ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

Variations on Pseudo-Free Groups

Takato Hirano and Keisuke Tanaka

January 2007, C–239

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Variations on Pseudo-Free Groups

Takato Hirano and Keisuke Tanaka *

Department of Mathematical and Computing Sciences
Tokyo Institute of Technology
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{hirano6, keisuke}@is.titech.ac.jp

January 15, 2007

Abstract

The notion of the pseudo-free group was informally introduced by Hohenberger [Hoh03], and was formalized by Rivest [Riv04a]. Rivest showed that many cryptographic assumptions (e.g. the RSA assumption, the strong RSA assumption, the discrete logarithm problem and so on) hold in pseudo-free groups. In this paper, we point out the fact that in the definition by Rivest, many cryptographic assumptions except for the RSA assumption do not hold. The reason is that the equation in pseudo-free groups contains no integer-valued exponent variables. Rivest probably supposed that we may not need the notion of exponent variables since the adversary can choose himself equations. In this paper, we also study some of the variations introduced in [Riv04a, Section 5-4] [Riv04b]. Using these variations, we show several properties for pseudo-free groups. Furthermore, we describe the subgroup of pseudo-free groups.

Keywords: pseudo-free groups, free groups, the RSA assumption, the strong RSA assumption, the discrete logarithm problem, group equation.

1 Introduction

The notion of pseudo-free groups was first introduced by Hohenberger [Hoh03]. She did only define informally. She used such groups to study the transitive signature schemes, and studied their variants where inversion is not efficiently computable, at least by the adversary.

After her works, the notion of pseudo-free groups is formalized by Rivest, and he presented an explicit definition [Riv04a]. He showed that the pseudo-freeness is a very strong assumption, and it implies many other computational assumptions typically used in cryptography, like the hardness of the computing discrete logarithms, the RSA assumption, and the strong RSA assumption[1].

The concept of the pseudo-freeness is the followings:

- Using a strong assumption that subsumes many other common cryptographic assumptions (like the discrete logarithm problem) may make proof easier.
- Assuming pseudo-freeness allows one to capture natural security proofs in a plausible framework.
- What assuming pseudo-freeness is implied by a cryptographic application? In other words, what are its necessary (and sufficient) conditions?

[*] Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 16092206.

[1] Many cryptographic problems can be found in the Appendix A.

Rivest left many open problems: for example, do pseudo-free groups exist? Rivest suggested the RSA group $(\mathbb{Z}/n\mathbb{Z})^\times$ (where $n = pq$ is the product of two large primes) as a possible candidate pseudo-free abelian groups. Micciancio [Mic05] solved Rivest's conjecture and proved that $(\mathbb{Z}/n\mathbb{Z})^\times$ is pseudo-free under the strong RSA assumption, at least when $n = pq$ is the product two safe primes (that is, odd primes such that $p' = (p-1)/2$ and $q' = (q-1)/2$ are also prime). He also showed that no adversary can efficiently compute an unsatisfiable system of equations together with a solution in the given pseudo-free group.

In this paper, we point out an important fact that many cryptographic assumptions except for the RSA assumption do not hold in the definition proposed by Rivest. The reason is that the equation chosen by an adversary contain no integer-valued exponent variables. For this reason, we cannot adapt the definition to several cryptographic assumptions which contain both element-valued variables and integer-valued exponent variables (like the strong RSA problem).

Rivest probably supposed that we may not need the notion of exponent variables since the adversary can choose himself equations. In this paper, we also study some of the variations introduced in [Riv04a, Section 5-4] [Riv04b], say pseudo-free with generalized exponential expression and weakly pseudo-free, and show several properties for pseudo-free with generalized exponential expression and weakly pseudo-free. In particular, in order to describe the intersection problem for cyclic subgroups, we consider the subgroup of pseudo-free groups, and give a result for subgroups of pseudo-free groups.

This paper is organized as follows: In Section 2 we introduce basic definitions and notations for groups. In Section 3 we see the definition of a pseudo-free group, and consider several variants of pseudo-free groups. In Section 4 we show many properties on pseudo-free groups. In Section 5 we conclude and provide some open problems.

2 Preliminaries

2.1 Groups and Computational Groups

First, we denote the definition of a (mathematical) group.

