FEAL-NX 詳細評価 概要

FEAL-NX に対して安全性評価を実施した。

差分解読により、選択入力差分をもつ平文とそれに対応する暗号文が 2^{64} 組（データ量は 2^{63}）入手できるという条件のもとで、秘密鍵の総当たり探索よりも少ない計算量で、秘密鍵を求めることができるであろう。

線形解読では、既に報告されている解読結果より効率の良い解読方法は得られなかった。

高階差分解読、補間攻撃、mod n 解読、鍵関連攻撃、スライド攻撃、中間一致攻撃を適用することは困難もしくは不可能であろう。

タイミング攻撃、電力差分攻撃、故障利用攻撃に関しては、実装時に注意すべきである。

鍵処理の構造から、拡大鍵が 6 段毎に繰り返す秘密鍵が、2^{32} 程度見つかった。ただし、この特性により強度の低下は認められない。また、鍵処理は単射構造であり、異なる秘密鍵から生成される拡大鍵に同じものは存在しない。

FEAL-N に対して既に発表されている論文からも、FEAL-NX の安全性に対して問題となる記述は見つからなかった。

これらの結果から、実際の運用において、FEAL-NX の安全性に対して問題はないと考える。