A5/1

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/A5/1#mw-head)[Jump to search](https://en.wikipedia.org/wiki/A5/1#searchInput)

**A5/1** is a [stream cipher](https://en.wikipedia.org/wiki/Stream_cipher) used to provide over-the-air communication [privacy](https://en.wikipedia.org/wiki/Privacy) in the [GSM](https://en.wikipedia.org/wiki/Global_System_for_Mobile_Communications) [cellular telephone](https://en.wikipedia.org/wiki/Cell_phone) standard. It is one of seven algorithms which were specified for GSM use.[[1]](https://en.wikipedia.org/wiki/A5/1#cite_note-ChangeReq-1) It was initially kept secret, but became public knowledge through leaks and [reverse engineering](https://en.wikipedia.org/wiki/Reverse_engineering). A number of serious weaknesses in the cipher have been identified.



**Contents**

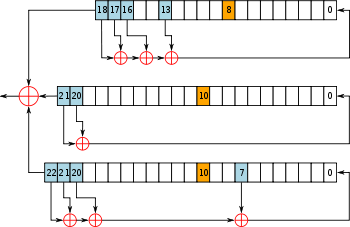
* [1History and usage](https://en.wikipedia.org/wiki/A5/1#History_and_usage)
* [2Description](https://en.wikipedia.org/wiki/A5/1#Description)
* [3Security](https://en.wikipedia.org/wiki/A5/1#Security)
  + [3.1Known-plaintext attacks](https://en.wikipedia.org/wiki/A5/1#Known-plaintext_attacks)
  + [3.2Attacks on A5/1 as used in GSM](https://en.wikipedia.org/wiki/A5/1#Attacks_on_A5/1_as_used_in_GSM)
* [4See also](https://en.wikipedia.org/wiki/A5/1#See_also)
* [5Notes](https://en.wikipedia.org/wiki/A5/1#Notes)
* [6References](https://en.wikipedia.org/wiki/A5/1#References)
* [7External links](https://en.wikipedia.org/wiki/A5/1#External_links)

History and usage[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=1)]

A5/1 is used in [Europe](https://en.wikipedia.org/wiki/Europe) and the United States. [A5/2](https://en.wikipedia.org/wiki/A5/2) was a deliberate weakening of the algorithm for certain export regions.[[2]](https://en.wikipedia.org/wiki/A5/1#cite_note-2) A5/1 was developed in 1987, when GSM was not yet considered for use outside Europe, and [A5/2](https://en.wikipedia.org/wiki/A5/2) was developed in 1989. Though both were initially kept secret, the general design was leaked in 1994 and the algorithms were entirely reverse engineered in 1999 by [Marc Briceno](https://en.wikipedia.org/w/index.php?title=Marc_Briceno&action=edit&redlink=1) from a GSM telephone. In 2000, around 130 million GSM customers relied on A5/1 to protect the confidentiality of their voice communications; by 2014, it was 7.2 billion.[[3]](https://en.wikipedia.org/wiki/A5/1#cite_note-3)

Security researcher [Ross Anderson](https://en.wikipedia.org/wiki/Ross_J._Anderson) reported in 1994 that "there was a terrific row between the [NATO](https://en.wikipedia.org/wiki/NATO) [signal intelligence agencies](https://en.wikipedia.org/wiki/SIGINT) in the mid-1980s over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the [Warsaw Pact](https://en.wikipedia.org/wiki/Warsaw_Pact); but the other countries didn't feel this way, and the algorithm as now fielded is a French design."[[4]](https://en.wikipedia.org/wiki/A5/1#cite_note-Ross94-4)

Description[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=2)]

[](https://en.wikipedia.org/wiki/File:A5-1_GSM_cipher.svg)

The A5/1 stream cipher uses three [LFSRs](https://en.wikipedia.org/wiki/LFSR). A register is clocked if its clocking bit (orange) agrees with the clocking bit of one or both of the other two registers.

