Selection Cryptanalysis: A Deadly Surname*

Raphael CW Phan[1] and Rachel YZ Phan

[1] SUT, Malaysia.
rphan@swinburne.edu.my
[2] ...

Abstract. The powerful deletion cryptanalysis method was introduced by Knudsen and Mirza and was shown to entirely break two popular cryptosystems, the one-time pad and the DES. In this paper, we generalize the attack and introduce the notion of selection cryptanalysis, and show that it is the superset of deletion cryptanalysis. We also introduce the insertion cryptanalysis, a dual to the deletion cryptanalysis. We show how this new attack completely demoralizes yes, the one-time pad, and the newly crowned AES.

1 Introduction

In a landmark paper [1], Knudsen and Mirza became the fathers of modern craptanalysis when they introduced the ever powerful deletion cryptanalysis. This method can be applied to any cryptosystem, and examples were shown how the one-time pad and DES are totally weak against this attack. As an attempt to make right what Knudsen and Mirza are trying to make wrong, Black [2] proposed to vigilantly put back whatever components that Knudsen and Mirza have deleted. This is quite noble indeed.

In this paper, we generalize the basic ideas behind deletion cryptanalysis and introduce a family of related cryptanalysis methods, collectively surnamed *selection cryptanalysis*. We present a dual to deletion cryptanalysis, the *insertion cryptanalysis*, and show that they share the same surname.

Section 2 presents a brief review of deletion cryptanalysis. In Section 3, we prove that selection cryptanalysis is a superset of deletion cryptanalysis. We introduce the insertion cryptanalysis, a dual to deletion cryptanalysis in Section 4 and apply it to the one-time pad and the AES. We then generalize it to apply to any cipher.

2 Review of Deletion Cryptanalysis

The deletion cryptanalysis enables the attacker to *selectively delete* vital components from a cryptosystem. Once deleted, the cryptosystem is totally defenseless against further attacks from the attacker.

* Submitted Nov 15, 2001. Accepted Jun 31, 2006.

3 Surnamed Selection Cryptanalysis

The basic idea behind deletion cryptanalysis is the word 'selectively delete', giving the attacker power beyond his wildest dreams. And it is from this very keyword that we discovered the family background of the deletion cryptanalysis.

Theorem 1. Deletion Cryptanalysis is surnamed Selection Cryptanalysis.

Proof.
We prove this by obviousness. It is obvious that deletion cryptanalysis *selectively* deletes components from cryptosystems, hence it must be a family member of selection cryptanalysis. □

4 Insertion Cryptanalysis

We present a new cryptanalysis method termed as *insertion cryptanalysis* [3]. The basic idea is to let the attacker selectively insert components into the cryptosystem he is attacking. We demonstrate this attack on the one-time pad and the AES.

4.1 Insertion Cryptanalysis of the One-time Pad

The one-time pad performs encryption on plaintext P by XORing it with the key K to obtain ciphertext C, based on the formula $C = P \oplus K$. By inserting an XOR into the cipher, we have

$$C = P \oplus K \oplus K = P. \tag{1}$$

Clearly, we see that without knowing the key, and regardless of what the key may be, the attacker can easily read the plaintext.

4.2 Insertion Cryptanalysis of the AES

The Advanced Encryption Standard (AES) is a new encryption standard set to replace the DES in the years to come. The AES is a 128-bit block cipher with a 128-, 192-, or 256-bit secret key. The input plaintext is passed through a round function which is iterated 10, 12 or 14 times for a secret key-size of 128, 192 or 256 bits respectively. The round function consists of SubBytes, a nonlinear 8×8 byte substitution; ShiftRows, a cyclic shift of each row by different byte offsets; MixColumns, a linear combination of all 4 bytes in the same column; and AddRoundKey, an XOR of the plaintext with the round key, generated from the secret key. Each round is identical except that an extra AddRoundKey is added before the first round and MixColumns is excluded from the last round.

[3] The author wishes to thank Key Bordd [3] for inspiring such a name.

To attack the AES by insertion cryptanalysis, consider a simple insertion of an XOR into each AddRoundKey component of the AES. Let X and Y be the input and output of AddRoundKey respectively, and K_i be the round key. Then

$$Y = \texttt{AddRoundKey}(X, K_i) \oplus K_i = X \oplus K_i \oplus K_i = X. \tag{2}$$

Due to the insertions, the output of each AddRoundKey component depends solely on its input and not on the round key, K_i. Hence since all the round function components of the AES are known to the attacker, then given any ciphertext, he can regain the plaintext without knowledge of the secret key.

4.3 Generic Insertion Attacks on any Cipher

We can do much better. Let $E_K(P)$ be the block cipher under attack. One anonymous referee suggests to obtain the insertion-attacked cipher as $E^*_K(P) = E_K(P)||P$. Clearly, this can apply to any cipher, regardless of the internal construction, and as such is a generic transform. The problem is that bandwidth is increased. It is an open problem to define a generic insertion cryptanalysis attack which does not increase bandwidth.

Another anonymous referee suggests to obtain the insertion-attacked cipher as $E^*_K(P) = E_K(P)||K$. While the first referee's suggestion had increased the bandwidth by a factor of 2, this suggestion has an additive fixed increase. Moreover, it is also possible to append only part of the key (thus reducing the additive constant).

4.4 Insertion and Deletion Cryptanalysis

Insertion cryptanalysis works by allowing the attacker to *selectively insert* components into cryptosystems. This leads us to the following theorem, the proof of which is trivial.

Theorem 2. Insertion Cryptanalysis is also surnamed Selection Cryptanalysis.

Corollary 1.
Insertion cryptanalysis and deletion cryptanalysis are siblings.

Proof.
We leave this proof as an exercise to the reader. □

5 Conclusions

We have presented a family of related cryptanalysis methods surnamed selection cryptanalysis. We showed that deletion cryptanalysis is surnamed selection cryptanalysis and also aided deletion cryptanalysis in locating its long-lost sibling, the insertion cryptanalysis.

Acknowledgement

We thank the anonymous referees Nigel and Orr for laughing at our work, and for respectively suggesting the generic insertion cryptanalysis techniques in Section 4.3.

References

1. Lars R. Knudsen and Fauzan Mirza, 'Deletion Cryptanalysis', *Journal of Craptology*, Vol. 0, No. 0, 1998.
2. John Black, 'Strengthening Cryptosystems by Re-Keying', *Journal of Craptology*, Vol. 0, No. 1, 1999.
3. Key Bordd, 'Insert and Delete', *private serial communication*, Nov 2001.