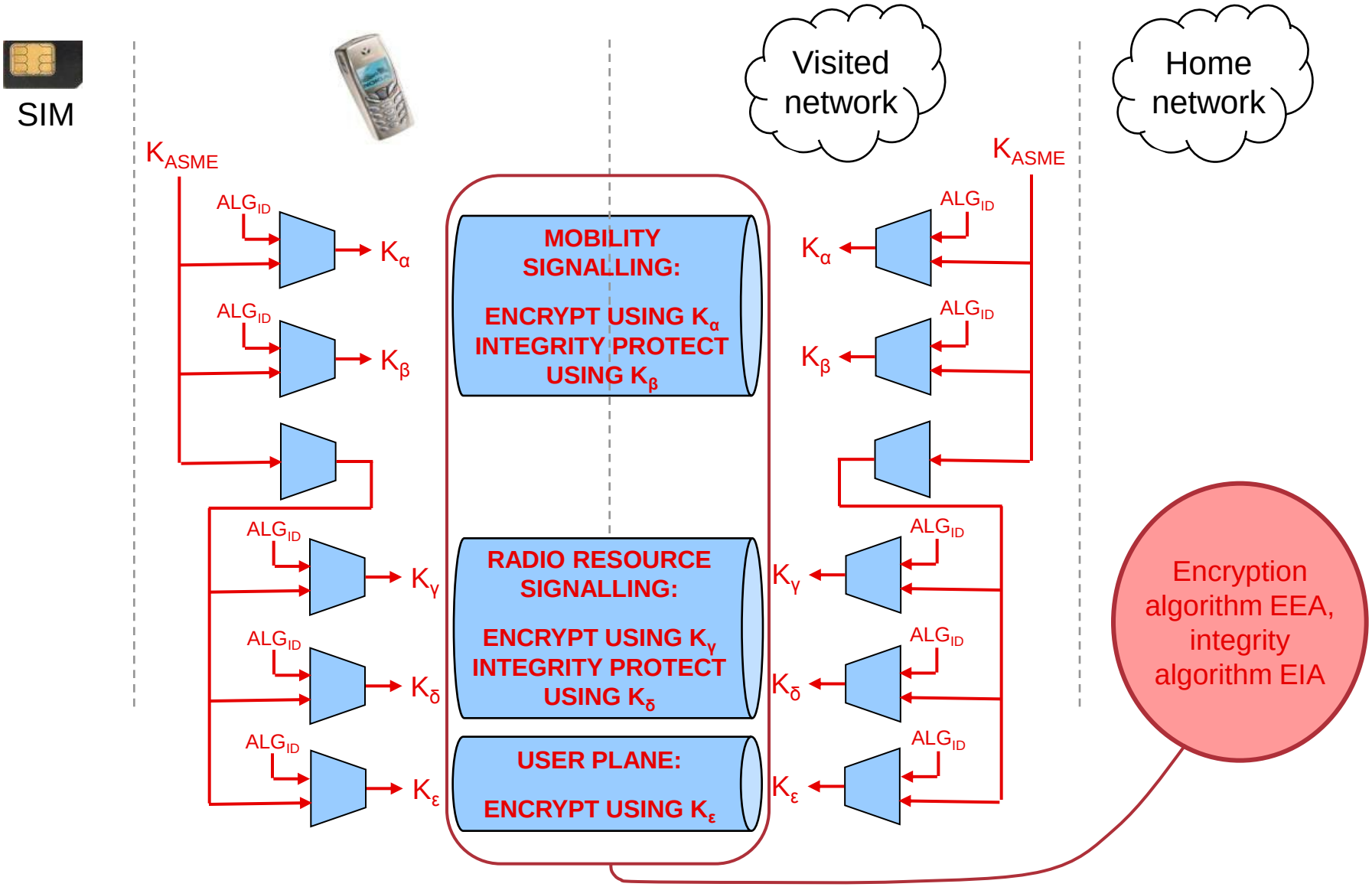
# LTE security architecture (part 1)



# GSM security limitations

- Key length
- One-way authentication
- Unprotected signalling
- A5/1, A5/2
- Same key regardless of algorithm choice

