The (Real-Time) Cryptanalysis of A5/2

Ian Goldberg
David Wagner
Lucky Green

presented by Nikita Borisov

August 26, 1999

GSM algorithms

- GSM cellphones contain a number of cryptographic algorithms:

A3	Authentication
A8	Key generation for A5
A5/x	Voice encryption

- Designed in secret

- Never (officially) published

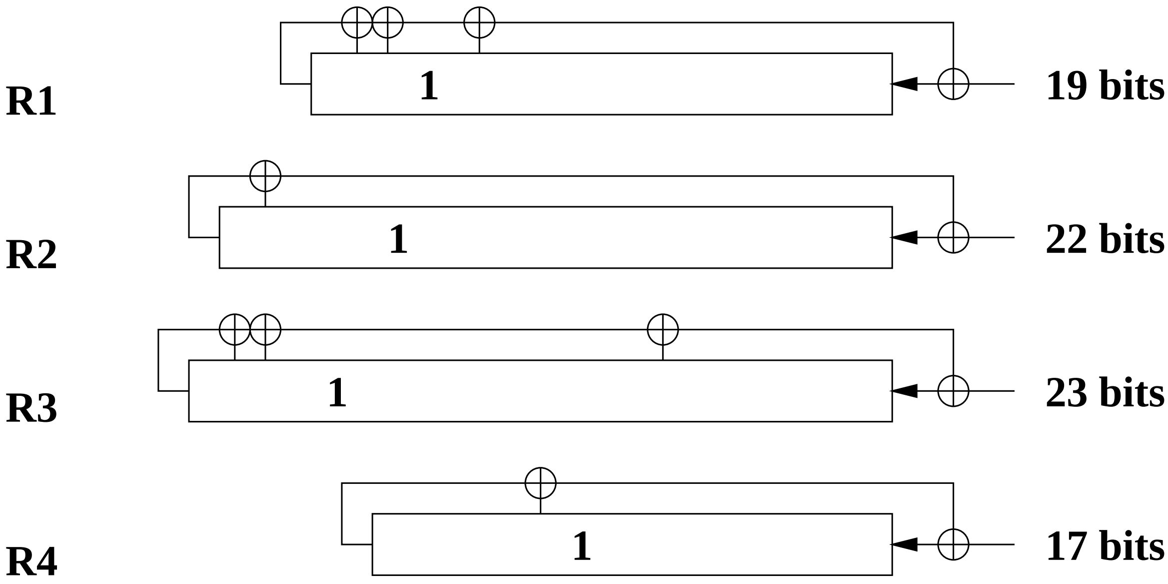
- **Very** widely deployed
  $\Rightarrow$ *someone* will get around to reverse-engineering them

Enter someone

- A3 + A8 (also known as COMP128) were reverse-engineered in April 1998
  - Were then broken 3 hours later
- A5/2 was reverse-engineered at CRYPTO'99 last week
  - Took longer to break (about 5 hours)

Structure of A5/2

4 LFSR's:



- Load key and frame number into registers
- Force one bit of each register to be set (?!)
- Use a non-linear function of bits of R4 to clock R1, R2, R3
- Output is a non-linear function of bits of R1, R2, R3 (stream cipher)

Cryptanalysis

- Given R4, the clocking function of R1, R2, R3 is linear.
- If we perform key set up for two frames 2^{11} apart, R1,R2,R3 will differ by a fixed delta, but R4 will be the same, because of the clobbered bit.
- Although the output is a non-linear function of R1,R2,R3, given a fixed delta in the initial state of R1,R2,R3, the expected output delta is a linear function of the initial state of R1,R2,R3.
- We can solve the linear system to compute the initial state
- Since it's overdetermined, we can first use redundancy in output as a check.

The Break!

- Need 2 frames (114 bits each) of ciphertext whose plaintext has a known difference.
  - Easy to find, since many frames are silence
- These frames need to be 2^{11} frames (about 6 seconds) apart.
- Obtain X (114 bits), the XOR of the keystreams.
- Guess R4 (2^{15} guesses on average)
- Check your guess by checking $V_{R4} \cdot X = 0$ (2 dot products on average)
- Once you find the right R4, calculate the initial state of R1,R2,R3 using 64 more dot products.
- Work factor of approx 2^{16} $\rightarrow$ **real-time**!