ＭＩＳＴＹ１の安全性に関する詳細評価の要約

MISTY1 は設計者によって、3 段での最大平均差分・線形確率が 2^{-56} 以下になることが理論的に証明されている。この証明可能安全性があるので、他の攻撃法が有効性である可能性は低いと考えられる。

実際、次の 3 種類の解析を行なったが、(a) と (b) に関しては明確な弱点は発見できなかった。しかし、(c) に関しては IC カード上での実装で電力解析が有効であり、ハードウェア等による対策が必要である。

(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・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・非全射解読法について解析した。

(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。

(c) **実装に関する攻撃に対する安全性**　個々の設計要素に対し、タイミング攻撃と電力解析に対する安全性を検討した。