Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 155–166

A PROPERTY FOR CRYPTOGRAPHY BASED ON INFINITE GROUPS

EONKYUNG LEE

Abstract. Cryptography using infinite groups has been studied since about twenty years ago. However, it has not been so fruitful as using finite groups. An important reason is the absence of research on probability in this area. Indeed, a number of cryptographic tools concerning probability are playing significant roles in analyses in the case of finite groups.

Our purpose is twofold—to deal with not a particular finite subset (as before) of an infinite group but the whole group itself, and to make cryptographic tools developed in finite groups still useful in infinite groups. As a first step to serve this purpose, we study a probability-theoretic property, the so-called *right-invariance*, that has been widely used in cryptography. Like the uniform distribution over finite sets, right-invariance property simplifies many complex situations. However, it can be unused or misused since it is not known when this property can be used.

We propose a method of deciding whether or not we can use this property in a given situation, and prove that there is no right-invariant probability distribution on most infinite groups which can be universally used. Therefore, we discuss weaker, yet practical alternatives with concrete examples.

1. Introduction

In modern cryptography, many schemes are designed based on groups. Compared to finite groups, cryptographic research has not been so active on infinite groups. Most proposed works on infinite groups [19, 10, 16, 17, 18, 3, 12, 2] are rather restricted to a few types of schemes such as key agreement protocol and public key encryption. A reason is because some cryptographic schemes (e.g. zero-knowledge proof system, pseudorandom function, hard-core predicate, etc.) have checkpoints concerning probability for their basic security. On the other hand, for the proposed schemes, probabilistic analysis has not been done as mathematically perfectly as the case in finite groups.

Instead, it was sometimes done by taking a particular finite subset of the group, and then by proceeding assuming a certain probability distribution in their interests (e.g. uniform distribution) on the finite subset [12, 13, 14]. However, this approach is somewhat problematic since that finite set is usually not closed under group operation though one sometimes needs to treat products of elements from that set.

Key words and phrases. Probabilistic cryptanalysis, Infinite group, Right-closedness, Right-invariance.

Our motivation is that in spite of this necessity, there is nothing discussed seriously for probability in the literature on cryptography based on infinite groups.

Our Results. A first approach to this issue might be to look into what makes dealing with finite groups so convenient in cryptography, and then think about how such a nice property is applicable to infinite groups. Among infinite groups, we deal with only finitely generated ones since groups with infinitely many generators are not practical.

This article discusses a particular property, the so-called *right-invariance*: we define a probability measure (cf. probability distribution in probability theory) P on a group G as right-invariant if $P(E) = P(Ex)$ for all $E \subset G$ on which P is defined and for all $x \in G$. For finite groups, this property accompanies the uniform distribution. It is the key to many important properties like random self-reducibility, zero-knowledgeness, and so on. However, it is hardly playing any role in infinite groups since it is known neither when nor how this property can be used.

It is ideal to handle not a particular finite subset of an infinite group but the group itself. In order to discuss right-invariance on the whole of the infinite group, we take a measure-theoretic approach. Via this approach, we discover how to decide whether or not right-invariance is applicable to a given situation.

For the situations where this property is allowable, we are curious about how it can be handled in practice. It is certainly easy to find a probability measure which is right-invariant *only* in a particular situation. However, what is more meaningful is to find a probability measure which is right-invariant in *all* situations where such property is allowable. Namely, a right-invariant probability measure that can be used universally on a given group. We prove that there does not exist such a probability measure at least over a particular class of groups. Most infinite groups that have appeared in cryptography belong to this class. So, we propose what can be used in place of such an ideal measure.

Organization. Sec. 2 gives basic notations and brief definitions for reading this paper. Sec. 3 discusses why right-invariance is attractive, and formalizes the notion. Sec. 4 explores right-invariance property through building a mathematical framework. Sec. 5 discusses the notion of universally right-invariant probability measure and its alternatives.

2. Preliminaries

Notation. $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ are the sets of natural numbers, integers, and real numbers, respectively. For $a < b$, $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ and $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$. For $n \in \mathbb{N}$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. For a set S, $|S|$ denotes the cardinal number of S, and the collection of all subsets of S is denoted by 2^S. By a *partition* of S we mean a family $\{S_i\}_{i \in I}$ of non-empty, mutually disjoint subsets of S such that $S = \cup_{i \in I} S_i$. $\emptyset$ denotes the empty set.

2.1. Probability.

This section reviews probability from a measure-theoretic point of view.

Definition 1. Let X be a non-empty set.

(a) $\mathcal{M} \subset 2^X$ is called a *σ-algebra in X* if (i) $\emptyset \in \mathcal{M}$, (ii) $E \in \mathcal{M}$ implies $X \backslash E \in \mathcal{M}$, and (iii) $E_1, E_2, \ldots \in \mathcal{M}$ implies $\cup_{i=1}^{\infty} E_i \in \mathcal{M}$.
(b) If $\mathcal{M}$ is a σ-algebra in X, then $(X, \mathcal{M})$ is called a *measurable space* and the members of $\mathcal{M}$ are called the *measurable sets* in X.