Definition 2.1. *((Mathematical) Groups) A group $G = (S, \circ)$ consists of a set S of elements, and a binary operator $\circ$ defined on S, such that:*

- **Closure:** $\forall x, y \in S$, $x \circ y \in S$.
- **Associativity:** $\forall x, y, z \in S$, $x \circ (y \circ z) = (x \circ y) \circ z$.
- **Identity:** $\exists e \in S$ *such that* $x \circ e = e \circ x = x$, *for* $\forall x \in S$.
- **Inverse:** $\forall x \in S$, $\exists y \in S$ *such that* $x \circ y = y \circ x = e$.

G is called abelian if $\circ$ holds the following:

- **Commutative:** $\forall x, y \in S$, $x \circ y = y \circ x$.

We use notations as follows: ab means $a \circ b$. The inverse of x is denoted x^{-1}. Let G also denote the set S. A group G is finite if and only if $|G| < \infty$ (i.e. $|S| < \infty$). We use the usual exponent notation: a^m is the word $aa \cdots a$ of length m, and a^{-m} is the corresponding inverse word $a^{-1}a^{-1} \cdots a^{-1}$ of length m.

A mathematical group G has some representation $[G]$. In particular, when we use some groups in cryptography, we have to implement some representation: for example, $(\mathbb{Z}/p\mathbb{Z})^\times$, which p is a prime, is represented by $\{1, \ldots, p-1\}$, as usual. We call such a representation $[G]$ a *computational group.* To demand for a computational group $[G]$ is that several operations in $[G]$ must be performed on polynomial-time. The formal definition of a computational group is the following:

Definition 2.2. *(Computational (Mathematical) Groups) A computational group $[G]$ is defined as the representation for an underlying mathematical group $G = (S, \circ)$, and it provides polynomial time algorithms for all of the following operations:*

- **Membership Test** *Given a string $[x]$, determine whether $[x] \in [G]$.*
- **Composition:** *Given $[x], [y] \in [G]$, compute $[x] \circ [y]$.*
- **Identity:** *Compute the identity element $[e] \in [G]$.*
- **Inverse:** *Given $x \in [G]$, compute $[x^{-1}] \in [G]$.*
- **Equality Test:** *Given $[x], [y] \in [G]$, determine whether $[x] = [y]$.*
- **Sampling:** *(Only if G is finite.) Return $[x] \in [G]$ chosen uniformly at random from $[G]$, or in a manner that is indistinguishable from uniformly at random to a probabilistic polynomial-time adversary. We denote such a procedure as $[x] \in_R [G]$.*

Many groups used in cryptography implies the notion of computational groups. Henceforth, if a set G is defined as a group then we assume that G also means a computational group $[G]$ with the identity 1.

2.2 Free Groups

Free groups are infinite groups with a set of generators that there is no non-trivial relationship. Free groups are defined formally as follows.

Definition 2.3. *(Free Groups) Let $A = \{a_1, a_2, \ldots, a_k\}$ be a nonempty set of distinct symbols. For each a_i, let a_i^{-1} be a new symbol representing the inverse of a_i, and let $A^{-1} = \{a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1}\}$. We define a word on $\tilde{A} = A \cup A^{-1}$ ($A \cap A^{-1} = \phi$) to be a finite string of symbols $\tilde{A}$. (where we allow a word to be the empty word ϵ). For words ab and c, define the concatenation $ab \circ c$ by abc. Then a set $W(\tilde{A})$ of all words in $\tilde{A}$ is a semigroup. Further, a word is called reduced if no cancellation in this word can be made; two words are called equivalent if they have the same reduced form. Then, a set of the equivalent class of $W(\tilde{A})$ is a group. We call such a group a free group, denote $F(A)$. If abelian, $FA(A)$.*

We note that if $A \subseteq B$, then $F(A)$ is a subgroup of $F(B)$.

Remark 2.1. *It is well-known that $FA(a_1, a_2, \ldots, a_n)$ is isomorphic to the n-fold direct sum $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Therefore, we can identify an element $a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n}$ of $FA(a_1, a_2, \ldots, a_n)$ with the vector $(e_1, e_2, \ldots, e_n)$, and implement $\circ$ with the vector addition.*

A free group has no surprising or anomalous identities. The only truths are implied by the axioms of the group theory.

2.3 Equations in Free Groups

Before we denote the definition of a pseudo-free group, we consider the equation in free groups. For a detailed introduction to equations below in free groups the reader is referred to [LS77]. We note that if we use such equations in pseudo-free group, we see that various problems arise then.

