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

Eonkyung Lee

Sejong University, Korea

	Finite-group-based cryptography (late 1970s $\sim$)	Infinite-group-based cryptography (early 1980s $\sim$)
Types of schemes	Various	A few (e.g. KAP, PKE)
Provably secure schemes	Many	None

Q. Why is not cryptography fruitful in infinite groups as in finite groups?

- An impediment is connected with probability.

  c.f.) The uniform distribution is popularly used in finite groups, but not available in infinite groups.

Our motivation. In infinite-group-based cryptography, probability has not been seriously discussed.

Our Results

(1) Choose a probability-theoretic property, right-invariance, from finite groups; and formalize the notion in arbitrary groups.

(2) Explore right-invariance property in infinite groups.

(3) Discuss probability measures for right-invariance and show application.

A Property Widely Used in Cryptography

Right-invariance of finite groups

- $\Pr[\mathcal{A}(p, g, g^X) = X] = \Pr[\mathcal{A}(p, g, g^X g^r) = X + r] \quad \forall r \in \mathbb{Z}_{p-1}$
- Usage: random self-reducibility, ZK proofs, PRF, PKE, HCP, ...

Generalization to arbitrary groups

- $\Pr[f(X) = 0] = \Pr[f(Xr) = 0] \quad \forall r \in G$
- It is true if G is finite and X has the uniform distribution.
  But, it is not always true if G is infinite.

A mathematical framework for correct, appropriate use of it in infinite groups is needed.

Warming up for Measure-theoretic Approach

Def. A collection $\mathcal{M}$ of subsets of X is a σ-algebra in X if

(i) $X \in \mathcal{M}$,

(ii) $E \in \mathcal{M}$ implies $X - E \in \mathcal{M}$,

(iii) $E_1, E_2, \ldots \in \mathcal{M}$ implies $\cup_{i=1}^{\infty} E_i \in \mathcal{M}$.

$(X, \mathcal{M})$ is a measurable space, $E \in \mathcal{M}$ is a measurable set in X.

e.g.) 2^X: atomic σ-algebra in X

Def. $\mu : \mathcal{M} \to [0, 1]$ is a probability measure on $\mathcal{M}$ if

$$\mu(X) = 1 \quad \text{and} \quad \mu(\coprod_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i).$$

$(X, \mathcal{M}, \mu)$ is a probability space.

Formalizing Right-invariance in Measure Theory

Def. For a probability space $(G, \mathcal{G}, P)$

(a) $E \in \mathcal{G}$ is right-invariant if for any $r \in G$

$$Er = \{xr \mid x \in E\} \in \mathcal{G} \quad \text{and} \quad P(Er) = P(E).$$

(b) $(G, \mathcal{G}, P)$ (or P) is right-invariant if every measurable set is right-invariant.

Our Results

(1) Formalize the notion of right-invariance property in arbitrary groups.

(2) Explore right-invariance property in finitely generated infinite groups analyzing the structure of their σ-algebra.

(3) Discuss probability measures for right-invariance and show application.

σ-algebra in Infinite Groups

Let G be a finitely generated infinite group and $\mathcal{G}$ a σ-algebra in G.

Def. For $x \in G$, $M_{\mathcal{G}}(x) = \cap_{x \in A \in \mathcal{G}} A$.

Property of $M_{\mathcal{G}}(x)$

(a) $M_{\mathcal{G}}(x)$ is the smallest measurable set containing x.

(b) Every measurable set is partitioned into $M_{\mathcal{G}}(x)$'s.

Right-invariance of Infinite Groups

Let G be a finitely generated infinite group and $\mathcal{G}$ a σ-algebra in G.

Def. $\mathcal{G}$ is right-closed if $\forall A \in \mathcal{G},\ \forall x \in G,\ Ax = \{ax \mid a \in A\} \in \mathcal{G}$.

Property of $M_{\mathcal{G}}(1_G) \stackrel{\text{def}}{=} M_{\mathcal{G}}$. The following are equivalent.

(a) $\mathcal{G}$ is a right-closed σ-algebra in G.

