COS Ciphers are not "extremely weak" ! The Design Rationale of COS Ciphers

Eric Filiol
ESAT/DEASR/SSI, B.P. 18, 35998 Rennes, FRANCE
eric.filiol@esat.terre.defense.gouv.fr
INRIA, projet CODES, Domaine de Voluceau
78153 Le Chesnay Cédex, FRANCE
Eric.Filiol@inria.fr

Caroline Fontaine
USTL, LIFL
59655 Villeneuve d'Ascq Cédex, FRANCE
Caroline.Fontaine@lifl.fr

September 17, 2001

Abstract

This note summarizes the results of Babbage's cryptanalysis of COS ciphers and shows that in fact COS ciphers are not weak as claimed. COS ciphers have been designed according a novel conception of encryption directly determined by the context of use. This concept is here defined more precisely.

Keywords: stream cipher, cryptanalysis, COS, nonlinear feedback shift register, adaptable encryption, dual technology, copyright protection, IFIC.

1 Introduction

In [1], S. Babbage presents a known plaintext cryptanalysis of COS ciphers and with a rather eye-catching and dramatizing title claimed that COS ciphers are extremely weak.

If its cryptanalysis partly fulfil the cryptanalytic challenge we propose, these ciphers remain however secure. COS Ciphers are meant for a new cryptographic encryption concept which could be called "*adaptable encryption*" and Babbage's claim makes clear that the COS design rationale has been misunderstood.

The purpose of this paper is to explain this design rationale. In the other hand we must precise that the challenge (known plaintext attack) was proposed maong others reasons to promote research in the area of Non Linear Feedback

Shitf Register (NLFSR). i In this sense, it is deconnected from the real-life context of use.

This paper is organized as follows. In section 2 we first present the main results of Babbages's cryptanalysis in the challenge context. Section 3 explains precisely the COS ciphers design rationale ad why COS ciphers can confidently be considered as highly secure for commercial applications. In this context we show that $(3, 512)$ version implemented in IFIC project (see [2, 4] for details) for cinema on Internet, is very secure. Finally Section 4 deals with the challenge issue.

2 Summary of Babbage's cryptanalysis

In [1], the COS cryptanalysis (particularly for the $(2, 128)$ version) is presented and we are going here to summarize the main results.

Beforehand we must precise one point. Contrary to what it is written in [1], even the $(2, 128)$ version has two different modes. In mode I the output blocks are 128 bits long and two 32-bits subblocks are randomly chosen at each step.

Here are the main results of cryptanalysis:

- Whatever may be the parameters n and L, $(n, 2L)$ COS ciphers in mode I are not broken at all.
- In a known plaintext context (precisely the challenge) and only for mode II (used for compressed data):
  - With probability of success $\frac{1}{2}$ (64 clockings of register) an exhaustive search on L bits are necessary. That is to say 2^{256} for the $(3, 512)$ version.
  - With probability of success $\frac{3}{4}$ a clever approach allows to cryptanalyze with only $6L$ bits of known plaintext (compressed plaintext) and negligible amount of work. In fact we show in Section 3 that the work factor can be considered to be equal to 2^{6L}.

3 COS Ciphers Design Rationale

The general trend in open cryptographic community is to consider that commercial cryptographic products need a strategical level of security. The general specialists'opinion indeed considers (*e.g.*) military applications and copyright protection as an equal, in terms of security. In fact it can turn to be very dangerous in case of misuse as History frequently teached us.

Moreover this idea is like swating a fly with a power-hammer. The main drawback is then that quite always the encryption speed is too weak for commercial applications requiring both a very good level of security (to strictly forbid pirates to access the products that are sold) and a very high encryption speed (*e.g.* video encryption). The COS ciphers rationale is motivated by this need and are particularly well adapted for copyright security (among other possible commercial applications).

We will not discuss the mode I COS ciphers security. This latter remains highly secure for very critical applications, whatever may be the nature of the plaintext (that is to say redundant or not). Mode I offers an excellent encryption speed but slower than that of mode II on which we now focus. Mode II has been specifically designed for compressed data encryption (or data without redundancy). We had a public key approach in mind:

- If c_l, p_l and s_l denote l bits of respectively ciphertext, plaintext and ciphering bits let us describe the encryption by the following bitwise equation $c_l = p_l \oplus s_l$. In an approach very similar to factoring, we claimed that with only the knowledge of c_l, for l large enough, it is extremely hard (as defined in complexity theory) to recover both p_l and s_l.

- Since p_l has a quite random structure (compressed data), guessing p_l is quite equivalent to guess l random bits. When considering the different compression schemes (see [5] for details), it is clear that guessing l bits of compressed data is equivalent to know most of the initial text: the encryption becomes then non sensical.

In terms of COS security and for ciphertext only attack, Babbage's cryptanalysis requires a complexity of 2^{384} for $\mathrm{COS}(2, 128)$ and of 2^{3072} for $\mathrm{COS}(3, 512)$.

More important is the way a cipher system is used. A very highly secure system can become very weak when badly used (the best example being the total or partial reuse of one time pad). On the contrary a good implementation is to greatly take part in the security concern. The best example is that of $(3, 512)$ implemented in IFIC [4] project. A film is described as a MPEG-4 compressed sequence. The key is changed for every different scene. In this case we claim that this cipher is more secure than ever.

4 Conclusion

The challenge we proposed was purposedly to promote the research in the area of Non Linear Feddback Shift Registers and was completely deconnected from real-life applications. In the context we defined (known plaintext attack) the mode II was likely to be less secure than mode I which was our essential aim for the challenge.

But to be fair, we now acknowledge that Steve Babbage has broken mode II Cos Ciphers as asked in the challenge. He will be awarded 500 euros. The remaining 500 euros will be awarded for mode I cryptanalysis.

References

[1] S. Babbage, The COS Stream Ciphers are extremely weak, *http://eprint.iacr.org/2001/078.ps*

[2] http://www-rocq.inria.fr/codes/Eric.Filiol/English/COS/COS.html

[3] E. Filiol, C. Fontaine A new Block Cipher Design: COS Ciphers, *Proceedings of the International Symposium on Information Theory 2001*, p. 134, Washington, 2001.

[4] http://www.industrie.gouv.fr/pratique/aide/appel/sp_priam.htm

[5] D. Solomon, *Data Compression: The Complete Reference*, Springer Verlag, 2000.