If $\mathcal{M}$ is any collection of subsets of X, it is known that there exists a smallest σ-algebra $\mathcal{M}^*$ in X such that $\mathcal{M} \subset \mathcal{M}^*$. This $\mathcal{M}^*$ is called the *σ-algebra generated by $\mathcal{M}$*.

Definition 2. (a) For a measurable space $(X, \mathcal{M})$, a set function $\mu : \mathcal{M} \to [0, 1]$ is called a *probability measure on $\mathcal{M}$* if it satisfies that (i) $\mu(X) = 1$ and (ii) if $E_1, E_2, \ldots \in \mathcal{M}$ are mutually disjoint, $\mu(\cup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$.
(b) For a measurable space $(X, \mathcal{M})$, if μ is a probability measure on $\mathcal{M}$, then $(X, \mathcal{M}, \mu)$ is called a *probability space*. In particular, it is called *atomic* if $\mathcal{M} = 2^X$. Measurable sets of a probability space are called *events*.

2.2. **Group.** Let G be a group and H a subgroup of G. For $x \in G$, the set $Z_H(x) = \{y \in H \mid yx = xy\}$ is called the *centralizer of x in H*. It is a subgroup of H. And the set $Hx = \{hx \mid h \in H\}$ is called a *right coset* of H in G and $xH = \{xh \mid h \in H\}$ a *left coset* of H in G. The *index of H in G*, denoted by $[G : H]$, is the cardinal number of the set of distinct right cosets of H in G. 1_G denotes the identity of G.

Definition 3. For a set X let $X^{-1} = \{x^{-1} \mid x \in X\}$.
(a) $w = w_1 \cdots w_\ell$ is called a *reduced word with respect to X* if w is the empty word or w satisfies that (i) $\ell \in \mathbb{N}$; (ii) $w_i \in X \cup X^{-1}$ for all $1 \leq i \leq \ell$; (iii) $w_{i+1} \neq w_i^{-1}$ for all $1 \leq i < \ell$. $|w| = 0$ (if w is the empty word) or ℓ (otherwise) denotes the word length.
(b) $F(X)$ denotes the *free group generated by X*. It is the set of all reduced words on X with the binary operation: for any $w_1, w_2 \in F(X)$, $w_1 \cdot w_2$ is the reduced form of the word obtained by the juxtaposition $w_1 w_2$ of the two words. The symbol '$\cdot$' is omitted if there is no confusion.

3. Role of Right-Invariance

For finite groups, numerous cryptographic techniques have been developed. In order to apply them to infinite groups as much as possible, this section looks into a particular property that has been widely used in cryptography.
Role in random self-reducibility. Informally, a problem is said to be *random self-reducible* if solving it on *any* instance can be efficiently reduced to solving it on a *random* instance. For a random self-reducible problem, if breaking a cryptographic scheme implies solving the problem on average, it means solving it in the worst case. Thus, since Blum and Micali [4] introduced this notion, it has played an invaluable role in showing provable security of many schemes. We refer to [1, 9] for detailed references on it and the cryptographic significance of this feature. We state it roughly via the discrete logarithm problem with proper parameters, a prime p and a generator g of $\mathbb{Z}_p^*$, where n is the bit-length of p.

Let $a, b \in \mathbb{N}$ and let $\mathcal{A}$ ba a probabilistic polynomial time algorithm such that

$$\Pr_x[\mathcal{A}(p, g, g^x \bmod p) = x] > \frac{1}{n^a},$$

where x is taken uniformly at random from $\mathbb{Z}_{p-1}$. Then, there exists a probabilistic polynomial time algorithm $\mathcal{D}$ such that for all $y \in \mathbb{Z}_{p-1}$,

$$\Pr[\mathcal{D}(p, g, g^y \bmod p) = y] > 1 - \frac{1}{n^b}.$$

$\mathcal{D}$ is designed based on the following idea: for any fixed $y \in \mathbb{Z}_{p-1}$, $\mathcal{D}$ chooses $x \in \mathbb{Z}_{p-1}$ uniformly at random, gets w by giving $\mathcal{A}$ a query $(p, g, g^y g^x \bmod p)$, outputs $w - x \bmod p - 1$ if $g^w = g^y g^x \bmod p$, otherwise repeats this process some polynomial times. A basic property used in computing the success probability of $\mathcal{D}$ is that for any $y \in \mathbb{Z}_{p-1}$

$$\Pr_x[\mathcal{A}(p, g, g^{y+x} \bmod p) = y + x \bmod p - 1] = \Pr_x[\mathcal{A}(p, g, g^x \bmod p) = x], \tag{1}$$

where x is taken uniformly at random from $\mathbb{Z}_{p-1}$.

