Understanding Phase Shifting Equivalent Keys and Exhaustive Search

Côme Berbain[1], Aline Gouget[2] and Hervé Sibert[3].

[1] Orange Labs, France, come.berbain@orange-ftgroup.com
[2] Gemalto, France, aline.gouget@gemalto.com
[3] NXP Semiconductors, France, herve.sibert@nxp.com.

Abstract. Recent articles [6, 3, 5, 7] introduce the concept of phase shifting equivalent keys in stream ciphers, and exploit this concept in order to mount attacks on some specific ciphers. The idea behind phase shifting equivalent keys is that, for many ciphers, each internal state can be considered as the result of an injection of a key and initialization vector. This enables speeding up the standard exhaustive search algorithm among the 2^n possible keys by decreasing the constant factor of 2^n in the time complexity of the algorithm. However, this has erroneously been stated in [5, 7] as decreasing the complexity of the algorithm below 2^n. In this note, we show why this type of attacks, using phase shifting equivalent keys to improve exhaustive key search, can never reach time complexity below 2^n, where 2^n is the size of the key space.

1 Speeding up exhaustive search by using phase shifting equivalent keys

In this section, we use (some of) the notations of [7].

1.1 Phase shifting equivalent keys

The concept of phase shifting equivalent keys can be summarized as follows. Most of the recent stream ciphers have two modes of operation, the initialization mode and the keystream generation mode. The keystream generation mode consists in outputting data computed from the internal state of the cipher, and updating the internal state of the cipher with an update function f. The initialization of the cipher, which determines the internal state of the cipher before keystream generation, most often uses the same building blocks as the keystream generation with some additional procedure to inject the key K and initialization vector IV into the internal state of the cipher. For a large number of stream ciphers, initialization consists in loading directly K and IV into the internal state, and then updating p times the internal state of the cipher with the same function f. In this section, we consider a stream cipher that fits this description. For such a cipher, we have the following definition:

Definition 1. *Two pairs of keys and initialization vectors* (K, IV) *and* $(\hat{K}, \hat{IV})$ *are called* i-bits-phase shifting equivalent *when the internal state of the stream cipher after loading* (K, IV) *and performing* i *updates of the internal state is equal to the internal state of the stream cipher after loading* $(\hat{K}, \hat{IV})$.

1.2 Exploiting phase shifting equivalent keys in exhaustive key search

Given the first bits of stream cipher keystream $s_0, \ldots, s_{\ell-1}$, where ℓ is the average length sufficient to match or dismiss a keystream, and an initialization vector IV, the standard exhaustive key search algorithm consists in the following:

- draw every possible key K,
- for each one of these keys, compute the cipher initialization using (K, IV), and match or dismiss K by generating bits of keystream until they differ from the provided keystream (with ℓ being the average number of keystream bits generated for this purpose),
- if the generated keystream matches the provided keystream, then the key has been recovered.

We evaluate the complexity of this algorithm in terms of updates of the internal state of the cipher. Testing a single key requires $p+\ell$ updates of the internal state, where p is the number of updates of the internal state during initialization. Therefore, the complexity of this algorithm is $(p+\ell) \times 2^n$.

Phase shifting equivalent keys can be used to speed up this algorithm as follows: suppose that, after i updates of the internal state during initialization, the current internal state is equal to the internal state obtained by loading a pair $(\hat{K}, IV)$ to the internal state, then, it is possible to test both K and $\hat{K}$ without having to compute two full initializations. Indeed, in order to test the key $\hat{K}$ simultaneously to the test of K, one only has to compute the generated keystream bits of indexes between i and $\ell+i-1$. Therefore, in order to test both K and $\hat{K}$ in a row, one has to compute $p+\ell+i$ updates of the internal state.

Suppose now that, for each key K, each one of the first i internal states during the initialization process provides a phase shifting equivalent key with the same initialization vector. Therefore, for each key K, by computing $p+\ell+i$ updates of the internal state, one can test $i+1$ keys. If, luckily enough, it is possible to avoid overlaps and ensure that every (phase shifted) key is tested only once, then, the overall complexity of the attack falls to $\frac{2^n}{i+1} \times (p+\ell+i)$. As i gets bigger, we see that the complexity decreases towards 2^n, but always remains more than 2^n. The result of this technique is thus a speed up of exhaustive search obtained by reducing the computational cost per tested key. The rationale behind this result is that testing a phase shifting equivalent key in this ideal case costs only 1 internal state update.

