SC2000 の安全性に関する詳細評価の要約

次の 3 種類の解析を行なったが、明確な弱点は発見できなかった。

(a) **データ攪拌部の従来型攻撃に対する安全性**　差分解読法・線形解読法・高階差分解読法について提案者達による解析結果を確認した。さらに、truncated 差分解読法、χ^2 解読法・分割解読法、不能差分解読法、ブーメラン解読法、法 n 解読法、非全射解読法の各解読法に対する安全性に考察した。

(b) **鍵スケジュール部の従来型攻撃に対する安全性**　全数探索、弱鍵、拡大鍵数、統計的性質を調べたが、脅威となる欠点は見つからなかった。

(c) **実装に関する攻撃に対する安全性**　構成要素ごとに検討を行ない、小さなコストで対処可能であることを確認した。

このように、現在のところ SC2000 の安全性上の欠陥は見つかっていないが、2 段 Feistel 型と SPN 型を交互に重ねた構造に対する解析はほとんど行なわれていない。今後、さらなる解析を重ねていくことが必要である。