A GSM transmission is organised as sequences of *bursts*. In a typical channel and in one direction, one burst is sent every 4.615 milliseconds and contains 114 bits available for information. A5/1 is used to produce for each burst a 114 bit sequence of [keystream](https://en.wikipedia.org/wiki/Keystream) which is [XORed](https://en.wikipedia.org/wiki/XOR) with the 114 bits prior to modulation. A5/1 is initialised using a 64-bit [key](https://en.wikipedia.org/wiki/Key_(cryptography)) together with a publicly known 22-bit frame number. Older fielded GSM implementations using Comp128v1 for key generation, had 10 of the key bits fixed at zero, resulting in an effective [key length](https://en.wikipedia.org/wiki/Key_length) of 54 bits. This weakness was rectified with the introduction of Comp128v3 which yields proper 64 bits keys. When operating in GPRS / EDGE mode, higher bandwidth radio modulation allows for larger 348 bits frames, and [A5/3](https://en.wikipedia.org/wiki/A5/3) is then used in a stream cipher mode to maintain confidentiality.

A5/1 is based around a combination of three [linear feedback shift registers](https://en.wikipedia.org/wiki/Linear_feedback_shift_register) (LFSRs) with irregular clocking. The three shift registers are specified as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LFSR number** | **Length in bits** | **Feedback polynomial** | **Clocking bit** | **Tapped bits** |
| 1 | 19 | {\displaystyle x^{19}+x^{18}+x^{17}+x^{14}+1} | 8 | 13, 16, 17, 18 |
| 2 | 22 | {\displaystyle x^{22}+x^{21}+1} | 10 | 20, 21 |
| 3 | 23 | {\displaystyle x^{23}+x^{22}+x^{21}+x^{8}+1} | 10 | 7, 20, 21, 22 |

The bits are indexed with the [least significant bit](https://en.wikipedia.org/wiki/Least_significant_bit) (LSB) as 0.

The registers are clocked in a stop/go fashion using a majority rule. Each register has an associated clocking bit. At each cycle, the clocking bit of all three registers is examined and the majority bit is determined. A register is clocked if the clocking bit agrees with the majority bit. Hence at each step at least two or three registers are clocked, and each register steps with probability 3/4.

Initially, the registers are set to zero. Then for 64 cycles, the 64-bit secret key is mixed in according to the following scheme: in cycle {\displaystyle 0\leq {i}<64}, the *i*th key bit is added to the least significant bit of each register using XOR —

{\displaystyle R[0]=R[0]\oplus K[i].}

Each register is then clocked.

Similarly, the 22-bits of the frame number are added in 22 cycles. Then the entire system is clocked using the normal majority clocking mechanism for 100 cycles, with the output discarded. After this is completed, the cipher is ready to produce two 114 bit sequences of output keystream, first 114 for downlink, last 114 for uplink.

Security[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=3)]

[](https://en.wikipedia.org/wiki/File:CipheringNotProvided.jpg)

The message on the screen of a mobile phone with the warning about lack of ciphering

A number of attacks on A5/1 have been published, and the American [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) is able to routinely decrypt A5/1 messages according to released internal documents.[[5]](https://en.wikipedia.org/wiki/A5/1#cite_note-5)

Some attacks require an expensive preprocessing stage after which the cipher can be broken in minutes or seconds. Until recently, the weaknesses have been passive attacks using the [known plaintext](https://en.wikipedia.org/wiki/Known_plaintext) assumption. In 2003, more serious weaknesses were identified which can be exploited in the [ciphertext-only scenario](https://en.wikipedia.org/wiki/Ciphertext_only_attack), or by an active attacker. In 2006 Elad Barkan, [Eli Biham](https://en.wikipedia.org/wiki/Eli_Biham) and Nathan Keller demonstrated attacks against A5/1, [A5/3](https://en.wikipedia.org/wiki/A5/3), or even GPRS that allow attackers to tap GSM mobile phone conversations and decrypt them either in real-time, or at any later time.

