Right-Invariance: A Property for Probabilistic Analysis of Cryptography based on Infinite Groups

Eonkyung Lee

Dept. of Applied Mathematics, Sejong University, Seoul, Korea
eonkyung@sejong.ac.kr

Abstract. Infinite groups have been used for cryptography since about twenty years ago. However, it has not been so fruitful as using finite groups. An important reason seems the lack of research on building a solid mathematical foundation for the use of infinite groups in cryptography. As a first step for this line of research, this paper pays attention to a property, the so-called right-invariance, which makes finite groups so convenient in cryptography, and gives a mathematical framework for correct, appropriate use of it in infinite groups.

1 Introduction

In modern cryptography, many schemes are designed based on groups. The most popular problems used for cryptography may be the integer factorization and discrete logarithm problems in finite groups. From these problems, many schemes have been developed. However, on quantum computer they turned out to be efficiently solved by Shor's algorithms [19].

Not to put all eggs in one basket as well as to enrich cryptography, people have attempted to use infinite groups for cryptography. Compared to finite groups, in infinite groups there are only a few types of schemes (e.g. key agreement protocol or public key encryption) [24, 9, 21–23, 13, 2] and a few ways of analyses of attacks (e.g. deterministic or empirical) [3, 10, 17, 12, 11, 16, 7]. A natural question is how we can proceed one more step. An impediment to this seems to be connected with "probability". Indeed, many cryptographic schemes have checkpoints concerning probability for their basic security, and many cases of cryptanalysis rely on probabilistic analysis. Furthermore, we do not see that we can build a provably secure cryptosystem without probability. However, there is nothing discussed seriously for it in the literature on infinite-group-based cryptography.

Our Results. When cryptosystems are designed or analyzed using infinite groups, we sometimes feel attracted to use nice properties or tools which are commonly used in finite groups. However, we do not since either it looks wrong or we are not sure if it is right or wrong. A possible approach to resolve this problem is to extract a nice property of finite groups, to generalize it in arbitrary groups, and then to construct a rigorous theory by which we can decide when we can or cannot use this property in infinite groups.

This paper follows this way focusing on 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 $x \in G$. We show that right-invariance property depends on a particular *subgroup* and the index of the subgroup determines when right-invariance can or cannot be used in infinite groups.

For the situations where this property is allowable, one may be curious about how it can be handled in practice. It is 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. As to this, we prove that most infinite groups dealt with in cryptography do not have such a probability measure. So we discuss weaker, yet practical alternatives with concrete examples. Using these, we illustrate how our theory is applied to infinite-group-based cryptography via two opposite types of situations.

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. Sec. 6 shows how the results developed in the previous sections can be applied to practice. This paper concludes with Sec. 7.

2 Preliminaries

$\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ denote the sets of all positive integers, all integers, and all real numbers, respectively. For $a < b$, $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ and $[a, b] = \{x \in \mathbb{R} \mid a \le x \le b\}$. 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 sets S and T, $S \backslash T = \{x \in S \mid x \notin T\}$. $|S|$ and 2^S denote the cardinal number of S and the collection of all subsets of S, respectively. $S^{-1} = \{x^{-1} \mid x \in S\}$. A *partition* of S means 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.

Definition 1. (a) Let $\mathcal{M} \subset 2^X$ for a non-empty set X. $\mathcal{M}$ 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 a non-empty set X, then $(X, \mathcal{M})$ is called a *measurable space* and the members of $\mathcal{M}$ are called the *measurable sets* in X.

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

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*.

Let G be a group and H a subgroup of G. For $x \in G$, let $Z_H(x) = \{y \in H \mid yx = xy\}$, which is a subgroup of H. $Hx = \{hx \mid h \in H\}$ 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 (or left) cosets of H in G. For a normal subgroup H of G, G/H denotes $\{Hx \mid x \in G\}$ and is called the *factor group of G over H*. 1_G denotes the identity of G.