Let $x_1, x_2, \ldots, x_m$ denote variables ranging over $F(A)$. An equation in $F(A)$ takes the form $w_1 = w_2$ where w_1 and w_2 are words formed from the symbols of $F(A)$ and from the variables $x_1, x_2, \ldots, x_m$. One can always put such equations in a reduced form of the form $w = 1$ for some word w.

Equations that have solutions in the free group are called satisfiable, otherwise unsatisfiable.

In 1982 Makanin [Mak82] showed that it is decidable whether or not an equation in the free group is satisfiable. More recently Gutiérrez has shown that this problem is decidable in PSPACE [Gut00].

When the free group is the abelian, it is easy to determine whether a given equation is satisfiable: the equation can always be rewritten in the form:

$$x_1^{d_1} x_2^{d_2} \cdots x_m^{d_m} = a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n}$$

for integers $d_1, d_2, \ldots, d_m, e_1, e_2, \ldots, e_n$. Such an equation is satisfiable over $F(A)$ if and only if for all i, $1 \leq i \leq n$, we have $\gcd(d_1, d_2, \ldots, d_m) \mid e_i$. An equation that is satisfiable over $F(A)$ is also satisfiable over $FA(A)$ (but not necessarily conversely). This is useful since it provides an easy way to prove that an equation is unsatisfiable over a free group. Therefore we prove that it is unsatisfiable over the corresponding free abelian group.

3 Pseudo-Free Groups

Intuitively, we say that a finite group G is a pseudo-free if it is indistinguishable from a free group. Informally, a finite group G is pseudo-free if a probabilistic polynomial-time adversary can not efficiently procedure an equation E and together with a solution in G where E has no solution in the corresponding free groups. If G is a pseudo-free group, then many cryptographic assumptions which hold in free groups satisfy over G. Hence, the pseudo-freeness means a strong assumption.

3.1 Definition of Pseudo-Free Groups

Rivest gave the following definition of pseudo-freeness.

Definition 3.1. *(Pseudo-Free Groups (PFG)) A family of computational groups $\{G_\lambda\}_{\lambda \in \Lambda}$ is pseudo-free if for any set of polynomial size $|A| = p(k)$ (where p is a polynomial and k is a security parameter), and any probabilistic polynomial-time algorithm $\mathcal{A}$ in k, the following holds. Let $\lambda \in \Lambda(k)$ be a randomly chosen group index. Let $\alpha_1, \alpha_2, \ldots, \alpha_{p(k)}$ be $|A|$ group elements chosen independently at random according to the computational group sampling procedure. Then, the probability that $\mathcal{A}(G_\lambda, \alpha_1, \alpha_2, \ldots, \alpha_{p(k)}) = (E, \beta_1, \beta_2 \ldots, \beta_{p'(k)})$ (where p' is a polynomial) outputs an unsatisfiable equation*

$$E = E(x_1, x_2, \ldots, x_{p'(k)}; a_1, a_2, \ldots, a_{p(k)})$$

over $F(A)$ (where $x_1, x_2, \ldots, x_{p'(k)} \in X$ and $a_1, a_2, \ldots,\ a_{p(k)} \in A$ are variables and generators, respectively, over $F(A)$) together with a solution $\beta_1, \beta_2, \ldots, \beta_{p'(k)} \in G_\lambda$ to the equation

$$E' = E'(x_1, x_2, \ldots, x_{p'(k)}; \alpha_1, \alpha_2 \ldots, \alpha_{p(k)})$$

over G_λ, is negligible in k.

For efficiency in describing his equation, we allow the adversary to use exponential expression, for example, $a((ab)^{-2}x^5)^3 = 1$. If a pseudo-free group is abelian, it is equivalent to $x^{15} = a^5 b^6$.

3.2 Variants of Pseudo-Free Groups

We observe the fact that all of the equations of many cryptographic assumptions except for the RSA problem contain integer-valued exponential variables. On the other hand, the equation for this definition do not contain integer-valued exponent variables. So it is hard that by using this definition, we describe whether these problems hold in pseudo-free groups. Rivest probably thought that we may not need exponent variables since the adversary can choose himself equations: he expected that in his definition, the equation implies ones with exponent variables. However, if the equation does not contain any exponent variables, we cannot describe the problems which have no group element variables (e.g. the order problem).