# LTE security architecture (part 2)



# Original LTE algorithms (from day one)

> Based on SNOW-3G

– 128-EEA1: straightforward stream cipher use

– 128-EIA1: polynomial evaluation UHF

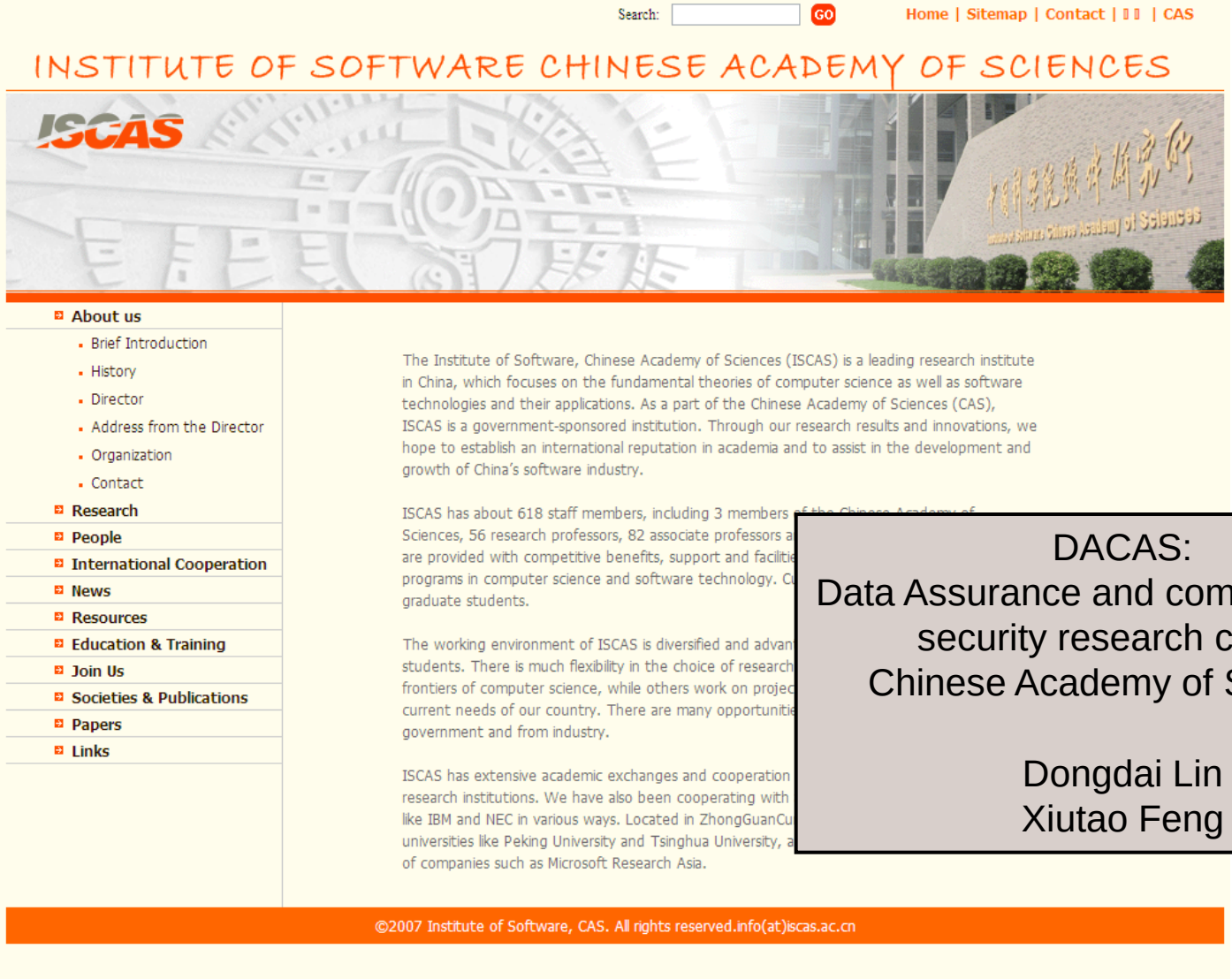
– Identical to UMTS algorithms

> Could have been based on Kasumi or AES; chose AES

– 128-EEA2: AES in counter mode

– 128-EIA2: AES in CMAC mode

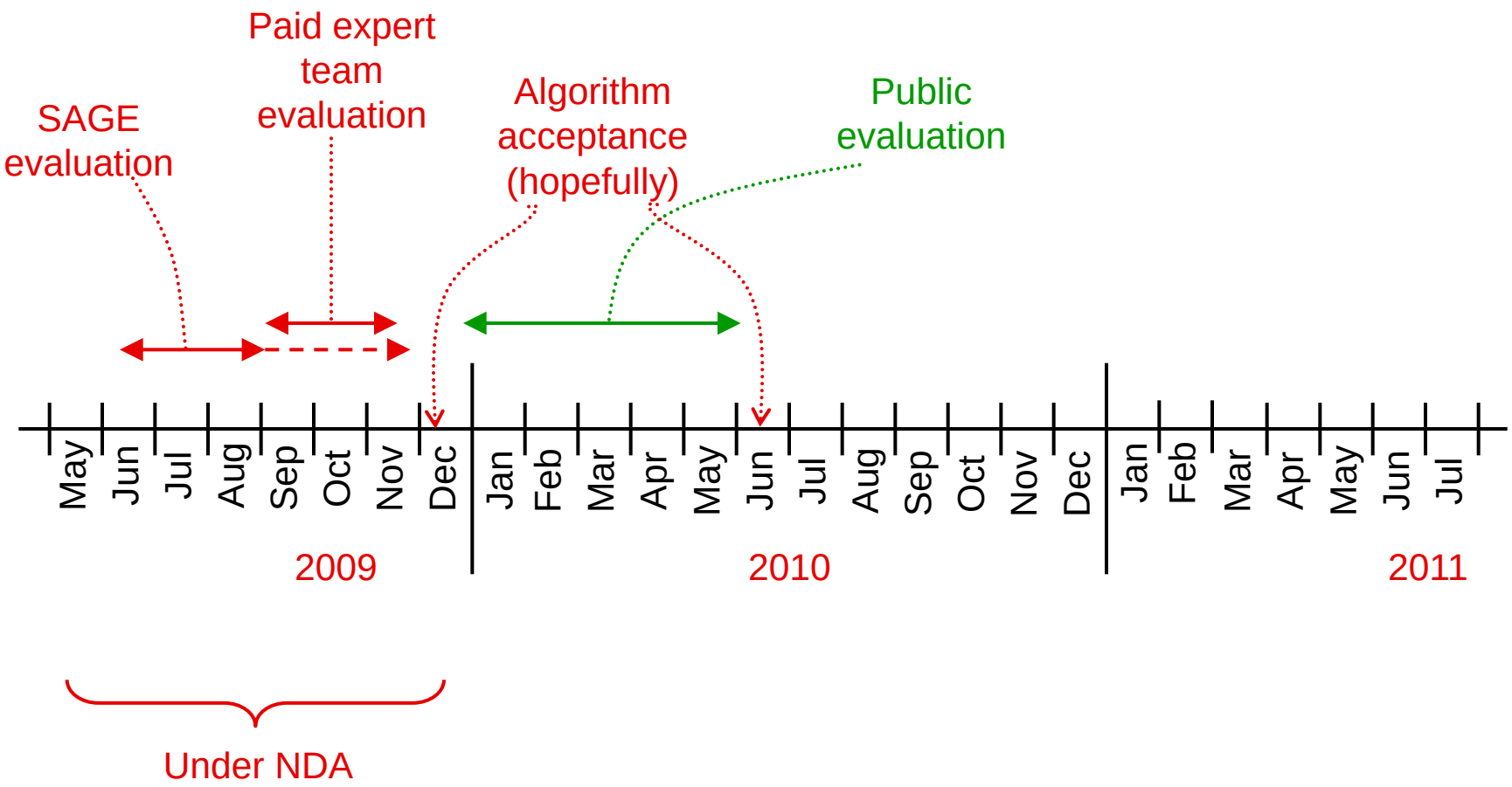
# The designers



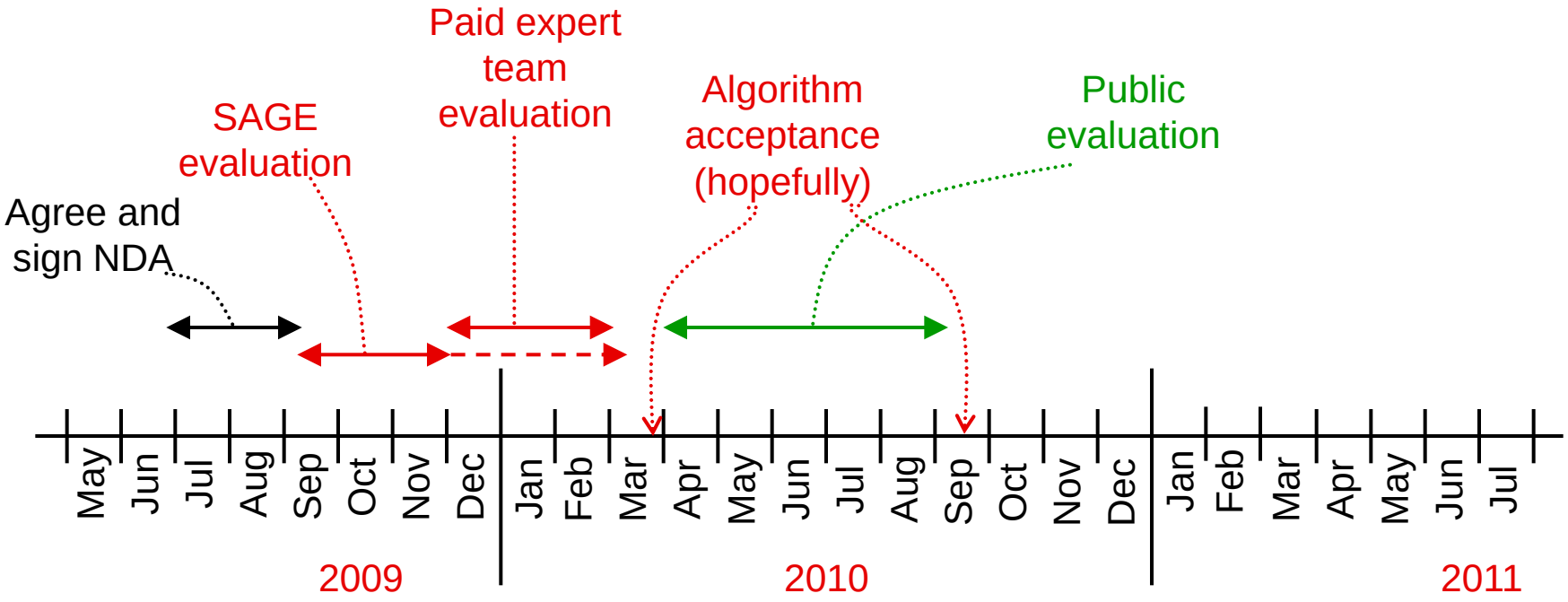

DACAS:
Data Assurance and communication security research center,
Chinese Academy of Sciences

Dongdai Lin
Xiutao Feng

# Plan A


Paid expert team evaluation
SAGE evaluation
Algorithm acceptance (hopefully)
Public evaluation
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011
Under NDA

# Plan B


Agree and sign NDA
SAGE evaluation
Paid expert team evaluation
Algorithm acceptance (hopefully)
Public evaluation
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Take your time

**Advanced Encryption Standard process**

From Wikipedia, the free encyclopedia

**Start of the process**

On January 2, 1997, NIST announced that they wished to choose a successor to DES to be known as AES ….

The result of this feedback was a call for new algorithms on September 12, 1997

**Rounds one and two**

In the nine months that followed, fifteen different designs were created and submitted ….

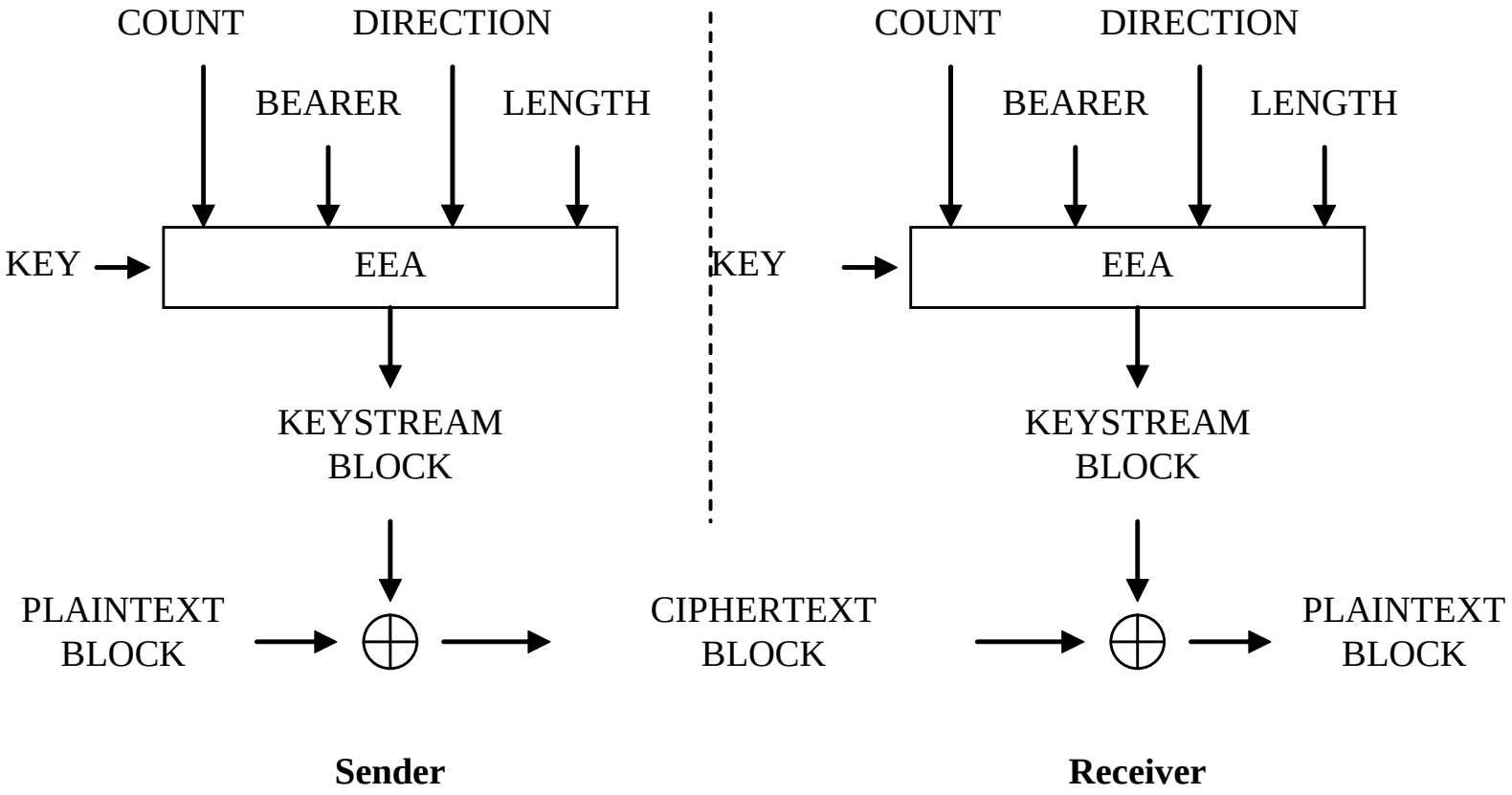
NIST held two conferences to discuss the submissions (AES1, August 1998 and AES2, March 1999), and in August 1999 they announced that they were narrowing the field from fifteen to five ….

… AES3 conference in April 2000 ….