Definition 3. (a) For a set X, $w = w_1 \cdots w_\ell$ is called a *reduced word on 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 of w.
(b) $F(X)$ is called 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 in Cryptography

This section shows why this paper selects right-invariance as a useful property.

Role in random self-reducibility. Informally, a problem is called *random self-reducible* if solving it on *any* instance is 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, 8] for detailed references on it and the cryptographic significance of this feature. We state it roughly in terms of the discrete logarithm problem with proper parameters; a prime p and a generator g of $\mathbb{Z}_p^*$. n is the length of p when it is represented in a bit-string.

> Let $a, b \in \mathbb{N}$ and let $\mathcal{A}$ be 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 built 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 running $\mathcal{A}$ on an input $(p, g, g^y g^x \bmod p)$, 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 $y \in \mathbb{Z}_{p-1}$

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

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 $r \in G$

$$\Pr(f(X) = 0) = \Pr(f(Xr) = 0) \quad \text{or} \quad (2)$$
$$\Pr(f(X) = 0) = \Pr(f(rX) = 0), \quad (3)$$

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

If G is a finite group and X has the uniform distribution, (2) is true. In this case, it is being used as an underlying assumption in probabilistically analyzing many kinds of cryptographic schemes. 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 on an infinite group is an analogue of the uniform distribution on a finite group.

For an arbitrary group G, let's recall the meaning of a random variable. 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 $E \subset G$. In order for (2) to hold when G is an infinite group, we see it from a measure-theoretic point of view. Namely, we consider not only 2^G but also a smaller σ-algebra $\mathcal{G}$ for P. 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 called *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 σ-algebra covering all the events in question (i.e. containing all the events in question as its measurable sets) can be constructed and there exists a right-invariant probability measure thereon, then we say that *right-invariance is allowable (or 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, $M_{\mathcal{G}}(x) = M_{\mathcal{G}}(y)$. $\square$

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 1. *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 $1_G \in A$, $x = 1_Gx \in Ax$ 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 1. *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 1 imply that right-invariance of $M_{\mathcal{G}}$ is extended to the whole space.

Theorem 2. *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 1 and 2, we have the following.

Corollary 2. *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 2, 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 3. *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 1. 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 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 2. Note that for any integer m there exists a finite-index subgroup H such that $[G : H] \geq m$ by Fact 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. $\square$

Corollary 3. *Any finitely-generated residually-finite infinite group has no universally right-invariant probability measure.*

5.2 Alternatives

From Theorem 3, 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 1 and 2 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 [25] 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 [18] and Borovik, Myasnikov, and Shpilrain [6], for any finite-index normal subgroup H of F

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

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 1, μ_s has the following property. For any $E \in \mathcal{F}$

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

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 1, $M_{\mathcal{F}}$ is a normal subgroup of F. Suppose that $P_{\mathcal{F}}$ is the right-invariant probability measure on $(F, \mathcal{F})$. Then, for any $E \in \mathcal{F}$

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

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

Fact 2. 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, $N x_1, \ldots, N x_t$, 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 2, for any $E \in \mathcal{F}$

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

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 Applications

This section shows two basic examples of how to apply our theory to real situations via recent works. These works are based on braid groups. For a survey of braid-group-based cryptography, see [14].

For $n \geq 2$, the *n-braid group* B_n can be presented by $(n-1)$-generators $\sigma_1, \ldots, \sigma_{n-1}$ and two kinds of relations: $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| > 1$ and $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ for $|i-j| = 1$. For the symmetric group S_n on n-letters, there is a natural projection $\pi : B_n \to S_n$ sending σ_i to the transposition $(i, i+1)$. $\pi(x)$ is written interchangeably with π_x. Define $P_n = \ker(\pi)$ and call its elements *pure braids*.

