アルゴリズム的情報理論とランダムオラクルモデル

只木孝太郎　　土居範久

中央大学 研究開発機構

Supported by the Ministry of Economy, Trade and Industry of Japan,
and by JSPS KAKENHI Grant Numbers 23340020, 23650001, 24540142

本発表で何をするか

現代の暗号理論において、ランダムオラクルモデルは、暗号方式の安全性を議論する“ 仮想的な枠組み ”として、広く用いられている。

ランダムオラクルモデルでは、暗号方式内で用いられる暗号学的ハッシュ関数を、ランダムオラクルと呼ばれる一様分布に従う確率変数として定式化し、暗号方式の正規利用者ならびに攻撃者は、ハッシュ関数を内部的に計算するのではなく、確率変数であるランダムオラクルにオラクルアクセスすることを通じて、その関数値を得るようにモデル化される。

ランダムオラクルモデルで安全性が証明できたとしても、その方式を現実世界で用いるためには、ランダムオラクルを何らかの具体的なハッシュ関数に置き換える必要がある。しかしその際、どのような要件を満たすハッシュ関数を選ぶべきか、またそもそも、元の安全性証明を維持したまま、ランダムオラクルを具現化できるものなのか、多くの点が不明のまま残されている。

本発表では、この問題についての理解を深めるため、アルゴリズム的情報理論の概念と方法をランダムオラクルモデルに適用する。

暗号理論において“ 乱数 ”とは何か？

暗号理論における“ 乱数 ”

真性乱数

- 真性乱数という概念は、確率分布（ないしは確率変数）に対して定義される概念である。

- 真性乱数とは一様な確率分布のことである。例えば、2048ビットの有限2進列に値を持つ確率変数 X に対して、

$$\forall x \in \{0,1\}^{2048} \quad \mathrm{Prob}\,[X = x] = \frac{1}{2^{2048}}$$

  が成り立つとき、確率変数 X は真性乱数である。

- ランダムオラクルも真性乱数であり、あるクラスの関数に実現値を持ち、一様分布に従う確率変数である。

- 確率変数の個々の実現値（上の例では、個々の2048ビット列）に対しては、“ 真性乱数 ”という概念は定義されない。

暗号理論における“ 乱数 ”

疑似乱数

- 疑似乱数という概念は、確率分布の列（ないしは確率変数の列）に対して定義される概念である。
- 確率変数の列$\{X_n\}_{n\in\mathbb{N}}$が疑似乱数であるとは、次が成り立つこととして定義される:

> 任意の確率的多項式時間アルゴリズム$\mathcal{A}$と任意の$d \in \mathbb{N}$に対し、十分大きい全てのnについて、
>
> $$|\mathsf{Prob}\left[\mathcal{A}(X_n) = 1\right] - \mathsf{Prob}\left[\mathcal{A}(U_n) = 1\right]| \leq \frac{1}{n^d}$$
>
> が成り立つ。ここで、$\{U_n\}_{n\in\mathbb{N}}$は真性乱数の列である。

- 疑似乱数というのは、確率変数の列に対して定義される、$n \to \infty$とする場合の漸近挙動に関する概念である。従って、列を構成する個々の確率変数や、その実現値に対しては、“ 疑似乱数 ”という概念は定義されない。

このように、暗号理論において、“ 乱数 ”とは、確率分布ないしは確率分布の列のことであり、暗号理論は、個別の具体的な有限２進列や無限２進列について、乱数か否かを定義しようとはしていない。

