Camellia 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 Camellia の安全性自己評価の妥当性を検証した。

Camellia の評価方針として active s-box の最少個数に基づいて最大差分特性確率と最大線形特性確率の上界値を見積もる手法を採用したことは、現在の暗号設計指針の観点からみて妥当な選択であるといえる。また、**理論的評価については、その評価手法が SAC2000 に採録されており、理論の正当性が第三者によっても確認されているものと考えられるので、これによる評価結果は十分に信頼**できる。**計算機実験結果についても、第三者評価である L. R. Knudsen の結果と矛盾しないことから、提案者の主張する安全性が十分に期待**できるものと考える。

また、現時点で知られている最良の攻撃方法は Knudsen のレポートに記述されており、それによれば、最長の攻撃可能段数は、truncated differential cryptanalysis による $\mathrm{FL}/\mathrm{FL}^{-1}$ 関数無しの 7 段攻撃である。

以上の結果より、**差分解読法及び線形解読法に対する安全性評価について、提案者の主張に誤りはない**と判断する。すなわち、16 段以上の有効な差分特性及び線形特性が存在しないことが理論上保証されているうえ、実際には 12 段以上の有効な差分特性及び線形特性が存在しないと十分に期待される。これより、**Camellia は（差分解読法や線形解読法に対して）実用的証明可能安全 (practical security) を満たしている**ことになる。

Abstract

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

In order to estimate the security of Camellia against the cryptanalyses, *it is a reasonable choice as the design criteria of Camellia to use the upper bounds of the maximum differential and linear characteristic probability, which is based on the minimum number of active s-boxes.* In addition, *the theoretical estimation seems to be reliable enough because the theory is recorded in SAC2000 proceeding and verified by third cryptographic researchers.* It is also expected that *Camellia satisfies the security level which submitter claimed because the computational results do not contradict the result of L. R. Knudsen.*

Knudsen's report shows the best attack that 7-round variant of Camellia without $\mathrm{FL}/\mathrm{FL}^{-1}$-functions is distinguishable to random function by truncated differential cryptanalysis.

Accordingly, *the submitter's claim is correct in terms of security evaluation against differential cryptanalysis and linear cryptanalysis.* That is, it is theoretically proven that there are no effective 16 (and more) rounds differential characteristics and linear characteristics, and it seems to be believed that there are no effective 12 (and more) rounds both characteristics, actually. Thus, it is proven that *Camellia is practically secure against differential cryptanalysis and linear cryptanalysis.*