6.1 The case that right-invariance is not allowable

Sibert, Dehornoy, and Girault [20] proposed entity authentication schemes using braid groups: Schemes I, II, II', III. As a two-pass scheme, Scheme I is perfectly honest-verifier zero-knowledge. As three-pass protocols, the other schemes were shown to be zero-knowledge under the assumption that the probability space is right-invariant (to polynomial-time distinguishers). Their assumption was made from some experiment over a certain finite subset of B_n.

This section discusses the security of Scheme II on the whole group B_n by disproving the assumption for zero-knowledge. Analogous arguments apply to Schemes II', III. Let's see Scheme II. Prover's secrete key is $z \in B_n$, and public key is $(b, b') \in B_n^2$, where $b' = zbz^{-1}$. Its three-pass process is given in Fig. 1.

Prover		Verifier
$r \in_R B_n$		
$x = rbr^{-1}$	$\xrightarrow{\quad x \quad}$	
	$\xleftarrow{\quad \epsilon \quad}$	$\epsilon \in_R \{0,1\}$
$y = \begin{cases} r & \text{if } \epsilon = 0, \\ rz^{-1} & \text{otherwise.} \end{cases}$	$\xrightarrow{\quad y \quad}$	$x = \begin{cases} yby^{-1} & \text{if } \epsilon = 0, \\ yb'y^{-1} & \text{otherwise.} \end{cases}$

Fig. 1. Scheme II

Assumption for perfect zero-knowledge. For perfect zero-knowledge of Scheme II, it is assumed that the distributions of r and rz^{-1} are identical, where $r \in_R B_n$. We show that they cannot be identical by defining a distinguisher $\mathcal{A}$ as follows.

$$\mathcal{A}: \text{ "On an input } x \in B_n, \text{ output 1 if } x = 1_{B_n}, \text{ and 0 otherwise."} \tag{6}$$

Since verifying that any two braids are identical can be done very efficiently, $\mathcal{A}$ is also efficient. Then the situation comparing the distributions of r and rz^{-1} by using the algorithm $\mathcal{A}$ yields the atomic σ-algebra 2^{B_n} as the right-closed σ-algebra in B_n. So, right-invariance is not allowable in this situation.

Assumption for computational zero-knowledge. For computational zero-knowledge of Scheme II, it is assumed that the distributions of r and rz^{-1} are computationally indistinguishable, where $r \in_R B_n$. This means that, for any polynomial-time distinguisher $\mathcal{A}$, $\left|\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Xz^{-1}) = 1]\right|$ is negligible. Here X is a random variable over B_n.

By using the algorithm (6), we show that it is not negligible in the word length of the secrete key z with respect to the probability measure μ_s which is defined on a free group F generated by $\{x_1, \ldots, x_{n-1}\}$. Considering a natural projection $\phi : F \to B_n$ defined by $x_i \mapsto \sigma_i$, let $K = \phi^{-1}(1_{B_n})$ and let the random variable X have the probability distribution induced by μ_s. Then

$$\Pr[\mathcal{A}(X) = 1] = \mu_s(K) \geq \mu_s(1_F) = s.$$

Let $\ell = \min_{w \in \phi^{-1}(z)} |w|$, and let $w_0 \in \phi^{-1}(z)$ satisfy $|w_0| = \ell$. Then

$$\Pr[\mathcal{A}(Xz^{-1}) = 1] = \mu_s(Kw_0) = \sum_{k=0}^{\infty} \mu_s(Kw_0 \cap C_k) = \sum_{k=0}^{\infty} s(1-s)^k \frac{|Kw_0 \cap C_k|}{|C_k|},$$

where $C_k = \{w \in F \mid |w| = k\}$. Note that $Kw_0 \cap C_k = \emptyset$ for $0 \leq k < \ell$. Thus,

$$\Pr[\mathcal{A}(Xz^{-1}) = 1] = s(1-s)^\ell \sum_{k=0}^{\infty} (1-s)^k \frac{|Kw_0 \cap C_{\ell+k}|}{|C_{\ell+k}|} \leq s(1-s)^\ell \sum_{k=0}^{\infty} (1-s)^k = (1-s)^\ell.$$

Therefore, $\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Xz^{-1}) = 1] \geq s - (1-s)^\ell$.