Equation (1) can be generalized as follows: given a group G, for all $r \in G$

$$\Pr(f(X) = 0) = \Pr(f(Xr) = 0) \quad \text{or} \tag{2}$$

$$\Pr(f(X) = 0) = \Pr(f(rX) = 0), \tag{3}$$

where X is a random variable over G and $f : G \to \{0, 1\}$ is a function. Without loss of generality, in this article we focus on Equation (2).

If G is a finite group and X has the uniform distribution, Equation (2) is true. In this case, it is being used as an underlying assumption in analyzing probabilistically cryptographic primitives or protocols. However, it is not true in general if G is an infinite group or if one cannot uniformly generate elements from even a finite group. We know that no probability distribution can ever be uniform on any infinite group, however the concept of uniformity makes infinite groups more flexibly handled in cryptography. A natural question is what distribution over infinite groups is an analogue of the uniform distribution over finite groups.

As for an infinite group G, we recall the meaning of Equation (2) with a given random variable X. The fact that X is a random variable over G with a probability distribution P means that P is the probability measure on the atomic measurable space $(G, 2^G)$ and $\Pr[X \in E] = P(E)$ for any $E \subset G$.

From a measure-theoretic point of view, we consider not only 2^G but also other σ-algebra $\mathcal{G}$ as the σ-algebra on which P is defined. By restricting P originally defined on 2^G to $\mathcal{G}$, $(G, 2^G, P)$ induces another probability space $(G, \mathcal{G}, P)$.

Definition 4. Let $(G, \mathcal{G}, P)$ be a probability space. $E \in \mathcal{G}$ is called a *right-invariant event* (resp. *left-invariant event*) if, for all $x \in G$, $Ex \in \mathcal{G}$ (resp. $xE \in \mathcal{G}$) and $P(E) = P(Ex)$ (resp. $P(E) = P(xE)$). $(G, \mathcal{G}, P)$ (or shortly P) is said to be *right-invariant* (resp. *left-invariant*) if all events are right-invariant (resp. left-invariant).

For a situation in which one is interested (e.g. points where one wants to compute probabilities or to compare them), if a proper σ-algebra covering all the events (i.e. containing all the events as measurable sets thereof) in question can be constructed and there exists a right-invariant probability measure thereon, then we say that *right-invariance is allowable (or is applicable, can be used, etc.) in the situation.*

4. Right-Invariant Probability Space

In order to discuss right-invariance from a measure-theoretic point of view, we first analyze the structure of an arbitrary σ-algebra in infinite groups, and then a special type of σ-algebra. From this we formulate a way of deciding whether or not right-invariance property is allowable in a given situation.

Throughout this paper, we deal with only finitely generated groups since groups with infinitely many generators are not practical. Note that any finitely generated infinite group is a countable set.

σ-algebra in finitely generated infinite groups. Let G be a finitely generated infinite group and $\mathcal{G}$ be a σ-algebra in G. For $x \in G$, define

$$\mathcal{M}_{\mathcal{G}}(x) = \{E \in \mathcal{G} \mid x \in E\} \quad \text{and} \quad M_{\mathcal{G}}(x) = \cap_{E \in \mathcal{M}_{\mathcal{G}}(x)} E.$$

In particular, denote $M_{\mathcal{G}}(1_G)$ by $M_{\mathcal{G}}$. The following proposition shows that $M_{\mathcal{G}}(x)$ is the smallest measurable set containing x.

Proposition 1. *For a finitely generated infinite group G, let $\mathcal{G}$ be any σ-algebra in it. Then, $M_{\mathcal{G}}(x) \in \mathcal{G}$ for all $x \in G$. Furthermore, any measurable set is partitioned into $M_{\mathcal{G}}(x)$'s.*

Proof. Let $x \in G$. Since $G \in \mathcal{M}_{\mathcal{G}}(x)$ and $x \in M_{\mathcal{G}}(x)$, $M_{\mathcal{G}}(x) \neq \emptyset$. We show that $M_{\mathcal{G}}(x)$ can be expressed as an intersection of a countable number of measurable sets. For $y \in G$, define a set A_y as follows.

$$A_y = \begin{cases} G & \text{if } y \in M_{\mathcal{G}}(x), \\ E \text{ such that } y \notin E \in \mathcal{M}_{\mathcal{G}}(x) & \text{if } y \notin M_{\mathcal{G}}(x). \end{cases}$$

Since G is a countable set, it suffices to show that $M_{\mathcal{G}}(x) = \cap_{y \in G} A_y$. (i) $M_{\mathcal{G}}(x) \subset \cap_{y \in G} A_y$: If $w \notin \cap_{y \in G} A_y$, there exists $y \in G$ such that $w \notin A_y$. Since $A_y \in \mathcal{M}_{\mathcal{G}}(x)$, $w \notin M_{\mathcal{G}}(x)$. (ii) $M_{\mathcal{G}}(x) \supset \cap_{y \in G} A_y$: If $w \notin M_{\mathcal{G}}(x)$, $w \notin A_w$. Thus, $w \notin \cap_{y \in G} A_y$. Therefore, $M_{\mathcal{G}}(x) \in \mathcal{G}$.