(b) $M_{\mathcal{G}}(x) = M_{\mathcal{G}}x$ for any $x \in G$.

(c) $M_{\mathcal{G}}$ is a subgroup of G, and $\mathcal{G}$ is generated by its right cosets.

Theorem. $(G, \mathcal{G}, P)$ is right-invariant iff $M_{\mathcal{G}}$ is right-invariant.

Our Results

(1) Formalize the notion of right-invariance property in arbitrary groups.

(2) Explore right-invariance property in finitely generated infinite groups.

(3) Discuss probability measures for right-invariance in two cases (ideal, practical), and show application.

Ideal Measure

Q. What are concrete examples of probability measure which is both useful and practical for right-invariance?

For a group G, to get a right-invariant probability measure

- is easy on a single right-closed σ-algebra $\mathcal{G}$ with $[G : M_{\mathcal{G}}] < \infty$,
- is meaningful on all right-closed σ-algebras $\mathcal{G}$ with $[G : M_{\mathcal{G}}] < \infty$.

Def. P defined on $(G, 2^G)$ is universally right-invariant on G if $P(H) = P(Hx)$ for any finite-index $H < G$ and any $x \in G$.

Note. Most of interesting infinite groups

- are finitely generated, and
- have infinitely many finite-index subgroups.

e.g.) free groups, groups of automorphisms of free groups, braid groups, ...

Theorem. If G is a finitely-generated group with infinitely many finite-index subgroups, then G has no universally right-invariant probability measure.

Therefore, as a probability measure for right-invariance, we have to use alternatives to the universally right-invariant probability measure.

Practical Measure

Given a group G, a good alternative may be P on $(G, 2^G)$ such that for any right-invariant $(G, \mathcal{G}, P_{\mathcal{G}})$ and for any $E \in \mathcal{G}$

$$|P(E) - P_{\mathcal{G}}(E)|$$

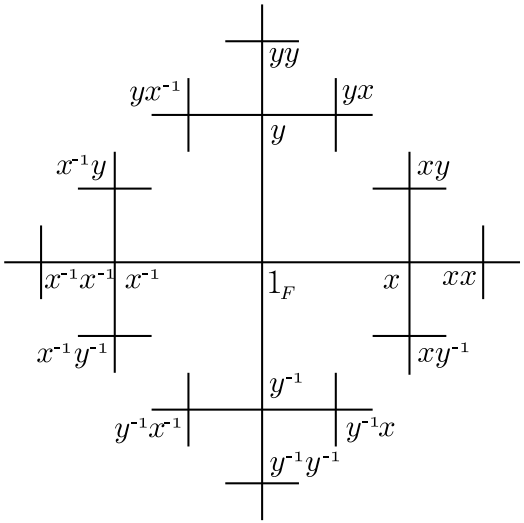
is "small".

- $|P(E) - P_{\mathcal{G}}(E)|$ will be presented in the factors coming from the characteristics of G, $\mathcal{G}$, P.
- We view P as a family $P = \{P_\alpha\}_{\alpha \in \mathcal{A}}$.

Our alternative. A family of probability measures $P = \{P_\alpha\}_{\alpha \in \mathcal{A}}$ on $(G, 2^G)$ such that for any right-invariant $(G, \mathcal{G}, P_{\mathcal{G}})$ and for any $E \in \mathcal{G}$

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

Examples of Our Alternative



Cayley graph $C(F, \{x, y\})$

- F: free group generated by a finite set X
- W_s: no-return random walk on $C(F, X)$ with stopping probability $0 < s < 1$
  - W_s generates all words of F.
  - The longer the word is, the lower its occurrence probability is.

e.g.1. $\mu_s(w) = \Pr[W_s \text{ walks from } 1_F \text{ to } w]$.

e.g.2. $\bar{\mu}_k(w) = \begin{cases} 0 & \text{if } w \in B_k = \{w \in F \mid |w| \leq k\}, \\ \frac{\mu_s(w)}{\mu_s(F - B_k)} & \text{otherwise.} \end{cases}$

