

Weak Keys

The strength of the encryption function $E_K(P)$ may differ significantly for different keys K . If for some set WK of keys the encryption function is much weaker than for the others this set is called a *class of weak keys*. The attack technique that succeeds against the keys in the class WK is called a *membership test* for the class. For example, if the test uses differential cryptanalysis, then it will be called a *differential membership test*.

Suppose the key space has k bits, so that complexity of exhaustive search is 2^k . Suppose there exists a class of weak keys of size 2^f , with a complexity of the membership test of 2^w . If $2^w < 2^f$ exploiting weak keys is more efficient than using the exhaustive search. In other words if the choice of the key of the cryptosystem is restricted to a weak-key class the attack succeeds if it is faster than exhaustive search over this restricted key-class.

The following attack model, allows to compare the conventional attacks and the attacks using weak keys. Suppose the attacker is given an access to the block box performing encryption/decryption function. Suppose that the box has a key-reset button, which causes the key to change inside the box uniformly at random. We call the attack successful if the attacker can recover at least one of the keys of the box faster than exhaustive search (or in a relaxed scenario, is able to distinguish a box with a cipher from a box with a collection of random-permutations). The measure of complexity of such an attack in a weak key scenario is 2^{k-f+w} . This can be compared directly to the complexities of the conventional attacks, in which the attacker will try to break a “fixed” key, i.e. will not touch the key-reset button. The larger the weak key class and the faster the membership test — the better the attack would be. A typical example of a cipher with large weak key classes is IDEA. For example, a class of 2^{63} weak keys out of total 2^{128} keys has been reported [2] for a full 8.5-round IDEA. The membership test has negligible complexity given only 20 chosen plaintexts. The measure of complexity in this case would be $2^{k-f+w} \approx 2^{128-63+4} = 2^{69}$ steps to recover one of the 128-bit keys of the black-box containing the IDEA cipher. An example of a cipher completely broken by the weak key analysis is *Lucifer* [1]. In this 128-bit block cipher half of the keys can be discovered by a differential membership test using 2^{36} chosen plaintexts and analysis steps. The attack complexity measure in this case is $2^{128-127+36} = 2^{37}$. In the case of DES there is a set of four keys for which the cipher is an involution, i.e. $DES_k(DES_k(m)) = m$.

–Alex Biryukov.

References

- [1] I. Ben-Aroya and E. Biham, “Differential cryptanalysis of Lucifer,” in *Advances in Cryptology – CRYPTO’93* (D. R. Stinson, ed.), vol. 773 of *Lecture Notes in Computer Science*, pp. 187–199, Springer-Verlag, 1993. see also *Journal of Cryptology*, Vol. 9, No. 1, pp. 21–34, 1996.
- [2] P. Hawkes, “Differential-linear weak key classes of IDEA,” in *Proceedings of Eurocrypt’98* (K. Nyberg, ed.), no. 1403 in *Lecture Notes in Computer Science*, pp. 112–126, Springer-Verlag, 1998.

Resynchronization Attack

Synchronous stream ciphers require some procedure for resynchronizing in the case of synchronization loss. This opens doors to new attack scenarios. A typical stream cipher encrypts the stream in fixed data blocks, called *frames* (or packets) by keeping the same secret key for all the frames but mixing the new *initial value (IV)* or the *frame-counter* for each frame (see for example the A5/1 cipher). This allows for easy synchronization as well as for the late entry mechanism in the case of multi-party communication. On the one hand such mode of operation produces only short streams for any fixed state which reduces the chances of some attacks but on the other hand it may open doors to new analysis techniques which will attack the resynchronization mechanism itself. Depending on the way IV and the key are loaded and mixed into the *state* of the stream cipher the scheme may be susceptible to differential, linear, slide or other attacks. A typical resynchronization attack on stream ciphers is given in [3]. For more recent results on the subject see [1, 2, 4, 5].

References

- [1] A. Biryukov and D. Wagner, “Slide attacks,” in *Proceedings of Fast Software Encryption – FSE’99* (L. R. Knudsen, ed.), no. 1636 in *Lecture Notes in Computer Science*, pp. 245–259, Springer-Verlag, 1999.
- [2] Y. Borissov, S. Nikova, B. Preneel, and J. Vandewalle, “On a resynchronization weakness in a class of combiners with memory,” in *Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers* (S. Cimato, C. Galdi, and G. Persiano, eds.), vol. 2576 of *Lecture Notes in Computer Science*, pp. 164–173, Springer-Verlag, 2002.
- [3] J. Daemen, R. Govaerts, and J. Vandewalle, “Resynchronization weaknesses in synchronous stream ciphers,” in *Advances in Cryptology – EUROCRYPT’93* (T. Helleseth, ed.), vol. 765 of *Lecture Notes in Computer Science*, pp. 159–167, Springer-Verlag, 1993.
- [4] P. Ekdahl and T. Johansson, “Another attack on A5/1,” *IEEE Transactions on Information Theory*, vol. 49, pp. 1–7, 2003.
- [5] J. D. Golic and G. Morgari, “On resynchronization attack,” in *Fast Software Encryption, FSE 2003* (T. Johansson, ed.), vol. 2887 of *Lecture Notes in Computer Science*, pp. 100–110, Springer-Verlag, 2003.

Truncated Differentials

The notion of a truncated differential was defined by Knudsen in [2] and was applied to cryptanalyse cipher *SAFER* due to its word-oriented operations [3]. Truncated differentials are an extension of the notion of differentials, used in differential cryptanalysis. The main idea is to leave part of the difference unspecified, thus clustering several differentials together. This can be done by specifying m -bit constraints on the whole block (where m is smaller than the block size n), like: $(A, -A, B, 2B)$, where A, B can take any value as was done in [2]; or by fixing part of the data block to certain value and allowing the rest to vary arbitrarily, like: $(0, *, 3, *, 255, *, *)$, where $*$ may take any value. Such "wild-card" differentials were introduced in cryptanalysis of hash-function *Snefru* [1]. Truncated differentials are a powerful tool against ciphers with word-oriented structure, and play important role in such extensions of differential technique as impossible-differentials and boomerang attack. Truncated differentials are often combined with a technique of packing data into *structures*, which sometimes allows to exploit truncated differentials even with probabilities lower than 2^{-n} . See also differential.

References

- [1] E. Biham and A. Shamir, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer," in *Advances in Cryptology – CRYPTO'91* (J. Feigenbaum, ed.), vol. 576 of *Lecture Notes in Computer Science*, pp. 156–171, Springer-Verlag, 1991.
- [2] L. R. Knudsen, "Truncated and higher order differentials," in *Fast Software Encryption, FSE'94* (B. Preneel, ed.), vol. 1008 of *Lecture Notes in Computer Science*, pp. 196–211, Springer-Verlag, 1995.
- [3] L. R. Knudsen and T. A. Berson, "Truncated differentials of SAFER," in *Fast Software Encryption, FSE'96* (D. Gollmann, ed.), vol. 1039 of *Lecture Notes in Computer Science*, pp. 15–26, Springer-Verlag, 1996.

IPES

IPES is an alternative name for the IDEA cipher. IPES stands for "improved PES", where *PES* is a cipher predecessor of IDEA which was cryptanalysed by differential cryptanalysis in [1].

References

- [1] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Proceedings of Eurocrypt'91* (D. W. Davies, ed.), no. 547 in Lecture Notes in Computer Science, pp. 17–38, Springer-Verlag, 1991.

Multiple Encryption

Composition of several ciphers is called multiple encryption or *cascade cipher*.
See also product cipher.