FACHHOCHSCHULE KIEL
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN | UNIVERSITY OF APPLIED SCIENCES

Stream Ciphers and Spies

On the Design and Cryptanalysis of the A5/1-Stream Cipher

Prof. Dr.-Ing. Ulrich Jetzek
Kiel University of Applied Sciences, Germany
Institute for Communications Technology and Microelectronics

13th International Symposium on
Ambient Intelligence and Embedded Systems
October 2nd – 4th, 2014

University of Aveiro, Portugal

Source: http://www.thehindu.com/multimedia/dynamic/01628/GERMANY_US_ALLIES__1628403f.jpg

Spiegel Online: October 27th, 2013

SPIEGEL ONLINE INTERNATIONAL

Front Page World Europe Germany Business Zeitgeist Newsletter

English Site > Germany > NSA Spying Scandal > Cover Story: How NSA Spied on Merkel Cell Phone from Berlin Embassy

Embassy Espionage: The NSA's Secret Spy Hub in Berlin

By SPIEGEL Staff

AP

According to SPIEGEL research, United States intelligence agencies have not only targeted Chancellor Angela Merkel's cellphone, but they have also used the American Embassy in Berlin as a listening station. The revelations now pose a serious threat to German-American relations.

Source: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

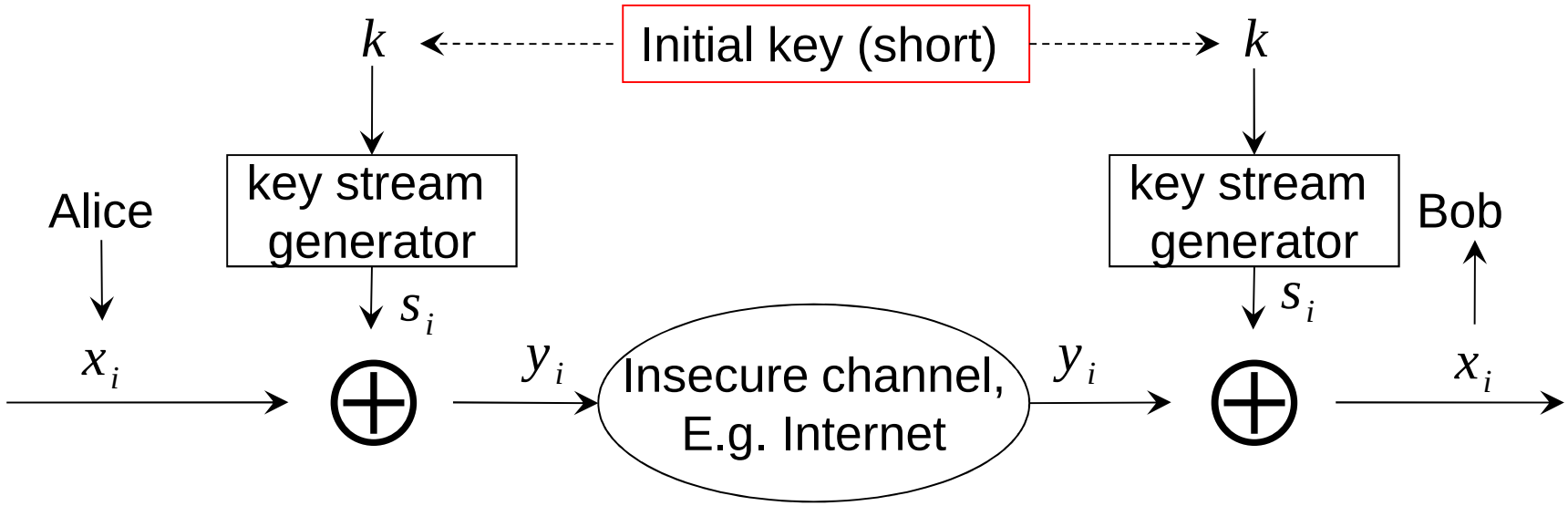
Overview:

1. Stream Ciphers
   - Pros and cons of stream ciphers
2. Random and pseudo random number generators
   - Linear feedback shift registers and
3. A5/1 – a stream cipher for GSM
   - Attacks on A5/1
4. Conclusions

Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.1 Encryption and Decryption with Stream Ciphers

