Chapter 6. Stream Cipher Design

1. Model for Secure Communications and Attacks
3. One-time-pad and Design Principles of Stream Ciphers
4. Addressed Problems in Wireless Security
5. Some Concerns in Multimedia Security and Low Cost Cryptography
6. Case Study: A5 stream cipher for GSM
7. Case Study: w7, an Analogue Cipher of A5
8. Correlation Attack to Stream Ciphers (self reading)
6.1. Model for Secure Communications

Three components of secure communications:

- Communication principles
- Trusted third party (or authority)
- Opponents (attackers)
Figure 1. Model for Secure Communications
Insecure information channel

Figure 2. Passive attacks
**Figure 3. Active attacks**

- **Active attacks (authentication)**
  - Interruption
  - Modification
  - Fabrication

- **Insecure information channel**

- **Sender**
- **Receiver**
- **Attacker**
Figure 4. Simplified Model of Conventional Encryption
Figure 5. Model of Conventional Cryptosystem
6.3 One-time-pad and Design Principles of Stream Ciphers

A. Model of Steam Ciphers
B. One-time-pad
C. Randomness Measurements for PRSG (Done in Chapter 2-4)
D. Known Key Generators for Stream Ciphers (done in Chapter 5)
Model of Stream Cipher

Message source: $m = m_1, m_2, \ldots$

Key generation: $k = k_1, k_2, \ldots$

Cipher: $c = c_1, c_2, \ldots$

$K$, seed
One-time-pad means that different messages are encrypted by different key streams.


- Massey's Discovery (1969): If a binary sequence has linear span $n$ then the entire sequence can be reconstructed from $2n$ consecutive known bits by the Berlekamp-Massey algorithm. Request for large linear span.
Randomness Measurements

Randomness Measurements for PSG:

• Long Period
• Balance Property
• Run Property
• $n$-tuple Distribution
• Two-level Auto Correlation and Low Cross Correlation
• Large Linear Span
• Indistinguishability: it cannot be distinguished from a truly random sequence in terms of polynomial algorithm.
Known Key Generators for Stream Ciphers

(All LFSR based nonlinear generators in chapter 5)

- Linear Feedback Shift Registers (LFSR) (1948-1969)
- Filter Function Generators (Key: 1973)
- Combinatorial Function Generators (Groth: 1971)
- Clock Controlled Generators (Beth and Piper: 1984)
- Shrinking Generators (Coppersmith-Krawczys-Mansour, 1993)
6.4 Addressed Problems in Wireless Security

- Security Algorithms used in GSM
- Possible Interception Attacks in GSM
- Possible Interception Attacks in IS-95 CDM
- Security Issues in 3G Systems
- Security Trends in 3G Systems
- Security in 4G Systems
Security Algorithms used in GSM
Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM Consortium. Other algorithms have been named as well, but almost every operator uses the COMP128 except a couple of exceptions.

The COMP128 generates both the SRES response (32 bits) and the session key, Kc, on one run. The last 54 bits of the COMP128 output form the session key, Kc, until the MS is authenticated again. Note that the key length at this point is 54 bits instead of 64 bits, which is the length of the key given as input to the A5 algorithm. Ten zero-bits are appended to the key generated by the COMP128 algorithm. Thus, we have a key of 64 bits with the last ten bits zeroed out.

The A5 algorithm is the stream cipher used to encrypt over-the-air transmissions, which will be discussed in detail in Section 6.
Possible Interception Attacks in GSM

- Accessing the Signaling Network
  The transmissions are encrypted only between the MS and the BTS. After the BTS, the traffic is transmitted in plain text within the operators network. The SS7 signaling network used in the operator's GSM network is completely insecure if the attacker gains direct access to it.
Possible Interception Attacks in GSM (Cont.)

Retrieving the Key from the SIM

The attack is based on a chosen-challenge attack that works, because the COMP128 algorithm is broken in such a way that it reveals information about the $K_i$ when the appropriate RANDs are given as arguments to the A8 algorithm. The SIM was accessed through a smartcard reader connected to a PC. The PC made about 150,000 challenges to the SIM and the SIM generated the SRES and the session key, $K_c$, based on the challenge and the secret key. The secret key could be deduced from the SRES responses through differential cryptanalysis. The smartcard reader used in implementing the attack could make 6.25 queries per second to the SIM card. So the attack required about eight hours to conduct.
Possible Interception Attacks in GSM (Cont.)

