# 要 旨

## アルゴリズム可変な暗号方式の安全性評価

福冨　英次

共通鍵暗号は鍵の全数探索によって解読が可能であるが，十分な長さの鍵を用いれば解読は困難になる．全数探索より少い計算量で真の鍵を算出するための方法として，差分解読法や線形解読法などが提案されている．一般に $N$ ビットの鍵を持つ共通鍵暗号方式に対して，$2^{-N}$ より高い確率で解読が成功すると，その暗号方式は脆弱性を持つとされる．解読法の多くは入出力の偏りなどを基に鍵の候補を絞り込むことで，計算量を削減している．多くの暗号方式は解読の危険性を評価するために，事前に解読の成功確率を求めている．これに対し，鍵の情報によって暗号アルゴリズム自体を変化させる方式が提案されている．暗号アルゴリズムを変化させることによって，攻撃者は使用しているアルゴリズムを特定することが困難になる．しかし，アルゴリズムの変化が暗号方式の安全性にどのように影響するか明らかにされていない．本論文では，FEAL と AES にアルゴリズム生成型共通鍵暗号方式を適用させ，アバランシュ性という観点から強度評価を行っている．その結果から，アルゴリズム生成鍵は暗号化鍵と同様のデータ撹拌作用があることが確認している．また，差分解読法に対してアルゴリズム生成型共通鍵暗号方式が脆弱性を持つ確率を示しており，安全に運用するためには確率の逆数倍程度の使用毎に鍵の更新が必要であることを述べている．

キーワード　情報セキュリティ，共通鍵暗号，差分解読法，アバランシュ性

# Abstract

## Security of cryptosystem using variable cipher function

FUKUTOMI Eiji

Common key cryptosystems can be analyze by brute-force attack, but analysis becomes difficult when enough length key is used. To calcurate true key in smaller calculation amount than brute-force attack, the differential cryptanalysis and the linear cryptanalysis are proposed. In generally, a cryptosystem which has $N$-bit length key has vulnerability when analysis is successful more than $2^{-N}$. Most cryptanalysis is reduced calculation amount by narrowing key candidates based on input and output biases. To evaluate vulnerability, existing cryptosystems' successful rates of analyses are calcurated. On the other hand, cyrptosystems which are changing cipher function are proposed. By changing cipher function, an attacker becomes difficult to identify using cipher funtion. However, it is not cleared that how cryptosystems' security is changed by changing cipher function. In this paper, algorithm-generated common key cryptosystems using FEAL and AES have evaluated from the viewpoint of the avalanche criterion. As results, we have showed that algorithm selection key has data randomizer function same as encryption key. Moreover, we have indicated the possibility that algorithm-generated commonkey cyrptosystems can be attack by differential cyrptanalysis. And we have presented number of updating key for solving above problem.

***key words*** Information security, Common key cryptosystem, Differential cryptanalysis, Avalanche criterion