Camellia 詳細評価 概要

我々は Camellia に対して安全性評価を行った.

いくつかの攻撃を試行した範囲で以下のような結果が得られた.

FL/FL^{-1} 関数を除いた変形 Camellia5 段において, バイト多項式による解析によって選択平文 2 文で 5 段目の副鍵 1 バイトを 1 つに絞り込めることがある.

また全単射なラウンド関数を用いていることから，FL/FL^{-1} 関数を除いた変形 Camellia6 段で秘密鍵長総当りよりも短い計算量で鍵推定が可能であろう.

Boomerang 攻撃を適用することにより，FL/FL^{-1} 関数を除いた変形 Camellia 8 段が，秘密鍵総当たりより少ない計算量で鍵を推定することが可能であろう.

以上のような Camellia への解析を行った結果では，Boomerang 攻撃の適用が最も有効な解析手法であった.

差分解読法や線形解読法，高階差分解読，補間攻撃などに関しても，安全性に関する問題は見つからなかった.

また Camellia の鍵生成部の特性として秘密鍵 5 バイトと中間鍵 6 バイトから, 不明な秘密鍵 1 バイトを計算できる場合が存在した.

我々が行った評価の限りでは，安全性に関する問題は見つからなかった．FL/FL^{-1} 関数で使用される鍵値によっては，全体がバイト単位での処理のみになってしまうことからも，より詳細に byte-oriented な評価を続けた方がよいであろう.