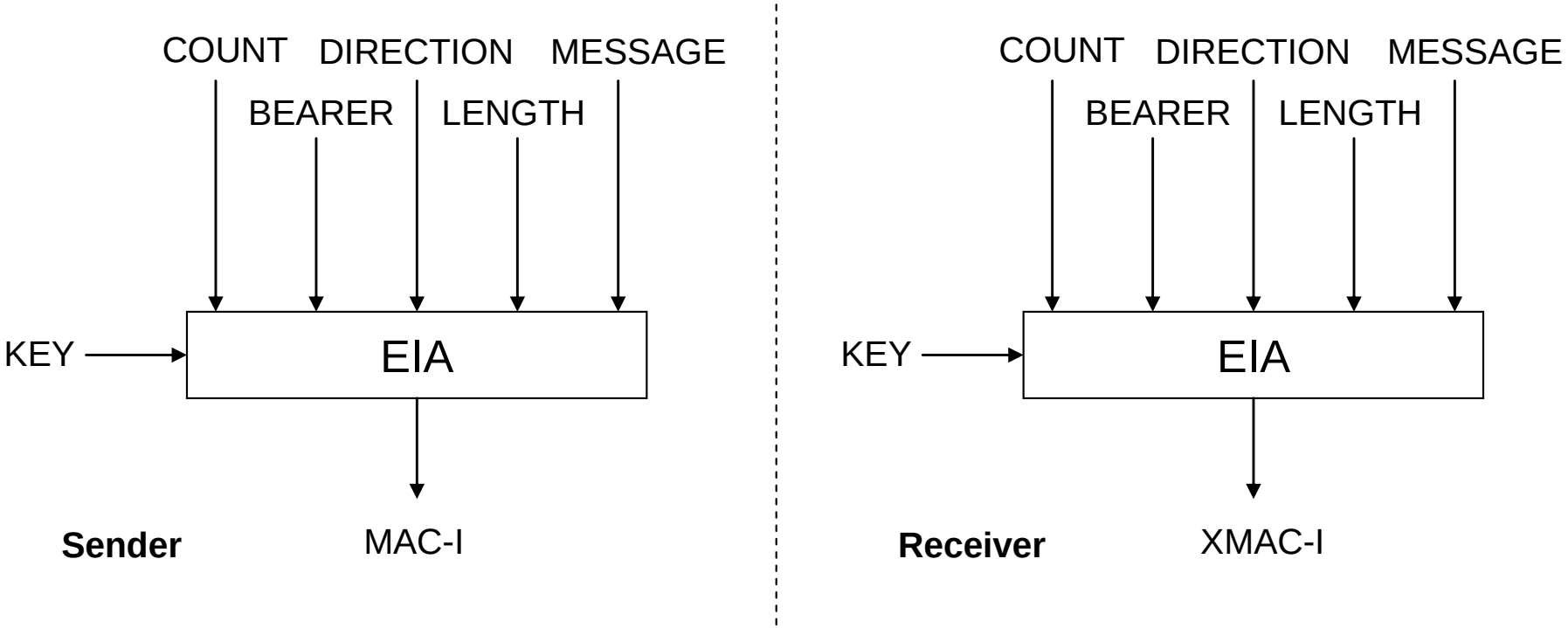
**Selection of the winner**

On October 2, 2000, NIST announced that Rijndael had been selected as the proposed AES ….

# Encryption

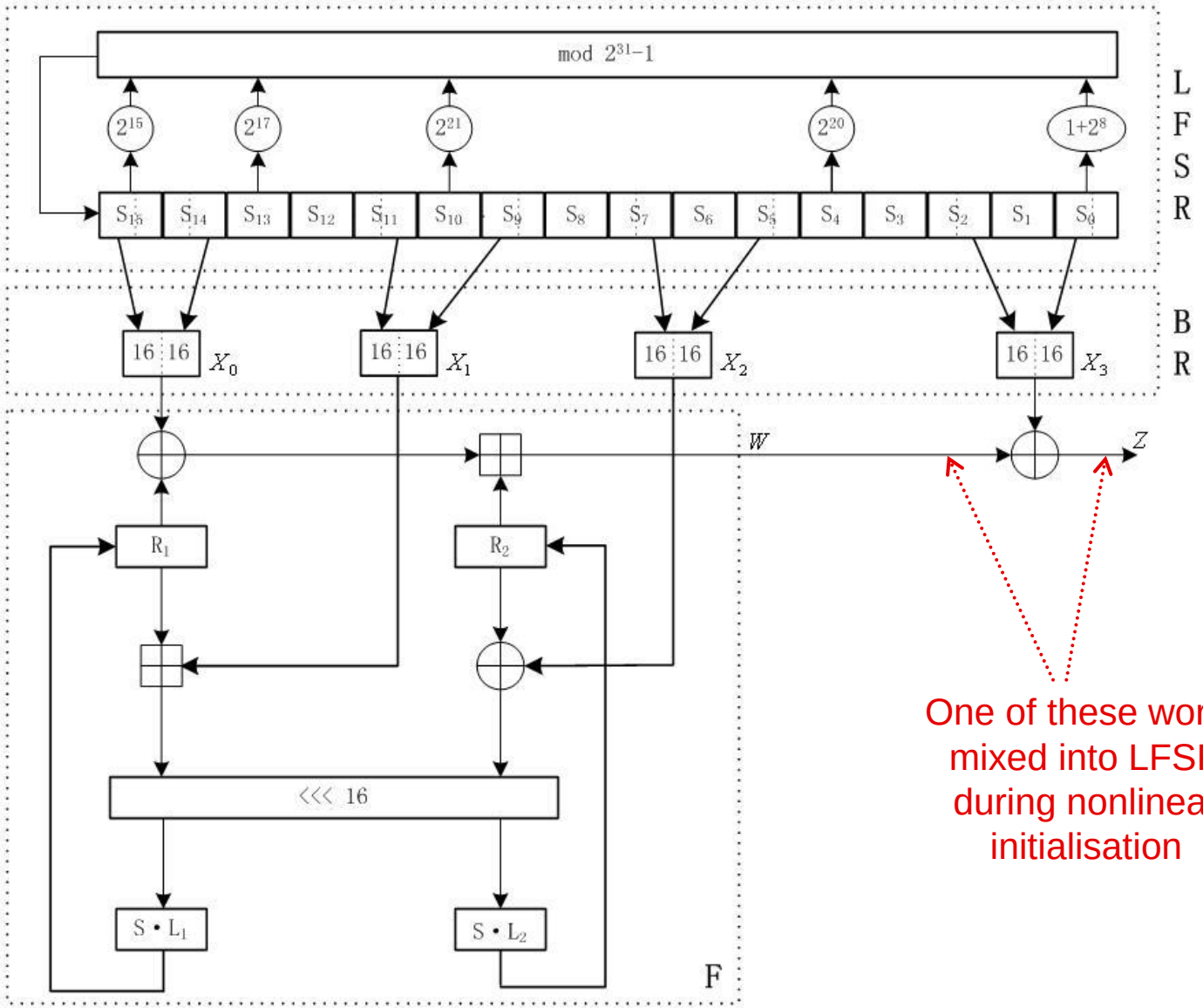

COUNT
DIRECTION
BEARER
LENGTH
KEY
EEA
KEYSTREAM BLOCK
PLAINTEXT BLOCK
CIPHERTEXT BLOCK
COUNT
DIRECTION
BEARER
LENGTH
KEY
EEA
KEYSTREAM BLOCK
PLAINTEXT BLOCK
Sender
Receiver

