標準暗号（AES）選定に用いられた離散フーリエ検定テストを完全修正

―15 年間乱数検定の最大の懸案であった参照分布の問題を完全解決―

概要

現在、携帯電話など世界中で標準暗号（AES）が用いられています。この AES が 2001 年に選定された際、評価ツールとして乱数性評価テスト NIST SP 800-22 が使われました。ところが、その一つである離散フーリエ検定テストにおいて、系列が乱数であると仮定した時、参照分布が厳密に求まらないと言う致命的な課題がありました。

京都大学大学院情報学研究科 岩崎淳 博士課程学生（研究当時、現：福岡工業大学助教）、梅野健 同教授らの研究グループは、この課題を完全に解決する離散フーリエ検定テストの完全な修正版を提案しました。今回の研究成果は、情報セキュリティの基盤や暗号通貨の流通で重要となる、全ての暗号自身の安全性や暗号文のランダム性、あるいはモンテカルロ計算や AI 機械学習で用いられる擬似乱数のランダム性の評価等、幅広い分野に用いることができます。さらに、AES の後継となる次世代標準暗号選定では、より正確なランダム性が要求されるため、その際の重要な標準乱数評価ツールとしても活用が期待されます。今後は、本研究成果を活用した評価結果等を積極的に発信して行きたいと考えています。

本成果は、2018 年 8 月 1 日に日本の電子情報通信学会の国際学術誌「IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences」にオンライン掲載されました。

イメージ図：数値は本研究で算出したパワースペクトル。中央のグラフはそれを図示したもの。

１．背景

2001 年に、主に金融機関で長年使われていた標準暗号 DES（Data Encryption Standard）に代わる標準暗号 AES（Advanced Encryption Standard）が選定されました。その際、数々の暗号アルゴリズムが提案されましたが、その評価の役割を担ったのが AES 選定機関であるアメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）でした。その NIST が暗号アルゴリズムの出力文の乱数性を評価するために用いたのが、NIST SP 800-22 と言う乱数性評価テストです。NIST SP 800-22 には、当時 16 のテストがあり、その中の一つが「離散フーリエ変換テスト」（略して DFT テストと言う）です。

DFT テストは当初、誤りが無いと考えられていました。しかし、CRL（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（NICT））のカオス暗号チッププロジェクト（当時、梅野教授が同プロジェクトリーダー）が、カオス暗号の安全性を評価するのに用いた NIST SP800-22 の DFT テストが理論的に誤っていることを発見し、2003 年世界に先駆けて公表しました。

DFT テストとは、乱数系列の周期性を離散フーリエ変換によって検出するテストです。離散フーリエ変換した後のパワースペクトルの大きさが、ある一定の閾値 T を何回超えるか超えないかを検出するものです。先述の 2003 年に公表した成果では、閾値 T を超えない数を N_1 とした時、正規化した N_1 の参照分布と閾値 T が理論的に誤っていたことを示しました。それ以降、世界中の多くの機関、研究者が、正しい DFT 検定の理論分布とは何かを追求し、数々の修正提案を出していました。しかし、それらの修正案は、ある”擬似乱数が良い乱数である”と言う仮定を基準として成立するものであり、評価対象である乱数の乱数性を仮定する評価に依らずに参照分布の正確性を数学的に独立に証明できる完全な修正提案はありませんでした。

今回の研究成果に関わる乱数生成評価プロジェクトは、2012 年に梅野教授が NICT から京都大学大学院情報学研究科に移籍し、岩崎博士課程学生が 2014 年に同研究科数理工学専攻の梅野教授の研究室（物理統計学分野）に入学することを契機に生まれました。

２．研究手法・成果

今までの研究は、単純にパワースペクトルがある設定閾値 T を超えない数 N_1 を評価する参照分布を求めることに主眼を置いてました。しかし、我々は全く異なる発想―パワースペクトル s_j の分散に関する参照分布を求める―に基づく新しいアプローチによる修正を試みました。すると、数学的に、与えられた系列が真に乱数であったと仮定する時、DFT 検定の s_j の正規化したパワースペクトルの分散 z が、標準ガウス分布（標準偏差 1、平均 0）に収束することを証明しました。つまり、今までの研究の手法で取られていた”〇〇乱数が完全な乱数である”という仮定の下に近似的に参照分布を求めていたアプローチと異なり、何の仮定も必要とせずに数学的かつ独立に、正しい参照分布を持つ正確な DFT テストを提案したことになります。

表 1 に、今までの修正提案と今回の提案（完全に修正）との関係を示します。また、現在用いられている DFT テストと今回提案した修正 DFT テストによって各種暗号、乱数を検定した時の結果が表 2、表 3 となります。

表 2、表 3 を見ると、LCG（Linear Congruential Generator：線形合同法）などは、修正前の現行 DFT テストでも修正後の DFT テストでも非ランダム性が検出できています。しかし、QCG-I（Quadratic Congruential Generator）や XORG（XOR-SHIFT Generator）については、現行の DFT テストでは非ランダム性が僅かに検出されるだけなのに対し、修正後の DFT テストでは、明確に非ランダム性を検出できるという結果が得られています。

すなわち、本修正後の DFT テストは、こういった僅かな非ランダム性に関して、従来の DFT テストと比較

してより鋭敏（センシティブ）であると言えます。
現在、Google Chrome の Java Script の標準的な乱数生成 API において、XOR-SHIFT32 ビット版が使われていますが、こうした標準的に使われている乱数のランダム性の判定にも、本修正 DFT テストで非ランダム性について厳密に検証を進めることが可能となります。

