The COS Stream Ciphers are Extremely Weak

Steve Babbage

Vodafone Group R&D, Newbury, UK
steve.babbage@vodafone.com

Abstract: A new family of very fast stream ciphers called COS (for "crossing over system") has been proposed by Filiol and Fontaine, and seems to have been adopted for at least one commercial standard. In this note we show that the COS ciphers are very weak indeed — it requires negligible effort to reconstruct the state of the keystream generator from a very small amount of known keystream.

Keywords: COS, stream cipher, nonlinear feedback shift register, cryptanalysis.

1. Introduction

The COS family of stream ciphers has been introduced by Filiol and Fontaine [1]. They are constructed from nonlinear feedback shift registers. COS(n,2L) uses n registers each of length 2L bits.

We will not describe the key loading procedure, since it is not pertinent to the attack we present here. The interested reader is referred to [1].

Once the n registers $L_1 \ldots L_n$ have been initialised, the following output generation step is repeated to generate keystream:

1. Clock L_i at least L times (the exact number of clocks to be applied is determined by the values of some of the register bits).
2. Generate the following blocks of L bits each, for all $j \neq i$ (so that there are 2(n-1) L-bit blocks altogether):

   $\textit{left-half}\,(L_i) \oplus \textit{right-half}\,(L_j)$

   $\textit{right-half}\,(L_i) \oplus \textit{left-half}\,(L_j)$
3. $i = i + 1$ (or if i=n then go back to i=1).

There are two modes of operation: mode II, in which all the 2(n-1) L-bit blocks are used as keystream each time, and mode I, in which only two of the L-bit blocks are used as keystream each time.

[1] concentrates on the definition of COS(2,128), and indeed a cryptanalysis challenge is proposed for that cipher. So in the rest of this paper we, too, concentrate on the cryptanalysis of COS(2,128). However, it is clear that the method described here applies to any other member of the COS family.

2. Cryptanalysis of COS(2,128)

2.1 Details of the cipher

There are two nonlinear feedback shift registers L_1 and L_2, of 128 bits each. At each output generation step:

1. One of the two registers is clocked 64, 65 or 66 times (with probabilities ½, ¼, ¼ respectively). (It is L_1 that it clocked on the first step, then L_2, then L_1, then L_2, etc.)
2. Generate the following two blocks of L bits each:

   left-half (L_1) ⊕ *right-half* (L_2)

   right-half (L_1) ⊕ *left-half* (L_2).

(Note that there is no difference between modes I and II when n=2.)

2.2 The space of unknowns is trivially reduced to 64 bits

First suppose that the keystream blocks are known for two consecutive steps, and that the number of times the register was clocked between the steps was 64 (this happens with probability ½). Then the contents of the registers look like this, where α, β, γ, δ, ε are 64-bit register halves:

Register that is clocked	$\boxed{\alpha}\boxed{\beta}$	$\boxed{\varepsilon}\boxed{\alpha}$
Register that is not clocked	$\boxed{\gamma}\boxed{\delta}$	$\boxed{\gamma}\boxed{\delta}$
Keystream blocks	$\alpha\oplus\delta$ $\beta\oplus\gamma$	$\varepsilon\oplus\delta$ $\alpha\oplus\gamma$

It is clear that, if any one of α, β, γ, δ or ε is known, then all the others can immediately be recovered, and so the state of both registers can be determined. This is despite the fact that the secret key used to initialise the registers has length 128, 192 or 256 bits.

But it gets much worse than that.

2.3 The effective key size is roughly one bit

Now suppose that the keystream blocks are known for three consecutive steps, that one register was clocked 64 times between the first and second step and that the other register was clocked 65 times between the second and third step (this happens with probability ½ × ¼). Then the contents of the registers look like this, where α, β, γ, δ, ε, ζ are 64-bit register halves:

First register to be clocked	$\boxed{\alpha}\boxed{\beta}$	$\boxed{\varepsilon}\boxed{\alpha}$	$\boxed{\varepsilon}\boxed{\alpha}$
Second register to be clocked	$\boxed{\gamma}\boxed{\delta}$	$\boxed{\gamma}\boxed{\delta}$	$\boxed{\zeta}\boxed{\gamma'}$
Keystream blocks	$\alpha\oplus\delta$ $\beta\oplus\gamma$	$\varepsilon\oplus\delta$ $\alpha\oplus\gamma$	$\varepsilon\oplus\gamma'$ $\alpha\oplus\zeta$

Here γ' means γ shifted to the right by one bit, with an unknown bit appearing in the leftmost position.

Let us number the bits of the register halves, so that for instance α_0 is the rightmost bit of α.

Now guess γ_0.

- We know $\alpha\oplus\gamma$, so we recover α_0.
- We know $\beta\oplus\gamma$, so we recover β_0.
- We know $\alpha\oplus\delta$, so we recover δ_0.
- We know $\varepsilon\oplus\delta$, so we recover ε_0.
- We know $\varepsilon\oplus\gamma'$, so we recover γ_1.
- We know $\alpha\oplus\gamma$, so we recover α_1.
- We know $\beta\oplus\gamma$, so we recover β_1.
- etc etc …
- … so we recover all of α, β, γ, δ and ε. And all we have had to "search" over is the single bit γ_0.

So we have an attack that requires three known keystream blocks and a 1-bit search, and works with probability 1/8. We have implemented this attack using the reference code for COS(2,128) provided at [1], and confirmed that it works as described here.

2.4 Variations of the above attack

The attack described in the previous section requires successive clocking amounts of 64 and 65. In fact it is easy to see that the attack can be generalised to work for any two successive clocking amounts that are not both equal to 64. (You may have to search over two, three or four bits instead of one ….) So, given any three consecutive blocks of known keystream, with probability ¾ there is an attack that recovers the entire state of the registers with negligible effort.

3. Conclusions

The stream ciphers in the COS family are all extremely weak. The state of the generator can be recovered with negligible effort, and high probability of success, from a very small amount of known keystream.

The only question perhaps outstanding is whether mode I of the cipher is any stronger for COS(n,2L) where n>2 (so that modes I and II are indeed different). We will not explore this further in the present paper, except to suggest that at least a probabilistic version of the attack described here is likely to hold.

4. References

[1] E.Filiol and C.Fontaine, *A New Ultrafast Stream Cipher Design: COS Ciphers*, http://www-rocq.inria.fr/codes/Eric.Filiol/English/COS/COS.html