Let $E \in \mathcal{G}$. Since, for any $x \in E$, $M_{\mathcal{G}}(x) \subset E$, $E = \cup_{x \in E} M_{\mathcal{G}}(x)$. Thus it suffices to show that any distinct $M_{\mathcal{G}}(x)$ and $M_{\mathcal{G}}(y)$ are disjoint. Assume $M_{\mathcal{G}}(x) \cap M_{\mathcal{G}}(y) \neq \emptyset$. If $x \notin M_{\mathcal{G}}(y)$, then $M_{\mathcal{G}}(x) \backslash M_{\mathcal{G}}(y) \in \mathcal{M}_{\mathcal{G}}(x)$ since $M_{\mathcal{G}}(x) \backslash M_{\mathcal{G}}(y) \in \mathcal{G}$ and $x \in M_{\mathcal{G}}(x) \backslash M_{\mathcal{G}}(y)$. Since $M_{\mathcal{G}}(x)$ is the intersection of all members of $\mathcal{M}_{\mathcal{G}}(x)$, $M_{\mathcal{G}}(x) \subset M_{\mathcal{G}}(x) \backslash M_{\mathcal{G}}(y)$. In particular, $M_{\mathcal{G}}(x) \cap M_{\mathcal{G}}(y) = \emptyset$ which contradicts to the assumption. Thus $x \in M_{\mathcal{G}}(y)$, so $M_{\mathcal{G}}(x) \subset M_{\mathcal{G}}(y)$. By the same argument, $M_{\mathcal{G}}(y) \subset M_{\mathcal{G}}(x)$. Therefore, $M_{\mathcal{G}}(x) = M_{\mathcal{G}}(y)$. □

Right-closed σ-algebra in finitely generated infinite groups.

Definition 5. *A measurable space $(G, \mathcal{G})$ (or a σ-algebra $\mathcal{G}$ in G) is called* right-closed *(resp.* left-closed*) if, for any $E \in \mathcal{G}$ and any $x \in G$, $Ex \in \mathcal{G}$ (resp. $xE \in \mathcal{G}$).*

A σ-algebra generated by a subgroup and all its right cosets is right-closed. The following shows that right-closed σ-algebras have only this form.

Theorem 2. *For a finitely generated infinite group G, the following conditions on a measurable space $(G, \mathcal{G})$ are equivalent.*

(i) *$\mathcal{G}$ is right-closed.*
(ii) *$M_{\mathcal{G}}(x) = M_{\mathcal{G}}x$ for all $x \in G$.*
(iii) *$M_{\mathcal{G}}$ is a subgroup of G, and $\mathcal{G}$ is generated by $M_{\mathcal{G}}$ and all its right cosets.*

Proof. (i)⇒(ii): Suppose that (i) holds. Let $x \in G$. Since $M_{\mathcal{G}}(x) = \cap_{A \in \mathcal{M}_{\mathcal{G}}(x)} A$ and $M_{\mathcal{G}}x = (\cap_{A \in \mathcal{M}_{\mathcal{G}}(1_G)} A)x = \cap_{A \in \mathcal{M}_{\mathcal{G}}(1_G)}(Ax) = \cap_{B \in \mathcal{M}_{\mathcal{G}}(1_G)x} B$, it suffices to show that $\mathcal{M}_{\mathcal{G}}(x) = \mathcal{M}_{\mathcal{G}}(1_G)x$.

Let Ax, where $A \in \mathcal{M}_{\mathcal{G}}(1_G)$, be an arbitrary element of $\mathcal{M}_{\mathcal{G}}(1_G)x$. Since $1_G \in A$, $x = 1_G x \in Ax$ and so $Ax \in \mathcal{M}_{\mathcal{G}}(x)$ by (i). Thus $\mathcal{M}_{\mathcal{G}}(1_G)x \subset \mathcal{M}_{\mathcal{G}}(x)$. Conversely, if $A \in \mathcal{M}_{\mathcal{G}}(x)$, then $1_G = xx^{-1} \in Ax^{-1} \in \mathcal{M}_{\mathcal{G}}(1_G)$ by (i). Thus, $\mathcal{M}_{\mathcal{G}}(x) \subset \mathcal{M}_{\mathcal{G}}(1_G)x$.

(ii)⇒(iii): Suppose that (ii) holds. Let $a, b \in M_{\mathcal{G}}$. Since $b \in M_{\mathcal{G}}$, $M_{\mathcal{G}} = M_{\mathcal{G}}(b)$ by Proposition 1. Then, $a \in M_{\mathcal{G}}(b) = M_{\mathcal{G}}b$ by (ii), and so $ab^{-1} \in M_{\mathcal{G}}$. Therefore, $M_{\mathcal{G}}$ is a subgroup of G.

For any $E \in \mathcal{G}$, $E = \cup_{x \in E} M_{\mathcal{G}}(x)$ by Proposition 1. $M_{\mathcal{G}}(x) = M_{\mathcal{G}}x \in \mathcal{G}$ by (ii), and so $E = \cup_{x \in E} M_{\mathcal{G}}x$. Thus, $\mathcal{G}$ is generated by all right cosets of $M_{\mathcal{G}}$.

