FEAL の最大差分特性確率および最大線形特性確率について（全体概要）

評価者：NTT（神田　雅透）

2001 年 1 月 12 日

全体概要

本レポートでは、差分解読法及び線形解読法に対する FEAL の安全性自己評価の妥当性を検証した。

FEAL は差分解読法や線形解読法が発見される以前に設計された暗号であるため、設計時点においてこれらの解読法が考慮されていなくても、そのこと自体はやむを得ない。また、幸運なことに、FEAL は**差分解読法や線形解読法に対する第三者評価が充実しており、そのいずれもが独立に行われた結果であることを考え合わせると第三者評価結果の信憑性はきわめて高い**ものと考えられる。以上の結果より、提案者の主張どおり、**差分解読法及び線形解読法に対して 32 段以上の FEAL-NX ($N \geq 32$) であれば安全**であると期待できる。

なお、今回の評価が、差分解読法に対する安全性評価の下限ともいえる最大差分特性確率を利用した評価であり、かつ FEAL-32X が学術的に安全であるために必要とされる閾値ぎりぎりである。このことは、**現在主流の暗号設計指針に照らし合わせれば、セキュリティマージンがない**ことを意味している。

Abstract

In this report, the validity of the self-evaluation of FEAL is discussed in terms of the security evaluation against differential cryptanalysis and linear cryptanalysis.

Since FEAL was designed in 1987 before differential cryptanalysis and linear cryptanalysis appeared, it is unavoidable that the design criteria of FEAL did not include the security countermeasures against the cryptanalyses. Fortunately, however, *many cryptographic researchers have been studying security evaluation of FEAL against differential cryptanalysis and linear cryptanalysis. Since their results are obtained independently, the reliability of their evaluation is very high.* Accordingly, it is expected that *FEAL-NX ($N \geq 32$) is invulnerable to differential cryptanalysis and linear cryptanalysis*, as submitter claimed.

The estimation is based on the maximum differential characteristic probability, which represents a lower bound of security evaluation against differential cryptanalysis. And, the probability of FEAL-32X is very close to the security threshold which proves that 64-bit block cipher is secure enough against differential cryptanalysis in an academic sense. This means that *FEAL-32X has no security margins from the point of view of recent cryptographic design criteria.*