- **Retrieving the Key from the SIM over the Air**
  
The attack might be conducted in a subway, where the signal of the legitimate BTS is not available, but the phone is still turned on. The subscriber would be unaware of such an attack though the fact that the battery of the phone has run out slightly quicker than usual might make him suspicious. The attack can also be performed in parts: instead of performing an eight-hour attack, the attacker could tease the phone for twenty minutes every day on the victim's way to work.
Possible Interception Attacks in IS-95 CDMA

- A recent paper in SAC 2000 workshop showed that the eavesdropping the downlink traffic channel 1 second, the eavesdropper can get enough information to recover the voice privacy.
The level of protection

- One weakness in GSM security protocol is that mobile identity is not always encrypted when transmitted over the air interface.
- In IP-world, denial of service attacks cannot be made impossible, but they can be made more difficult to implement by using sophisticated firewalls, good network design, etc.
- The algorithms used should be made public so that they can be tested.
- System should also be modular so that an algorithm, if found flawed, could be replaced with a better algorithm.
Security Issues in 3G Systems (Cont.)

- **Charging**
  - Nowadays the charge of the SMS (Short Message Service) or WAP (Wireless Application Protocol) based service is typically not indicated by the service provider to the user when he or she uses the service.
  - Another issue is that the on-line indication of the charges could cut down the use of the services. This flaw has recently been criticized by the Finnish Consumer Office.
Privacy

The location and consumer habits of users are valuable information for service creation and marketing purposes. A policy about the collection, storage, use, disclosure, and selling of this data is required. In Finland the constitution and different laws.
Security Issues in 3G Systems (Cont.)

**Terminal Security:** Smart Card with PIN number has been used to protect terminal security.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Name</th>
<th>Defining Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
<td>GSM</td>
</tr>
<tr>
<td>UIM</td>
<td>User Identity Module</td>
<td>IS-95</td>
</tr>
<tr>
<td>USIM</td>
<td>Universal SIM</td>
<td>UMTS</td>
</tr>
<tr>
<td>R-UIM</td>
<td>Removable UIM</td>
<td>CDMA2000</td>
</tr>
<tr>
<td>WIM</td>
<td>Wireless Identity Module</td>
<td>WAP</td>
</tr>
</tbody>
</table>
Lawful Interception

The UMTS and GSM, like all telecom systems, allow lawful interception for authorized law and enforcement agencies. This is required by national laws and EU directives, and is used for crime investigation and national security. The Internet users have traditionally very negative attitudes towards monitoring of their communications, and lawful interception can become at least an image problem for the new IP-services of the telecom systems.
Security Trends in 3G Systems

- Offer complete security solutions—not just provide protection over the radio link
- Offer negotiation
- Offer mutual authentication
- Offer data confidentiality and data/signaling authentication
- Prevent replay attack on the signaling
- Provide period data authentication
- Use SIM card
- Mobile handset shows “um-encrypted mode”
- Universal roaming
- Continuously migrate to 4G systems in terms of enhanced security, services, access media, data rate, capabilities
Security in 4G Systems

- Use public-key algorithms for key agreement, privacy and authentication
- Provide non-repudiation services
- Provide key recovery (escrow)
- Universal access to any type of media and devices
- Integrate services, including payment and charging
6.5. Some Concerns in Multimedia Security and Low Cost Cryptography

- **Adopt AES or Standardize a New Cipher:** For multimedia encryption, the working group of multimedia security is in discussion of to adopt the AES (will be introduced in next chapter) or standard a particular cipher for that. The main concern here is the nature of multimedia signals, it may not need the cipher as strong as the AES. For example, for pay-for-view TV, if only partial of content of a movie is encrypted, then it is secure enough since human being’s tolerance of eyes is limited.
6.6 Case Study: A5 Stream Cipher

A. A5/1 stream cipher key generator for secure GSM conversations

Note. A GSM conversation is sent as a sequence of frames per 4.6 millisecond, and each frame contains 228 bits.
Description of the A5/1 stream cipher: 64-bit key to generate a key stream where each 228-bit is used for one frame (228-bit) encryption.

GSM message:

… 228-bit 228-bit

1 frame

Output: 228-bit ciphertext, one frame of cipher
Construction of A5/1 Generator:

Parameters:

(a) Three LSFRs which generate $m$-sequences with periods $2^{19} - 1$, $2^{22} - 1$, $2^{23} - 1$, respectively.