(iii)⇒(i): It is trivial. □

Analogous result holds for left-closed σ-algebras. By combining these, we get the following.

Corollary 3. *For a finitely generated infinite group G, the following conditions on a measurable space $(G, \mathcal{G})$ are equivalent.*

(i) *$\mathcal{G}$ is both left- and right-closed.*
(ii) *$xM_{\mathcal{G}} = M_{\mathcal{G}}(x) = M_{\mathcal{G}}x$ for all $x \in G$.*
(iii) *$M_{\mathcal{G}}$ is a normal subgroup of G and $\mathcal{G}$ is generated by $M_{\mathcal{G}}$ and all its cosets.*

Right-invariance property of finitely generated infinite groups. Right-invariance property is what belongs to a probability measure defined on a right-closed σ-algebra. When a probability space is right-invariant, any measurable set is, of course, right-invariant. Conversely, Proposition 1 and Theorem 2 imply that right-invariance of $M_{\mathcal{G}}$ is extended to the whole space.

Theorem 4. *For a finitely generated infinite group G, let $\mathcal{G}$ be a right-closed σ-algebra in G. $P(M_{\mathcal{G}}) = P(M_{\mathcal{G}}x)$ for all $x \in G$ if and only if $P(E) = P(Ex)$ for all $E \in \mathcal{G}$ and all $x \in G$.*

From Theorems 2 and 4, we have the following.

Corollary 5. *Let G be a finitely generated infinite group. If $(G, \mathcal{G}, P)$ is a right-invariant probability space, then $[G : M_{\mathcal{G}}]$ is finite and $P(M_{\mathcal{G}}x) = [G : M_{\mathcal{G}}]^{-1}$ for all $x \in G$. Therefore, if $[G : M_{\mathcal{G}}]$ is infinite, $(G, \mathcal{G}, P)$ cannot be right-invariant for any probability measure P.*

5. Universally Right-Invariant Probability Measure and Alternatives

Now we can decide whether or not right-invariance is allowable in a given situation. Suppose that it is allowable. Then, what are the concrete examples of the probability measure which is both *useful* and *practical* for such property?

5.1. **Universally right-invariant probability measure.** Given a right-closed measurable space $(G, \mathcal{G})$, if $M_{\mathcal{G}}$ is of finite-index, it is easy to get a probability measure that is right-invariant *only* on $(G, \mathcal{G})$. However, what is more meaningful is the one that is right-invariant on *any* right-closed σ-algebra $\mathcal{G}$ with finite-index $M_{\mathcal{G}}$. By Corollary 5, it can be defined as follows.

Definition 6. *A probability measure P defined on an atomic measurable space $(G, 2^G)$ is called a* universally right-invariant probability measure on G *if $P(H) = P(Hx)$ for any finite-index subgroup H of G and any $x \in G$.*

Most infinite groups that have emerged in cryptography are finitely generated residually-finite groups (e.g. free groups, groups of automorphisms of free groups, braid groups, etc.). A group is *residually-finite* if the intersection of all finite-index normal subgroups consists of only the identity. Here, we consider a larger class of groups, finitely generated groups with infinitely many finite-index subgroups. Finitely-generated residually-finite infinite groups belong to this class.

Theorem 6. *Let G be a finitely generated group with infinitely many finite-index subgroups. Then the intersection of all finite-index subgroups of G is a subgroup of G with infinite-index. Furthermore, G has no universally right-invariant probability measure.*

Proof. For the proof, we use the following fact.

Fact. Let G be a finitely generated infinite group. Then, for any $m \in \mathbb{N}$, G has only finitely many subgroups of index m.

Let $\mathcal{H}$ be the collection of all finite-index subgroups of G and $H_0 = \cap_{H \in \mathcal{H}} H$. Clearly H_0 is a subgroup of G. Assume that $[G : H_0] = k$ is finite. Then any $H \in \mathcal{H}$ has index k or less. By Fact 5.1, $\mathcal{H}$ is a finite set which contradicts to the hypothesis. Therefore, $[G : H_0]$ is infinite.

Assume that P is a universally right-invariant probability measure on G. Then for any $x \in G$ and any $H \in \mathcal{H}$,

$$P(H_0 x) \leq P(Hx) = P(H) = [G : H]^{-1}$$

by Corollary 5. Note that for any integer m there exists a finite-index subgroup H such that $[G : H] \geq m$ by Fact 5.1 and by the hypothesis. Thus $P(H_0 x) = 0$. Since H_0 is an infinite-index subgroup of G, there exist $x_1, x_2, \ldots \in G$ such that G is partitioned into $H_0 x_1, H_0 x_2, \ldots$. So $P(G) = \sum_{i=1}^{\infty} P(H_0 x_i) = 0$ which contradicts to $P(G) = 1$. Therefore, P cannot be universally right-invariant. □

Corollary 7. *Any finitely-generated residually-finite infinite group has no universally right-invariant probability measure.*

5.2. **Alternatives.** From Theorem 6, a question arises: what are weaker, yet practical alternatives to the universally right-invariant probability measure? We approach this question via random walk on a free group $F = F(X)$, where $X = \{x_1, \ldots, x_m\}$. It is because any finitely generated infinite group is a homomorphic image of a finitely generated free group, and random walk yields a natural probability measure on F in the following sense: it generates all words of F with positive probability, and the longer the word is, the lower its occurrence probability is.