個別の有限２進列や無限２進列について乱数か否かを定義することは可能であろうか？

アルゴリズム的情報理論

無限２進列の分類

アルゴリズム的情報理論は、各々の無限２進列に対し、**ランダムなもの**と**ランダムでないもの**への分類を可能にする。

000000000000000000000000000000000000000000 ・・・・・・・・・・・・・・

これはランダムでない。

010101010101010101010101010101010101010101 ・・・・・・・・・・・・・・

これはランダムでない。

010110010010110010100110101110011011100 1 ・・・・・・・・・・・・・・

これはランダムである。

110010010000111111011010101000100010000 1 ・・・・・・・・・・・・・・

これはランダムでない。

無限２進列の分類

アルゴリズム的情報理論は、各々の無限２進列に対し、**ランダムなもの**と**ランダムでないもの**への分類を可能にする。

000000000000000000000000000000000000000000 ・・・・・・・・・・・・・・

これはランダムでない。

010101010101010101010101010101010101010101 ・・・・・・・・・・・・・・

これはランダムでない。

010110010010110010100110101110011011100 1 ・・・・・・・・・・・・・・

これはランダムである。

110010010000111111011010101000100010000 1 ・・・・・・・・・・・・・・

πの２進展開　　**これはランダムでない。**

アルゴリズム的情報理論における乱数: Random Real

$\{0,1\}^\infty$: 無限２進列全体の集合

アルゴリズム的情報理論の考え方

$\{0,1\}^\infty$ のどのような構成的零集合にも属さない無限２進列が、乱数である。これをRandom Realと呼ぶ。 □

これを正当化する思考実験

1. 偏りのないコインを無限回投げて生成した具体的な無限２進列は“ 乱数 ”である。
2. $A_1, A_2, A_3, \ldots\ldots$ をアルゴリズムによって機械的に生成した $\{0,1\}^\infty$ の部分集合列とし、$\mathcal{L}(A_n) \leq 2^{-n}$ が成り立っているとする（$\mathcal{L}$ はLebesgue測度）。
3. 前提: α を与えられた無限２進列とする。$\alpha \in \bigcap_n A_n$ が成り立つとする。
4. もし仮に α が“ 乱数 ”であるならば、α は偏りのないコインを無限回投げて生成したものである。一方、各 A_n は、アルゴリズムという機械が指定する事象であるが、それらが生起する確率は $\mathcal{L}(A_n) \to 0$ となる。従って、確率がいくらでも小さい人工的な事象が生じたことになる。これはおかしい。仮定が間違っている。
5. 結論: α は乱数でない。 □

Martin-Löf Randomness

Definition [Martin-Löf 1966]

(i) A *Martin-Löf test* is a uniformly recursively enumerable sequence $\{A_n\}_{n\in\mathbb{N}}$ of subsets of $\{0,1\}^*$ such that, for every $n \in \mathbb{N}$,

$$\mathcal{L}\left([A_n]^{\prec}\right) \leq 2^{-n},$$

where $[A_n]^{\prec} = \{\alpha \in \{0,1\}^{\infty} \mid \text{Some finite prefix of } \alpha \text{ is in } A_n\}$.

(ii) $\alpha \in \{0,1\}^{\infty}$ is called *Martin-Löf random* if for every Martin-Löf test $\{A_n\}_{n\in\mathbb{N}}$,

$$\alpha \notin \bigcap_{n=1}^{\infty} [A_n]^{\prec}.$$

□

非常に大雑把に言うと，一つのMartin-Löf testは一つの乱数検定に対応する。
あらゆるMartin-Löf test，即ち，あらゆる乱数検定にパスする無限２進列が，Martin-Löf randomな無限２進列である。

ランダムオラクルモデル

ランダムオラクルモデルの一般的形式

ランダムオラクルモデルおいて、暗号方式Πの安全性は次の形で表現される:

For all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\mathrm{Prob}\left[\mathrm{Expt}_{\mathcal{A}^H,\Pi^H}(n) = 1\right] \leq \gamma + \frac{1}{n^d},$$

where the probability is taken over random choice of H as well as the random choices of the parties running Π and the adversary $\mathcal{A}$.

ここで、秘匿方式の場合は$\gamma = \frac{1}{2}$であり、署名方式の場合は$\gamma = 0$.

これは以下のように書き換えることができる:

For all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\frac{1}{(\#\text{ of } x)} \sum_x \mathrm{Prob}\left[\mathrm{Expt}_{\mathcal{A}^H,\Pi^H}(n) = 1 \;\middle|\; H = x\right] \leq \gamma + \frac{1}{n^d}.$$

Digital Signature Schemes

ℓ-Functions

Definition [ℓ-Function] Let $\ell(n)$ be a polynomial. An *ℓ-Function* is a function $H\colon \mathbb{N} \times \{0,1\}^* \to \{0,1\}^*$ such that $|H(n,x)| = \ell(n)$ such for all $n \in \mathbb{N}$ and $x \in \{0,1\}^*$. □

ℓ-functionは、以下で考察するランダムオラクルモデルで、本来確率変数であるランダムオラクルの実現値となるものであり、ランダムオラクルの具現化としての役割を果たす。

Signature Scheme Relative to ℓ-Functions

Definition A *signature scheme relative to ℓ-functions* is a tuple (Gen, Sign, Vrfy) of probabilistic polynomial-time algorithms such that, for every ℓ-function H,

(i) The *key generation algorithm* Gen takes as input the security parameter 1^n and outputs a pair of keys (pk, sk).