- Plaintext x_i, ciphertext y_i and key s_i consist of individual bits



- Encryption and decryption:
  - Work in the **SAME** way
  - Are simple **modulo-2 addtions (XOR)**
- Advantage of stream ciphers:
  - **Simple and power efficient encryption and decryption possible!**

Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.1 Introduction to stream ciphers

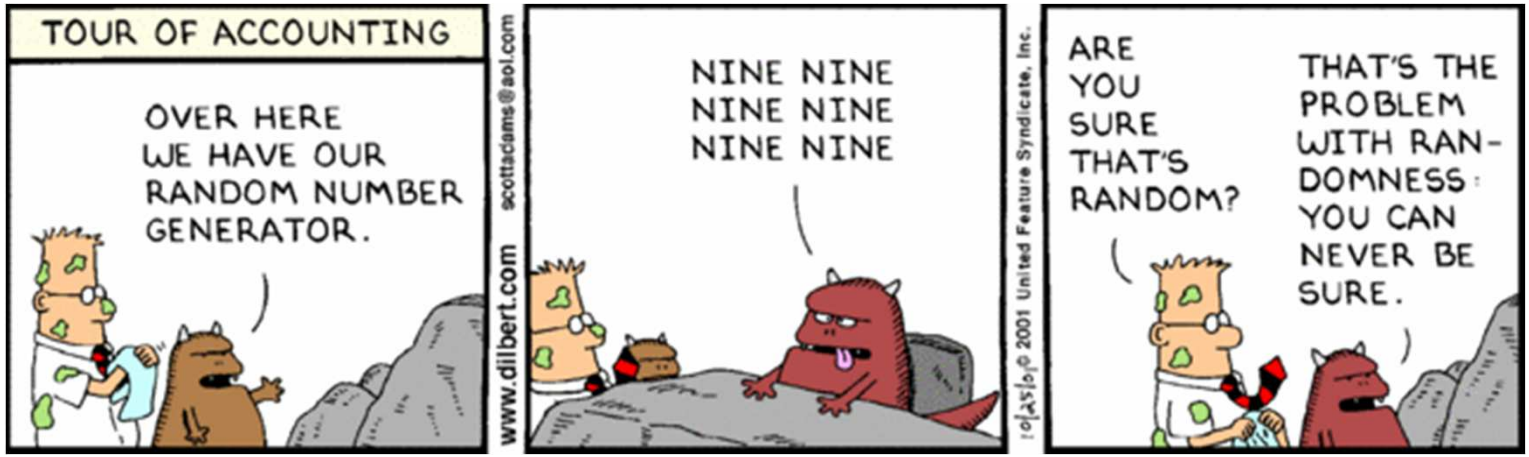
- IMPORTANT: We need to clearly distinguish between:
  - The **key of a stream cipher** and
  - The **key stream** (, which is derived from the key)

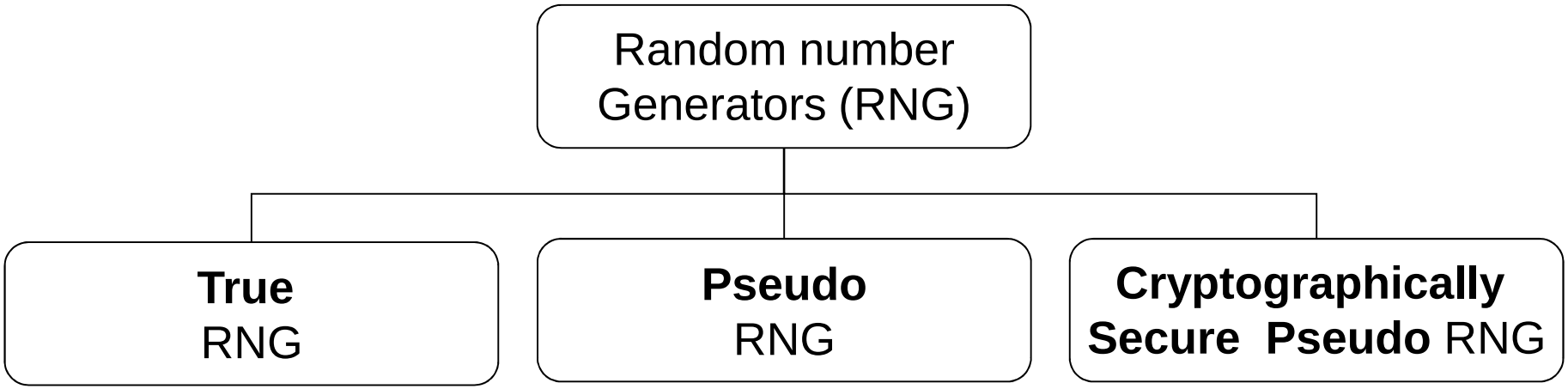
- Why is the choice of a „good“ key stream essential for stream ciphers (disadvantage!) ?
  - Security of a stream ***completely depends*** *on the key stream.*
  - Key stream bits s_i must be ***absolutely random*** *in nature*.

Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.2.1 Random Number Generators (RNG)

- **Randomness of the key stream is the „key to security“ for stream ciphers!**





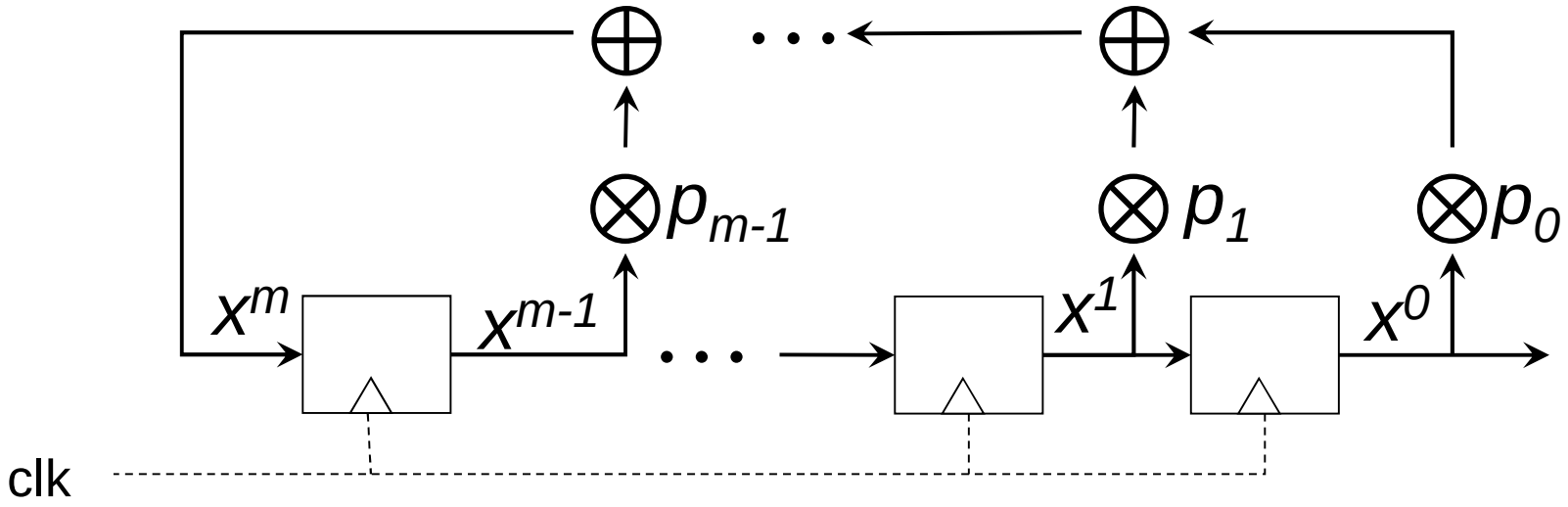
Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.2.1 **True** Random Number Generators (TRNG)

- TRNG characterized by the fact that the SAME sequence cannot be reproduced
- Example: flipping a coin
  - is random in nature.
  - Flipping a coin 100 times yields 100 bits.
  - SAME sequence with probability of $1/2^{100}=7{,}9*10^{-31}$

Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.2.1 **Pseudo** Random Number Generators



- PRNGs created by LFSRs, based on Gallois field theory
  - Feedback parameter p_i determined by Primitive polynomial (Gallois Field Theory)
  - LFSR produces sequence of maximum length: $2^m - 1$
- Pseudo-random sequence contains the
  - Balance property and the
  - Run-length property

- **Disadvantage: Output reproducible and predictable**

2.2.1 **Cryptographically Secure Pseudo RNGs**

- Additional property as compared to PRNGs:
  - Unpredictable, i.e. given a sequence of n bits of the key stream, it is NOT possible to compute the following bits.

- Needed in cryptography, in particular for stream ciphers

- NOTE: **Need for unpredictability** is **unique** to **cryptography**.