On the other hand, Theorems 2 and 4 reduce finding such an alternative measure to finding an atomic probability measure in an infinite group which is close to the uniform distribution over the family of all right-cosets of any finite-index subgroup. The latter has been studied independently in group theory for a long time. So we attempt to search for alternatives in the results from this area.

For $s \in (0,1)$, let W_s be a no-return random walk on the Cayley graph $C(F,X)$ of F with respect to the generating set X. See Appendix for Cayley graph. W_s starts at 1_F and either does nothing with probability s, or moves to one of the $2m$ adjacent vertices with equal probabilities $\frac{1-s}{2m}$. If W_s is at a vertex $v \neq 1_F$, it either stops at v with probability s, or moves with probability $\frac{1-s}{2m-1}$ to one of the $2m-1$ adjacent vertices lying away from 1_F producing a new freely reduced word $vx_i^{\pm 1}$. So $\Pr(|w| = k) = s(1-s)^k$ and the resulting atomic probability measure on F is

$$\mu_s(w) = \begin{cases} s & \text{if } w = 1_F, \\ \frac{s(1-s)^{|w|}}{2m(2m-1)^{|w|-1}} & \text{otherwise.} \end{cases}$$

Thus, $\mu_s(w)$ is the probability that the random walk W_s stops at w. From the results of Woess [20] and Borovik, Myasnikov, and Remeslennikov [5], for any finite-index subgroup H of F and any $x \in F$

$$\lim_{s \to 0} \mu_s(Hx) = [F : H]^{-1}.$$

On the other hand, for the case that we are working with only sufficiently long words, let's consider a variant of μ_s. For $k \in \mathbb{N}$, define

$$\bar{\mu}_k(w) = \begin{cases} 0 & \text{if } w \in B_k, \\ \frac{\mu_s(w)}{\mu_s(F \setminus B_k)} & \text{otherwise,} \end{cases}$$

where $B_k = \{w \in F \mid |w| \leq k\}$ is a ball of radius k. Then $\bar{\mu}_k$ is a probability measure on $(F, 2^F)$. From the results of Pak [**?**] and Borovik, Myasnikov, and Shpilrain [6], for any finite-index normal subgroup H of F

$$\frac{1}{2} \sum_{\bar{x} \in F/H} \left| \bar{\mu}_k(\bar{x}) - [F : H]^{-1} \right| = o(e^{-k}). \tag{4}$$

Discussion of property of μ_s and $\bar{\mu}_k$. Let $(F, \mathcal{F})$ be a right-closed measurable space with $[F : M_{\mathcal{F}}] < \infty$. Suppose that $P_{\mathcal{F}}$ is the right-invariant probability measure on $(F, \mathcal{F})$. Then, by Proposition 1 and Theorem 2, μ_s has the following property. For

any $E \in \mathcal{F}$

$$\begin{aligned} |\mu_s(E) - P_{\mathcal{F}}(E)| &= \left| \sum_{i=1}^{t} \mu_s(M_{\mathcal{F}} x_i) - t P_{\mathcal{F}}(M_{\mathcal{F}}) \right| \\ &\leq \sum_{i=1}^{t} \left| \mu_s(M_{\mathcal{F}} x_i) - [F : M_{\mathcal{F}}]^{-1} \right| \ \to \ 0 \quad \text{as } s \to 0, \end{aligned}$$

where $M_{\mathcal{F}} x_i$'s are distinct right-cosets of $M_{\mathcal{F}}$ in F such that $E = \cup_{i=1}^{t} M_{\mathcal{F}} x_i$.

On the other hand, by the normality of H in (4), $\bar{\mu}_k$ has a slightly different property, so that it can be used in two cases. In the first case, let $(F, \mathcal{F})$ be a both left- and right-closed measurable space with $[F : M_{\mathcal{F}}] < \infty$. Then, by Corollary 3, $M_{\mathcal{F}}$ is a normal subgroup of F. Suppose that $P_{\mathcal{F}}$ is the right-invariant probability measure on $(F, \mathcal{F})$. Then, for any $E \in \mathcal{F}$

$$|\bar{\mu}_k(E) - P_{\mathcal{F}}(E)| \ \leq \ \frac{1}{2} \sum_{\bar{x} \in F/M_{\mathcal{F}}} \left| \bar{\mu}_k(\bar{x}) - [F : M_{\mathcal{F}}]^{-1} \right| \ = \ o(e^{-k}) \tag{5}$$

for $k \to \infty$. The above inequality comes from the following fact.

