2 Description of A5/2 and GSM Security Background

In this section we describe the internal structure of A5/2 and the way it is used. A5/2 consists of 4 maximal-length LFSRs: R1, R2, R3, and R4. These registers are of length 19-bit, 22-bit, 23-bit, and 17-bit respectively. Each register has taps and a feedback function. Their irreducible polynomials are: $x^{19} \oplus x^5 \oplus x^2 \oplus x \oplus 1$, $x^{22} \oplus x \oplus 1$, $x^{23} \oplus x^{15} \oplus x^2 \oplus x \oplus 1$, and $x^{17} \oplus x^5 \oplus 1$, respectively. For the representation of the registers we adopt the notation of [2,4,5,17], in which the bits in the register are given in reverse order, i.e., x^i corresponds to a tap with index $len - i - 1$, where len is the register size. For example, when R4 is clocked, the XOR of R4[$17 - 0 - 1 = 16$] and R4[$17 - 5 - 1 = 11$] is computed. Then, the register is shifted by one bit to the right, and the value of the result of the XOR is placed in R4[0].

At each step of A5/2 R1, R2 and R3 are clocked according to a clocking mechanism that we describe later. Then, R4 is clocked. After the clocking is performed, one output bit is ready at the output of A5/2. The output bit is a non-linear function of the internal state of R1, R2, and R3.

After the initialization 99 bits[3] of output are discarded, and the following 228 bits of output are used as the output key-stream.

Denote the i'th bit of the 64-bit session-key K_c by $K_c[i]$, the i'th bit of register j by $Rj[i]$, and the i'th bit of the 22-bit publicly known frame number by $f[i]$.

The initialization of the internal state with K_c and the frame number is done in the following way:

```
– Set all LFSRs to 0 ($R1 = R2 = R3 = R4 = 0$).
– For $i := 0$ to 63 do
    1. Clock all 4 LFSRs.
    2. $R1[0] \leftarrow R1[0] \oplus K_c[i]$
    3. $R2[0] \leftarrow R2[0] \oplus K_c[i]$
    4. $R3[0] \leftarrow R3[0] \oplus K_c[i]$
    5. $R4[0] \leftarrow R4[0] \oplus K_c[i]$
– For $i := 0$ to 21 do
    1. Clock all 4 LFSRs.
    2. $R1[0] \leftarrow R1[0] \oplus f[i]$
    3. $R2[0] \leftarrow R2[0] \oplus f[i]$
```

[3] Some references state that A5/2 discards 100 bits of output, and that the output is used with a one-bit delay. This is equivalent to stating that it discards 99 bits of output, and that the output is used without delay.

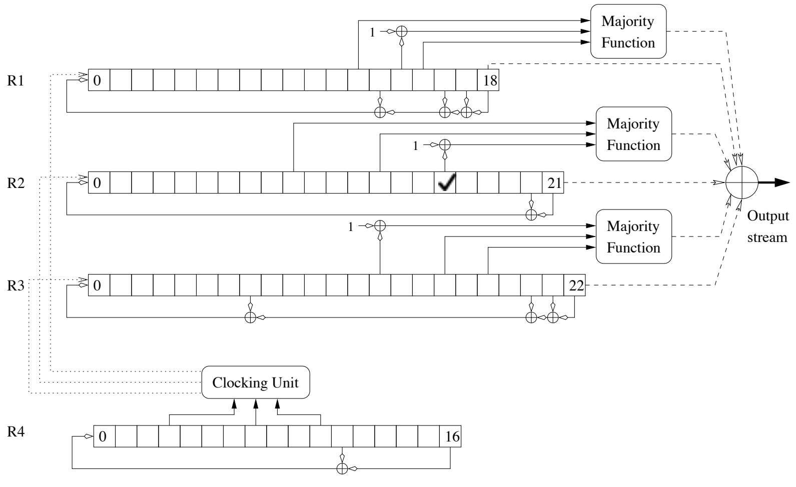

Fig. 1. The A5/2 internal structure

4. $R3[0] \leftarrow R3[0] \oplus f[i]$
5. $R4[0] \leftarrow R4[0] \oplus f[i]$

The key-stream generation is as follows:

1. Initialize the internal state with K_c and frame number.
2. Force the bits R1[15], R2[16], R3[18], R4[10] to be 1.
3. Run A5/2 for 99 clocks and ignore the output.
4. Run A5/2 for 228 clocks and use the output as key-stream.

After the first clocking is performed the first output bit is ready at the output of A5/2. In Figure 1 we show the internal structure of A5/2. The clocking mechanism works as follows: R4 controls the clocking of R1, R2, and R3. When clocking of R1, R2, and R3 is to be performed, bits R4[3], R4[7], and R4[10] are the input of the clocking unit. The clocking unit performs a majority function on the bits. R1 is clocked if and only if R4[10] agrees with the majority. R2 is clocked if and only if R4[3] agrees with the majority. R3 is clocked if and only if R4[7] agrees with the majority. After these clockings, R4 is clocked.

Once the clocking is performed, an output bit is ready. The output bit is computed as follows: in each register the majority of two bits and the complement of a third bit is computed; the results of all the majorities and the rightmost bit from each register are XORed to form the output (see Figure 1). Note that the majority function is quadratic in its input: $maj(a, b, c) = a \cdot b \oplus b \cdot c \oplus c \cdot a$.

A5/2 is built on a somewhat similar framework of A5/1. The feedback functions of R1, R2 and R3 are the same as A5/1's feedback functions. The initialization process of A5/2 is also somewhat similar to that of A5/1. The difference is that A5/2 also initializes R4, and that one bit in each register is forced to be 1 after initialization . Then A5/2 discards 99 bits of output while A5/1 discards

100 bits of output. The clocking mechanism is the same, but the input bits to the clocking mechanism are from R4 in the case of A5/2, while in A5/1 they are from R1, R2, and R3. The designers meant to use similar building blocks to save hardware in the mobile phone [16].

This algorithm outputs 228 bits of key-stream. The first block of 114 bits is used as a key-stream to encrypt the link from the network to the customer, and the second block of 114 bits is used to encrypt the link from the customer to the network. Encryption is performed as a simple XOR of the message with the key-stream.

Although A5 is a stream cipher, it is used to encrypt 114-bit "blocks", called *frames*. The frames are sequentially numbered (modulo 2^{22}) by a *TDMA frame number*. The frame number f that is used in the initialization of a A5 frame is actually a fixed bit permutation of the TDMA frame number. In the rest of this paper we ignore the existence of this permutation, since it does not affect our analysis.