6.2 The case that right-invariance is allowable

For notational convenience, this section assumes that n is even. Define B_ℓ (resp. B_u) be a subgroup of B_n generated by $\sigma_1, \ldots, \sigma_{n/2-1}$ (resp. $\sigma_{n/2+1}, \ldots, \sigma_{n-1}$). Likewise, define S_ℓ (resp. S_u) be a subgroup of the symmetric group S_n generated by $(1,2), \ldots, (\frac{n}{2}-1, \frac{n}{2})$ (resp. $(\frac{n}{2}+1, \frac{n}{2}+2), \ldots, (n-1,n)$). Then, any two elements chosen from B_ℓ and B_u (resp. S_ℓ and S_u) commute with each other. The *decisional Diffie-Hellman-type conjugacy problem in* B_n is defined as follows.

> Given $(a, w_\ell^{-1}aw_\ell, w_u^{-1}aw_u, x_u^{-1}x_\ell^{-1}ax_\ell x_u)$, distinguish $x_u^{-1}x_\ell^{-1}ax_\ell x_u$ and $w_u^{-1}w_\ell^{-1}aw_\ell w_u$, where $a \in B_n$, $w_\ell, x_\ell \in B_\ell$, and $w_u, x_u \in B_u$.

This problem is used as an underlying problem of a public-key encryption [13], pseudorandom number generator, and pseudorandom synthesizer [15]. Gennaro and Micciancio [10] proposed how to solve it for some parameters. We supplement their attack with quantifying the success probability of their adversary. The adversary is described as follows.

$\mathcal{A}$: "On an input $(a,\ w_\ell^{-1}aw_\ell,\ w_u^{-1}aw_u,\ x_u^{-1}x_\ell^{-1}ax_\ell x_u)$
where $a \in B_n \backslash P_n$, $w_\ell, x_\ell \in B_\ell$, and $w_u, x_u \in B_u$,
1. find any $\theta \in S_\ell$ such that $\theta^{-1}\pi_a\theta = \pi(w_\ell^{-1}aw_\ell)$;
2. output 1 if $\pi(x_u^{-1}x_\ell^{-1}ax_\ell x_u) = \theta^{-1}\pi(w_u^{-1}aw_u)\theta$, and 0 otherwise."

Define $B_\ell B_u = \{xy \mid x \in B_\ell, y \in B_u\}$ and $S_\ell S_u = \{\tau\omega \mid \tau \in S_\ell, \omega \in S_u\}$. Then they are subgroups of B_n and S_n, respectively. Let $C = Z_{S_\ell S_u}(\pi_a)$. Since θ (at Step 1) can be easily and perfectly computed and such θ satisfies $\theta^{-1}\pi(w_u^{-1}aw_u)\theta = \pi(w_u^{-1}w_\ell^{-1}aw_\ell w_u)$, the success probability equals

$$\Pr[\mathcal{A}(a, w_\ell^{-1}aw_\ell, w_u^{-1}aw_u, X^{-1}aX) = 0] = \Pr[\pi(X) \notin C\pi(w_\ell w_u)], \qquad (7)$$

where X is a random variable over $B_\ell B_u$.

