Vol.2013-CSEC-62 No.46
Vol.2013-SPT-6 No.46
2013/7/19

音声入力を利用した乱数生成器の開発

川村大河† 中林赳明† 長瀬智行†

今日の暗号技術において，乱数生成技術は様々な局面で必要不可欠な技術であり，性能の良い暗号論的乱数生成器は現在でも広く求められている．特に，限りなく真の乱数に近い乱数系列を発生させることのできる物理乱数生成器は，比較的高価である，系列生成に時間がかかる，など様々な制限が存在している．そのため安価に実現できる優れた物理乱数生成器の開発は，セキュリティの向上という面において急務であるといえるだろう．そこで，ほぼ全てのデバイスに標準的に付加されているマイク入力から得られる雑音を利用して乱数生成器を開発することはできないかと考えた．本研究では，マイク入力から得られた雑音データの最下位ビットをとり，Barak, Impagliazzo & Wigderson 抽出器を利用することによって，乱数生成器を設計した．

Evaluation of Random Number Sequences Generated from Microphone Input

TAIGA KAWAMURA† TAKEAKI NAKABAYASHI†
TOMOYUKI NAGASE†

Designing a considerable random number generator plays a crucial role in computer security especially in cryptography. Recently, generating an unpredictable random number with high performance is a great challenge and widely sought. In particular, physical sources are capable to produce a random sequence that is very close to true random numbers. In this paper, we generate a random sequence using a physical resource such noise that is produced from a microphone input.
In this study, a least significant bit of noise's data which is obtained from the microphone input is considered to be resources whose entropy rate is unknown, and then we use a randomness extractor which is developed by [1].

1. はじめに

昨今の暗号技術において，乱数生成技術はさまざまな局面にて必要とされている.そのとき使われる乱数生成器は，暗号論的乱数生成器と呼ばれ，線形合同法や，M 系列，メルセンヌツイスタ法[2]などに代表される，漸化式を用いて乱数系列を発生させるような，暗号論的ではない擬似乱数生成器はそのままでは扱うことができない．それゆえ良質な暗号論的乱数生成器は現在なお必要とされており，真の乱数，及びそれに近い性質を持つ乱数生成器は絶えず研究されている．中でも周期性を持たず，高い乱数性を持つ系列を生成する物理乱数生成器は，比較的高価なハードウェアを必要とするものが多く，安価で容易に物理乱数を生成する乱数生成器は広く求められている．

上述の背景により，本研究では身近な自然現象である「音」を利用して，良質な乱数を生成する乱数生成器の実現を最終目標に据える．具体的には，音声入力から得た雑音を情報源とし，決定性乱数抽出器を用いることで，乱数生成器を構成，実験的に乱数を生成し，それを評価した．ただし，乱数はその性質上，絶対の評価を下すことはできず，評価基準も多々存在し，曖昧である．そのため本研究では，その乱数性評価に NIST(米国標準技術研究所)により発表された Special Publication 800-22(以下 NIST 乱数検定)[3]を使用して統計的評価を行った．

† 弘前大学
Hirosaki University

2. 本研究で扱う音声ファイルの形式及び性質

2.1 ファイル形式

標準的なコンピュータにおいて，音声は一般的に「WAVE」という形式で表現されることが多く，その実態は Pulse Code Modulation (PCM：パルス符号変調)によって標本化されたものである．この WAVE というフォーマットを論ずるときに必要となるものが，サンプリング周波数とビット数である．サンプリング周波数は，音声の波形を一秒間に何回標本化するかを示した数字である．例えば市販されている一般的な音楽 CD は, サンプリング周波数が 44.1kHz に設定されており, 一秒間に 44100 回標本化を行っているということである. ビット数は, サンプリングの際に，ひとつのデータを何ビットで量子化するかを示した数値であり，一般的な音楽 CD は 16 ビットである．これは波形の振幅を 65536 段階で表現するということである．その性質を考えればわかるように，サンプリング周波数を高くすれば高くするほどその音声ファイルは，高周波の音まで表現することができるようになり，ビット数を多くすれば多くするほど，より細かい音量の違いを表現することができるようになる．

