Results of Switching-Closure-Test on FEAL
(Extended abstract)

Hikaru Morita Kazuo Ohta Shoji Miyaguchi
NTT Laboratories

Abstract

The closure tests, CCT and MCT, were introduced to analyze the algebraic properties of
"cryptosystems by Kaliski et al. [KaRiSh]. If a cryptosystem is closed, the tests give the
same results "Fail" and the cryptosystem might be breakable. Though CCT requires much
less memory and time than MCT, we cannot apply CCT to check cryptosystems having the
same data and key block lengths such as FEAL with non-parity mode. Because CCT
utilizes the differences in data and key block lengths.

Though CCT experiments performed by Kaliski et al. detected that DES is not
closed, how should FEAL be checked? Does FEAL pass in MCT? Since MCT needs a lot
of memory and time, to check FEAL, we developed a switching closure test SCT [MoOhMi],
which is practical version of MCT. In this paper, by using SCT, it is confirmed that FEAL
is not closed with high probability.

1. Introduction

To find the algebraic structure of cryptosystems in general, Kaliski et al. [KaRiSh] proposed
two closure tests: CCT (cycling closure test) and MCT (meet-in-the-middle closure test).
These tests can detect features such as algebraic closure. Moreover, they also proposed
two cryptattack methods based on the algebraic features.

Generally, both CCT and MCT can determine if a cryptosystem is closed or not. If
a cryptosystem is closed, they give the same results "Fail", which means the cryptosystem
might be breakable. However, if a cryptosystem is not closed, you cannot be sure that they
will give the same results because it isn't known whether they can detect the same algebraic
structure or not. When each closure test detects that a cryptosystem is not closed, we say
the cryptosystem "Passes." A "Passed" cryptosystem is secure against cryptattack methods
based on the closure property. CCT experiments performed by Kaliski et al. detected that
DES is not closed.

Our interest was that MCT might prove to be a fertile avenue for cryptographic
research. MCT offers the possibility of extracting information from a not-closed cryptosystem
that would allow the cryptosystem to be broken. However, MCT needs an excessive
amount of memory. On the other hand, though CCT requires much less memory, we
cannot apply CCT to a cryptosystem having the same data and key block lengths such as
FEAL with non-parity mode. Because CCT utilizes the property that if a cryptosystem is
closed, the cycling period approaches $O\left(\sqrt{|K|}\right)$, otherwise it approaches $O\left(\sqrt{|M|}\right)$ where $K$ and $M$ are key and message space, respectively, and $|S|$ indicates the number of elements of a set $S$. Consequently, we presented a switching closure test (SCT) [MoOhMi] so that MCT's memory requirements are dropped from $O\left(\sqrt{|K|}\right)$ to a constant value. While up to now the memoryless method has been applied to collision search [QuDe], we applied it to a closure test for cryptosystems.

We wanted to know if all FEAL-N including FEAL-8 fails in MCT or not. If FEAL fails in MCT, FEAL may be broken by the known-plaintext attack with high probability because MCT can be easily applied to the known-plaintext attack. We tested FEAL by using SCT.

Section 2 shows SCT procedures. Section 3 presents experimental results of FEAL-8. This paper is concluded in Section 4.

2. Switching Closure Test [MoOhMi]
2.1 Background

When a cryptosystem is defined by $\Pi = (K, M, C, T)$, where $K$, $M$, and $C$ are key space, message space, and ciphertext space, respectively and $T$ is a set of all encryption transformations defined by $T \equiv \{E_k|k \in K\}$ where the ciphertext $c = E_k(p), (p \in M, c \in C)$, its algebraic system is $(T, \cdot)$ where $E_{k_2} \cdot E_{k_1}(p) \equiv E_{k_2}(E_{k_1}(p))$ for $\forall p \in M$.

If the set $T$ is closed under the product operation $\cdot$, the double-encryption transformation $E_{k_2} \cdot E_{k_1}$ equivalent to a given encryption transformation $E_k$ for any plaintext can be found. Thus, you can decrypt ciphertext $c$ by using double-encryption key pair $(k_1, k_2)$ instead of the real key $k$, and it is known that the algebraic system $(T, \cdot)$ constitutes a group.

If the system $(T, \cdot)$ is a group, it is not difficult to find pairs of double-encryption transformations. This is because, for arbitrary keys $k$ and $k_1$, there exists a key $k_2$ such that $E_k = E_{k_2} \cdot E_{k_1}$. Though the number of all double-encryption pairs is the square of key size $|K|$, the number of double-encryption key pairs $(k_1, k_2)$ equivalent to the encryption key $k$ is the key size $|K|$. Consequently, if you search $|K|$ times, you should find one equivalent double-encryption key pair. Therefore, we do not need a large number of search operations.

In the meet-in-the-middle strategy, $r_1$ values of $E_k(p)$ and $r_2$ values of $E^{-1}_{k_2}(c)$ (inverse transformation of $E_{k_1}$) are generated like this. Then, values of $\{E_k(p)\}$ and $\{E^{-1}_{k_2}(c)\}$ are matched against each other. If you select $r_1 = r_2 = \sqrt{|K|}$, you can check $|K|^2$ pairs. The meet-in-the-middle strategy can reduce the order of $|K|$ to $\sqrt{|K|}$. So, if the cryptosystem has an algebraic structure such that $(T, \cdot)$ forms a group, a key pair found by this strategy becomes equivalent to the real key for an arbitrary plaintext with high probability.