Deciding whether right-invariance is allowable or not. Restricting π defined on B_n to $B_\ell B_u$ induces another natural projection $\tilde{\pi} : B_\ell B_u \to S_\ell S_u$. Define $H = \tilde{\pi}^{-1}(C)$ and $P_\ell P_u = \ker(\tilde{\pi})$. See Fig. 2. Then H is a subgroup of $B_\ell B_u$, $\Pr[\pi(X) \notin C\pi(w_\ell w_u)] = \Pr[X \notin Hw_\ell w_u]$, and $P_\ell P_u$ is a normal subgroup of $B_\ell B_u$ contained in H. Define $\mathcal{B}$ as the σ-algebra in $B_\ell B_u$ generated by all cosets of $P_\ell P_u$. Then $H \in \mathcal{B}$ and $\mathcal{B}$ is both left- and right-closed. Since $[B_\ell B_u : M_\mathcal{B}] = [B_\ell B_u : P_\ell P_u] = ((\frac{n}{2})!)^2$ is finite, we can use right-invariance property in order to compute the success probability $\Pr[X \notin Hw_\ell w_u]$.

Computing the success probability. Let $F = F(\{x_1, \ldots, x_{n/2-1}, x_{n/2+1}, \ldots, x_{n-1}\})$ be a free group. Then, there is a natural projection $\phi : F \to B_\ell B_u$ defined by $x_i \mapsto \sigma_i$. Let $K = \phi^{-1}(H)$ and $N = \phi^{-1}(P_\ell P_u)$. See Fig. 2. Let $\mathcal{F}$ be the σ-algebra in F generated by all cosets of N. Since N is a finite-index normal subgroup of F and $M_\mathcal{F} = N$, $\bar{\mu}_k$ can be used on $(F, \mathcal{F})$ for right-invariance.

$$\boxed{\begin{array}{ccccc}
(F,\bar{\mu}_k) & \xrightarrow{\phi} & (B_\ell B_u, P) & \xrightarrow{\tilde{\pi}} & S_\ell S_u \\
| & & | & & | \\
K & \longmapsto & H & \longmapsto & C \\
| & & | & & | \\
N & \longmapsto & P_\ell P_u & \longmapsto & 1_{S_\ell S_u}
\end{array}}$$

Fig. 2. Correspondences among groups

Define a set function $P : \mathcal{B} \to [0,1]$ by $P(E) = \bar{\mu}_k(\phi^{-1}(E))$ for all $E \in \mathcal{B}$. Since $\mathcal{F} = \{\phi^{-1}(E) \mid E \in \mathcal{B}\}$, P is a probability measure on $(B_\ell B_u, \mathcal{B})$. Let the random variable X in (7) induce P. Then, $\Pr[X \notin Hw_\ell w_u] = 1 - P(Hw_\ell w_u)$. On the other hand, from the definition of P and (5)

$$\left|P(Hw_\ell w_u) - [B_\ell B_u : H]^{-1}\right| = \left|\bar{\mu}_k(K\phi^{-1}(w_\ell w_u)) - [K : N]/[F : N]\right| = o(e^{-k}).$$

Therefore, the success probability of the adversary is

$$1 - [B_\ell B_u : H]^{-1} - o(e^{-k}) \leq 1 - P(Hw_\ell w_u) \leq 1 - [B_\ell B_u : H]^{-1} + o(e^{-k}).$$

Note that $[B_\ell B_u : H] = [S_\ell S_u : C]$ and $C = Z_{S_\ell S_u}(\pi_a)$. So $[B_\ell B_u : H]$ can be evaluated if π_a is specified. For all $a \in B_n \backslash P_n$, its upper bound is $(n/2)!^2$, and lower bound is $n(n-2)/8$ for $n \geq 10$ from the following theorem.

Theorem 4. *If $\alpha \in S_n \backslash \{1_{S_n}\}$, $Z_{S_\ell S_u}(\alpha)$ is a proper subgroup of $S_\ell S_u$ for $n \geq 6$. Precisely,*

$$[S_\ell S_u : Z_{S_\ell S_u}(\alpha)] \;\geq\; \begin{cases} n(n-2)/8 & \text{for } n \geq 10, \\ 3 & \text{for } n = 8, \\ 2 & \text{for } n = 6. \end{cases}$$