  In most (possibly all) other (technical) applications or systems where random numbers are needed unpredictability is *not* needed!

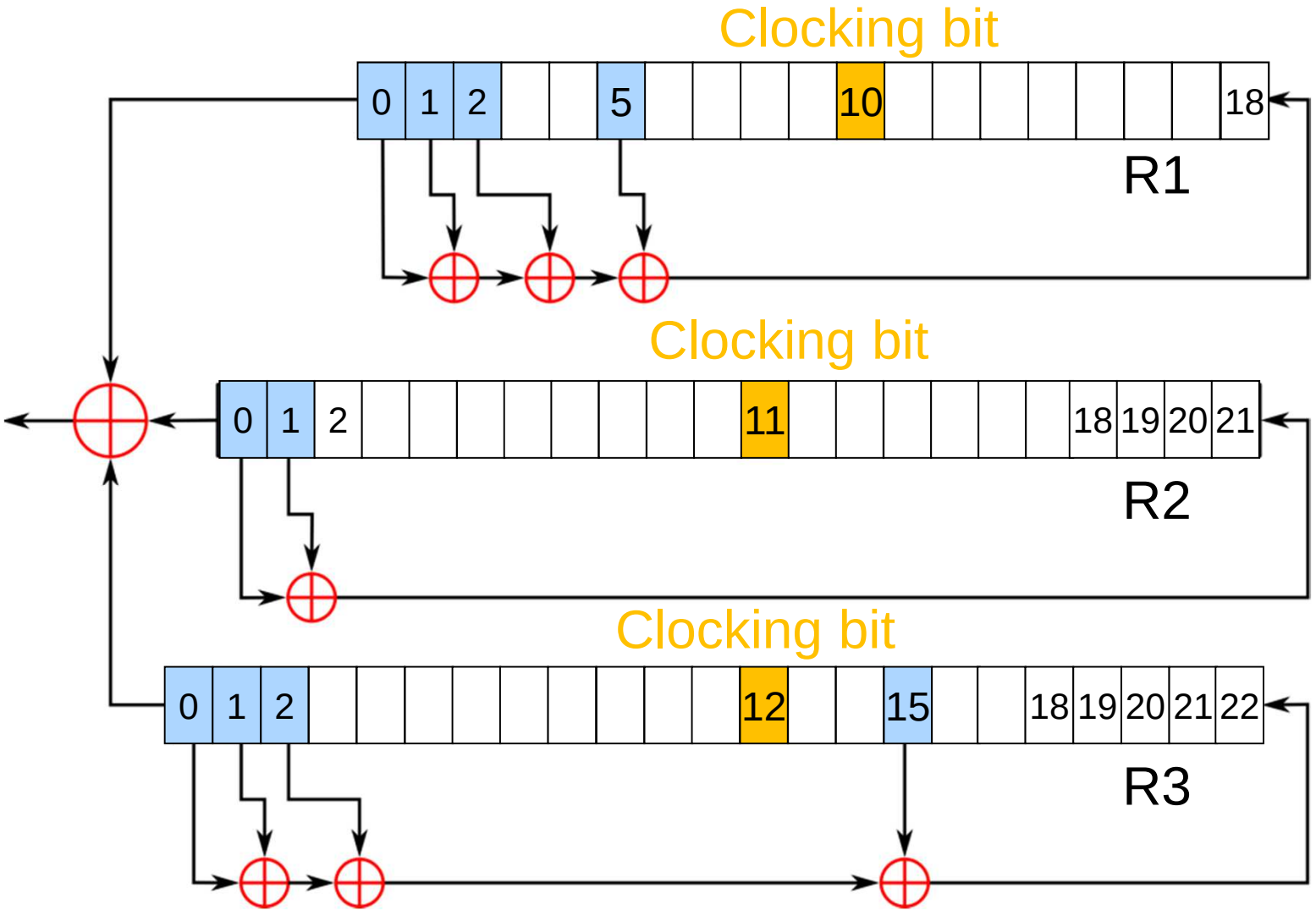
Source: Paar, Pelzl: *Understanding Cryptography, chapter 2*

2.3.2 A5/1-Stream Cipher (used in GSM)

- A5/1:
  - Shall provide over-the-air-communication privacy in GSM
  - In 2000 around 130 Million GSM users relied on A5/1
  - By 2011 approx. 4 billion users relied on A5/1
  - Initally kept secret, but became publically known through leaks (1994) and reverse engineering (1999).
  - Used in Europe and the United States.

