T-79.514 Special Course on Cryptology

A3/A8 & COMP128

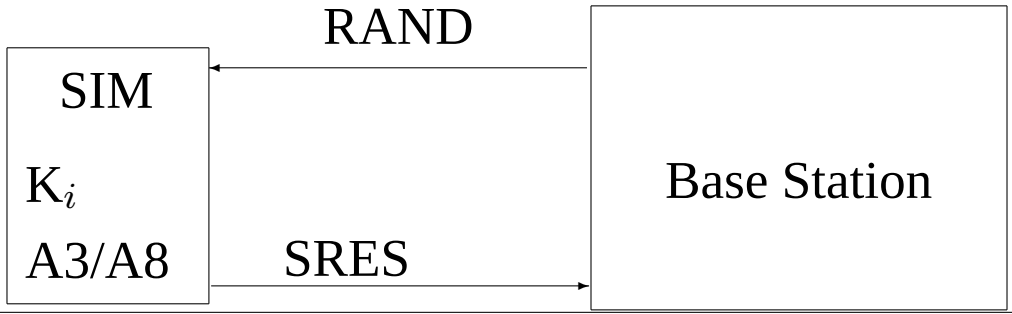
Billy Brumley
Helsinki University of Technology
bbrumley@cc.hut.fi

Overview

- Summary of GSM security concepts
- A3/A8 and COMP128 Algorithm
- COMP128 Attack, second round of the compression function
- Small example of the attack
- Other attacks (3-5 round attack, partitioning attack)

GSM Authentication

- RAND is a 128-bit random challenge issued from the base station to the mobile
- SRES is a 32-bit signed response generated by A3 issued from the mobile to the base station
- K_i is the SIM's 128-bit individual subscriber key (located only on the SIM and the GSM network)



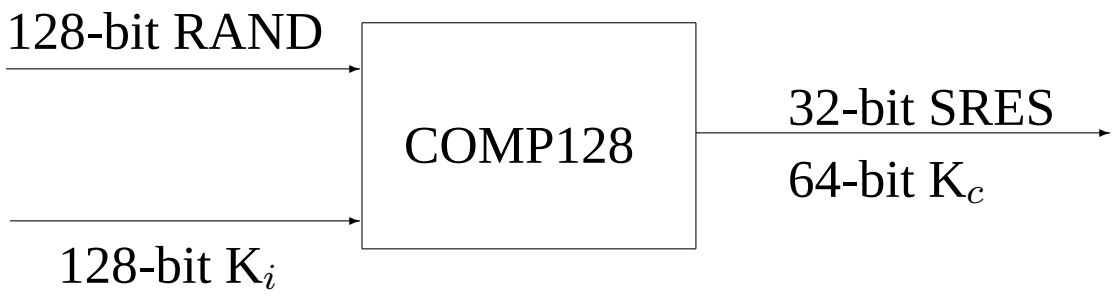
A3 - Authentication / A8 - Key Generator

- A3 Input: 128-bit RAND random challenge, K_i 128-bit private key
- A3 Output: 32-bit SRES signed response
- A8 Input: 128-bit RAND random challenge, K_i 128-bit private key
- A8 Output: 64-bit K_c Cipher Key, used for A5
- Since both take the same inputs, A3/A8 are usually implemented together as..

COMP128 at a Glance

- COMP128 design was completely private. The algorithm was not released to the public, thus it lacks much needed peer review.

- In 1997, a leaked document led to publication of COMP128. The majority of the code was produced from that document, and what was missing (about 4-6 lines) was reverse engineered.