Proof. Let $\alpha \in S_n$, and let $\alpha_1, \ldots, \alpha_s$ be disjoint cycles in S_n such that

$$\alpha = \alpha_1 \cdots \alpha_s \quad \text{and} \quad \alpha_i \in \begin{cases} S_\ell & \text{for } 1 \leq i \leq t_\ell, \\ S_n \backslash S_\ell S_u & \text{for } t_\ell < i \leq t_u, \\ S_u & \text{for } t_u < i \leq s, \end{cases}$$

for some $0 \leq t_\ell \leq t_u \leq s$. Let

$$\alpha_\ell = \alpha_1 \cdots \alpha_{t_\ell} \in S_\ell,\ \tilde{\alpha} = \alpha_{t_\ell+1} \cdots \alpha_{t_u} \in (S_n \backslash S_\ell S_u) \cup \{1_{S_n}\},\ \alpha_u = \alpha_{t_u+1} \cdots \alpha_s \in S_u.$$

For every $1 \leq i \leq s$, let $\alpha_i = (a_{k_{i-1}+1}, \ldots, a_{k_i})$ with $k_0 = 0$. Then

$$\alpha = (a_1, \ldots, a_{k_1})(a_{k_1+1}, \ldots, a_{k_2}) \cdots (a_{k_{s-1}+1}, \ldots, a_{k_s}).$$

Note that for any $\tau \in S_n$, the cycle decomposition of $\tau\alpha\tau^{-1}$ is as follows.

$$\tau\alpha\tau^{-1} = (\tau(a_1), \ldots, \tau(a_{k_1}))(\tau(a_{k_1+1}), \ldots, \tau(a_{k_2})) \cdots (\tau(a_{k_{s-1}+1}), \ldots, \tau(a_{k_s}))$$

Table 1. Maximum of $|Z_{S_\ell}(\alpha_\ell)|$ and minimum of $[S_\ell : Z_{S_\ell}(\alpha_\ell)]$

$\frac{n}{2}$	max. of $\lvert Z_{S_\ell}(\alpha_\ell)\rvert$	min. of $[S_\ell : Z_{S_\ell}(\alpha_\ell)]$	number of cycles
3	3	2	$\ell_3 = 1$, $\ell_k = 0$ for $k \neq 3$
4	8	3	$\ell_2 = 2$, $\ell_k = 0$ for $k \neq 2$
≥ 5	$2 \times (\frac{n}{2} - 2)!$	$\frac{n}{4}(\frac{n}{2} - 1)$	$\ell_1 = \frac{n}{2} - 2$, $\ell_2 = 1$, $\ell_k = 0$ for $k \geq 3$

Let $\tau \in Z_{S_\ell S_u}(\alpha)$. Then $\tau\alpha_1\tau^{-1}, \ldots, \tau\alpha_s\tau^{-1}$ are disjoint cycles of α. If $\alpha_i \in S_\ell$, $\alpha_j \in S_n \backslash S_\ell S_u$, and $\alpha_k \in S_u$, then $\tau\alpha_i\tau^{-1} \in S_\ell$, $\tau\alpha_j\tau^{-1} \in S_n\backslash S_\ell S_u$, and $\tau\alpha_k\tau^{-1} \in S_u$ for all i, j, k. So $\tau\alpha_\ell\tau^{-1} = \alpha_\ell$, $\tau\tilde{\alpha}\tau^{-1} = \tilde{\alpha}$, and $\tau\alpha_u\tau^{-1} = \alpha_u$. Namely, $\tau \in Z_{S_\ell S_u}(\alpha_\ell) \cap Z_{S_\ell S_u}(\tilde{\alpha}) \cap Z_{S_\ell S_u}(\alpha_u)$. On the other hand, it is clear that $Z_{S_\ell S_u}(\alpha_\ell) \cap Z_{S_\ell S_u}(\tilde{\alpha}) \cap Z_{S_\ell S_u}(\alpha_u) \subset Z_{S_\ell S_u}(\alpha)$. So

$$Z_{S_\ell S_u}(\alpha) = Z_{S_\ell S_u}(\alpha_\ell) \cap Z_{S_\ell S_u}(\tilde{\alpha}) \cap Z_{S_\ell S_u}(\alpha_u).$$

Let $\alpha \neq 1_{S_n}$, and let $\tau = \tau_\ell\tau_u \in S_\ell S_u$ mean that $\tau_\ell \in S_\ell$ and $\tau_u \in S_u$.