Fact. Let Ω be a finite set, and let P_1 and P_2 be probability measures on $(\Omega, 2^{\Omega})$. Then,

$$\max_{E \subset \Omega} |P_1(E) - P_2(E)| = \frac{1}{2} \sum_{\omega \in \Omega} |P_1(\omega) - P_2(\omega)|.$$

In the second case, let $(F, \mathcal{F})$ be a right-closed measurable space such that $M_{\mathcal{F}}$ contains a finite-index normal subgroup N of F. Then, there exist distinct cosets, $Nx_1, \ldots, Nx_t$, of N in F such that $M_{\mathcal{F}} = \cup_{i=1}^{t} N x_i$. Let $P_{\mathcal{F}}$ be the right-invariant probability measure on $(F, \mathcal{F})$. Then, from Fact 5.2, for any $E \in \mathcal{F}$

$$\begin{aligned} |\bar{\mu}_k(E) - P_{\mathcal{F}}(E)| &\leq \frac{1}{2} \sum_{M_{\mathcal{F}} x \in \mathcal{R}} \left| \bar{\mu}_k(M_{\mathcal{F}} x) - [F : M_{\mathcal{F}}]^{-1} \right| \\ &\leq \frac{1}{2} \sum_{M_{\mathcal{F}} x \in \mathcal{R}} \sum_{i=1}^{t} \left| \bar{\mu}_k(N x_i x) - [F : N]^{-1} \right| \ = \ o(e^{-k}) \end{aligned}$$

for $k \to \infty$, where $\mathcal{R}$ is the set of all right-cosets of $M_{\mathcal{F}}$ in F.

Discussion of alternatives. Given a group G, a good alternative to the universally right-invariant probability measure may be a probability measure P on $(G, 2^G)$ such that for any right-invariant probability space $(G, \mathcal{G}, P_{\mathcal{G}})$ and for any $E \in \mathcal{G}$, $|P(E) - P_{\mathcal{G}}(E)|$ is very small. Here, we should be careful with the word, "small". Small in what? The factors which determine the value of $|P(E) - P_{\mathcal{G}}(E)|$ come from the characteristics of G, $\mathcal{G}$, and P. Note that the group G is given, the σ-algebra $\mathcal{G}$ is arbitrarily selected to some extent, and we are discussing the measure P. So focusing on P, it seems more reasonable to view P not as a single probability measure but as a family of probability measures indexed by factors representing its characteristics. For example, $\mu = \{\mu_s\}_{s \in (0,1)}$ and $\bar{\mu} = \{\bar{\mu}_k\}_{k \in \mathbb{N}}$. From this point of view, let's define our alternative in general terms.

Let $P = \{P_\alpha\}_{\alpha \in \mathcal{A}}$ be a family of probability measures on $(G, 2^G)$ for an index set $\mathcal{A}$. And let some α_0 be given. For any right-invariant probability space $(G, \mathcal{G}, P_\mathcal{G})$ and for any $E \in \mathcal{G}$, P has the following property.

$$\lim_{\alpha \to \alpha_0} |P_\alpha(E) - P_\mathcal{G}(E)| = 0$$

μ serves as a good example of this alternative. On the other hand, $\bar{\mu}$ can serve as another example if $(G, \mathcal{G}, P_\mathcal{G})$ is a both left- and right-invariant probability space, or if $(G, \mathcal{G}, P_\mathcal{G})$ is a right-invariant probability space and $M_\mathcal{G}$ contains a finite-index normal subgroup of G. In these cases, $|P_\alpha(E) - P_\mathcal{G}(E)|$ decreases exponentially.

6. Conclusions

We know that it is impossible to overestimate the role of the uniform distribution in cryptography. However, no infinite group has such a nice distribution. Noticing that this fact is an impediment to the use of infinite groups for cryptography, this paper has formalized the notion of right-invariance on an infinite group which in a sense corresponds to the uniform distribution on a finite set, and then shown *when* and *how* this notion can be used for infinite-group-based cryptography.

Our work is a first attempt to formalize and resolve probability-theoretic problems arising in the process of using infinite groups for cryptography. Although our work cannot resolve all the problems, we hope that it contributes to widening the scope of what provably secure cryptosystems can be built on. We close this paper with the following research topics.

- Find different types of alternatives to the universally right-invariant probability measure from ours.
- Find examples of practical problems which right-invariance can resolve in cryptography.
- For complex problems (e.g. proving security of a cryptosystem), discover, formalize, and solve its constituent problems other than right-invariance.

Acknowledgement

The author would like to thank all the members of Daewoo Workshop 2004 committee. This work was supported by the Korea Science and Engineering Foundation grant, KOSEF R04-2004-000-10039-0.

References

[1] D. Angluin and D. Lichtenstein, *Provable Security of Cryptosystmes: A Survey*, Computer Science Department, Yale University, TR-288, 1983.