# Integrity


COUNT
DIRECTION
MESSAGE
BEARER
LENGTH
KEY
EIA
Sender
MAC-I
COUNT
DIRECTION
MESSAGE
BEARER
LENGTH
KEY
EIA
Receiver
XMAC-I

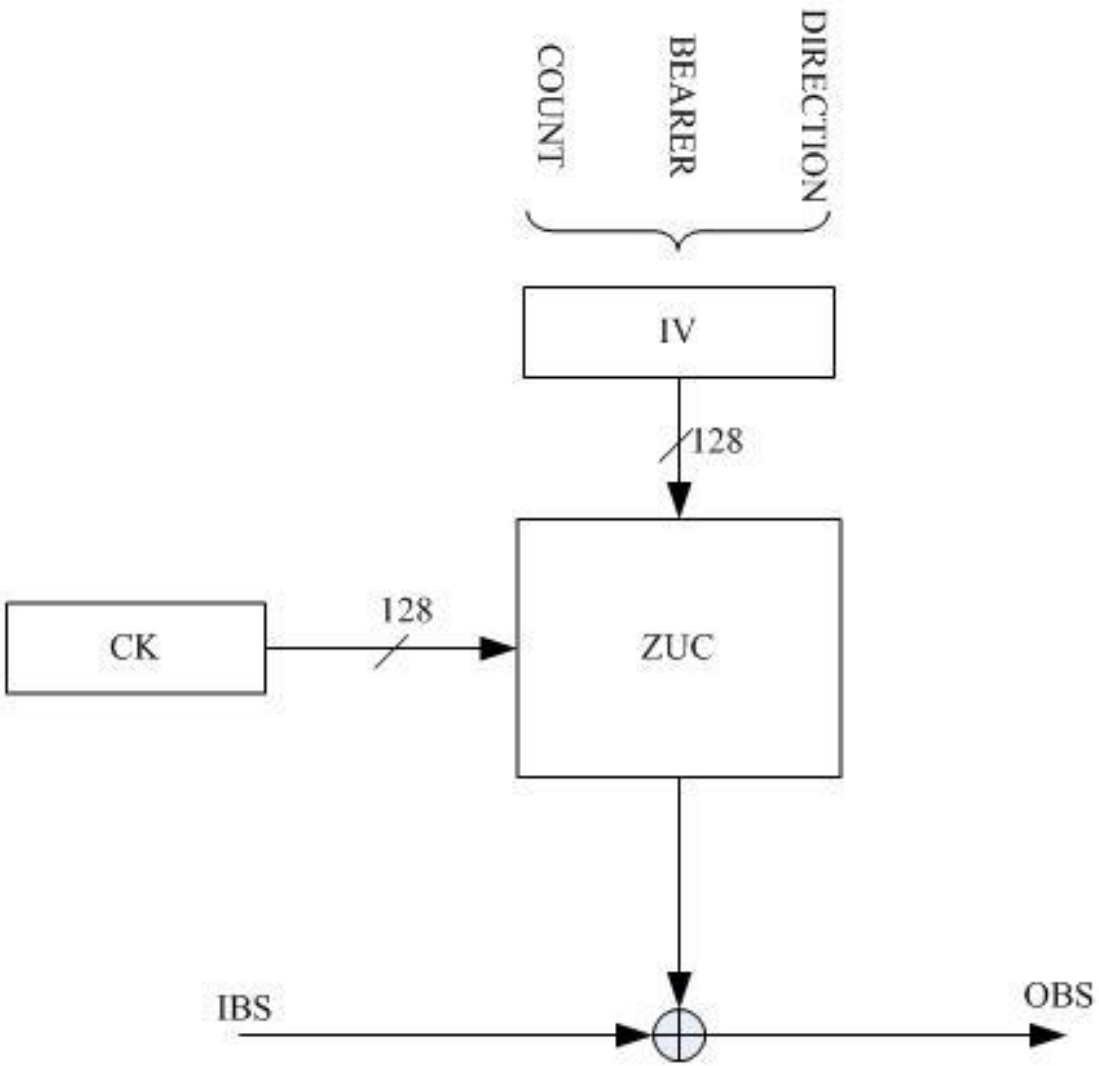
# ZUC – named after Zu Chongzhi

# ZUC



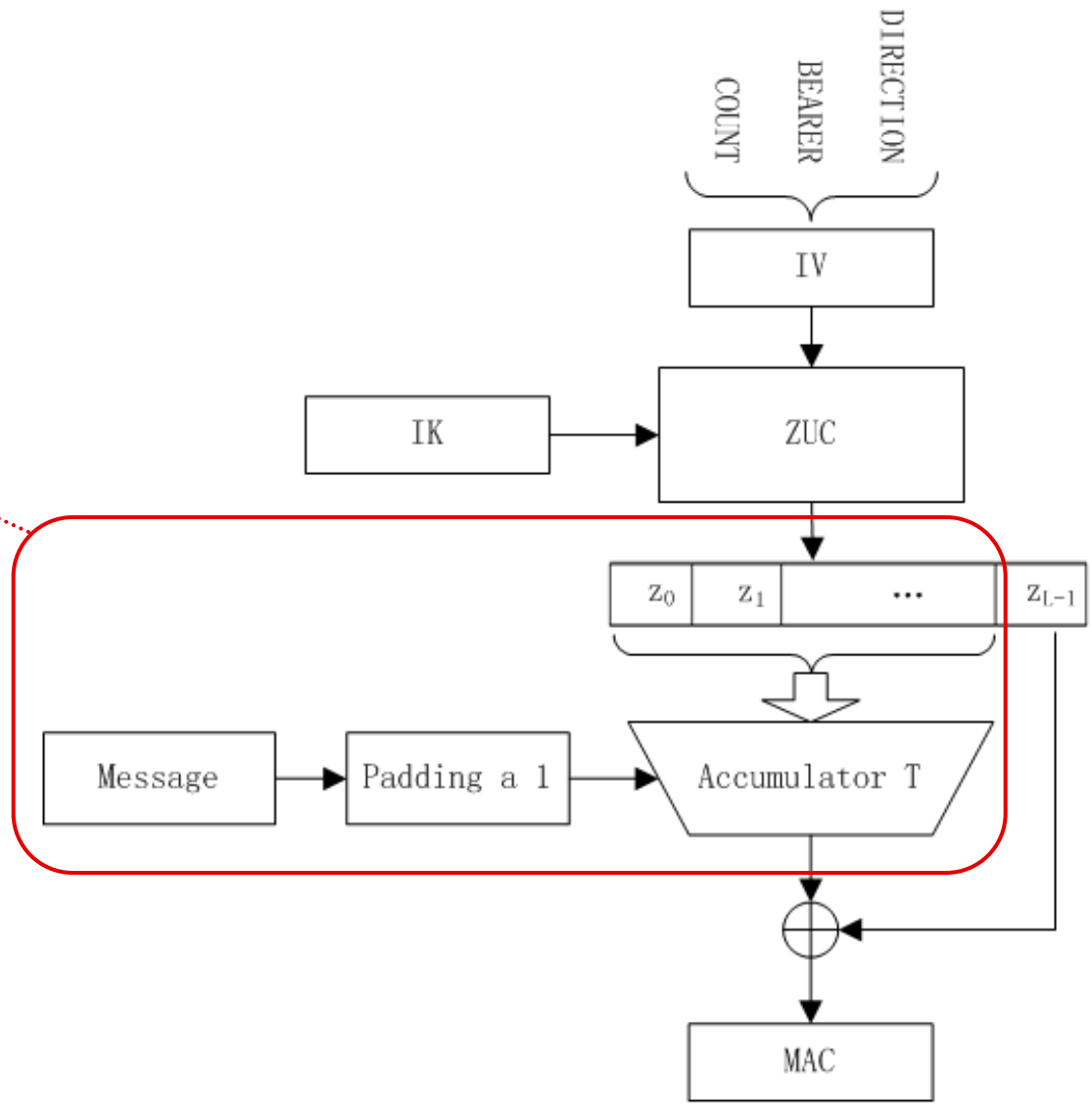

One of these words mixed into LFSR during nonlinear initialisation

# Encryption algorithm 128-EEA3



# Integrity algorithm 128-EIA3

Universal
Hash Function



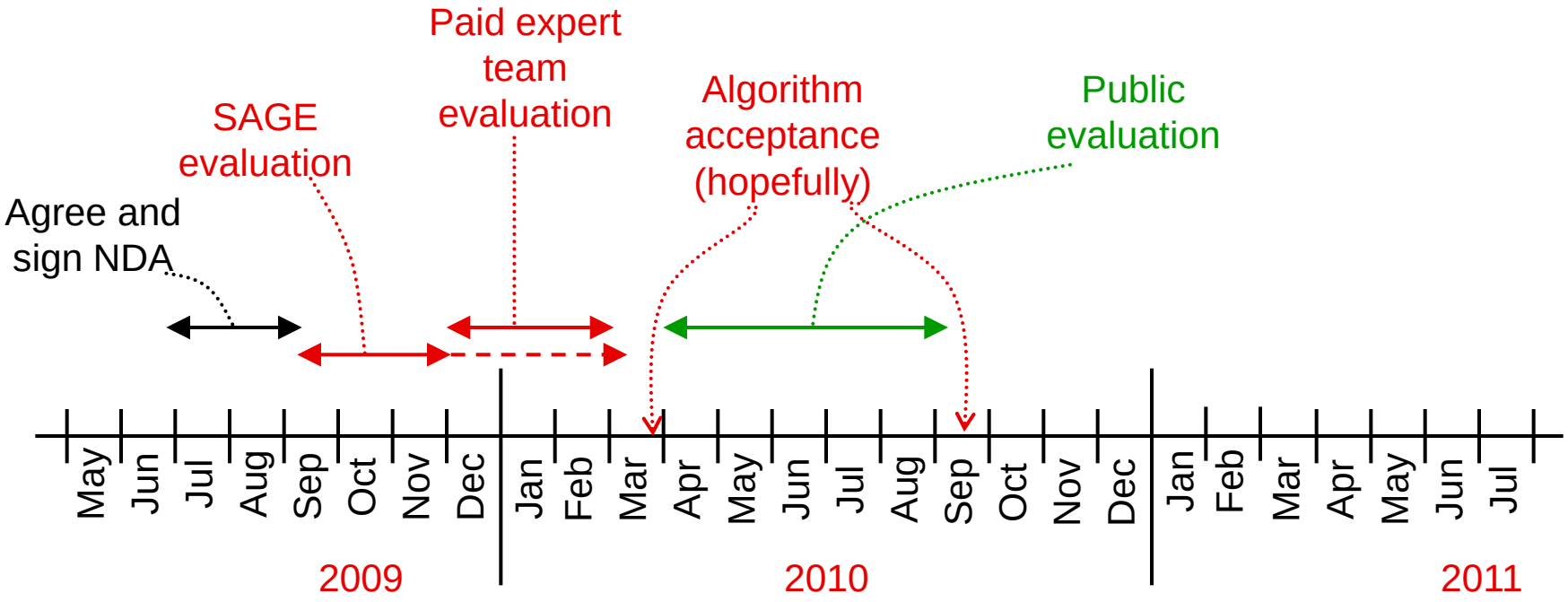
# Initial SAGE evaluation

> Fit for purpose

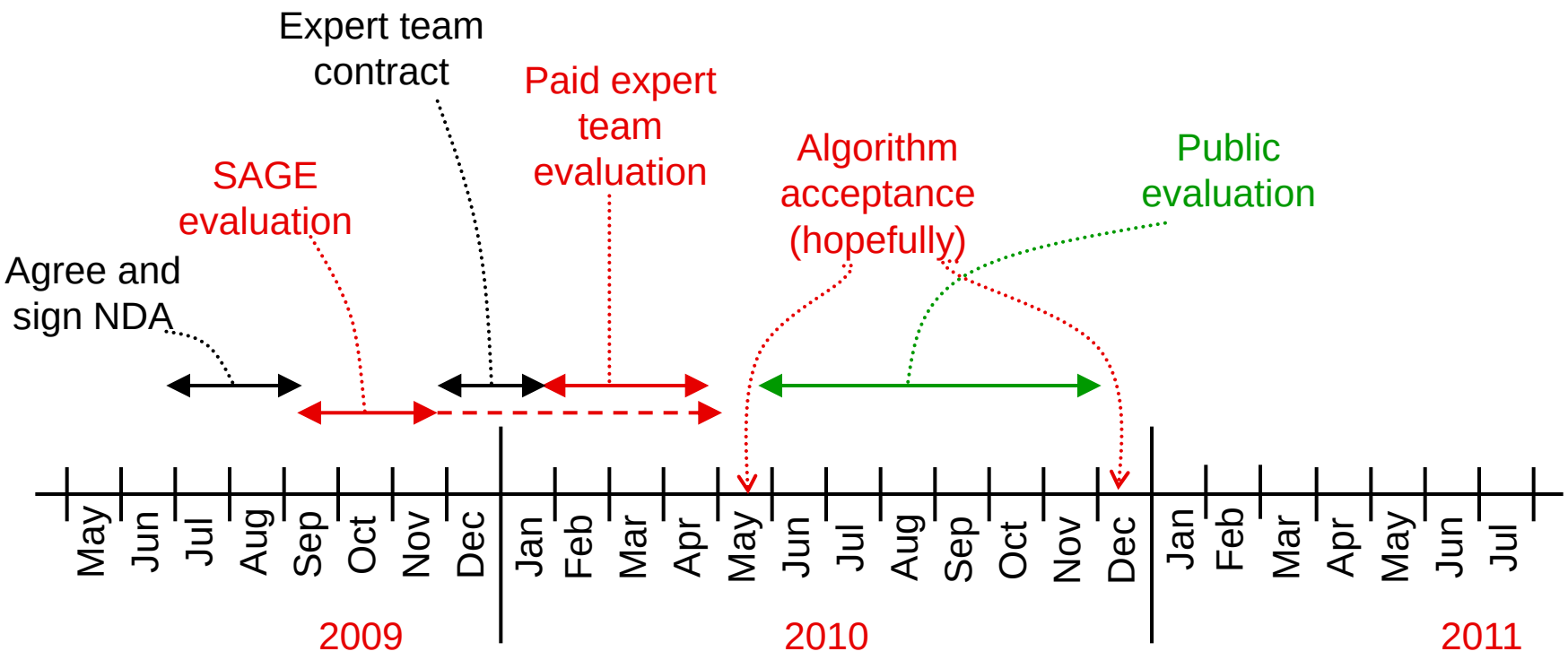
> Smells OK

– Must be not just strong, but free of suspicion

# Plan B


Agree and sign NDA
SAGE evaluation
Paid expert team evaluation
Algorithm acceptance (hopefully)
Public evaluation
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Plan C