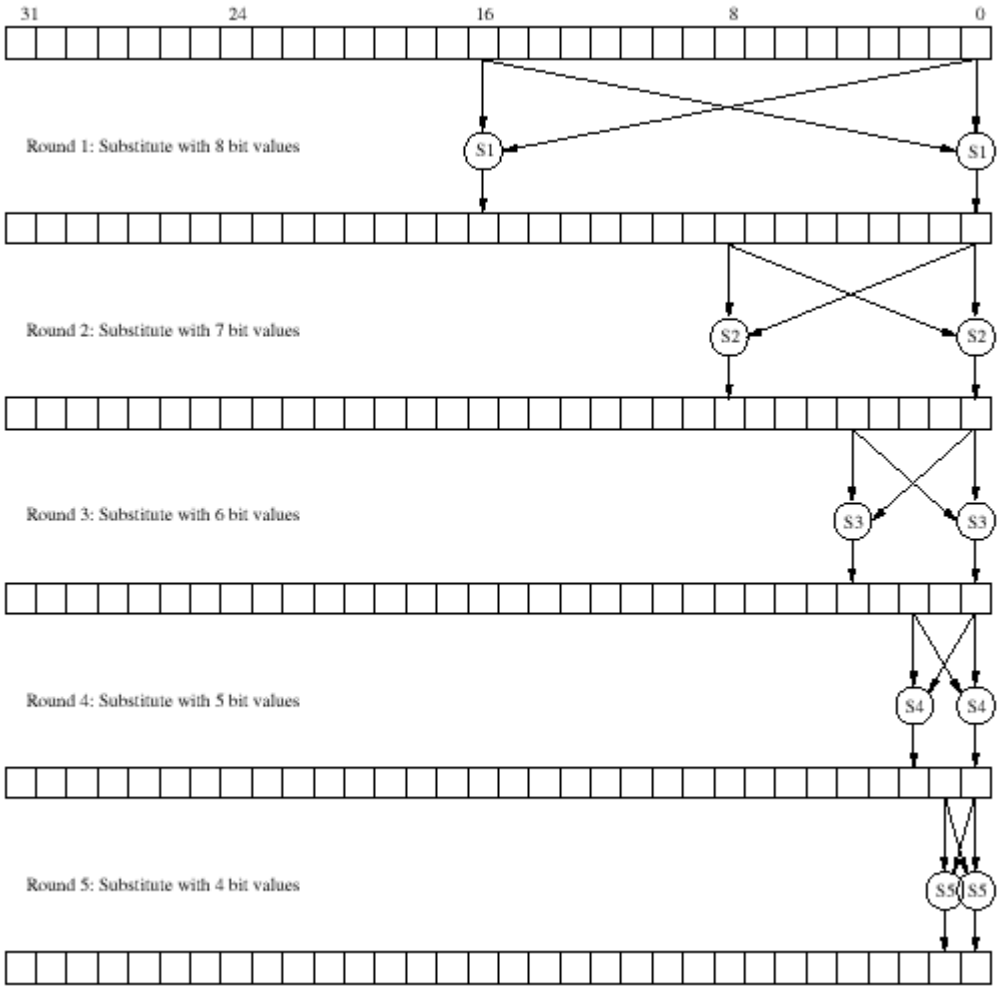


COMP128 - Details

```
1. x[16-31] = RAND
2. for 0<i<8
     x[0-15] = Ki
     call Compression (5 rounds)
     call FormBitsFromBytes
     if i<7 call Permute
```

Compress 16-byte result to 12-bytes, store in simoutput[] and return.

COMP128 - Compression Function



COMP128 - Compression Function (2)

- This is commonly called 'Butterfly Structure.' In each of the 5 levels, compression is performed on 2 equal sized sections. e.g. In round 0, 2-16 byte sections, round 1, 4-8 bit sections, etc.

- For level i, T_i (table) contains 2^{9-i} (8-i)-bit values. e.g. T_0 has 512 8-bit values, while T_4 has 32 4-bit values.

- In each level, two input bytes are used to calculate the index for the table and the result is the output byte.

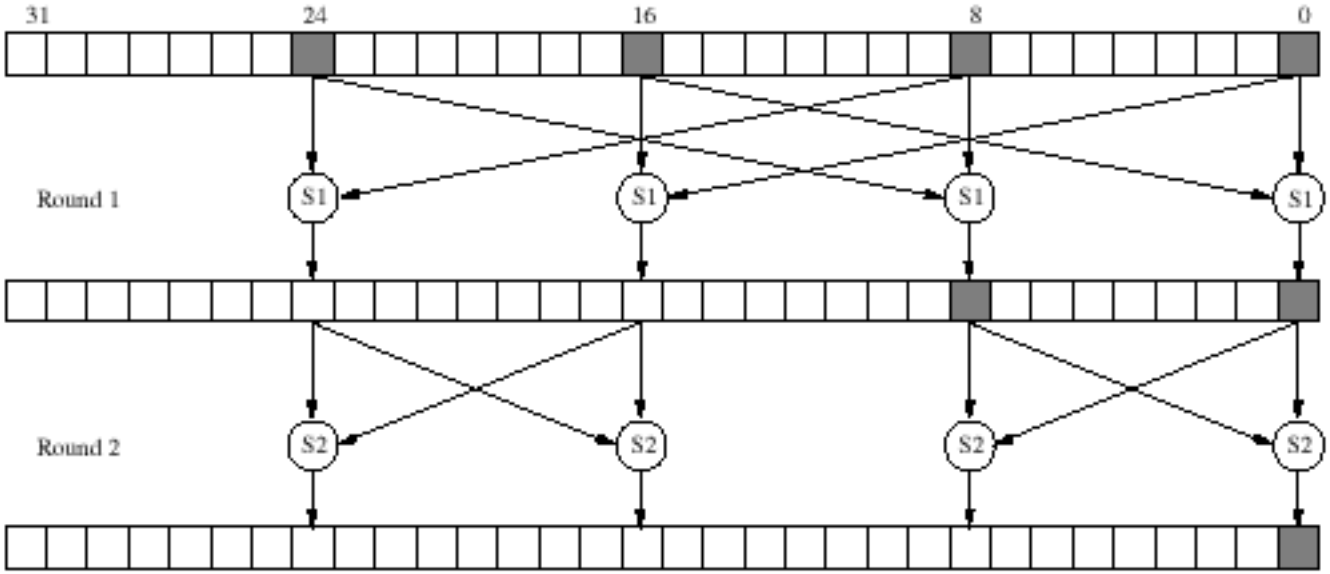
COMP128 - First Public Attack

- In April of 1998, the Smartcard Developer Association along with 2 UC Berkeley researchers (Wagner/Goldberg) produced the first publicized attack on COMP128.