According to professor Jan Arild Audestad, at the standardization process which started in 1982, A5/1 was originally proposed to have a key length of 128 bits. At that time, 128 bits was projected to be secure for at least 15 years. It is now believed that 128 bits would in fact also still be secure until the [advent of quantum computing](https://en.wikipedia.org/wiki/Post-quantum_cryptography). Audestad, Peter van der Arend, and [Thomas Haug](https://en.wikipedia.org/wiki/Thomas_Haug) says that the British insisted on weaker encryption, with Haug saying he was told by the British delegate that this was to allow the British secret service to eavesdrop more easily. The British proposed a key length of 48 bits, while the West Germans wanted stronger encryption to protect against East German spying, so the compromise became a key length of 54 bits.[[6]](https://en.wikipedia.org/wiki/A5/1#cite_note-6)

**Known-plaintext attacks**[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=4)]

The first attack on the A5/1 was proposed by [Ross Anderson](https://en.wikipedia.org/wiki/Ross_J._Anderson) in 1994. Anderson's basic idea was to guess the complete content of the registers R1 and R2 and about half of the register R3. In this way the clocking of all three registers is determined and the second half of R3 can be computed.[[4]](https://en.wikipedia.org/wiki/A5/1#cite_note-Ross94-4)

In 1997, Golic presented an attack based on solving sets of linear equations which has a time complexity of 240.16 (the units are in terms of number of solutions of a system of linear equations which are required).

In 2000, [Alex Biryukov](https://en.wikipedia.org/wiki/Alex_Biryukov), [Adi Shamir](https://en.wikipedia.org/wiki/Adi_Shamir) and [David Wagner](https://en.wikipedia.org/wiki/David_A._Wagner) showed that A5/1 can be [cryptanalysed](https://en.wikipedia.org/wiki/Cryptanalysis) in real time using a time-memory tradeoff attack,[[7]](https://en.wikipedia.org/wiki/A5/1#cite_note-7) based on earlier work by Jovan Golic.[[8]](https://en.wikipedia.org/wiki/A5/1#cite_note-8) One tradeoff allows an attacker to reconstruct the key in one second from two minutes of known plaintext or in several minutes from two seconds of known plain text, but he must first complete an expensive preprocessing stage which requires 248 steps to compute around 300 GB of data. Several tradeoffs between preprocessing, data requirements, attack time and memory complexity are possible.

The same year, [Eli Biham](https://en.wikipedia.org/wiki/Eli_Biham) and [Orr Dunkelman](https://en.wikipedia.org/w/index.php?title=Orr_Dunkelman&action=edit&redlink=1) also published an attack on A5/1 with a total work complexity of 239.91 A5/1 clockings given 220.8 bits of [known plaintext](https://en.wikipedia.org/wiki/Known_plaintext). The attack requires 32 GB of data storage after a [precomputation](https://en.wikipedia.org/wiki/Precomputation) stage of 238.[[9]](https://en.wikipedia.org/wiki/A5/1#cite_note-9)

Ekdahl and Johansson published an attack on the initialisation procedure which breaks A5/1 in a few minutes using two to five minutes of conversation plaintext.[[10]](https://en.wikipedia.org/wiki/A5/1#cite_note-10) This attack does not require a preprocessing stage. In 2004, Maximov *et al.* improved this result to an attack requiring "less than one minute of computations, and a few seconds of known conversation". The attack was further improved by [Elad Barkan](https://en.wikipedia.org/w/index.php?title=Elad_Barkan&action=edit&redlink=1) and [Eli Biham](https://en.wikipedia.org/wiki/Eli_Biham) in 2005.[[11]](https://en.wikipedia.org/wiki/A5/1#cite_note-11)

**Attacks on A5/1 as used in GSM**[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=5)]

In 2003, Barkan *et al.* published several attacks on GSM encryption.[[12]](https://en.wikipedia.org/wiki/A5/1#cite_note-12) The first is an active attack. GSM phones can be convinced to use the much weaker [A5/2](https://en.wikipedia.org/wiki/A5/2) cipher briefly. A5/2 can be broken easily, and the phone uses the same key as for the stronger A5/1 algorithm. A second attack on A5/1 is outlined, a [ciphertext-only](https://en.wikipedia.org/wiki/Ciphertext-only) time-memory tradeoff attack which requires a large amount of precomputation.