Expert team contract
Paid expert team evaluation
Algorithm acceptance (hopefully)
Public evaluation
SAGE evaluation
Agree and sign NDA
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# External expert team evaluation

> Codes and Ciphers Limited

  – Carlos Cid, Sean Murphy, Fred Piper, Matthew Dodd

> Alice and Bob Technologies

  – Lars Knudsen, Bart Preneel, Vincent Rijmen

> Several corrections / improvements to existing evaluation

> All standard attack types considered – all seem unlikely to succeed

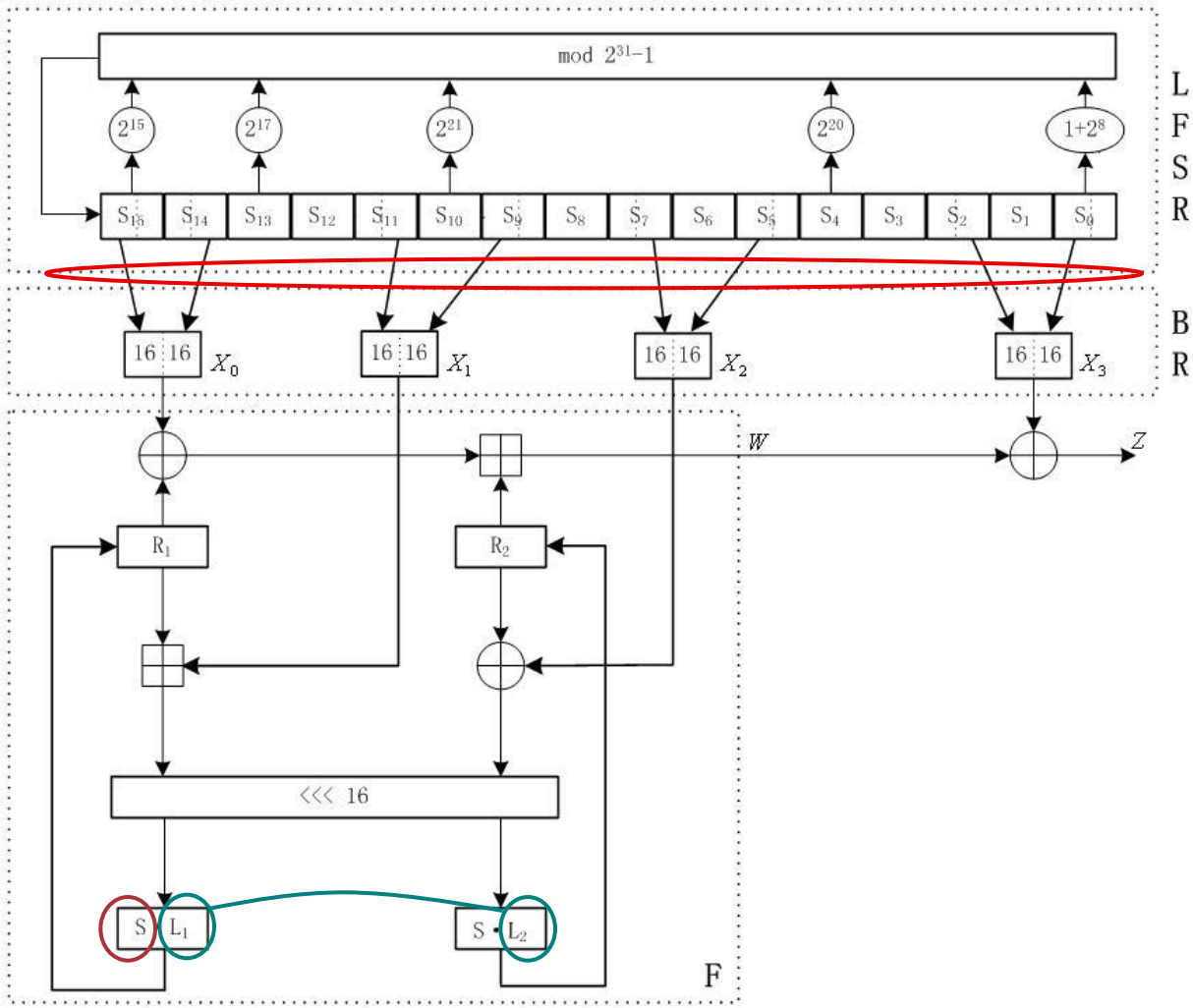
> Strength inherited from SNOW-like construction

> Some components not fully explained

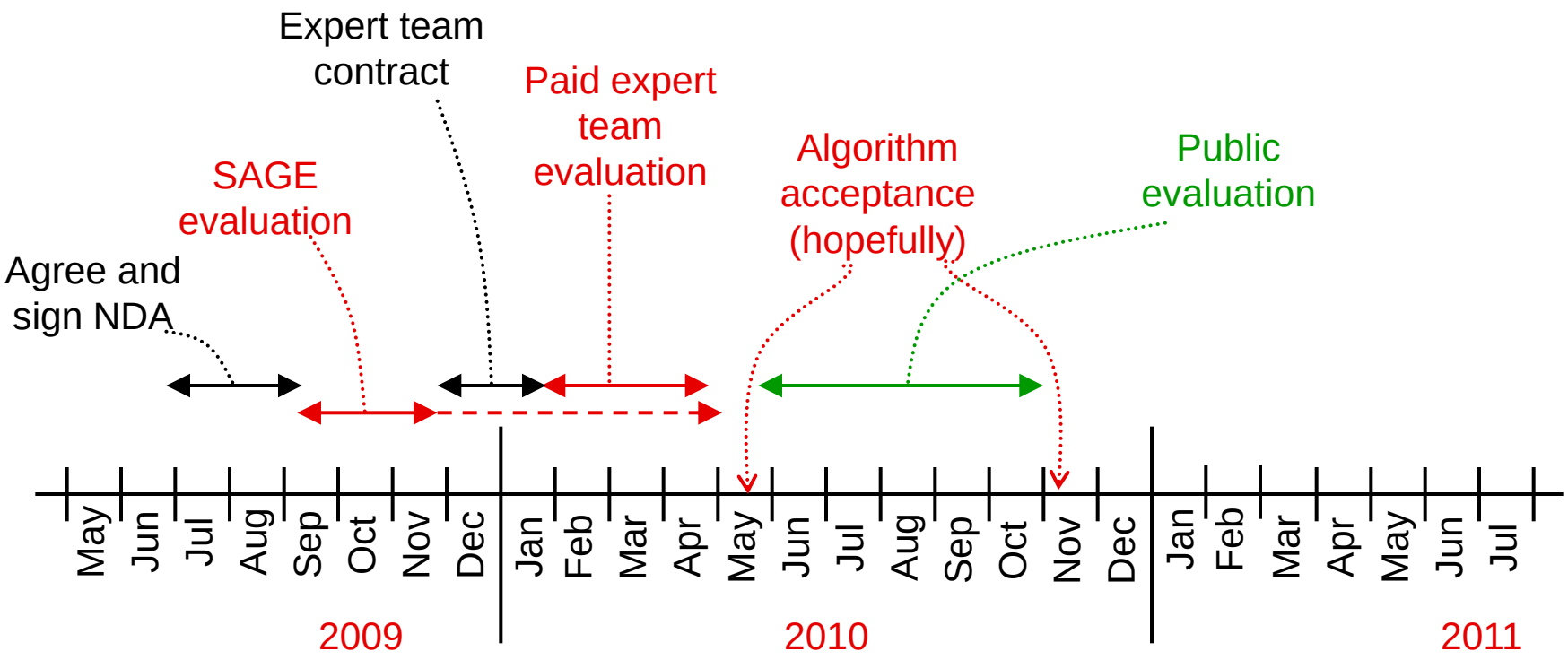
> Like most UHF MACs – not robust against nonce reuse