[2] I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld, *New Key Agreement Protocols in Braid Group Cryptography*, CT-RSA 2001, LNCS **2020**, 13–27, 2001.

[3] I. Anshel, M. Anshel, and D. Goldfeld, *An Algebraic Method for Public-key Cryptography*, Math. Res. Lett. **6** (1999), 287–291.

[4] M. Blum and S. Micali, *How to Generate Cryptographically Strong Sequences of Pseudorandom Bits*, SIAM J. Comput. **13** (1984) 850–864.

[5] A.V. Borovik, A.G. Myasnikov, and V.N. Remeslennikov, *Multiplicative Measures on Free Groups*, To appear in Internat. J. Algebra Comp., Available at `http://www.ma.umist.ac.uk/avb/pdf/multiplicative35.pdf`.

[6] A.V. Borovik, A.G. Myasnikov, and V. Shpilrain, *Measuring Sets in Infinite Groups*, Contemporary Mathematics **298** (2002), 21–42.

[7] J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, and J.H. Cheon, *An Efficient Implementation of Braid Groups*, ASIACRYPT 2001, LNCS **2248**, 144–156, 2001.

[8] J.H. Cheon and B. Jun, *A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem*, CRYPTO 2003, LNCS **2729**, 212–225, 2003.

[9] J. Feigenbaum, *Locally Random Reductions in Interactive Complexity Theory*, Advances in Computational Complexity Theory, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **13**, American Mathematical Society, 73–98, 1993.

[10] M. Garzon and Y. Zalcstein, *The Complexity of Grigorchuk Groups with Application to Cryptography*, Theoretical Computer Sciences **88** (1991), 83–88.

[11] J. Hughes, *A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem*, ACISP 2002, LNCS **2384**, 176–189, 2002.

[12] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, and C. Park, *New Public-key Cryptosystem Using Braid Groups*, CRYPTO 2000, LNCS **1880**, 166–183, 2000.

[13] E. Lee, S.J. Lee, and S.G. Hahn, *Pseudorandomness from Braid Groups*, CRYPTO 2001, LNCS **2139**, 486–502, 2001.

[14] E. Lee and J.H. Park, *Cryptanalysis of the Public-key Encryption based on Braid Groups*, EUROCRYPT 2003, LNCS **2565**, 477–490, 2003.

[15] I. Park, *Random Walks on Finite Groups with Few Random Generators*, Electronic J. of Prob., **4** (1999), 1–11.

[16] R. Siromoney and L. Mathew, *A Public key Cryptosystem based on Lyndon Words*, Information Processing Letters **35** (1990), 33–36.

[17] A. Yamamura, *Public-Key Cryptosystems Using the Modular Group*, PKC '98, LNCS **1431**, 203–216, 1998.

[18] A. Yamamura, *A Functional Cryptosystem Using a Group Action*, ACISP '99, LNCS **1587**, 314–325, 1999.

[19] N.R. Wagner and M.R. Magyarik, *A Public-key Cryptosystem based on the Word Problem*, CRYPTO '84, LNCS **196**, 19–36, 1984.

[20] W. Woess, *Cogrowth of groups and simple Random Walks*, Arch. Math. **41** (1983), 363–370.

Appendix: Cayley Graph

The *Cayley graph* $C(G, X)$ of a group G with generating set X is a graph such that the vertices are in one-to-one correspondence with the group elements and there is a (directed) edge from the vertex labelled by v to the vertex labelled by vx for each $v \in G$ and $x \in X \cup X^{-1}$. So if G is an infinite group, its Cayley graph is also an infinite graph. See Figure 1 for the Cayley graph of the free group freely generated by $\{x, y\}$. The Cayley graph is a metric space by defining the length of each edge to be the unit length. The distance between two vertices v, w in the Cayley graph is exactly the shortest word-length of $v^{-1}w$ with respect to the given generating set.

Department of Applied Mathematics, Sejong University, Korea
E-mail address: `eonkyung@sejong.ac.kr`

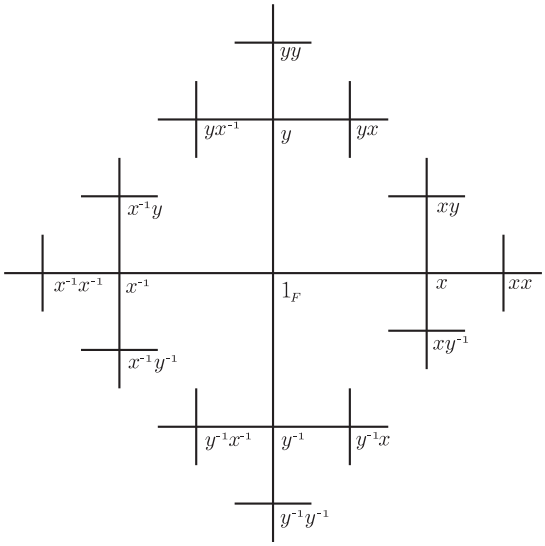

FIGURE 1. Cayley graph of the free group generated by x, y