In 2006, [Elad Barkan](https://en.wikipedia.org/w/index.php?title=Elad_Barkan&action=edit&redlink=1), [Eli Biham](https://en.wikipedia.org/wiki/Eli_Biham), [Nathan Keller](https://en.wikipedia.org/w/index.php?title=Nathan_Keller&action=edit&redlink=1) published the full version of their 2003 paper, with attacks against A5/X сiphers. The authors claim:[[13]](https://en.wikipedia.org/wiki/A5/1#cite_note-13)

We present a very practical ciphertext-only cryptanalysis of GSM encrypted communication, and various active attacks on the GSM protocols. These attacks can even break into GSM networks that use "unbreakable" ciphers. We first describe a ciphertext-only attack on A5/2 that requires a few dozen milliseconds of encrypted off-the-air cellular conversation and finds the correct key in less than a second on a personal computer. We extend this attack to a (more complex) ciphertext-only attack on A5/1. We then describe new (active) attacks on the protocols of networks that use A5/1, A5/3, or even GPRS. These attacks exploit flaws in the GSM protocols, and they work whenever the mobile phone supports a weak cipher such as A5/2. We emphasize that these attacks are on the protocols, and are thus applicable whenever the cellular phone supports a weak cipher, for example, they are also applicable for attacking A5/3 networks using the cryptanalysis of A5/1. Unlike previous attacks on GSM that require unrealistic information, like long known plaintext periods, our attacks are very practical and do not require any knowledge of the content of the conversation. Furthermore, we describe how to fortify the attacks to withstand reception errors. As a result, our attacks allow attackers to tap conversations and decrypt them either in real-time, or at any later time.

In 2007 [Universities of Bochum](https://en.wikipedia.org/wiki/University_of_Bochum) and Kiel started a research project to create a massively parallel [FPGA](https://en.wikipedia.org/wiki/FPGA)-based cryptographic accelerator [COPACOBANA](http://www.sciengines.com/copacobana/). COPACOBANA was the first commercially available solution[[14]](https://en.wikipedia.org/wiki/A5/1#cite_note-14) using fast time-memory trade-off techniques that could be used to attack the popular A5/1 and A5/2 algorithms, used in GSM voice encryption, as well as the [Data Encryption Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES). It also enables [brute force attacks](https://en.wikipedia.org/wiki/Brute_force_attack) against GSM eliminating the need of large precomputed lookup tables.

In 2008, the group [The Hackers Choice](https://en.wikipedia.org/w/index.php?title=The_Hackers_Choice&action=edit&redlink=1) launched a project to develop a practical attack on A5/1. The attack requires the construction of a large look-up table of approximately 3 terabytes. Together with the scanning capabilities developed as part of the sister project, the group expected to be able to record any GSM call or SMS encrypted with A5/1, and within about 3–5 minutes derive the encryption key and hence listen to the call and read the SMS in clear. But the tables weren't released.[[15]](https://en.wikipedia.org/wiki/A5/1#cite_note-nohl26c3-15)

A similar effort, the [A5/1 Cracking Project](https://web.archive.org/web/20090821163913/http:/reflextor.com/trac/a51/wiki), was announced at the [2009 Black Hat security conference](https://en.wikipedia.org/wiki/Black_Hat_Briefings) by cryptographers [Karsten Nohl](https://de.wikipedia.org/wiki/Karsten_Nohl) and Sascha Krißler. It created the look-up tables using [Nvidia](https://en.wikipedia.org/wiki/Nvidia) [GPGPUs](https://en.wikipedia.org/wiki/GPGPU) via a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) [distributed computing](https://en.wikipedia.org/wiki/Distributed_computing) architecture. Starting in the middle of September 2009, the project ran the equivalent of 12 Nvidia GeForce GTX 260. According to the authors, the approach can be used on any cipher with key size up to 64-bits.[[16]](https://en.wikipedia.org/wiki/A5/1#cite_note-nohl-16)