前述したように，サンプリング周波数を高くすると，それだけ高周波の音を表現することができるが，サンプリング周波数によって表現できる周波数は制限されている．サンプリング周波数で表現することができる最高の周波数をナイキスト周波数と呼び，サンプリング周波数を f，ナイ

表 1　データ部の構造
Table 1. The Construction of data parts

Format	1st byte	2nd byte	3rd byte	4th byte
8bit mono	右 ch			
16bit mono	右 ch			
8bit streo	右 ch	左 ch		
16bit streo	右 ch		左 ch	

キスト周波数を f_n とすると $f_n=f/2$ によって表される．例えば一般的な音楽 CD であれば，サンプリング周波数が 44.1kHz なので，ナイキスト周波数は 22.05kHz である．これは人間の可聴域よりも高い周波数であり，音楽 CD のサンプリング周波数はそれを考慮した値である．

2.2 WAVE ファイルの構造

WAVE ファイルは一般的に 44 バイトのヘッダを持ち,それぞれ，サンプリング周波数や，ビット数等，基本的な情報が記述されている．これらはもちろん，実際の音声データでは無いので，本研究ではこの部分をカットし，データ部だけを評価するものとする．

データ部の構造は，チャンネル数，ビット数によって異なり，例えば 16 ビットのステレオ(2ch) 信号ではデータは 1 ブロック 4 バイトで表現される．1・2 バイト目，つまり最初の 16 ビットが右チャンネルのデータであり，次の 16 ビットが左チャンネルのデータとなる．

表 1 は WAVE ファイルのデータ部の構造を表にしたものである．今回は，マイク入力から得られる雑音がモノラルのものであるため,モノラル 16 ビットの信号を対象とする.

3. 音声入力を利用した情報源

本研究では，音声入力から得た雑音を情報源として利用している．しかし，音声の実体は連続的な波形を量子化及び標本化したものであるため，そのまま利用したとしても豊富なエントロピーを得ることはできない．さらに，音声入力から得た雑音は，入力電圧の低さから，とりうる値の種類が少なく，その点でも豊富なエントロピーを得ることはできなかった．本研究では，音声をより優れた情報源として利用するための方法を提案する．

3.1 ダウンサンプリングによる波形の複雑化

前述したように，音声入力から得た雑音は，その入力電圧の低さから，とりうる値の種類が少なく情報源として利用するには聊か力不足であると言える．そのため，その波形をより高い音量の雑音として扱うために，ダウンサンプリングを利用し，波形を複雑化する．その手順を以下に示す.

i)　**オーディオインターフェースのマイクインプットに何も挿入せずに，96000Hz にて雑音を録音する**
ii)　**雑音の音量を正規化(ノーマライズ)する**
iii)　**サンンプリング周波数を 44100Hz にダウンサンプリングする**

この手順を実行することにより，より大きなレベルの雑音を取得することができる．

3.2 最下位ビットの有するエントロピー

本研究では，前述した方法で得た雑音としての音声ファイルのデータそれぞれの最下位ビットを取得することによって，情報源としての利用を可能にしている．最下位ビットの平均エントロピーは 6.999999 bit/byte であり，最小エントロピーは 6.99400 bit/byte となっており，高いエントロピーを有していることがわかる．

4. 乱数抽出

4.1 乱数抽出器

一般的に物理乱数生成器を構成する際には，アナログ情報から適当にサンプリングし AD 変換を施し，変換されたデジタル情報から乱数性の高い状態へ変換する，といったような処理を行う．この最後の変換が乱数抽出器であり，古典的な例としては，情報源が 0 から 1 へ変化した時に 0 を出力，情報源が 1 から 0 へ変化した時に 0 を出力，情報源が 0 のまま，あるいは，1 のままの場合は入力情報を捨てる，という von Neumann の方法[4]によって，一様乱数が得られるということが知られている．乱数抽出器の言葉で言うと，von Neumann の方法は(0 と 1 の頻度の偏りはあるものの独立であるという)特定情報源の場合の乱数抽出器と見ることができる[5].

本研究では，乱数抽出器として Barak, Impagliazzo & Wigderson による決定性抽出器[1]を利用している．この節では Barak, Impagliazzo & Wigderson 抽出器について簡単に説明を行う.