Source: http://en.wikipedia.org/wiki/A5/1

2.3.2 A5/1 key stream generation



Source: http://en.wikipedia.org/wiki/A5/1

2.3.2 A5/1-Stream Cipher mechanism

- Clock control (nonlinear element) according to **majority rule:**
  - If 2 or all 3 clocking bits are ‘0’, clocking is applied to all registers, where the clocking bit is ‘0’.
  - If 2 or all 3 clocking bits are ‘1’, clocking is applied to all registers, where the clocking bit is ‘1’.
- Hence:
  - At least 2 of the 3 registers are being clocked
  - Probability for one register to be clocked is: 75%

if probability for a single register bit is

$$p(0) = p(1) = 0{,}5 \rightarrow$$

$$p(\textit{register being clocked}) = \left(\frac{2}{8}\cdot 3 + \frac{6}{8}\cdot 2\right)\cdot\frac{1}{3} = \frac{18}{24} = \frac{3}{4}$$

Source: P.Südmeyer: Die Stromchiffre A5

2.3.2 A5/1-Stream Cipher mechanism

- General:
  - Burst Transmission: 114 bits of information, sent every 4.615 ms,
  - Key stream generated by use of 64-bit secret key K and publicly known frame counter Fn.
- Initialization (warm-up) phase:
  - Registers initialized with all-zero-state.
  - First 64 clock cycles (no clock control): for each bit of *K(i):*

$$R_j(0) = R_j(0) \oplus K(i),\ j = 1,2,3$$

  - Additional 22 clock cycles (no clock control): for each bit of *Fn(i):*

$$R_j(0) = R_j(0) \oplus Fn(i),\ j = 1,2,3$$

  - Register state at the end of warm-up phase: **Initial state**
- Warm-up phase:
  - Additional 100 clock cycles (with clock control): Output discarded
- Cipher stream generation:
  - Additional 228 clock cycles (with clock control): Output produced.

Source: http://en.wikipedia.org/wiki/A5/1

Attack 1: Basic Attack of Golic, 1997 [1]

- Type: **Known Plaintext Attack**
- Attacker needs to know only a plaintext/ciphertext pair, in fact only needs to know 64 successive keystream bits.
- Total number of states in the 3 registers relatively small:

$$2^{(19+22+23)} = 2^{64}\, states$$

- Set of all reachable states is a subset with $5 \bullet 2^{61}$ states
- First guess n bits of the 3 registers R_i, $i=1,2,3$
- This leads to 1+3n+4n/3 linearly independent equations, if n≤19 (size of smallest register)
- System can be attacked by solving the set of linear equations.→ Initial state can be reconstructed, then key can be reconstructed.
- **Complexity: in the order of $O(2^{40,16})$.**

Attack 2: Time-Memory Tradeoff (Golic, 1997) [1]

- **Type: Known Plaintext attack**
- Objective: reconstruct the unknown register state at a known time for known keystream sequence.
- Key stream generator can be considered as 64-bit vectorial Boolean Function.
- Idea: Store for all possible $5 \bullet 2^{61}$ *states the inverse vectorial Boolean Function in a Lookup-Table and find out the preceding register states for a known time* t_0.
- Condition to be fulfilled:

$$T \cdot M \geq 5 \cdot 2^{61}$$

- Tradeoff:
  - If more plaintext is known, less memory is needed,
  - If less plaintext is known, more memory is needed.

Attack 3: Biased Birthday Attack – Biryukov et al. 2000 [2]

- Idea 1: Use Time-Memory Tradeoff of Golic (see above)
- Idea 2: Identify states by prefixes of their output sequences:
  - Forward: Each state defines an infinite sequence of output bits
  - Backwards: States are usually uniquely defined by the first log(n) bits in the output sequence.
- Pick subset A of states, compute their prefixes, and store all (prefix, state)-pairs in a lookup-table.
- Define actual output of the algorithm as set B of states. Efficient search for common states in A and B by probing sorted data A with prefix queries from B.
- Idea 3: A5/1 can be efficiently inverted:
  - Up to 4 states can converge to a common state
  - Run A5/1 backwards by exploring the tree of possible predecessors states.