In December 2009, the A5/1 Cracking Project attack tables for A5/1 were announced by Chris Paget and Karsten Nohl. The tables use a combination of compression techniques, including [rainbow tables](https://en.wikipedia.org/wiki/Rainbow_table) and distinguished point chains. These tables constituted only parts of the 1.7 TB completed table and had been computed during three months using 40 distributed [CUDA](https://en.wikipedia.org/wiki/CUDA) nodes and then published over [BitTorrent](https://en.wikipedia.org/wiki/BitTorrent_(protocol)). [[15]](https://en.wikipedia.org/wiki/A5/1#cite_note-nohl26c3-15)[[16]](https://en.wikipedia.org/wiki/A5/1#cite_note-nohl-16)[[17]](https://en.wikipedia.org/wiki/A5/1#cite_note-17)[[18]](https://en.wikipedia.org/wiki/A5/1#cite_note-18) More recently the project has announced a switch to faster ATI [Evergreen](https://en.wikipedia.org/wiki/Evergreen_(GPU_family)) code, together with a change in the format of the tables and [Frank A. Stevenson](https://en.wikipedia.org/wiki/Frank_A._Stevenson) announced breaks of A5/1 using the ATI generated tables.[[19]](https://en.wikipedia.org/wiki/A5/1#cite_note-19)

Documents leaked by Edward Snowden in 2013 state that the NSA "can process encrypted A5/1".[[20]](https://en.wikipedia.org/wiki/A5/1#cite_note-20)

See also[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=6)]

* [A5/2](https://en.wikipedia.org/wiki/A5/2)
* [KASUMI](https://en.wikipedia.org/wiki/KASUMI_(block_cipher)), also known as A5/3
* [Cellular Message Encryption Algorithm](https://en.wikipedia.org/wiki/Cellular_Message_Encryption_Algorithm)

Notes[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=7)]