- It exploits the weakness in diffusion of the second round in the compression function. This is commonly referred to as a 'Narrow Pipe.'

- Specifically, the output bytes of the second round of compression i, i+8, i+16, i+24 are dependent ONLY upon their corresponding input bytes. Thus, the 'pipe' has a width of 4 bytes.

COMP128 - Narrow Pipe



Collision Attack

- Involves sending lots of challenges to the card, and collecting the responses. Only bytes i and i+8 are varied; the rest are held constant.

- How can we detect a collision in the second round? Since each byte depends only upon 2 bytes of the previous rounds output, a collision in the second round will propagate throughout the rest of the algorithm, causing a collision in the response as well. (huge weakness)

- Since the pipe is 4 bytes wide (7-bit values), the birthday paradox says we can expect a collision to occur after $2^{4*7/2} = 2^{14}$ challenges. One challenge equals one query to the card. (collision example)

Collision - Now What?

- Once a collision is found, the corresponding bytes in the key can be recovered trivially. Rinse and Repeat for the remaining unknown key bytes. This attack requires $8*2^{4*7/2} = 2^{17}$ 131K queries.

```
for(i=0; i<256; i++)
  for(j=0; j<256; j++)
    key[0]=i; key[8]=j;
    //chal1 chal2 are the 2 colliding challenges
    A3A8(chal1,key,hash1);
    A3A8(chal2,key,hash2);
    if hash1=hash2 //you found your bytes.
```

- Using a smartcard reader, one can submit 6 queries per second. For 131K queries, this would take roughly 6 hours. (and access to the physical SIM, of course)

Collision and Key - Example

```
Using key:
Ki= 048BC1EA93B0F82733D67C19267C91D6
Took 16065 steps / 9 seconds
found k=29 l=153 i=62 j=193
X=      3E0000000000000C100000000000000
F(X)=   80B3A76AD121F66903D0F800
Y=      1D0000000000000990000000000000
F(Y)=   80B3A76AD121F66903D0F800
In 1076 steps found partial key:
Ki= 040000000000000330000000000000
```

I Have the Key, Now What?

- Once one has obtained the key, the card could be cloned. Cloning could let an attacker do any number of bad things, such as eavesdropping on phone conversations, SMS, Voice Mail, make calls charged to the SIM owner, etc.

- However, in practice, most newer SIMs will stop functioning after about 2^{16} queries.

- And how could one get access to a SIM for 6+ hours?!

So for Practicality...

- Once one has attacked the second round, an attack can be mounted on the third round, one byte at a time. this requires some computation, but severely reduces the amount of queries.

- Rounds three through five can be obtained with less than 3K queries, meaning an attack can be mounted to recover the full key in 20K queries, or less than an hour!

- this was implemented in SIMSCAN v2 (Dejan Kaljevic) and demonstrated at DEFCON 2004 (David Hulton)

Partitioning Attack

- Developed by IBM. Uses side channels and specifically chosen challenges. The lookup tables, specifically the first round of compression (9-bit index), leak data to side channels. This data consists of power consumption, EM emissions, etc.

- Using carefully chosen challenges, the IBM team was able to obtain the key in as few as 8 queries. Using random challenges, it takes about 1000.

Conclusion

- When the first successful attack was mounted against COMP128, the GSM Committee issued a response that COMP128 was just an example, and providers should come up with their own algorithms.

- COMP128-2, COMP128-3 have since been developed; however, the technicalities as to their design are also a mystery.

- While not so practical anymore, this is a good example of why 'Security Through Obscurity' just doesn't work. Even with high costs involved to patch SIM cards globally, providers ignore the threats.

- COMP128-4 for 3G networks is based on AES.

References

- Goldberg, Wagner. ”GSM Cloning.” http://www.isaac.cs.berkeley.edu/isaac/gsm.html

- Rao, Rohatgi, Scherzer, Tinguely. ”Partitioning Attacks.” http://www.research.ibm.com/intsec/gsm.ps

- Hulton, David. ”Smart Card Security.” http://www.dachb0den.com/projects/scard/smartcards.ppt

- Sin, Susan. ”COMP128.” http://calliope.uwaterloo.ca/ ssjsin/COMP128.pdf