３．波及効果、今後の予定

今回の研究成果は、全ての暗号評価・乱数の乱数性の評価に直接応用することができます。今後は、学会（日本応用数理学会 応用カオス研究部会 乱数生成評価分科会）等で、他の乱数検定テスト結果との依存関係を調べ、議論し、有効な乱数性評価システムの構築および乱数性標準化を目指すとともに、AES に代わる次世代標準暗号選定にツールとして寄与する予定です。

＜用語解説＞

離散フーリエ変換：離散時間の信号系列に対するフーリエ変換手法。高速フーリエ変換が提案され，現在の圧縮アルゴリズム、4G、無線 LAN 等の無線通信方式等、数多くの分野で使われる。

パワースペクトル：信号系列を離散フーリエ変換した後の信号のエネルギー成分。もし系列がランダムではなく特定の周期を持つ信号成分がある場合、当該周期の逆数で与えらえる周波数成分に対応するエネルギー成分に特徴的なピークを有する。系列がランダムな場合、パワースペクトルに、この様な特徴的なピークを持たない。

＜参考リンク＞

「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―」（平成２９年７月４日京都大学発表）
http://www.kyoto-u.ac.jp/ja/research/research_results/2017/170701_1.html

＜論文タイトルと著者＞

タイトル：Randomness Test to Solve Discrete Fourier Transform Test Problems
著者：Atsushi Iwasaki and Ken Umeno
掲載誌：IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences
DOI：10.1587/transfun.E101.A.1204

<参考図表>

年		参照分布
2001年	$z = \frac{N_1 - \frac{n}{2}(0.95)}{\sqrt{\frac{n}{2}(0.95)(0.05)}}$ NIST(米国),-オリジナル-	不正確
2001年	NIST(米国) AES暗号(標準暗号)を選定 -標準暗号の評価手法にNIST SP 800-22を利用-	
2003年	$z = \frac{N_1 - \frac{n}{2}(0.95)}{\sqrt{\frac{n}{4}(0.95)(0.05)}}$ CRL(現NICT,日本),-修正案-	数値計算近似 (SHA-1乱数ベース)
2007年	$z = \frac{N_1 - \frac{n}{2}(0.95)}{\sqrt{\frac{n}{3.8}(0.95)(0.05)}}$ Ferrara大（伊）,- 修正案-	数値計算近似 (BBS乱数ベース)
2010年	$z = \frac{N_1 - \frac{n}{2}(0.95)}{\sqrt{\frac{n}{4}(0.95)(0.05)}}$ NIST SP 800-22修正 1.a にCRL案(2003年)が採用	数値計算近似 (SHA-1乱数ベース)
2017年	検定方法を抜本変更 (直列→並列に読む)　京大(日本) -修正案-	系列数無限の極限で正確
2018年	$z = \frac{1}{\sqrt{2n^5}} \sum_{j=0}^{\frac{n}{2}-1} \lvert s_j \rvert^4 - \sqrt{\frac{n}{2}}$ 京大(日本), -完全修正案(今回)-	厳密

表１ DFT 検定（NIST SP800-22）の 17 年間の修正履歴（2001 年-2018 年）

	サクセス率	一様性	総合
VSC128	5	0	5
VSC 2.0	1	0	1
VSC 2.1	3	0	3
MT	2	0	2
AES-128 CTR	3	0	3
LCG	82	82	82
QCG-I	2	0	2
QCG-II	100	100	100
CCG	100	100	100
XORG	8	0	8

表２　　現行 DFT テストによる各種暗号、乱数の評価結果

	サクセス率	一様性	総合
VSC128	0	0	0
VSC 2.0	0	0	0
VSC 2.1	0	0	0
MT	0	0	0
AES-128 CTR	0	0	0
LCG	82	82	82
QCG-I	95	98	99
QCG-II	100	100	100
CCG	100	100	100
XORG	21	1	21

表 3　修正 DFT テストによる各種暗号、乱数の評価結果

二段階検定による評価結果。 n ビットの乱数列×M 本の検定を考えると, M 個の p 値が得られる。それら M 個の p 値に対して, さらに以下の 2 種類の方法で検定を行う。「サクセス率」による検定(その 1): 得られた M 個の p 値のうち, 0.01 を下回る個数を r とする. 検定仮説「与えられた乱数列は, 独立な理想的な乱数列」の下では、M 個の p 値は独立に区間[0,1]上に一様分布するので, r は二項分布に従う。r が $0.01M \pm 3\sigma$ の中に入っていたら合格, そうでなければ帰無仮説を棄却する。表中の各乱数の「サクセス率」の数は, 100 回中何個、帰無仮説が棄却されたかの「不合格数」をあわわす。「一様性」による検定(その 2):検定仮説の下では, M 個の p 値は独立に区間[0,1]上に一様分布する。その仮定の下で χ^2 検定をかけて新たに p 値 p'を一つ得る。p'>0.0001 なら合格. そうでなければ棄却する. 表中の各乱数の「一様性」の数は, 100 回中何個、棄却されたかの「不合格数」をあらわす。表中の各乱数の「総合」の数は、100 回中、何個「サクセス率」または「一様性」で棄却されたかを示す。M=100 は検定数としては決して十分な数ではないが, 比較的少量の検定数で乱数の種類によって、検定の微妙な修正が検定結果にどう反映するかを示す。それぞれの各乱数は, VSC128(Vector Stream Cipher 128bit), VSC 2.0 (Vector Stream Cipher version 2.0), VSC(Vector Stream Cipher 2.1), MT(Mersenne twister), AES-128 CTR(AES 128 bit Counter Mode), LCG(Linear Congruential Generator), QCG-I(Quadratic Congruential Generator-I), QCG-II(Quadratic Congruential Generator-II), CCG(Cubic Congruential Generator), XORG(Xorshift Generator)を用いた。表 2 と表 3 の評価結果は, 「SICS2017」にて発表。