# Conclusion of the SAGE and paid evaluation

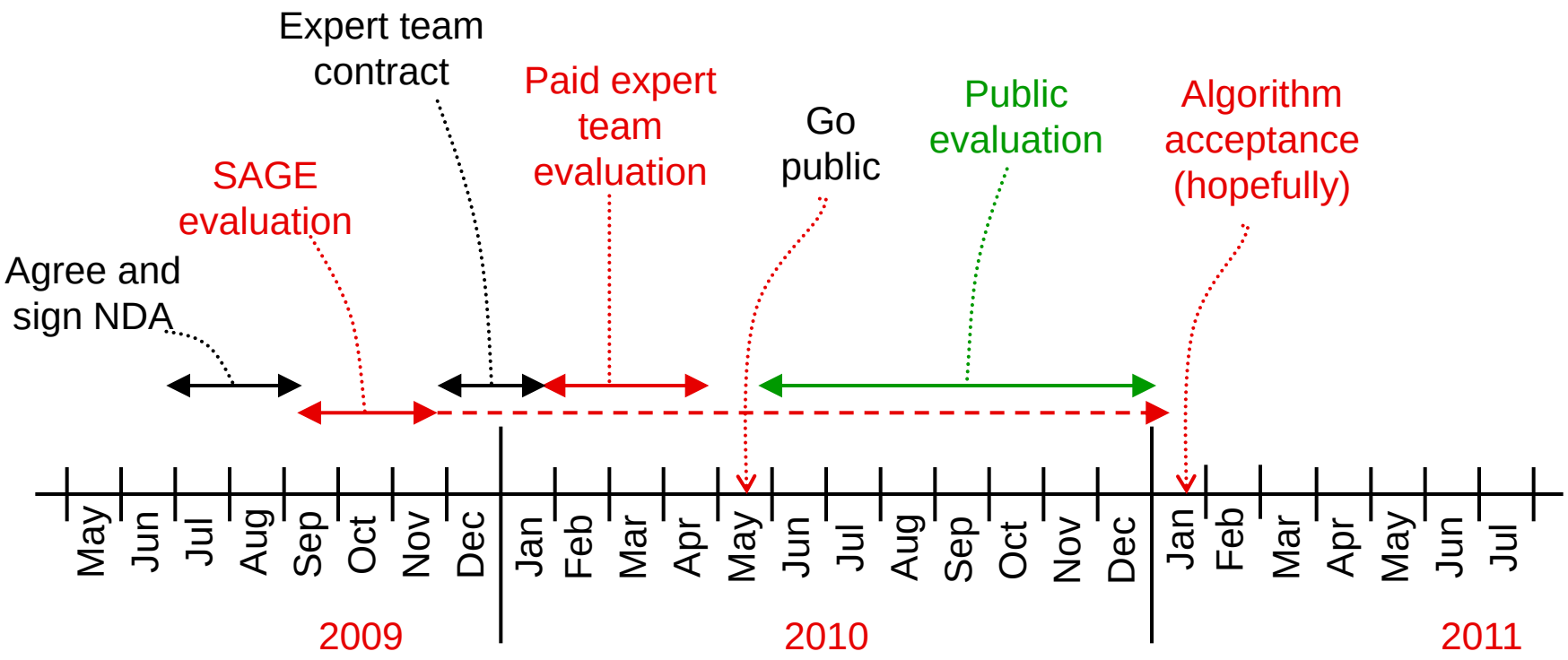
> Transparency is vital – nothing suspicious



# Plan C


Expert team contract
Paid expert team evaluation
Algorithm acceptance (hopefully)
Public evaluation
SAGE evaluation
Agree and sign NDA
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Plan D


Expert team contract
Paid expert team evaluation
Go public
Public evaluation
Algorithm acceptance (hopefully)
SAGE evaluation
Agree and sign NDA
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Crypto rump session

## New mobile phone security algorithms

- New set of algorithms proposed for inclusion in the "4G" mobile standard called LTE (Long Term Evolution):
  - Stream cipher ***ZUC***, the core of both new LTE algorithms
  - LTE encryption algorithm ***128-EEA3***, defined straightforwardly using ZUC
  - LTE integrity algorithm ***128-EIA3***, a Universal Hash Function with ZUC as its core
- Assessed by well known cryptologists – so far so good
- Now open for public evaluation
- http://zucalg.forumotion.net/

# IACR newsletter

## IACR Newsletter

The newsletter of the International Association for Cryptologic Research.

Vol. 25, No. 2, Autumn 2010, (Publication date: *3 October 2010*).

### Contents



### New Mobile Phone Security Algorithms - Public Evaluation Invited

A new set of cryptographic algorithms is being proposed for inclusion in the "4G" mobile standard called LTE (Long Term Evolution).

The algorithms are:

- a stream cipher called ZUC, which is the core of both new LTE algorithms;
- the LTE encryption algorithm called 128-EEA3, defined straightforwardly using ZUC;
- the LTE integrity algorithm called 128-EIA3, designed as a Universal Hash Function using ZUC as its core.

The algorithms are here: http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm. All of the algorithms were designed by DACAS, the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences. They have been evaluated by the algorithm standardisation group ETSI SAGE, and also by two other teams of well known cryptologists, and are believed to be strong and suitable for LTE.

Now the algorithms are open for public evaluation. Comments and analysis are invited, before a final decision is taken in (probably) January 2011 as to whether to include the new algorithms in the LTE standard. A discussion forum http://zucalg.forumotion.net/ has been created for this - please post any evaluation results there.

# The ZUC Forum

Search... Search

## ZUC Algorithm

Discussion of ZUC algorithm designed by DACAS

Home FAQ Search Register Log in



Current date/time is Mon Feb 07, 2011 2:19 pm

ZUC ALGORITHM DISCUSSION

This forum is for discussion of the new cryptographic algorithms that are proposed for inclusion in the "4G" mobile standard called LTE (Long Term Evolution).

The algorithms are:
* a stream cipher called ZUC, which is the core of both new LTE algorithms;
* the LTE encryption algorithm called 128-EEA3, defined straightforwardly using ZUC;
* the LTE integrity algorithm called 128-EIA3, designed as a Universal Hash Function using ZUC as its core.

All of the algorithms were designed by DACAS, the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences. They have been evaluated by the algorithm standardisation group ETSI SAGE, and also by two other teams of eminent experts, and are believed to be strong and suitable for LTE. Now the algorithms are open for public evaluation. Welcome to this forum for discussing them! Please share your analysis.

Please visit the following web pages for more information.

* Official ZUC algorithm web site
* ZUC algorithm web page at GSMA

View unanswered posts

| FORUM | TOPICS | POSTS | LAST POSTS |
|---|---|---|---|
| **Algorithm specifications and design documents**<br>Algorithm specifications and design documents | 5 | 14 | Tue Nov 23, 2010 3:09 am<br>**mathack** |
| **Discussion**<br>Discussions on ZUC Algorithm | 19 | 57 | Fri Feb 04, 2011 4:42 am<br>**zeshan** |

Today's active topics • Today's top 20 posters • Overall top 20 posters

WHO IS ONLINE ?

In total there is **1** user online :: 0 Registered, 0 Hidden and 1 Guest
Most users ever online was **19** on Tue Sep 14, 2010 10:51 am

# The first post

## History repeats itself

NEWTOPIC POSTREPLY ZUC Algorithm :: Discussion

Page 1 of 1 • Share • Actions !

### History repeats itself

random on Wed Aug 11, 2010 2:09 pm

**random**

Posts: 1
Join date: 2010-08-11

<rant>
My first reaction when seeing this news was to ask myself whether it was a joke. Unfortunately it seems it is not.

My 2nd reaction was to take this almost as an insult. Lots of efforts have been done in the cryptographic community to design state-of-the-art algorithms that could fit as best as possible the requirements of mobile phone communications. A well known project is "eStream". Cryptographers all around the world are competing against each other to provide the best algorithm that the industry could dream of.

But no of course that was not enough. I guess greediness is too strong. *AGAIN* you are doing the same mistake. Choose an algorithm from nowhere, without any serious external evaluation, with as sole design goal some random business requirement: "We need to pick an algorithm from China (so that we can win lots of $$$... we are so smart!) because that's a requirement from Chinese government". Sorry, don't want to be mean or anything to my Chinese peers, but "algorithm from China" does not ring with "confidentiality & privacy" to me.

Now, of course I guess you're only trying to cover yourselves by launching this pseudo-external evaluation. Hope you'll win the contest. By the way, how many submissions are there?
</rant>

# Questions

> Why not AES?

> Why not eStream?

> “Chinese algorithm” means China can break it?

> Is there something wrong with the other LTE algorithms?

> What happens now to the other LTE algorithms?

> Why does China get this special privilege?

> If every other country insists on a home-grown algorithm, will every LTE phone have to support 200 algorithms?

> Authenticated encryption?