4.2 抽出器の構成

Barak, Impagliazzo & Wigderson 抽出器は Barak, Impagliazzo & Wigderson によって提案された決定性乱数抽出器である. ある体 F 上の関数 ε^{i} を以下のように帰納的に定義する.

i) ε^0:F → F を $\varepsilon^0(x) \stackrel{def}{=} x$ とする.

ii) ε^i: F^{3i+1} → F を任意の $x_1, x_2, x_3 \in F^{3i}$ に対して,

$$\varepsilon^{i+1}(x_1, x_2, x_3) \stackrel{def}{=} \varepsilon^i(x_1) \times \varepsilon^i(x_2) + \varepsilon^i(x_3)$$

i の値は 3^i が $1/\tau$ の多項式程度の値でよいので，明示的かつ非常に単純な構成の決定性乱数抽出器となっている[5].

本研究では，情報源から乱数を抽出する機構として以上の乱数抽出器を利用している

5. 評価方法

本研究にて使用する NIST 乱数検定について説明する．NIST 乱数検定では，表 2 に示す 15 種類の検定法が示されており，それら全ては，0 と 1 からなる乱数列を対象としている．

各検定は標準正規分布またはカイ 2 乗分布に基づいて行われ，それにより p-value と呼ばれる値が算出される．p-value とは，真の乱数生成器が検定を行っている系列よりもランダムでない系列を生成する確率と解釈でき，個々の検定に対して，p-value<0．01 の時に良い乱数列ではないと判断される．

標準正規分布に基づいて検定が行われる場合，p-value は以下の関数 erfc (complementary error function)を用いて計算される．

$$\mathbf{erfc}(z) = \int_z^\infty \frac{2}{\sqrt{\pi}} e^{-x^2} dx \qquad (1)$$

カイ 2 乗分布に基づいて検定が行われる場合，以下の関数 igamc(incomplete gamma function)を用いて p-value が計算される．

$$\mathbf{igamc}(a, z) = \frac{1}{\Gamma(a)} \int_z^\infty e^{-t} t^{a-1} dt \quad (2)$$

$$\Gamma(a) = \int_0^\infty e^{-t} t^{a-1} dt \qquad (3)$$

各検定では，複数の標本系列(NIST では 1000 程度を推奨)に対し検定を行い，(1)p-value が 0．01 以上になる比率(Proportion)，(2)p-value の一様性 (Uniformity)，によって乱数列の評価を行う．

(1)については，p-value が 0．01 以上になる系列数は正規分布 $N(\mu, \sigma^2)$に従うと考え，$\mu \pm 3\sigma$ 以内に収まれば良いとする．

(2)については，区間[0,1)を 10 分割し，各区間に属する p-value の個数が均等であるかどうかをカイ 2 乗分布によって検定する．具体的には，乱数列の個数が m 個の場合，1≦i≦10 について，F_i を区間[(i-1)/10,i/10)に属する p-value の個数とするとき，次式を計算し，

$$\chi^2 = \sum_{i=1}^{10} \frac{(Fi - m/10)^2}{m/10} \qquad (4)$$

igamc(9/2, χ^2/2)を求め，それが 0.0001 以上となった場合，良い乱数生成器であると判定される．

表 2　NIST 乱数検定に含まれる検定法一覧
Table 2. Statistical methods of NIST SP 800-22

	検定名
1	一次元度数検定
2	ブロック単位の頻度検定
3	累積和検定
4	連の検定
5	ブロック単位の最長列検定
6	2 値行列ランク検定
7	離散フーリエ変換検定
8	重なりのないテンプレート検定
9	重なりのあるテンプレート検定
10	Maurer のユニバーサル統計検定
11	近似エントロピー検定
12	ランダム偏差検定
13	種々のランダム偏差検定
14	系列検定
15	線形複雑度検定

6. 計算機実験

本研究で構成した乱数生成器の構成をまとめると以下のようになる．

i) オーディオインターフェースのマイクインプットに何も挿入せずに，96000Hz にて雑音を録音する
ii) 雑音の音量を正規化(ノーマライズ)する
iii) サンプリング周波数を 44100Hz にダウンサンプリングする
iv) 各データの最下位ビットを取得
v) 乱数抽出器によって乱数系列を抽出

以上の工程によって生成された系列を NIST 乱数検定にて，検定した結果が表 3 である．今回の研究では，A: 10 万ビット 1000 本，B:10 万ビット 5000 本，C:100 万ビット

