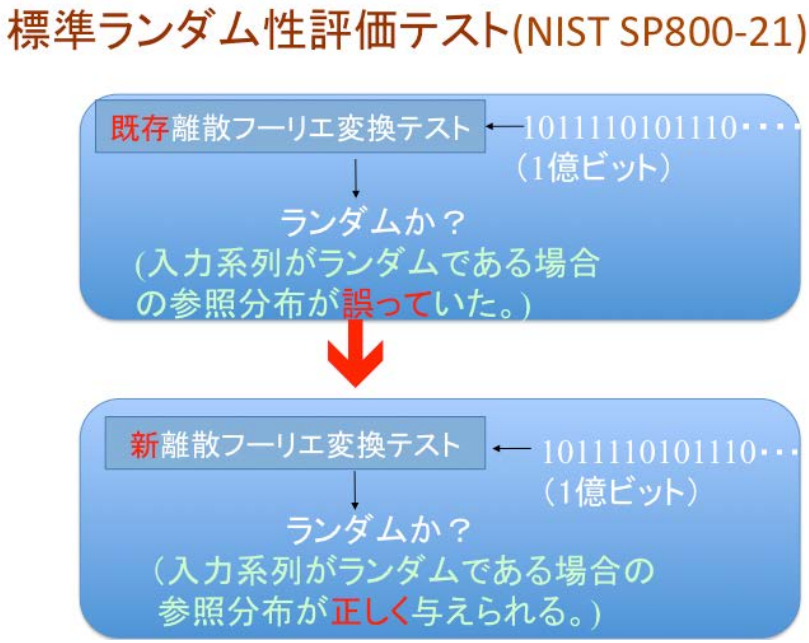
暗号安全性評価テストの欠陥を克服し、
証明可能な安全性を持つカオス暗号を提案
―今後の暗号安全性や乱数性評価に貢献―

概要

梅野健　情報学研究科教授、岡田大樹　元同博士前期課程学生(現 KDDI 社員)及び岩﨑淳　元同博士後期課程学生(現 福岡工業大学助教)らの研究グループは、一般の乱数の乱数性評価や世界標準暗号 AES の選定にも用いられてきた標準ランダム性評価テスト NIST SP800-22 の離散フーリエ変換検定において、2003 年から指摘されていた「参照分布が理論的に求まらない」という課題に対して、新たに改良した離散フーリエ変検定テストを提案し、厳密な参照分布が求められることを示しました。平文が本当にランダムに暗号化されたかどうかは暗号の安全性を左右する重要な要素です。今回の研究によりランダム性評価が正しく行われ、暗号安全性評価に寄与できることが期待されます。

本研究の暗号安全性評価テストに関わる成果は、米国電気電子学会(IEEE)の学術誌 *IEEE Transactions on Information Forensics and Security* に発表されています。また、安全性証明可能なカオス暗号に関わる成果は 7 月 1 日、電子情報通信学会(IEICE)の学術誌 *IEICE Nonlinear Theory and Its Applications* に掲載されました。



１．背景

暗号には、公開鍵暗号と共通鍵暗号の２種類があり、主に前者は認証用、後者は主にデータの暗号化に用いられており、インターネットサービスの基盤として、両者が併用して使われております。これらの暗号は、データのランダム化という操作が必ず入りますが、暗号を設計する際に、平文を暗号化したデータが本当にランダムかどうかのランダム性評価は、情報通信社会の基盤となる暗号の安全性評価の重要な評価項目です。また、LSI 等の様々なデバイスで構成され、コンピュータ等の CPU 等の様々な用途に用いられている物理乱数や擬似乱数のランダム性評価も、それらの乱数の品質管理の基礎となります。現在、ランダム性評価として世界中で使われている米国国立標準技術研究所の「NIST SP800-22」ランダム性評価テストは、第３世代移動体通信システム(3G)でも使われている標準暗号の AES(Advanced Encryption Standard)の選定の際にも用いられました。しかし、2003 年に独立行政法人通信総合研究所(現 国立研究開発法人情報通信研究機構)と防衛省技術研究本部(現 防衛装備庁)の２つのグループが、「NIST SP800-22」の中の離散フーリエ変換テスト(DFT テスト)の系列がランダムであった時に持つべき参照分布に理論的な誤りがあるとの致命的なエラーを指摘しました。この指摘以降、世界各国で正しい参照分布を求めて様々な研究が行われてきましたが、ランダム性評価基準の評価方法自身が誤っていることに対して、正しい参照分布を導くような抜本的な解決手法は提案されていませんでした。

