Known Algorithm Attacks on Standard Ciphers

William L. Millan

ISRC, QUT
GPO Box 2434, Brisbane 4001, Australia
millan@isrc.qut.edu.au

Abstract. The conventional world of cryptology *does not consider* the possibility of heuristic cryptanalysis being effective against modern standard ciphers like Rijndael, the new Advanced Encryption Standard (AES). However, this paper presents evidence that evolutionary computation should *be expected* to be able to develop approximations (in an attacker's model) that seriously reduce the effective security of any targeted cipher. This clash of security paradigms is analysed, prospects for the success of EC in cryptanalysis are discussed and solutions to the attendant problems are offered.

1 Introduction

In this paper we consider the prospects for evolutionary algorithms to perform effective cryptanalysis of standard block ciphers like the old Data Encryption Standard [2] and the new Advanced Encryption Standard [1]. We argue that the very existance of *standard* ciphers risks the possibility of a new class of *known algorithm* attacks (KAA). These attacks would operate in two stages. Firstly, an evolutionary pre-computation develops an approximation, or attacker's model, to be used in the second (active) phase which uses the evolved model and known plaintext to suggest key-bit values. We argue that attacker's models can be evolved that allow the second phase to guess key bits with probability strictly greater than one half.

To be precise, we claim (and outline how it can be shown) that *every* block cipher must have some weakness and that such weaknesses can be discovered by EC precomputation, but *only* if the algorithm is known. Hence we dare to critique the decision to set single encryption standards. The techniques we outline are currently theoretical, but we argue that they are increasingly likely to be attempted, with possibly drastic implications for information security globally. Hence we choose to offer some suggestions to reduce or solve the problem.

2 The Inevitable Weakness of Ciphers

A block cipher is a keyed reversible mapping. For every value of the k-bit key, there is a different permutation induced on the b-bit message space. The correlation between output functions is a value in the range [-1,...,1] and its magnitude

describes how well the functions approximate each other. Zero correlation occurs for pairs functions that are statisticaly independant (for samples taken uniformly over the whole input space). The set of functions that minimize the maximum correlation are called the *bent* functions [4]. They are said to posses maximum possible nonlinearity.

Of particular interest to cryptanalysis is the set of Linear functions. Linear approximation is a well-known topic in cryptology and modern ciphers are designed to resist linear approximation. However there is a well-known theorem of Parseval which states that for every Boolean function, the sum of the squares of the correlations to all linear functions is exactly one [5]. This means that even the best functions have some correlation to some linear functions. Another recent development is the splitting (or decomposition) of Boolean functions, introduced in [3]. Adapting those results to cryptanalysis, it can be shown that *any* existing bias can be *increased* by suitable choice of a linear form to define a splitting of the input space. Combining these results and iterating, we obtain an algorithm that uses evolutinary techniques to develop a data structure or model that well approximates the target function.

3 New models for EC cryptanalysis

The attacks we warn about are based on a modified attacker's model of the encryption process. Let $C = E_K(P)$ denote an encryption algorithm E taking key K to transform plaintext P into Ciphertext C. Decryption is the inverse operation $P = E_K^{-1}(C)$.

The first phase of the attack is a massive pre-computation directed at finding linear correlations in the subspaces of a function closely related to the target encryption algorithm. Without giving all the details here (exact models, data structures and possibility for distributed computation), it is clear that *this can be done only for known algorithms*, and once that approximate model has been developed, it can be quickly and easily used to estimate the value of unknown key bits. In phase 2, a set of known plaintext/ciphertext pairs (obtained from encryption with the unknown target key) can be used to generate approximations to the key bits, with bias equal to that of the developed approximation.

The pre-computed model can be re-used on other target users, thus spreading the (substantial) cost over many actual attacks. Once the cost of an attack is reduced to less than the value of the data, then it becomes cost-effective and hence more attractive. We have a single standard cipher protecting all the data.

3.1 Comparison with Existing Techniques

This approach contrasts with the traditional paradigm where "provable security" versus first order structural cryptanalysis is the only yardstick apart from the size of the key. Briefly, modern block ciphers all follow the iterated product cipher paradigm. So a block cipher is constructed as a (reversible) nonlinear operation which is repeated a fixed number of times, each instance modified

by a sequence of values derived from the secret key. Structural analysis of the probability of linear approximations and bias of differential characteristics results in arguements that the number of known or chosen message blocks required to perform these attacks exceeds the amount available, and hence that attack is impossible and so the security against it has been proved.

These arguements are compelling, but only so far as they go. They do not consider the resistance against improved or modified attacks, only the generic form. They ignore higher order versions of the attacks, and they ignore attacks on subspaces, such as we suggest here. It is well known in the history of cryptanlysis that attacks get improved, yet this trend seeems to have been overlooked while setting criteria for standards.

4 How to defend against KAA

Known Algorithm Attacks can be performed in any environment where the encryption algorithms are known. Given we must have standard communication protocols, this places modern society in a vulnerable position unless alternative methods are provided. Here we suggest two defences: many multiple standards and negotiated algorithms. Firstly, multiple standards reduces the probability of an individual actually using the cipher that EC cryptanalysis has attacked. Secondly, if the details of the encryption algorithm can be negotiated during the key-set-up protocol, then an attacker has no known algorithm to attack.

5 Conclusion

It is inevitable that, one day, someone, somewhere, will set running an open-ended adaptive evolutionary computation with the sole objective of discovering exploitable weaknesses in the current encryption standard. When those exploits appear on the web for anyone to download, the standard becomes untrustworthy. To defend against this event, we must make ready *several* alternative algorithms, or offer new protocols that securely negotiate the details of on-the-fly encryption algorithms.

References

1. J. Daemen and V. Rijmen. "AES Proposal: Rijndael". Available at http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1997.
2. "Data Encryption Standard". NBS FIPS PUB 46, National Bureau of Standards, U.S. Department of Commerce, Jan 1977.
3. J. Fuller, W. Millan and E. Dawson. "Evolutionary Generation of Bent functions", presented at IEEE Congress on Evolutinary Computation, CEC'03, December 2003.
4. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error Correcting Codes", North-Holland publishing company, 1978.
5. W. Meier and O. Staffelback, "Nonlinearity Criteria for Cryptographic Functions". Eurocrypt'89, LNCS vol 434, pages 549-562, Springer-Verlag, 1990.