暗号アルゴリズム「RC６」

詳細評価（攻撃評価）レポートサマリー

ＡＥＳ仕様のＲＣ６については、理論的なものを含め、鍵の全数探索よりも高速であるようないかなる解読法も発見されていない。その意味では、現時点ではＲＣ６は十分安全な暗号アルゴリズムといってよい。しかしながら、暗号理論的な観点からは以下の点に注意すべきである。

（１） ＲＣ６の安全性評価のいくつかは、これに先立つＲＣ５の安全性評価結果をもとにしており、ＲＣ５の安全性を根拠にＲＣ６の安全性を帰結している。しかしながら、ＲＣ５は鍵によって暗号の強度がばらつくことがしられている。そのひとつの例はχ^2攻撃であり、またＲＣ６に対する現在しられている最も強力な攻撃法はχ^2攻撃である。したがってこの種の統計解析による強度評価結果には今後も注目していく必要がある。

（２） ＲＣ６を特徴づけるコンポーネントである、乗算とデータ依存回転シフト演算が、タイミング攻撃や差分電流解析に対してどのように作用するか、すなわちこれらの解読法に対する防御実装にどの程度のコストがかかるかは、いまだ研究途上であるが、その情報はＲＣ６を特定の環境で利用する上で重要になる可能性がある。