Property of $\mu = \{\mu_s\}_{0<s<1}$ [Woess, Borovik-Myasnikov-Remeslennikov]

For any right-invariant $(G, \mathcal{G}, P_{\mathcal{G}})$ and for any $E \in \mathcal{G}$,

$$\lim_{s \to 0} |\mu_s(E) - P_{\mathcal{G}}(E)| = 0.$$

Property of $\bar{\mu} = \{\bar{\mu}_k\}_{k \in \mathbb{N}}$ [Park, Borovik-Myasnikov-Shpilrain]

If $(G, \mathcal{G}, P_{\mathcal{G}})$ is both left- and right-invariant, or
if $(G, \mathcal{G}, P_{\mathcal{G}})$ is right-invariant and $M_{\mathcal{G}}$ includes a finite-index normal subgroup of G, then for any $E \in \mathcal{G}$

$$\left|\bar{\mu}_k(E) - P_{\mathcal{G}}(E)\right| = o(e^{-k}).$$

Application: Braid-group-based Cryptography

B_n: non-commutative infinite group with $(n-1)$-generators

Decisional Diffie-Hellman problem (D-DHP) in B_n

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

B_ℓ, B_u: subgroups of B_n commuting with each other

- $w_\ell w_u = w_u w_\ell \in B_\ell B_u = \{xy \mid x \in B_\ell,\ y \in B_u\}$

Gennaro-Micciancio's Algorithm

Gennaro-Micciancio proposed how to solve the D-DHP in B_n (2002).

Idea. Easy to compute $\pi(w_u)$ from $(a, w_u^{-1} a w_u)$

- Symmetric group on n-letters, S_n, has $(n-1)$-generators
- There is a natural projection $\pi : B_n \to S_n$

Algorithm $\mathcal{A}$: Let $a \in B_n$ with $\pi(a) \neq 1_{S_n}$.

- Input: $(a,\ w_\ell^{-1} a w_\ell,\ w_u^{-1} a w_u,\ x_u^{-1} x_\ell^{-1} a x_\ell x_u)$
- Output $\begin{cases} 1 & \text{if } \pi(x_u^{-1} x_\ell^{-1} a x_\ell x_u) = \pi(w_u^{-1} w_\ell^{-1} a w_\ell w_u) \\ 0 & \text{otherwise} \end{cases}$

Computing the Success Probability

Success probability that $\mathcal{A}$ solves the D-DHP in B_n

$$\Pr_{X \in B_\ell B_u}[\pi(X^{-1}aX) \neq \pi(w_u^{-1}w_\ell^{-1}aw_\ell w_u)] = \Pr_{X \in B_\ell B_u}[X \in H].$$

Step 1. Construct a σ-algebra, $\mathcal{B}$, in $B_\ell B_u$ such that

(i) $\mathcal{B}$ is right-closed,

(ii) $H \in \mathcal{B}$,

(iii) $[B_\ell B_u : M_{\mathcal{B}}] < \infty$.

Step 2. Define a probability measure P on $(B_\ell B_u, \mathcal{B})$.

- Let F be a free group with $(n-2)$-generators.
- There is a natural projection $\phi : F \to B_\ell B_u$.
- Let $\bar{\mu}_k$ be the atomic probability measure on F induced by W_s.
- $P = \bar{\mu}_k \circ \phi^{-1}$

Success probability of $\mathcal{A} = P(H)$ depends on $a \in B_n$.

- Upper bound: $1 + o(e^{-k}) - ((\frac{n}{2})!)^{-2}$
- Lower bound: $1 - o(e^{-k}) - \begin{cases} 8/n(n-2) & \text{for } n \geq 10, \\ 1/3 & \text{for } n = 8, \\ 1/2 & \text{for } n = 6. \end{cases}$

Conclusions

For right-invariance of infinite groups, we showed

(1) it corresponds to the uniform distribution over all the right cosets of some finite-index subgroup,

(2) how to use it for a given situation,

(3) non-existence of universally right-invariant probability measure,

(4) alternatives to universally right-invariant probability measure (Application: To evaluate success probability of an attack).