CIPHERUNICORN-E 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 CIPHERUNICORN-E の安全性評価について、自己評価書の記述内容に沿って、その妥当性を検証した。

提案者は、15 段での最大差分特性確率と最大線形特性確率の上界値はそれぞれ 2^{-84} と $2^{-447.3}$ であり、差分解読法及び線形解読法に対して十分に安全であると述べている。

しかし、評価者が自己評価書の記載内容を検討した結果、記載内容の正当性を確認できない点がいくつかあり、また、自己評価書の線形解読法に対する安全性評価（第 3.1 節）が完全に誤りであることを発見した。

以上の点を考慮すると、**自己評価書の安全性評価に対する信頼性は、少なくとも学術的にはあまり高くない**といわざるを得ない。しかし、幸いにして、**CIPHERUNICORN-E の段数は 16 段であるので、差分解読法や線形解読法に対しておそらく安全であろう**と期待できる。なお、これらの結果からは、現在主流の暗号設計指針に照らし合わせた場合に、どれだけのセキュリティマージンがあるかを見積もることはかなり困難であるが、**学術的な意味においてセキュリティマージンが高いとは思われない**。

Abstract

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

In the self-evaluation, submitter claims that the upper bounds of the maximum differential and linear characteristic probability with 15 rounds are 2^{-84} and $2^{-447.3}$, respectively. Thus, this means that CIPHERUNICORN-E is invulnerable enough against differential cryptanalysis and linear cryptanalysis.

Unfortunately, however, I found out that there are some doubtful arguments in his self-evaluation report, and that the security estimation against linear cryptanalysis described in Sect. 3.1 in his report is wholly wrong.

Accordingly, *the reliability of the security evaluation against differential cryptanalysis and linear cryptanalysis in his self-evaluation report seems not to be high from the point of view of academic security evaluation.* Fortunately, however, it is expected that *CIPHERUNICORN-E seems currently secure against differential cryptanalysis and linear cryptanalysis regardless of the lack of the reliability of his self-evaluation report, since the number of rounds is 16.* It is very difficult to estimate the security margin of CIPHERUNICORN-E from the point of view of recent cryptographic design criteria, but it is considered that *CIPHERUNICORN-E probably has low (not high) security margins in an academic sense.*