# ZUC-10 Workshop


-->

- Home
- General Information
  - What is ZUC?
  - Important Dates
  - Sponsors
  - Contact Us
- Workshop Committees
  - Organizing Committee
- Call For Papers
  - Call for Papers
- Submission

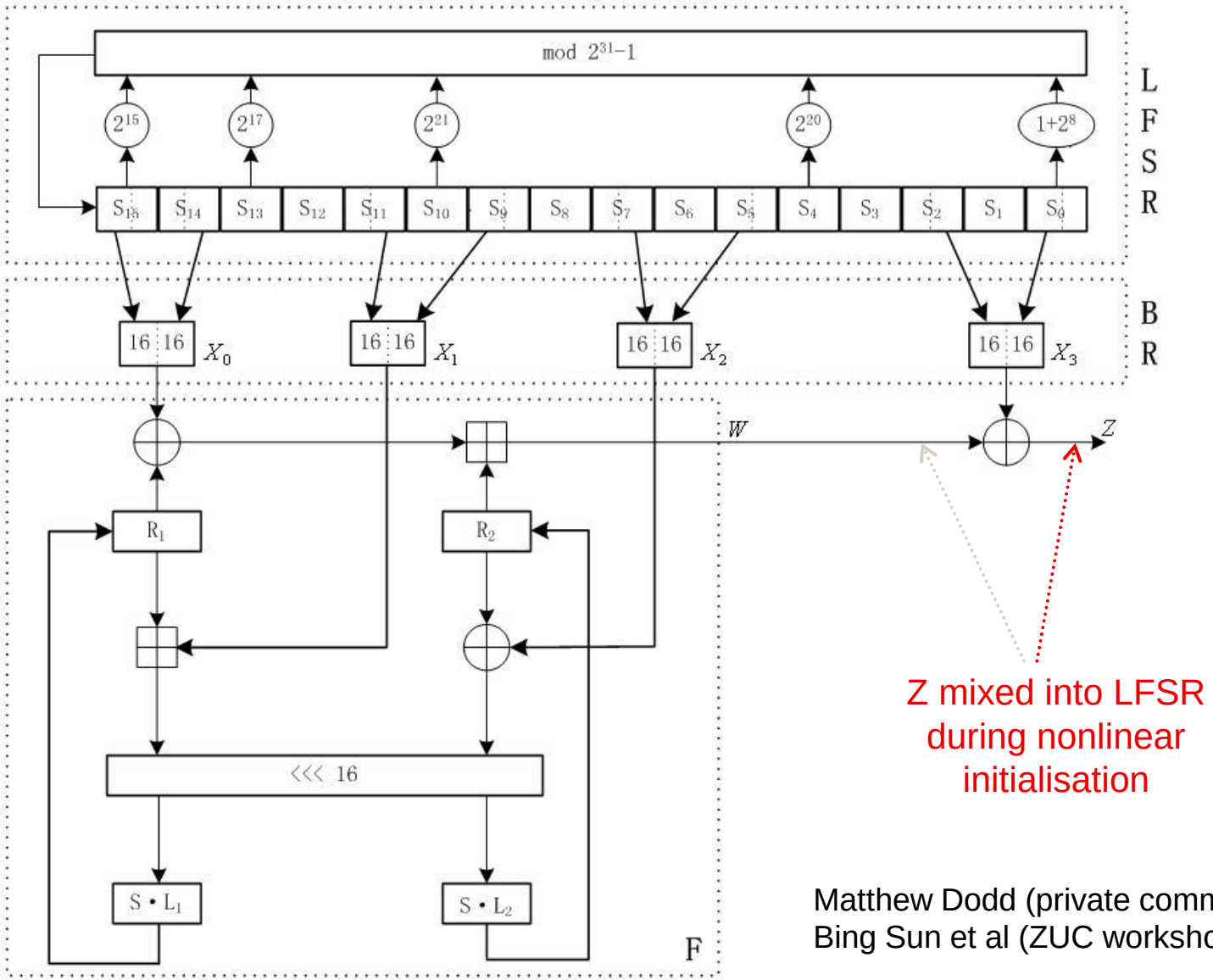
## Welcome to Workshop on ZUC Algorithm

The first International Workshop on ZUC algorithm will be held from December 2-3, 2010, in Beijing China. The workshop will be organized by the Data Assurance and Communication Security Research Center (DACAS) of the Chinese Academy of Sciences. The aim of the workshop is to provide a platform for discussion of the new cryptographic algorithms that are proposed for inclusion in the "4G" mobile standard called LTE (Long Term Evolution).

The workshop seeks original investigation results related to ZUC algorithm, topics of the workshop include but not limited to security analysis, performance and cost evaluation, hardware and software implementations and so on. Free accommodations will be provided to the correspondence author of accepted papers.

## Invitation letter

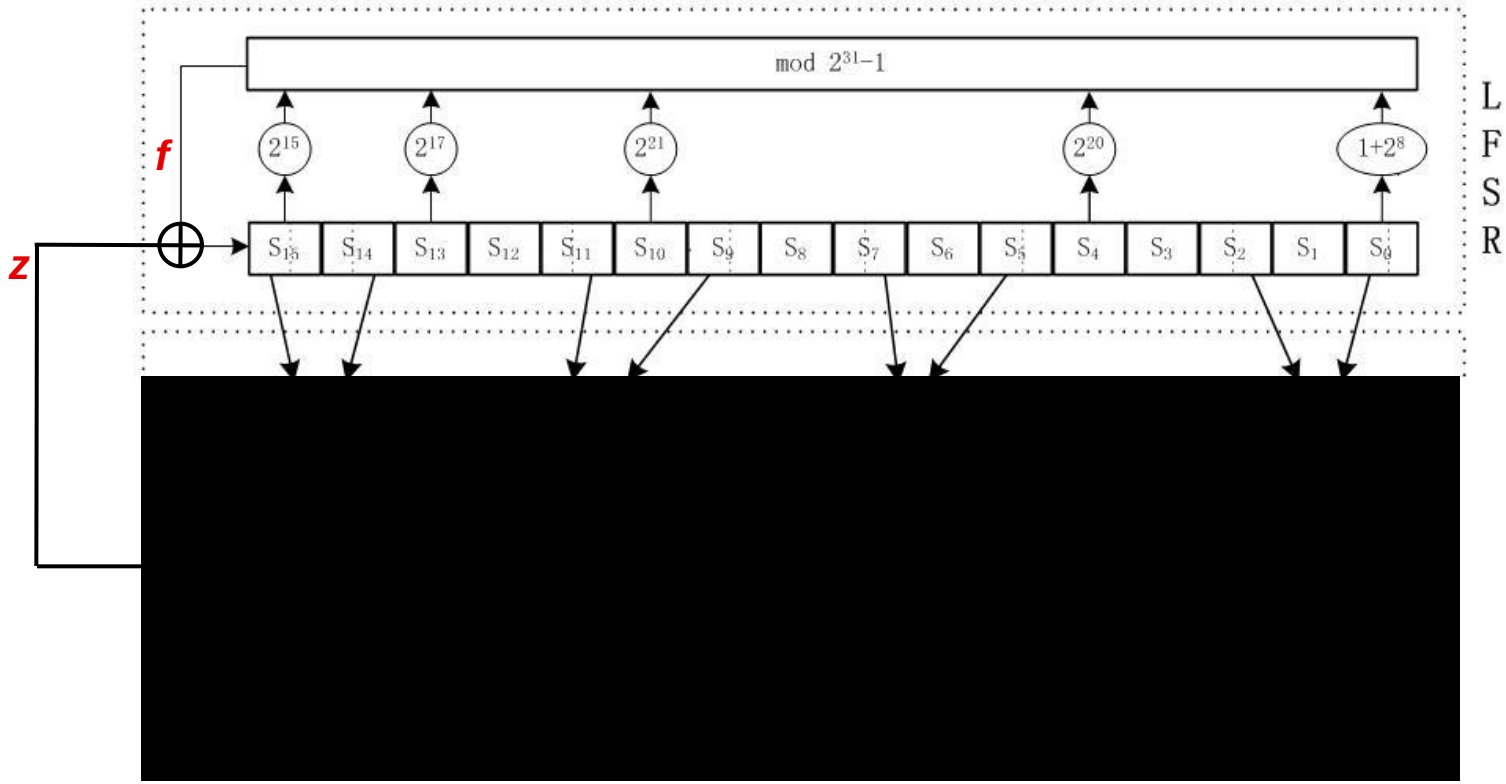
# Loss of entropy in initialisation (1)




Z mixed into LFSR during nonlinear initialisation

Matthew Dodd (private communication)
Bing Sun et al (ZUC workshop)

# Loss of entropy in initialisation (2)




$s_{16} = f \oplus z$

If $s_{16} = 0$, set $s_{16} = 2^{31}-1$

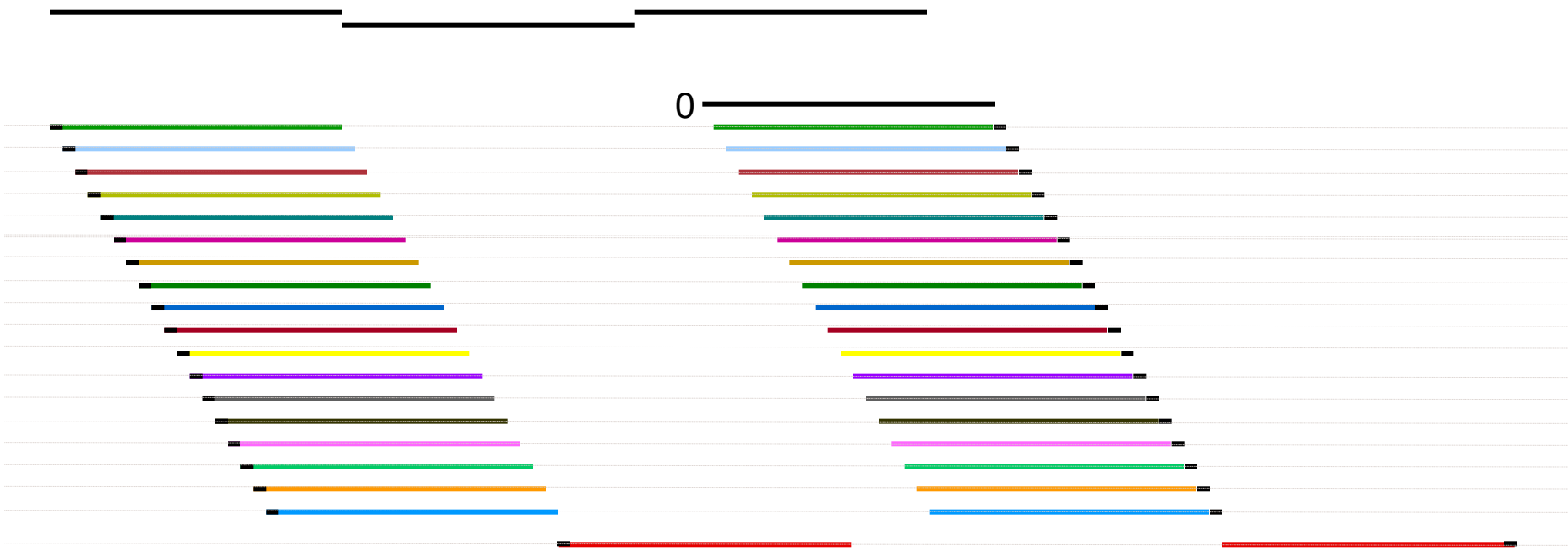
Whatever $f$ is …

… $z = 2^{31}-1-f$ gives the same result as $z = f$

Two IVs → colliding state

Hongjun Wu et al (AsiaCrypt rump session, IACR ePrint archive)

# Forgery attack on EIA3




Fuhr/Gilbert/Reinhard/Videau (ZUC workshop, IACR ePrint archive)

# New versions

GSM World

Our Work - Industry Technical Solutions - Fraud & Security - GSM Security Algorithms

**3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3**

** NEW ** REVISED VERSIONS of the Algorithms 128-EEA3 & 128-EIA3 are available for download prior to approval and publication of a final version by 3GPP. These revised versions were published in January 2011. They are still preliminary draft algorithm specifications, provided for evaluation purposes only, and subject to change.