表 3　検定結果

table 3. Evaluation Results

P:合格比率(合格数)　U:一様性
A. 10 万ビット×1000 本　　B. 10 万ビット×5000 本
C. 100 万ビット×1000 本
x:FAILURE　—:未測定

	A		B		C	
	P	U	P	U	P	U
1						
2						
3						
4						
5						
6				X		
7	X			X		
8	—	—	—	—		
9	—	—	—	—		
10	—	—	—	—		
11				X		
12	—	—	—	—		
13	—	—	—	—		
14						
15	—	—	—	—		

1000 本の 3 つの系列について，検定を行った．表の空欄は合格，「X」は不合格，「-」は系列数が推奨値に満たないため，検定を行わなかったことを示している．

結論として，100 万ビット 1000 本の結果において，15 項目の検定項目全てに合格という，乱数として十分に使用することができる一様乱数の生成に成功した．ただし，真のランダム性を持った乱数列を NIST 乱数検定に通した場合でも，全ての検定項目において合格する確率は，二項分布を用いて概算すると約 54%，正規分布を用いて求めた場合の確率は約 78%となる[6]．したがって，全ての検定項目において合格したときに限り，より良い乱数性を持つというようには一概に判断はできない．

7. おわりに

本研究では音声入力を利用した乱数生成器に成功した．しかし，音声を利用しているという点を顧みると，速度という点で大きな制限があることは否めない．今回，最終的に情報源として利用した音声ファイルのサンプリング周波数は 44.1kHz である．つまり，一秒間に 44100 個のデータが記述されている．今回乱数抽出器の i の値として利用したのは 2 であるため，9 個の情報源から，1 つの乱数を生成している．乱数を生成する処理にかかる時間を無視すると，本研究で構成した乱数生成器の考えられる速度は最高でも 4.9Kbps であり，生成速度はお世辞にも速いとは言えないだろう．16 ビットのデータの内，15 ビットを捨てているのであるから，無駄が多く，効率性に欠けるのは明白である．

更に早い速度を出すためには，まず一つ目として情報源として利用する音声ファイルのサンプリング周波数をより高く設定するという方法が考えられる．しかし，高いサンプリング周波数で録音するためには，高価な機材が必要であり，本研究の，「安価で簡易，及び普遍的な物理乱数生成器の開発」，という目標に反する．二つ目としては，最下位ビットを取得する，という方法と同等以上のエントロピーを確保しながら，一秒間にさらに多くのビットを取得することができる方法を考案することである．

さらに，もう一つ検証する必要のある点がある．それは音声の最下位ビットの暗号論的安全性である．これについては実際に様々な観点から攻撃してみる必要があるだろう．

また，今回は音声入力に入力が無い状態で取得することができる雑音を情報源として利用したが，本研究の動機である，「音声を利用した乱数生成器」としてはまだ不十分である．スマートフォンなどでの利用を考えたとき，雑音以外の一般的な音声を利用することができるように拡張することが必要不可欠である．

以上のように，様々な課題が残った本研究ではあるが，安価で簡易に乱数を生成することができる乱数生成器という点においてはひとまずの成功を収めたと言えるのではないだろうか．

参考文献

(1) B. Barak, R. Impagliazzo and A. Wigderson:Extracting randomness using few independentsources. SIAM J. Computing, 36-4, 1095/1118(2006).
(2) M. Matsumoto and T. Nishimura, "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator", ACM Trans. on Modeling and Computer Simulation Vol. 8, No. 1, January pp.3-30,(1998).
(3) Andrew Rukhin, Juan Soto, James Nechvatal, MilesSmid, Elaine Barker, Stefan Leigh, Mark Levenson, MarkVangel, David Banks, Alan Heckert, James Dray,and San Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Special Publication 800-22 Revision 1a, Lawrence E. Bassham III .ed.,(2010).
(4) J. von Neumann: Various techniques used in connectionwith random digits. *Applied Math.*, Series12, National Bureau of Standards, 36/38 (1951).
(5) 小柴健史,埼玉大学, 「乱数抽出の基礎」,(2007).
(6) 廣瀬勝 一,京都大学,擬似乱数生成系の検定方法に関する調査　調査報告書,(2004).