Case 1. $\alpha_\ell\alpha_u \neq 1_{S_n}$: WLOG, let $\alpha_\ell \neq 1_{S_n}$. Define $\ell_1 = |\{1 \leq i \leq n/2 \mid \alpha_\ell(i) = i\}|$ and ℓ_i as the number of i-cycles of α_ℓ for $2 \leq i \leq n/2$. Then

$$|Z_{S_\ell}(\alpha_\ell)| \; = \; \prod_{i=1}^{n/2} i^{\ell_i}(\ell_i)!.$$

Table 1 shows the maximum values of $|Z_{S_\ell}(\alpha_\ell)|$ and the corresponding values of $[S_\ell : Z_{S_\ell}(\alpha_\ell)]$ over $\alpha_\ell \in S_\ell\backslash\{1_{S_n}\}$. Since $[S_\ell S_u : Z_{S_\ell S_u}(\alpha)] \geq [S_\ell S_u : Z_{S_\ell S_u}(\alpha_\ell)] = [S_\ell : Z_{S_\ell}(\alpha_\ell)]$, for all $\alpha \in S_n$ such that $\alpha_\ell\alpha_u \neq 1_{S_n}$

$$[S_\ell S_u : Z_{S_\ell S_u}(\alpha)] \;\geq\; \begin{cases} n(n-2)/8 & \text{for } n \geq 10, \\ 3 & \text{for } n = 8, \\ 2 & \text{for } n = 6. \end{cases}$$

Case 2. $\alpha_\ell\alpha_u = 1_{S_n}$: In this case, $Z_{S_\ell S_u}(\alpha) = Z_{S_\ell S_u}(\tilde{\alpha})$. Define

$$A_\ell = \left\{1 \leq i \leq \frac{n}{2} \mid \tilde{\alpha}(i) \neq i\right\}, \; A_u = \left\{\frac{n}{2} < i \leq n \mid \tilde{\alpha}(i) \neq i\right\}, \; N_\ell = |A_\ell|, \; N_u = |A_u|.$$

WLOG, we assume $1 \leq N_u \leq N_\ell \leq n/2$. Note that for any $\tau_\ell\tau_u \in Z_{S_\ell S_u}(\tilde{\alpha})$, $\{(i, \tau_\ell(i)) \mid i \in A_\ell\}$ is uniquely determined by $\{(i, \tau_u(i)) \mid i \in A_u\}$. So

$$\begin{aligned} |Z_{S_\ell S_u}(\tilde{\alpha})| \leq \left(\frac{n}{2} - N_\ell\right)! \left(\frac{n}{2} - N_u\right)! N_u! &\leq \begin{cases} (n/2-1)!^2 & \text{if } N_u < n/2, \\ (n/2)! & \text{if } N_u = n/2, \end{cases} \\ &\leq \begin{cases} (n/2-1)!^2 & \text{if } n \geq 8, \\ 6 & \text{if } n = 6. \end{cases} \end{aligned}$$

Therefore, for all $\alpha \in S_n\backslash\{1_{S_n}\}$ such that $\alpha_\ell\alpha_u = 1_{S_n}$

$$[S_\ell S_u : Z_{S_\ell S_u}(\alpha)] \;\geq\; \begin{cases} (n/2)^2 & \text{if } n \geq 8, \\ 6 & \text{if } n = 6. \end{cases}$$

From Cases 1 and 2, the conclusion follows. $\square$

7 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 more various 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.