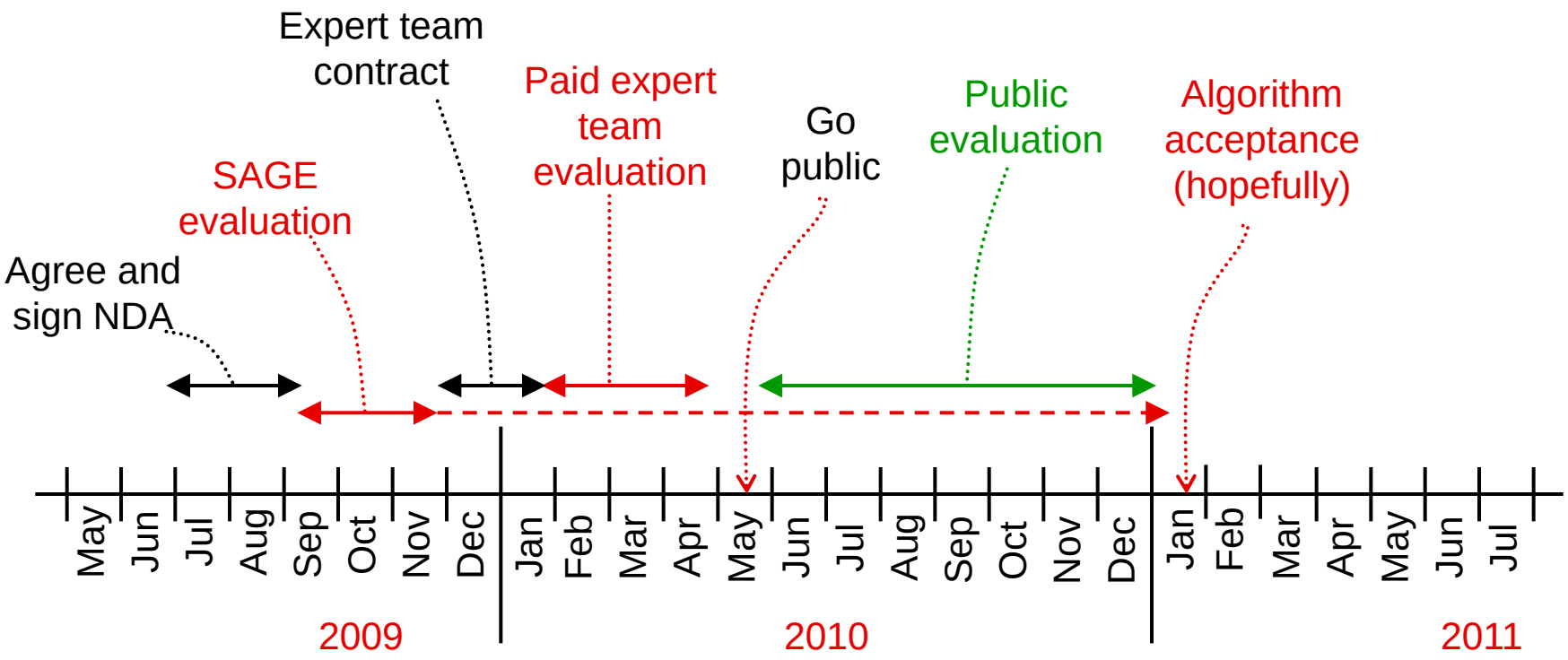
Individuals or companies intending to implement and/or use the 128-EEA3 & 128-EIA3 Algorithms will be required to sign appropriate usage undertakings with an appointed custodian, such as the GSM Association. Commercial implementors of the algorithms will need to demonstrate that they satisfy approval criteria yet to be specified and formal permission to use the algorithms will need to be obtained by way of signing appropriate usage undertakings and intellectual property agreements and paying any relevant administrative charges. These arrangements will be published by the GSM Association in due course.

The draft specifications are as follows:

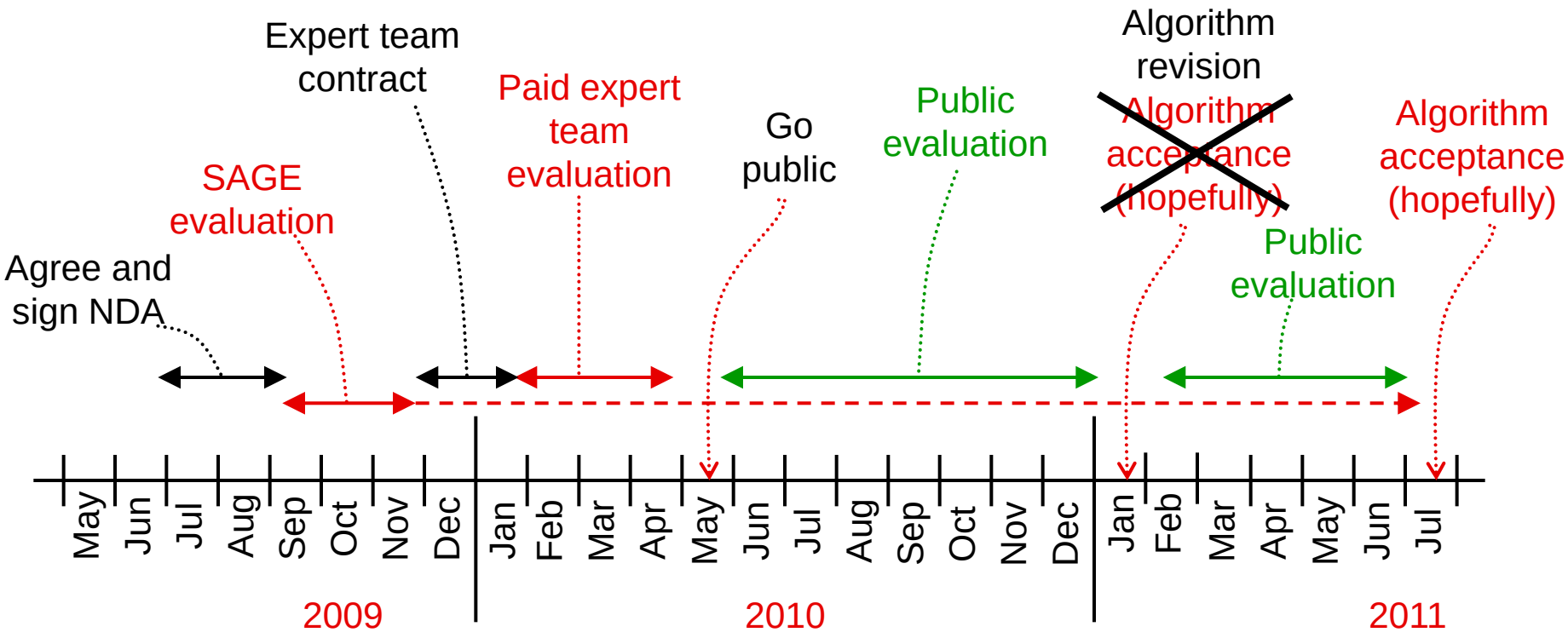
| | | |
|---|---|---|
| Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3 Revised versions published January 2011 | **Document 1:** Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: 128-EEA3 & 128-EIA3 Specification | pdf<br>doc |
| | **Document 2:** Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: ZUC Specification | pdf<br>doc |
| | **Document 3:** Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: Implementor's Test Data | pdf<br>doc |
| | **Document 4:** Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3: Design and Evaluation Report | pdf<br>doc |

Please note, that by obtaining or distributing this algorithm you may also be bound by laws in your own country about cryptographic algorithms. It is your responsibility to conform to all these restrictions.

# Plan D


Expert team contract
Paid expert team evaluation
Go public
Public evaluation
Algorithm acceptance (hopefully)
SAGE evaluation
Agree and sign NDA
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Plan E


Agree and sign NDA
SAGE evaluation
Expert team contract
Paid expert team evaluation
Go public
Public evaluation
Algorithm revision
Algorithm acceptance (hopefully)
Public evaluation
Algorithm acceptance (hopefully)
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2009
2010
2011

# Thank you

http://zucalg.forumotion.net/

http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm

or http://tinyurl.com/33ezbmj

# f8 construction for UMTS

> Note: a single frame of UMTS keystream will contain no more than 20000 bits (so ≈312 64-bit blocks)

– Pre-whitening constant is fixed within a frame, different for different frames

> Pre-whitening constant prevents known input/output pairs for single KASUMI

> Simple OFB mode allows short cycles — unlikely, but bad if they do happen

> Pre-whitening plus simple counter mode gives distinguisher with $2^{32}$ keystream blocks:

– e.g. if A is pre-whitening constant and C is block counter,
if $[A \oplus C] = [A' \oplus C']$ then likely that $[A \oplus (C + d)] = [A' \oplus (C' + d)]$ for some small d

> Simple counter mode without pre-whitening also gives $2^{32}$-block distinguisher:

– No collisions

> With the *f*8 construction, and individual frames limited to ≈312 64-bit blocks, the only distinguishers we found needed substantially more than $2^{32}$ blocks

– In fact, more than $2^{32}$ frames — and frame counter COUNT is only 32 bits anyway