1. LFSR 1: $f_1(x) = x^{19} + x^5 + x^2 + x + 1$ generates $a = \{a(t)\}$.

2. LFSR 2: $f_2(x) = x^{22} + x + 1$ generates $b = \{b(t)\}$.

3. LFSR 3: $f_3(x) = x^{23} + x^{16} + x^2 + x + 1$ generates $c = \{c(t)\}$.

4. Tap positions: $d_1 = 11$, $d_2 = 12$ and $d_3 = 13$. 
(b) Majority function \( f(x_1, x_2, x_3) = (y_1, y_2, y_3) \) is defined by

\[
\begin{array}{c|ccc|ccc|ccc}
\hline
f(a(t+11), b(t+12), c(t+13)) & a(t+11) & b(t+12) & c(t+13) \\
= (y_1, y_2, y_3) & & & & \hline
(1,1,1) & 0 & 0 & 0 \\
 & 1 & 1 & 1 \\
(1,1,0) & 0 & 0 & 1 \\
 & 1 & 1 & 0 \\
(0,1,1) & 0 & 1 & 1 \\
 & 1 & 0 & 0 \\
(1,0,1) & 1 & 0 & 1 \\
 & 0 & 1 & 0 \\
\hline
\end{array}
\]

**Output:**
The output sequence \( u = \{ u(t) \} \) which performs at time \( t \),

\[
u(t) = a(i_1) + b(i_2) + c(i_3), \quad t = 0, 1, ...
\]

where \( i_1, i_2, \) and \( i_3 \) are determined in a stop-and-go clock controlled model by the majority function \( f \).
A5/1 Key Stream Generator
For example, at time $t$, if

$$f(a(t+11), b(t+12), c(t+13)) = (1, 1, 0)$$

i.e., $(y_1, y_2, y_3) = (1, 1, 0)$, then LFSR 1 and LFSR 2 are clocked and LFSR 3 has no clock pulse.

**Session key or seed:** initial states for three LFSRs, a total of 64 bits.
Note 2. The first 'original' A5 algorithm was renamed A5/1. Other algorithms include A5/0, which means no encryption at all, and A5/2, a weaker over-the-air privacy algorithm. Generally, the A5 algorithms after A5/1 have been named A5/x. Most of the A5/x algorithms are considerably weaker than the A5/1, which has the time complexity of 254 at most as, shown above. The estimated time complexity of A5/2 is as low as 216. A5/3 is available in the work group of wireless communications.
What does A5/1 suffer?

- It can be broken with few hours by a PC.
- Short period problem: Without stop/go operation, the period of sum of the three LFSRs is given by
  \[(2^{19}-1)(2^{22}-1)(2^{23}-1)\].
  However, the experiment shows that the period of A5/1 is around
  \[(4/3)(2^{23}-1)\].
- Collision problem: different seeds (i.e., different initial states of three LFSRs) may result in the same key stream (our new results shows that only 70% seeds produce different key streams.)
- The majority function is the worst function in terms of correlation with all affine functions.
Possible Attacks on A5/1

- **Brute-Force Attack against A5**
  If we have a Pentium III class chip with approximately 20 million transistors and the implementation of one set of LSFRs (A5/1) would require about 2000 transistors, we would have a set of 10,000 parallel A5/1 implementations on one chip. If the chip was clocked to 600 MHz, we could try approximately 2M keys per second per A5/1 implementation. A key space of $2^{54}$ keys would thus require about 900,000 seconds, 250 hours, with one chip.

- Alex Biryukov and Adi Shamir (co-inventor of the RSA) claim to be able to penetrate the security of a A5/1 ciphered GSM call in less than one second using a PC with 128 MB RAM and large hard drives.
w7 stream cipher algorithm is proposed by S. Thomas, D. Anthony, T. Berson, and G. Gong published as an INTERNET DRAFT, April 2002.

**Description of w7:** The w7 algorithm is a byte-wide, synchronous stream cipher optimized for efficient hardware implementation at very high data rates. It is a symmetric key algorithm supporting key lengths of 128 bits. It contains eight similar models, C1, C2, ..., C8 where C2 is illustrated as follows.
K, 128-bit key

C1  C2  ...  C8

1-bit output

1-byte output
The W7 Cipher Algorithm
6.8. Correlation Attack to Stream Ciphers

Self reading.
References