2 Attacks based on phase shifting equivalent keys

Phase shifting equivalent keys have been used to speed up key recovery with chosen IV in the stream ciphers Grain v1[4] and DECIM^{v2} [1], which are both candidates to the ECRYPT stream cipher eSTREAM project. For both Grain v1 and DECIM^{v2}, the attacks require an adaptation due to the fact that the initialization process differs from the keystream generation process, thus limiting the application of phase shifting to only one particular IV (all 1 for Grain and all 0 for DECIM^{v2}) and to at most one equivalent key $\hat{K}$ per key K in the standard exhaustive search algorithm.

In [6], Küçük observes that it is possible to use phase shifting in order to enhance exhaustive key search in Grain v1, but then concludes that the resulting tweak would not yield an efficient attack.

In [3], De Cannière, Küçük and Preneel also propose a 1-bit-phase-shifted-key based algorithm to improve the *standard exhaustive search algorithm* for Grain v1. However, by calling the section *Speeding Up Exhaustive Key Search*, and by stating that their algorithm on the average performs *only* 2^{78} *initializations, making it twice as fast as the standard exhaustive search algorithm*, they underline that the resulting algorithm still has a complexity that is also a function of the complexity of initialization. Thus, the resulting algorithm still requires far more than 2^{80} computations of updates of the internal state of the cipher. The same result was also claimed independently by Isobe *et al.*[5], but they conclude that their attack has complexity $2^{78.4}$ or $2^{78.7}$, thus hiding the fact that the decrease in the exponent is done at the expense of increasing a constant product factor, with an overall complexity that remains above 2^{80} updates of the internal state.

The same issue appears in [7], in which Nakagami *et al.* claim to reach time complexity $2^{79.90}$. Moreover, the absence of a precise, mathematical description of the attack algorithm prevents from computing the real complexity (time and data) of the algorithm[4]. In any case, we point out that the same issue appears, as the exponent is decreased at the expense of increasing the constant factor whose cost is hidden. Again, the overall time complexity of the resulting attack remains far more than 2^{80} updates of the internal state of Decim^{v2}.

Anyhow, it seems to be quite difficult to compare attacks of complexity very close to exhaustive search, since the effective cost of exhaustive search is quite difficult to compute [2]. It varies depending on several trade-offs and cost evaluators. Nevertheless, in the precise case of the generic phase shifting based attacks considered in this note, we have shown that the effective overall cost always remains more than 2^n updates of the internal state of the cipher.

3 Conclusion

Attacks based on phase shifting equivalent keys can improve over standard exhaustive key search in some stream ciphers, by testing some candidate keys without having to compute a full initialization of the keystream, but only one more update of the cipher. Nevertheless, in the case of Grain v1 and Decim^{v2}, differences between initialization and keystream generation prevent these attacks from being effective. Moreover, recent claims that these attacks reach complexity less than 2^n are erroneous, due to the fact that their authors forgot to take into account the time complexity of the attack per key. As shown in this note, the time complexity of this type of phase shifting equivalent key based attacks is always at least 2^n updates of the cipher state, with n being the length of the key.

References

1. C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Decim^{v2}. In *ECRYPT Stream Cipher Workshop SASC 2007*. Available at `http://www.ecrypt.eu.org/stream/`.
2. D. J. Bernstein. Understanding brute force, 2005. `http://cr.yp.to/snuffle/bruteforce-20050425.pdf`,.
3. C. De Cannière, Ö. Küçük, and B. Preneel. Analysis of Grain s initialization algorithm. In *Proceedings of AfricaCrypt 2008*, Lecture Notes in Computer Science. Springer-Verlag, 2008.

[4] In the original version of [7], the authors claimed time complexity of $2^{79.56}$, but, due to a misunderstanding of the ABSG mechanism within the Decim^{v2} scheme, they had to reconsider their attack as 1-phase shifting keys cannot be used. However, despite the remarks from the authors of this note, they did not provide a more precise description of the algorithm in the revised version.

4. M. Hell, T. Johansson, and W. Meier. Grain: a stream cipher for constrained environments. *International Journal of Wireless and Mobile Computing*, 2(1):86–93, 2007.
5. T. Isobe, T. Ohigashi, H. Kuwakado, and M. Morii. A chosen-IV attack against Grain. Proc. Information and Communication System Security, ICSS2007-3, 2007.
6. Ö. Küçük. Slide resynchronization attack on the initialization of Grain 1.0. COSIC internal report, 2006. `http://www.ecrypt.eu.org/stream/papersdir/2006/044.ps`.
7. H. Nakagami, R. Teramura, T. Ohigashi, H. Kuwakado, and M. Morii. A chosen IV attack using phase shifting equivalent keys against DECIM^{v2}. Cryptology ePrint Archive, Report 2008/128, 2008. `http://eprint.iacr.org/`.