(ii) The *signing algorithm* Sign takes as input a private key sk and a message m. It is given oracle access to $H(n, \cdot)$, and then outputs a signature σ.

(iii) The *verification algorithm* Vrfy takes as input a public key pk, a massage m, and a signature σ. It is given oracle access to $H(n, \cdot)$, and then outputs a bit b, with $b = 1$ meaning valid and $b = 0$ meaning invalid.

It is required that, for every $n \in \mathbb{N}$, for every ℓ-function H, for every (pk, sk) output by $\mathsf{Gen}(1^n)$, and for every $m \in \{0,1\}^*$,

$$\mathsf{Vrfy}^{H(n,\cdot)}(pk, m, \mathsf{Sign}^{H(n,\cdot)}(sk, m)) = 1. \qquad \square$$

Experiment for Existential Unforgeablity

Consider the following experiment defined for a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-functions, a probabilistic polynomial-time adversary $\mathcal{A}$, a parameter n, and a function $h\colon \{0,1\}^{\leq q(n)} \to \{0,1\}^{\ell(n)}$ where $q(n)$ is the maximum value between the running time of $\mathcal{A}$ and the running time of Sign on the parameter n:

The signature experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n,h)$**:**

1. $\mathsf{Gen}(1^n)$ *is run to obtain keys* (pk, sk).
2. *Adversary* $\mathcal{A}$ *is given* pk *and oracle access to* $\mathsf{Sign}^{h(\cdot)}(sk,\cdot)$ *and* $h(\cdot)$*, and then outputs* (m,σ).
3. *The output of the experiment is defined to be* 1 *if* $(\mathbf{1})$ $m \notin \mathcal{Q}$ *and* $(\mathbf{2})$ $\mathsf{Vrfy}^{h(\cdot)}(pk,m,\sigma) = 1$*, and* 0 *otherwise. Here* $\mathcal{Q}$ *denotes the set of messages whose signatures were requested by* $\mathcal{A}$ *during its execution.*

Existential Unforgeability

Definition [Existential Unforgeability Relative to Specific ℓ-Function]

Let H be an ℓ-function. A signature scheme Π relative to ℓ-functions is *existentially unforgeable under an adaptive chosen-message attack relative to H* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\text{Prob}\left[\text{Sig-forge}_{\mathcal{A},\Pi}(n, H(n,\cdot)) = 1\right] \leq \frac{1}{n^d}.$$

□

Definition [Existential Unforgeability in the Random Oracle Model]

A signature scheme Π relative to ℓ-functions is *existentially unforgeable under an adaptive chosen-message attack in the random oracle model* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\frac{1}{\#\text{Func}^{\ell(n)}_{\leq q(n)}} \sum_{h \in \text{Func}^{\ell(n)}_{\leq q(n)}} \text{Prob}\left[\text{Sig-forge}_{\mathcal{A},\Pi}(n, h) = 1\right] \leq \frac{1}{n^d}.$$

where $\text{Func}^{\ell(n)}_{\leq q(n)}$ is the set of all functions mapping $\{0,1\}^{\leq q(n)}$ to $\{0,1\}^{\ell(n)}$.

□

アルゴリズム的情報理論の適用

ℓ-Functionと無限2進列との同一視

We choose a particular bijective total recursive function $b\colon \mathbb{N} \to \mathbb{N} \times \{0,1\}^*$. We then identify an ℓ-function $H\colon \mathbb{N} \times \{0,1\}^* \to \{0,1\}^*$ with the infinite binary sequence

$$H(b(1))H(b(2))H(b(3))H(b(4))H(b(5))\cdots\cdots\cdots .$$

Main Results: Equivalent Condition to Existential Unforgeability

We can define a set $\mathsf{TESTS}_{\Pi}^{\mathsf{EUF\text{-}ACMA}}$ of Martin-Löf tests, depending on a signature scheme Π and a security notion (i.e., the existential unforgeability under an adaptive chosen-message attack in this case).

