# CIPHERUNICORN-A 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

## 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-A 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の上界値を $2^{-120}$、最大線形特性確率の上界値が $2^{-157.29}$ であると主張し、特に、線形解読法に対しては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、いくつかの点で記載内容の正当性を確認できない、あるいは不十分な評価であると疑われる個所が見られた。このため、結果として、提案者による差分解読法及び線形解読法に対する安全性自己評価結果は正確性、妥当性を欠くことになり、評価者は、提案者の記述内容が正当であるとは同意できない。例えば、自己評価書のデータだけでは、15 段での最大差分特性確率の上界値が、$2^{-120}$ ではなく、$2^{-98}$ であることしか導き出していないと評価者は考える。また、変形ラウンド関数での最大線形特性確率も、提案者の主張よりも大きな値であると考えられる。

したがって、**自己評価書における差分解読法及び線形解読法に対する安全性評価結果は、少なくとも学術的には信憑性があるとは認められない**といわざるを得ない。評価者の現時点の見解として、CIPHERUNICORN-A は、**実用上の使用に関して、差分解読法や線形解読法に対して安全であると期待されるが、学術的な安全性評価の観点からは差分解読法及び線形解読法に対して安全であるとはいえない**と判断する。

## Abstract

In this report, the validity of the self-evaluation of CIPHERUNICORN-A 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 $2^{-120}$ and $2^{-157.29}$, respectively. In particular, this means that CIPHERUNICORN-A is invulnerable enough against linear cryptanalysis.

Unfortunately, however, I found out that there are some doubtful arguments, and incomplete estimation in his self-evaluation report. As the result, I cannot agree that his self-evaluation is correct, because of the lack of reliability of his security evaluation against differential cryptanalysis and linear cryptanalysis. For example, I believe that the self-evaluation makes the upper bound of maximum differential characteristic probability with 15 rounds $2^{-98}$, not $2^{-120}$. And, the maximum linear characteristic probability of the modified round function is also higher than his argument.

Accordingly, *the security evaluation against differential cryptanalysis and linear cryptanalysis in his self-evaluation report seems not to be received at least by the academic cryptographic community.* In my opinion at this moment, *CIPHERUNICORN-A seems currently secure against differential cryptanalysis and linear cryptanalysis in terms of daily use, but insecure from the point of view of academic security evaluation.*