要 旨

アルゴリズム生成型 FEAL の強度評価

福冨英次

共通鍵暗号方式に対する攻撃として，差分解読法や線形解読法などの解析的な攻撃法が提案されている．これらの攻撃法が成立する原因は，暗号化関数が固定されていることにある．現在開発されている共通鍵暗号方式は，これらの攻撃に耐性を持つように設計されているが，新しい攻撃法の危険性が常に存在している．そこで，既存の暗号方式を複数の要素に分割し，アルゴリズム生成鍵によって再構成を行うアルゴリズム生成型共通鍵暗号方式が提案されている．この方式では，エンドユーザはアルゴリズム生成鍵を変化させることで，異なった暗号アルゴリズムを生成することができる．

安全なアルゴリズム生成型共通鍵暗号方式を設計するためには，一定の暗号強度を持った要素を複数蓄積しておく必要がある．本研究では，FEAL にアルゴリズム生成型共通鍵暗号方式を適用した暗号方式について，差分特性の観点から評価を行った．その結果から，段数の要素は差分攻撃に弱くなる可能性があることを示す．

キーワード　共通鍵暗号，ブロック暗号，差分解読，差分特性確率，FEAL

Abstract

Evaluation of Algorithm-generated FEAL

FUKUTOMI Eiji

To analysis common key cryptosystem, there are some attack such as differential cryptanalysis and linear cryptanalysis is represented. The cause of witch these attack were success is cipher function does not change. The latest common key cryptosystem have high tolerance against any attacks, but new attack method keeps being developed and using, so common key cryptosystem is not safety. To decrease these dangerous, the algorithm-generated common key cryptosystem is represented. In this system, different algorithm cipherment was generated by changing algorithm selection key data.

To design more safe algorithm-generated common key cryptosystem, it is necessary to stock many elements which has some cipher itensity. In this paper, I evaluate a FEAL using algorithm-generated common key cryptosystem based on differential characteristic.

key words common key cryptosystem, block ciphers, differential cryptanalysis, differential characteristic probability, FEAL