Theorem [Main Result I]

Suppose that a signature scheme Π relative to ℓ-functions is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. For every ℓ-function $H\colon \mathbb{N}\times\{0,1\}^* \to \{0,1\}^*$, the following conditions are equivalent:

(i) Π is existentially unforgeable under an adaptive chosen-message attack relative to H.

(ii) H is Martin-Löf random with respect to $\mathsf{TESTS}_{\Pi}^{\mathsf{EUF\text{-}ACMA}}$. □

Martin-Löf testは乱数検定に対応しているが，あらゆるMartin-Löf test，即ち，あらゆる乱数検定を考えるのではなく，乱数検定の種類を適当に間引くことにより，Πのexistential unforgeabilityを実現するのに必要かつ十分な，程良いランダムさを持つランダムネス概念を定義することができる。

Main Results: Instantiation by Martin-Löf Random Sequence

Corollary [Main Result II]

Suppose that a signature scheme Π relative to ℓ-functions is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. For every ℓ-function $H\colon \mathbb{N}\times\{0,1\}^* \to \{0,1\}^*$, if H is Martin-Löf random then Π is existentially unforgeable under an adaptive chosen-message attack relative to H. □

Main Results: Existential Unforgeability Almost Everywhere

Corollary [Main Result III]

Suppose that a signature scheme Π relative to ℓ-functions is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then

$$\mathcal{L}\left(\mathsf{SecrH}_{\Pi}^{\text{EUF-ACMA}}\right) = 1,$$

where $\mathsf{SecrH}_{\Pi}^{\text{EUF-ACMA}}$ is the set of all ℓ-functions relative to which Π is existentially unforgeable under an adaptive chosen-message attack, and $\mathcal{L}$ is Lebesgue measure. □

Secure Instantiation by Computable Function

From the Random Oracle Model to the Standard Model I

The conjecture below means that, in the case where a scheme Π satisfies a certain condition $\mathcal{C}$, the existential unforgeability of Π proved in the random oracle model can be firmly maintained in the standard model after instantiating the random oracle by some deterministic polynomial-time computable function.

Conjecture [The Most Desirable Result]

Let $\ell(n)$ be a polynomial. Suppose that a signature scheme Π relative to ℓ-functions is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. If Π satisfies $\mathcal{C}$, then there exists a polynomial-time computable ℓ-function (or a polynomial-time computable family of ℓ-functions) relative to which Π is existentially unforgeable under an adaptive chosen-message attack. □

However, it would seem very difficult to prove it with identifying an appropriate nontrivial condition $\mathcal{C}$ at present.

From the Random Oracle Model to the Standard Model II

The second best thing is to investigate whether the conjecture below holds true or not, where we consider the instantiation of the random oracle by simply a (deterministic) computable function, which is not necessarily polynomial-time computable.

Conjecture [The Second most Desirable Result]

Let $\ell(n)$ be a polynomial. Suppose that a signature scheme Π relative to ℓ-functions is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then there exists a computable ℓ-function $H\colon \mathbb{N} \times \{0,1\}^* \to \{0,1\}^*$ such that Π is existentially unforgeable under an adaptive chosen-message attack relative to H. □

In what follows, we prove that an "effective" variant of this conjecture holds true.

Effective Security I

We introduce the effective security by requiring in each of the following definitions that, given $\mathcal{A}$ and d, N can be computed.

Definition [posted again]

Let H be an ℓ-function. A signature scheme Π relative to ℓ-functions is *existentially unforgeable under an adaptive chosen-message attack relative to H* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\text{Prob}\left[\text{Sig-forge}_{\mathcal{A},\Pi}(n, H(n,\cdot)) = 1\right] \leq \frac{1}{n^d}. \qquad \square$$

Definition [posted again]

A signature scheme Π relative to ℓ-functions is *existentially unforgeable under an adaptive chosen-message attack in the random oracle model* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$\frac{1}{\#\text{Func}^{\ell(n)}_{\leq q(n)}} \sum_{h \in \text{Func}^{\ell(n)}_{\leq q(n)}} \text{Prob}\left[\text{Sig-forge}_{\mathcal{A},\Pi}(n, h) = 1\right] \leq \frac{1}{n^d}. \qquad \square$$

Effective Security II

Specifically, we introduce the notion of *effective existential unforgeability* as follows.