Attack 3: Biased Birthday Attack – Biryukov et al. 2000 [2]

- Idea 4: key can be extracted from initial state
  - Run A5/1 backwards within the warm-up phase (no clock control mechanism) → Effect of frame counter eliminated
  - Result: 64 linear combinations of 64 bit keys.
- Idea 5: use special states:
  - Prefix length: $\alpha = 16$ bit →

$$2^{64} \cdot 2^{-16} = 2^{48} \, special \;\; states$$

  - Pick arbitrary 19-bit value for Register R1, and arbitrary values for the rightmost 11 bits in R2 and R3.
  - Clock control can be determined and hence, the output, that will be generated.
  - This reduces the number of disk probes by a factor of 2α=32

Attack 3: Biased Birthday Attack – Biryukov et al. 2000 [3]

- Result:

Attack Type	**Preprocessing Steps**	**Available data**	**Nomber of 73 GB disks**	**Attack time**
Biased Birthday attack (1)	**2^{42}**	2 minutes	4	**1 second**
Biased Birthday attack (2)	2^{48}	2 minutes	2	**1 second**
Random subgraph attack	2^{48}	**2 seconds**	4	minutes

2.3.2 security of A5/1 [4]

- Known-Plaintext attacks:
  - **2003:** Ekdahl and Johannson published an attack on the initialisation procedure which **breaks A5/1 in a few minutes using two to five minutes of conversation plaintext.**
  - **No preprocessing stage required.**
  - **2004**: Maximov et al. improved this result to an attack requiring **"less than one minute of computations, and a few seconds of known conversation**“

Source: http://en.wikipedia.org/wiki/A5/1

2.3.2 security of A5/1[4]

- Attacks on A5/1 as used in GSM:
  - **2003:** Barkan *et al.* published several attacks on GSM encryption. The first one is an active attack.
    - **GSM phones can be convinced to use the much weaker A5/2 cipher briefly.**
    - A5/2 can be broken easily, and the phone uses the same key as for the stronger A5/1 algorithm.

Source: http://en.wikipedia.org/wiki/A5/1

2.3.2 security of A5/1[4]

- Attacks on A5/1 as used in GSM:
  - **2006:** E. Barkan, E. Biham, N. Keller published a paper:
  - "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. .... . 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.

Source: http://en.wikipedia.org/wiki/A5/1

2.3.2 security of A5/1[5]

- Attacks on A5/1 as used in GSM (2013):
  - Encryption experts have complained for years that the most commonly used technology, known as A5/1, is vulnerable and have urged providers to upgrade to newer systems that are much harder to crack. Most companies worldwide have not done so, even as controversy has intensified in recent months over NSA collection of cellphone traffic, including of such world leaders as **German Chancellor Angela Merkel**.

    The extent of the NSA's collection of cellphone signals and its use of tools to decode encryption are not clear from a top-secret document provided by former contractor Edward Snowden. But it states that the [NSA] agency **"can process encrypted A5/1" even when the agency has not acquired an encryption key, which unscrambles communications so that they are readable.**

- Source: http://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

Conclusions

- Security of stream ciphers very much depends on the randomness of the key stream. Pseudo Random Number Generators are NOT suitable as key stream generators.
- A5/1 uses 3 registers with total „only“ length 64 bits to generate the key stream and non-linear clocking mechanism.
- First attacks onto A5/1 go back until 1994.
- In 2000 the REAL-TIME ATTACK of Biryukov et al. Has already been published.
- More Known plaintext- and ciphertext-only attacks have been published (2003 – 2006).
- Therefore it is no surprise, that mobile phone conversations could have been attacked in recent years (2013), as e.g. phone conversations of Angela Merkel.

Thank you very much for your attention!

References

1. J. D. Golic, „Advances in Cryptography - EUROCRYPT'97, LNCS 1233,“ in *Cryptanalysis of Alleged A5 Stream Ciphers*, Heidelberg, 1997.
2. A. Biryukov, A. Shamir und D. Wagner, „Real Time Cryptanalysis of A5/1 on a PC,“ *Cryptome,* 27 April 2000
3. Arber Ceni: “GSM Security: Cryptanalysis of A5/1” – Presentation slides, 2011
4. wikipedia-authors, „A5/1,“ 2014. [Online]. Available: http://en.wikipedia.org/wiki/A5/1. [Zugriff am 26 08 2014].
5. C. Timberg und A. Soltani, „By cracking cellphone code, NSA has ability to decode private conversations,“ 13 12 2013. [Online]. Available: http://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