* 1. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-ChangeReq_1-0) [*"Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support"*](http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip)*.*
  2. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-2) *Quirke, Jeremy (1 May 2004).*[*"Security in the GSM system"*](https://web.archive.org/web/20040712061808/http:/www.ausmobile.com/downloads/technical/Security%20in%20the%20GSM%20system%2001052004.pdf)*(PDF). AusMobile. Archived from*[*the original*](http://www.ausmobile.com/downloads/technical/Security+in+the+GSM+system+01052004.pdf)*(PDF) on 12 July 2004. Retrieved 8 September 2008.*
  3. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-3) [*"There are officially more mobile devices than people in the world"*](https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html)*. The Independent. 7 October 2014. Retrieved 19 December 2017.*
  4. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/A5/1#cite_ref-Ross94_4-0) [***b***](https://en.wikipedia.org/wiki/A5/1#cite_ref-Ross94_4-1) [*Ross Anderson*](https://en.wikipedia.org/wiki/Ross_J._Anderson)*(17 June 1994).*[*"A5 (Was: HACKING DIGITAL PHONES)"*](https://groups.google.com/groups?selm=2ts9a0%2495r%40lyra.csx.cam.ac.uk)*.*[*Newsgroup*](https://en.wikipedia.org/wiki/Usenet_newsgroup)*:*[*uk.telecom*](news:uk.telecom)*.*[*Usenet:*](https://en.wikipedia.org/wiki/Usenet_(identifier))[*2ts9a0$95r@lyra.csx.cam.ac.uk*](news:2ts9a0$95r@lyra.csx.cam.ac.uk)*.*
  5. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-5) [NSA Able To Crack A5/1 Cellphone Crypto - Slashdot](http://yro.slashdot.org/story/13/12/14/0148251/nsa-able-to-crack-a51-cellphone-crypto)
  6. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-6) <http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html#.UtBeNpD_sQs>
  7. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-7) [*Biryukov, Alex*](https://en.wikipedia.org/wiki/Alex_Biryukov)*;*[*Adi Shamir*](https://en.wikipedia.org/wiki/Adi_Shamir)*;*[*David Wagner*](https://en.wikipedia.org/wiki/David_A._Wagner)*.*[*"Real Time Cryptanalysis of A5/1 on a PC"*](http://www.crypto.com/papers/others/a5.ps)*. Fast Software Encryption—FSE 2000: 1–18.*
  8. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-8) *Golic, Jovan Dj. (1997).*[*"Cryptanalysis of Alleged A5 Stream Cipher"*](https://web.archive.org/web/20100715211638/http:/saluc.engr.uconn.edu/refs/stream_cipher/golic97A5.pdf)*(PDF). Eurocrypt 1997: 239–55. Archived from*[*the original*](http://saluc.engr.uconn.edu/refs/stream_cipher/golic97A5.pdf)*(PDF) on 15 July 2010. Retrieved 13 January 2016.*
  9. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-9) *Biham, Eli; Orr Dunkelman (2000). "Cryptanalysis of the A5/1 GSM Stream Cipher". Indocrypt 2000. Lecture Notes in Computer Science.****1977****: 43–51.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1007/3-540-44495-5\_5*](https://doi.org/10.1007%2F3-540-44495-5_5)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-3-540-41452-0*](https://en.wikipedia.org/wiki/Special:BookSources/978-3-540-41452-0)*.*
  10. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-10) *Ekdahl, Patrik; Thomas Johansson (2003).*[*"Another attack on A5/1"*](https://web.archive.org/web/20050525191646/http:/www.it.lth.se/patrik/papers/a5full.pdf)*(PDF). IEEE Transactions on Information Theory.****49****(1): 284–89.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/TIT.2002.806129*](https://doi.org/10.1109%2FTIT.2002.806129)*. Archived from*[*the original*](http://www.it.lth.se/patrik/papers/a5full.pdf)*(PDF) on 25 May 2005.*
  11. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-11) *Barkan, Elad; Eli Biham (2005). "Conditional Estimators: An Effective Attack on A5/1". Selected Areas in Cryptography 2005: 1–19.*
  12. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-12) *Barkan, Elad;*[*Eli Biham*](https://en.wikipedia.org/wiki/Eli_Biham)*; Nathan Keller (2003).*[*"Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication"*](https://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf)*(PDF). Crypto 2003. Lecture Notes in Computer Science.****2729****: 600–16.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1007/978-3-540-45146-4\_35*](https://doi.org/10.1007%2F978-3-540-45146-4_35)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-3-540-40674-7*](https://en.wikipedia.org/wiki/Special:BookSources/978-3-540-40674-7)*.*
  13. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-13) *Barkan, Elad; Eli Biham; Nathan Keller.*[*"Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication by Barkan and Biham of Technion (Full Version)"*](https://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf)*(PDF).*
  14. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-14) *Gueneysu, Tim; Timo Kasper; Martin Novotný; Christof Paar; Andy Rupp (2008).*[*"Cryptanalysis with COPACOBANA"*](http://www.sciengines.com/copacobana/paper/TC_COPACOBANA.pdf)*(PDF).*[*IEEE Transactions on Computers*](https://en.wikipedia.org/wiki/IEEE_Transactions_on_Computers)*.****57****(11): 1498–1513.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/TC.2008.80*](https://doi.org/10.1109%2FTC.2008.80)*.*
  15. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/A5/1#cite_ref-nohl26c3_15-0) [***b***](https://en.wikipedia.org/wiki/A5/1#cite_ref-nohl26c3_15-1) *Nohl, Karsten; Chris Paget (27 December 2009).*[*GSM: SRSLY?*](https://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html)*. 26th Chaos Communication Congress (26C3).*[*Archived*](https://web.archive.org/web/20100106084817/http:/events.ccc.de/congress/2009/Fahrplan/events/3654.en.html)*from the original on 6 January 2010. Retrieved 30 December 2009.*
  16. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/A5/1#cite_ref-nohl_16-0) [***b***](https://en.wikipedia.org/wiki/A5/1#cite_ref-nohl_16-1) [*"Archived copy"*](https://web.archive.org/web/20110726142029/https:/har2009.org/program/attachments/119_GSM.A51.Cracking.Nohl.pdf)*(PDF). Archived from*[*the original*](https://har2009.org/program/attachments/119_GSM.A51.Cracking.Nohl.pdf)*(PDF)on 26 July 2011. Retrieved 29 December 2009.* Subverting the security base of GSM. Karsten Nohl and Sascha Krißler
  17. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-17) *O'Brien, Kevin (28 December 2009).*[*"Cellphone Encryption Code Is Divulged"*](https://www.nytimes.com/2009/12/29/technology/29hack.html)*. New York Times.*[*Archived*](https://web.archive.org/web/20110429225151/http:/www.nytimes.com/2009/12/29/technology/29hack.html)*from the original on 29 April 2011. Retrieved 29 December 2009.*
  18. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-18) *McMillan, Robert.*[*"Hackers Show It's Easy to Snoop on a GSM Call"*](http://www.pcworld.com/article/185542/hackers_show_its_easy_to_snoop_on_a_gsm_call.html)*. IDG News Service.*
  19. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-19) *Frank A. Stevenson (1 May 2010).*[*"Cracks beginning to show in A5/1"*](https://web.archive.org/web/20120306125406/http:/lists.lists.reflextor.com/pipermail/a51/2010-May/000605.html)*. Archived from*[*the original*](http://lists.lists.reflextor.com/pipermail/a51/2010-May/000605.html)*on 6 March 2012.*
  20. [**^**](https://en.wikipedia.org/wiki/A5/1#cite_ref-20) *Timberg, Craig; Soltani, Ashkan (13 December 2013).*[*"By cracking cellphone code, NSA has ability to decode private conversations"*](https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html)*.*[*The Washington Post*](https://en.wikipedia.org/wiki/The_Washington_Post)*. Retrieved 28 September2016.*