To begin with, we choose a particular recursive enumeration $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \ldots$ of all probabilistic polynomial-time adversaries as the standard one for use throughout the rest of this talk. It is easy to show that such an enumeration exists.

Definition [Effective Existential Unforgeability Relative to Specific ℓ-Function]
Let H be an ℓ-function. A signature scheme Π relative to ℓ-functions is *effectively existentially unforgeable under an adaptive chosen-message attack relative to H* if there exists a computable function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for all $i, d, n \in \mathbb{N}$, if $n \geq f(i, d)$ then

$$\text{Prob}\left[\text{Sig-forge}_{\mathcal{A}_i,\Pi}(n, H(n, \cdot)) = 1\right] \leq \frac{1}{n^d}. \qquad \square$$

Note that if a signature scheme Π relative to ℓ-functions is effectively existentially unforgeable under an adaptive chosen-message attack relative to H then Π is simply existentially unforgeable under an adaptive chosen-message attack relative to H.

Effective Security III

On the other hand, the effective existential unforgeability in the random oracle model is formulated as follows.

Definition [Effective Existential Unforgeability in the Random Oracle Model]

A signature scheme Π relative to ℓ-functions is *effectively existentially unforgeable under an adaptive chosen-message attack in the random oracle model* if there exists a computable function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for all $i, d, n \in \mathbb{N}$, if $n \geq f(i, d)$ then

$$\frac{1}{\#\mathsf{Func}^{\ell(n)}_{\leq q(n)}} \sum_{h \in \mathsf{Func}^{\ell(n)}_{\leq q(n)}} \mathsf{Prob}\left[\mathsf{Sig\text{-}forge}_{\mathcal{A}_i,\Pi}(n, h) = 1\right] \leq \frac{1}{n^d}. \qquad \square$$

Note that if a signature scheme Π relative to ℓ-functions is effectively existentially unforgeable under an adaptive chosen-message attack in the random oracle model then Π is simply existentially unforgeable under an adaptive chosen-message attack in the random oracle model.

Secure Instantiation by Computable Function

Theorem [Main Result IV]

Let $\ell(n)$ be a polynomial. Suppose that a signature scheme Π relative to ℓ-functions is effectively existentially unforgeable under an adaptive chosen-message in the random oracle model. Then there exists a computable ℓ-function $H\colon \mathbb{N} \times \{0,1\}^* \to \{0,1\}^*$ such that Π is effectively existentially unforgeable under an adaptive chosen-message to H. □

The above theorem is proved using the following lemma.

Lemma Let S be a recursively enumerable subset of $\{0,1\}^*$. Suppose that $\mathcal{L}\left([S]^{\prec}\right) < 1$ and $\mathcal{L}\left([S]^{\prec}\right)$ is a computable real. Then there exists $\alpha \in \{0,1\}^{\infty}$ such that α is computable and $\alpha \notin [S]^{\prec}$. □

This lemma is Exercise 1.9.21 of Nies's textbook of algorithmic randomness:
A. Nies, *Computability and Randomness*. Oxford University Press, Inc., New York, 2009.

Concluding Remarks

Our results use the general form of definitions of security notions for signature schemes, and depend neither on specific schemes nor on specific security notions.

It is challenging to prove the following conjecture with identifying an appropriate computational assumption COMP and an appropriate nontrivial condition $\mathcal{C}$ on a scheme Π in the future.

Conjecture

Let $\ell(n)$ be a polynomial. Suppose that a signature scheme Π relative to ℓ-functions is polynomial-time effectively existentially unforgeable under an adaptive chosen-message in the random oracle model. Under the assumption COMP, if Π satisfies the condition $\mathcal{C}$, then there exists a polynomial-time computable ℓ-function (or a polynomial-time computable family of ℓ-functions) relative to which Π is polynomial-time effectively existentially unforgeable under an adaptive chosen-message attack. □

The conjecture states that the security in the random oracle model implies one in the standard model.