また暗号安全性には、ランダム性評価だけでなく、暗号文を解読しようとする様々な暗号攻撃に対する耐性が必要となりますが、この暗号攻撃に関する耐性を証明するのは困難であり、その様な証明可能な暗号安全性を有する暗号は少なく、実用性を有する 128bit 鍵長のカオス暗号では、今まで証明可能な暗号安全性を有するカオス暗号はありませんでした。

２．研究手法・成果

今回の研究では、まず「NIST SP 800-22」の既存の離散フーリエ変換検定(DFT)テストの各パワースペクトルの分布を評価しました。その結果、入力系列がランダムであるならばパワースペクトル分布が特定の分布（独立なカイ二乗分布）に従うことを厳密に証明しました。更に DFT テストのビット列の評価手法をそのまま使うのではなく、評価対象のビット列(1 億ビット)を充分多数の独立なパワースペクトルが得られる様に、標準的な DFT テストと比較してより多くの系列に分割し(独立な系列を多数用意し)、得られたパワースペクトルがカイ二乗分布に従うかどうかの統計的仮説検定(KS 検定)を行うという新しい離散フーリエ変換検定(新 DFT テスト)を提案しました(論文 1)。その結果、従来手法と比較して、高い信頼性(ランダムである時に、誤って非ランダムだと判定される Type I エラーが低い)と、高い検出力(非ランダムである時に、誤ってランダムだと判定される Type II エラーが低い)を持つことが解りました。

また、ある一般的な暗号攻撃(線形攻撃)に対する耐性が証明される初めての 128bit カオス暗号 VSC2.1 を、２冪剰余環上の置換多項式の理論を用いて構成しました(論文 2)。

この提案方式含めいくつかの暗号方式のランダム性を評価したところ、今まで安全だとされた AES や通信総合研究所が 2004 年に提案した VSC128、安全性が証明されたカオス暗号アルゴリズムである VSC 2.0 や VSC2.1(論文 2)、擬似乱数発生アルゴリズムのメルセンヌツイスター等が高いランダム性を持つグループに入ることが分かりました。一方、これまでの評価手法ではランダムだと考えられていた QCG-1 や LCG1 といった既存の擬似乱数アルゴリズムや他の多くは、上記の高いランダム性を持つグループとは異なるグループ(厳密な参照分布により明確にランダム性が否定できるグループ)に分類されることも確認できました。

３．波及効果、今後の予定

今後は更に様々な場面で用いられている暗号アルゴリズムや擬似乱数アルゴリズム、物理乱数のランダム性評価を行っていきその評価結果を公表する予定です。また、今回の手法を標準的なランダム性評価方法とするべく改良する研究を進め、暗号評価に関わる機関とも連携しサイバー･セキュリティの基盤を支える評価技術を確立していきます。

4. 発表関連論文

(1) 著者：岡田　大樹(Hiroki Okada)、 梅野　健(Ken Umeno)

タイトル：Randomness Evaluation With the Discrete Fourier Transform Test Based on Exact Analysis of the Reference Distribution

掲載誌：IEEE Transactions on Information Forensics and Security、 Vol. 12、 No.5、 May 2017

DOI: 10.1109/TIFES.2017.2656473

(2)著者:岩﨑 淳(Atsushi Iwasaki)、 梅野 健(Ken Umeno)

タイトル:Further improving security of Vector Stream Cipher

掲載誌: IEICE Nonlinear Theory and Its Applications、 Vol. E8-N、 No. 3、 July 2017

(2017年7月1日出版)