Acknowledgements

The author would like to thank Prof. Kouichi Sakurai and the anonymous referees for helpful remarks and suggestions.

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. S.R. Blackburn, *Cryptanalysis of two cryptosystems based on group actions*, ASIACRYPT '99, LNCS **1716**, 52–61, 1999
4. M. Blum and S. Micali, *How to Generate Cryptographically Strong Sequences of Pseudorandom Bits*, SIAM J. Comput. **13**, 850–864, 1984
5. A.V. Borovik, A.G. Myasnikov, and V.N. Remeslennikov, *Multiplicative Measures on Free Groups*, To appear in Internat. J. Algebra Comp.
6. A.V. Borovik, A.G. Myasnikov, and V. Shpilrain, *Measuring Sets in Infinite Groups*, Contemporary Mathematics **298**, 21–42, 2002
7. J.H. Cheon and B. Jun, *A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem*, CRYPTO 2003, LNCS **2729**, 212–225, 2003
8. J. Feigenbaum, *Locally Random Reductions in Interactive Complexity Theory*, Advances in Computational Complexity Theory, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **13**, AMS, 73–98, 1993
9. M. Garzon and Y. Zalcstein, *The Complexity of Grigorchuk Groups with Application to Cryptography*, Theoretical Computer Sciences **88**, 83–88, 1991

10. R. Gennaro and D. Micciancio, *Cryptanalysis of a Pseudorandom Generator Based on Braid Groups*, EUROCRYPT 2002, LNCS **2332**, 1–13, 2002
11. D. Hofheinz and R. Steinwandt, *A Practical Attack on Some Braid Group based Cryptographic Primitives*, PKC 2003, LNCS **2567**, 187–198, 2003
12. J. Hughes, *A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem*, ACISP 2002, LNCS **2384**, 176–189, 2002
13. 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
14. E. Lee, *Braid Groups in Cryptology*, IEICE Trans. Fund. **E87-A**, 986-992, 2004
15. E. Lee, S.J. Lee, and S.G. Hahn, *Pseudorandomness from Braid Groups*, CRYPTO 2001, LNCS **2139**, 486–502, 2001
16. E. Lee and J.H. Park, *Cryptanalysis of the Public-key Encryption based on Braid Groups*, EUROCRYPT 2003, LNCS **2565**, 477–490, 2003
17. S. J. Lee and E. Lee, *Potential Weaknesses of the Commutator Key Agreement Protocol based on Braid Groups*, EUROCRYPT 2002, LNCS **2332**, 14–28, 2002
18. I. Pak, *Random Walks on Finite Groups with Few Random Generators*, Electronic J. of Prob. **4**, 1–11, 1999
19. P.W. Shor, *Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a quantum Computer*, SIAM J. Comput. **26**, 1484–1509, 1997
20. H. Sibert, P. Dehornoy, and M. Girault, *Entity Authentication Schemes Using Braid Word Reduction*, Proceedings International Workshop on Coding and Cryptography, March 24-28 2003, Versailles (France), 153–164
21. R. Siromoney and L. Mathew, *A Public key Cryptosystem based on Lyndon Words*, Information Processing Letters **35**, 33–36, 1990
22. A. Yamamura, *Public-Key Cryptosystems Using the Modular Group*, PKC '98, LNCS **1431**, 203–216, 1998
23. A. Yamamura, *A Functional Cryptosystem Using a Group Action*, ACISP '99, LNCS **1587**, 314–325, 1999
24. N.R. Wagner and M.R. Magyarik, *A Public-key Cryptosystem based on the Word Problem*, CRYPTO '84, LNCS **196**, 19–36, 1984
25. W. Woess, *Cogrowth of groups and simple Random Walks*, Arch. Math. **41**, 363–370, 1983

Appendix: Cayley Graph

The *Cayley graph* $C(G, X)$ of a group G with a 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. 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.