理想的乱数の代わりに擬似乱数を用いた暗号システム実装の安全性評価*

縫田　光司（物理解析研究チーム）**

問題

情報理論的安全性 ＋ **擬似乱数生成器** ＝ **？**

- **計算量的仮定を除去**
- 乱数を大量に使う傾向

- 必要な真正乱数の削減
- **計算量的仮定が必要**

主結果

擬似乱数適用前の系が情報理論的安全性を持ち、

- 擬似乱数生成器（PRG)が暗号学的識別不可能性を持つ
- 攻撃者に渡る情報の多様性が充分小さい

ならば、擬似乱数適用後の系の安全性は以下のような特徴を持つ：

- **攻撃者の攻撃アルゴリズムの計算量、計算環境（CPU速度など）と無関係**
- **素因数分解/離散対数ベースのPRGを用いても量子計算機での攻撃に安全**

つまり、情報理論的安全性をほぼ達成できる

定量的評価

擬似乱数適用後の定量的な安全性評価を、攻撃者に渡る情報の多様性及びある方法で定まるアルゴリズムたちの計算量の上界から導出する手法を考案

数値例：「離散Tardos型電子指紋符号」＋「DDH　generator」の場合
あるパラメータ設定の下、**素の状態の75% ～ 0．0002%の真正乱数**を
PRGの乱数種に用いると、素の状態と同等に低い攻撃成功確率を保証可

＊本研究の一部は、財団法人国際科学技術財団平成19年度研究助成の援助を受けました
＊＊産総研RCIS 花岡悟一郎研究員（セキュリティ基盤技術研究チーム）との共同研究