

An update from ETSI SAGE Security Algorithms Group of Experts

by Steve Babbage¹, Chairman

1. Introduction to the work of SAGE

SAGE specifies cryptographic algorithms for use in standardised telecoms systems. In recent years most of our work has been for mobile telephone standards (GSM, GPRS, UMTS), with some work on TETRA.

SAGE only meets when it has major work to do (which generally means during the specification of major new algorithms). Otherwise we generally carry out business by email or conference call.

2. Major recent algorithm developments: UEA2, UIA2

The current radio interface protection algorithms for UMTS — UEA1 for encryption, and UIA1 for integrity of signalling messages — were designed by SAGE back in 1999. They are published algorithms, as all new mobile telephony algorithms are these days.

No weakness has been discovered in these algorithms², and there is no indication that a weakness is likely to be found. However, if one ever were found, it would be much better to have a replacement already in place on mobile phones. So 3GPP SA3, together with the GSM Association, asked SAGE to specify a second set of algorithms, UEA2 and UIA2.

Apart from the obvious requirements on speed and implementation complexity, the main design criterion for these new algorithms was that they should be fundamentally different in nature from UEA1 and UIA1. That way, if an advance in cryptanalytic theory ever threatens one set of algorithms, it will be unlikely to affect the other.

SAGE delivered the UEA2 and UIA2 specifications in January 2006. At the heart of these algorithms is the SNOW 3G stream cipher — a variant of the well respected SNOW 2.0 cipher designed by Thomas Johansson and Patrik Ek Dahl. SNOW 3G was designed by SAGE, with the variations from SNOW 2.0 introduced specifically to strengthen it against a kind of cryptanalytic threat called “algebraic attacks”.

¹ Vodafone Group R&D, steve.babbage@vodafone.com, +44 7787 153932

² One cryptanalytic attack has been published on the block cipher KASUMI that lies at the heart of the UEA1 and UIA1 algorithms. However, this is a type of attack that makes *extremely* optimistic assumptions about the sort of information that is available to the attacker (so many would not accept it as a valid attack at all). It in no way weakens the UEA1 and UIA1 algorithms as they are used in UMTS.

3. Other activities

3.1. *Phasing out of A5/2*

The A5/2 encryption algorithm for GSM is extremely weak — it provides no protection at all against eavesdropping. (The hard part for an attacker is extracting the target's voice traffic off the radio interface; after that, stripping off the A5/2 encryption is simple and practically instantaneous.)

The fact that handsets support A5/2 at all is a point of vulnerability, even in networks that operate the stronger A5/1 algorithm. This is because of the “Barkan-Biham-Keller attack” — see figures 1 and 2.

The correct immediate response is for new phones not to support A5/2. All networks that do not support A5/1 should allow A5/0 (no encryption), so there should be no interoperability issue. The GSM Association have been leading the work to persuade various elements of industry to go along with this change; SAGE has been supporting this campaign in various ways.

3.2. *TETRA*

During 2005, SAGE undertook a study for TETRA on whether the existing encryption algorithms could safely be used to protect the longer traffic frames that would be introduced by the new TETRA standard. The study was in fact subcontracted to Codes & Ciphers Ltd, for resourcing reasons. (The answer was: yes, they can.)

Apart from that there have been few requests from the TETRA group. We have agreed pragmatic changes to the rules for management of certain secret algorithms. We have just been asked to specify a new function as part of the TETRA authentication algorithm set, but this will only be a small piece of work.

3.3. *Others*

Right at the end of 2005 we worked with 3GPP SA3 to define a key generation algorithm for the GSM/UMTS Voice Group Call Service, based on the well known (SAGE-specified) MILENAGE algorithm for UMTS authentication and key agreement.

In 2006 we carried out a review of the DECT security algorithms, which have been in place for quite a long time. We will recommend new DECT algorithms based on public designs (e.g. on AES, although that is not decided yet).

4. The outlook

A5/1 is a mid-strength algorithm. Various cryptanalytic attacks against it have been published; however, we have not seen any substantiated claims of anyone eavesdropping on GSM calls by breaking A5/1 in practice.

There is a chance, though, that equipment to break A5/1 encryption on GSM will begin to emerge in the next few years. If it does, the good news is that the replacement is already available: A5/3 was designed by SAGE in 2002, and is much stronger. The less good news is that it is barely supported yet: as far as I know, no operator has deployed A5/3 in their network, and it is only just beginning to be introduced by terminal manufacturers.

A5/3 (and the GPRS algorithm GEA3) were adapted from UEA1. A possible piece of work for SAGE in the near future would be to adapt UEA2 to create an A5/4 algorithm for GSM. That would give two strong GSM encryption algorithms, as we now have for UMTS. However, given the slow deployment of new algorithms for GSM³, it could be a very long time before this would add value in practice.

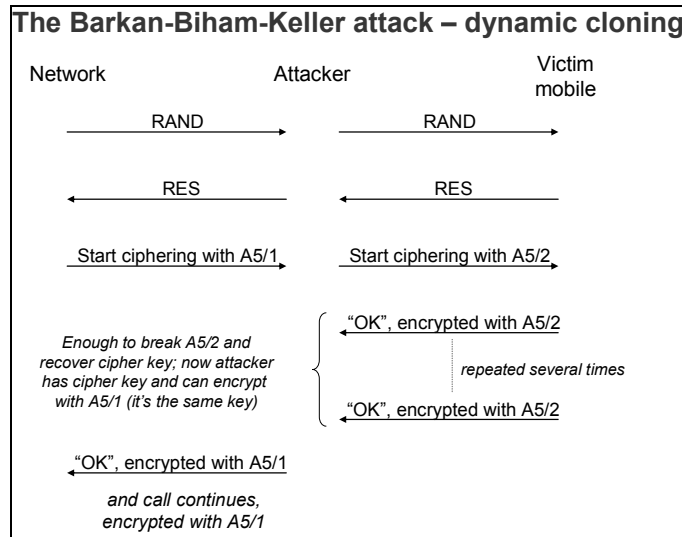


Figure 1

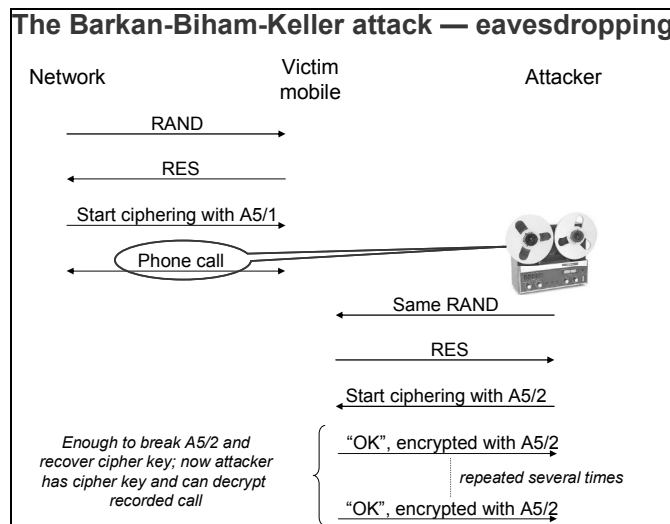


Figure 2

³ GSM encryption is performed in the base station — and there are an awful lot of base stations in an operator network. Introducing substantially different algorithms typically requires a hardware upgrade, not just a software change. So upgrading a network to support a new GSM algorithm is very expensive.