References[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=8)]

* *Rose, Greg (10 September 2003).*[*"A precis of the new attacks on GSM encryption"*](https://web.archive.org/web/20110927122703/http:/www.qualcomm.com.au/PublicationsDocs/GSM_Attacks.pdf)*(PDF).*[*QUALCOMM*](https://en.wikipedia.org/wiki/QUALCOMM)*Australia. Archived from*[*the original*](http://www.qualcomm.com.au/PublicationsDocs/GSM_Attacks.pdf)*(PDF) on 27 September 2011. Retrieved 17 October 2004.*
* *Maximov, Alexander; Thomas Johansson; Steve Babbage (2004). "An Improved Correlation Attack on A5/1". Selected Areas in Cryptography 2004: 1–18.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=A5/1&action=edit&section=9)]

* *Briceno, Marc; Ian Goldberg; David Wagner (23 October 1999).*[*"A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms"*](https://web.archive.org/web/20181008224515/http:/www.scard.org/gsm/a51.html)*. Archived from*[*the original*](http://www.scard.org/gsm/a51.html)*on 8 October 2018. Retrieved 23 January 2017.*
* [*"Huge GSM flaw allows hackers to listen in on voice calls"*](http://arquivo.pt/wayback/20091014125402/http:/www.neowin.net/news/main/09/08/25/huge-gsm-flaw-allows-hackers-to-listen-in-on-voice-calls)*. 25 August 2009. Archived from*[*the original*](https://www.neowin.net/news/main/09/08/25/huge-gsm-flaw-allows-hackers-to-listen-in-on-voice-calls)*on 14 October 2009.*
* *Horesh, Hadar (3 September 2003).*[*"Technion team cracks GSM cellular phone encryption"*](https://web.archive.org/web/20160303212346/http:/www.cs.technion.ac.il/~barkan/GSM-Media/HaaretzInternetEnglish.pdf)*(PDF).*[*Haaretz*](https://en.wikipedia.org/wiki/Haaretz)*. Archived from*[*the original*](https://www.cs.technion.ac.il/~barkan/GSM-Media/HaaretzInternetEnglish.pdf)*(PDF) on 3 March 2016. Retrieved 15 September 2019.*
* *Barkan, Elad; Eli Biham; Nathan Keller (July 2006).*[*"Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication (Technical Report CS-2006-07)"*](https://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-info.cgi?2006/CS/CS-2006-07)*.*
* [*"Nathan Keller's Homepage"*](https://web.archive.org/web/20080604000934/http:/www.ma.huji.ac.il/~nkeller/)*. Archived from*[*the original*](http://www.ma.huji.ac.il/~nkeller)*on 4 June 2008.*
* [*"Animated SVG showing A5/1 stream cypher"*](https://web.archive.org/web/20120326211404/http:/l-system.net.pl/crypto/A5_1_stream_cipher.svg)*. Archived from*[*the original*](http://l-system.net.pl/crypto/A5_1_stream_cipher.svg)*on 26 March 2012.*