In order to solve the problems as mentioned above, we use generalized exponential expression. This notion is a natural extension to exponential expression.

The expression allows the equations to contain integer-valued exponent variables, for example: $a((ab)^e y)^f = x^2$ where x and y are variables (over the group), a and b are constants (group elements), and e and f are integer-valued variables. However, we cannot determine whether a given equation with the above expression is satisfiable over free groups. We nonetheless allow an adversary to use one.

The following definition with generalized exponential expression was also introduced in [Riv04a, Section 5-4]. Perhaps, using this definition, Rivest showed that many cryptographic assumptions hold in pseudo-free groups.

Definition 3.2. *(Pseudo-Free Groups with Generalized Exponential Expression (PFGwGEE)) A family of computational groups $\{G_\lambda\}_{\lambda\in\Lambda}$ is pseudo-free if for any set of polynomial size $|A| = p(k)$ (where p is a polynomial and k is a security parameter), and any probabilistic polynomial-time algorithm $\mathcal{A}$ in k, the following holds. Let $\lambda \in \Lambda(k)$ be a randomly chosen group index. Let $\alpha_1, \alpha_2, \ldots, \alpha_{p(k)}$ be $|A|$ group elements chosen independently at random according to the computational group sampling procedure. Then, the probability that $\mathcal{A}(G_\lambda, \alpha_1, \alpha_2, \ldots, \alpha_{p(k)}) = (E, \beta_1, \beta_2, \ldots, \beta_{p_1(k)}; \gamma_1, \gamma_2, \ldots, \gamma_{p_2(k)})$ (where p_1 and p_2 are polynomials) outputs an unsatisfiable equation*

$$E = E(x_1, x_2, \ldots, x_{p_1(k)}; a_1, a_2, \ldots, a_{p(k)}; z_1, z_2, \ldots, z_{p_2(k)})$$

over $F(A)$ (where $x_1, x_2, \ldots, x_{p_1(k)} \in X$, $a_1, a_2, \ldots, a_{p(k)} \in A$ and $z_1, z_2, \ldots, z_{p_2(k)} \in X_{\mathbb{Z}}$ are variables, generators, and integer-valued variables, respectively, over $F(A)$) together with a solution $\beta_1, \beta_2, \ldots, \beta_{p_1(k)} \in G_\lambda; \gamma_1, \gamma_2, \ldots, \gamma_{p_2(k)} \in \mathbb{Z}$ to the equation

$$E' = E'(x_1, x_2, \ldots, x_{p_1(k)}; \alpha_1, \alpha_2, \ldots, \alpha_{p(k)}; z_1, z_2, \ldots, z_{p_2(k)})$$

over G_λ, is negligible in k.

Remark 3.1. *If a pseudo-free group G is abelian, then the equation can be always rewritten in the form:*

$$x_1^{z_1} x_2^{z_2} \cdots x_m^{z_m} = a_1^{z_{m+1}} a_2^{z_{m+2}} \cdots a_n^{z_{m+n}}.$$

We compare Definition 3.1 with the definition above. Then, we obtain the following proposition.

Theorem 3.1. *If a finite group G is pseudo-free with generalized exponential expression, G implies pseudo-free.*

Proof. If G is pseudo-free with generalized exponential expression, any probabilistic polynomial-time adversary never outputs an equation E together with a solution. Therefore, the adversary never solves the equation with a non-trivial restriction that $(z_1, z_2, \ldots, z_{p_2(k)}) = (d_1, d_2, \ldots, d_{p_2(k)})$, where each d_i is a fixed integer (i.e. set all integer-valued exponent variables as fix integers). The equation with above restriction is just the equation for pseudo-free. Hence, if G is a pseudo-free with generalized exponential expression, no probabilistic polynomial-time adversary solves the equation for pseudo-free. That is, a pseudo-free group with generalized exponential expression implies a pseudo-free group. □

3.3 The Other Definitions

By the way, in [Riv04b] Rivest suggested an interesting formalization for pseudo-free groups. The notion is a natural extension to pseudo-free groups. We find that the following definition depends on no adversary being able to make any non-trivial identity.

Definition 3.3. *(Weakly Pseudo-Free Groups (WPFG)) A family of computational groups* $\{G_\lambda\}_{\lambda\in\Lambda}$ *is (weakly) pseudo-free if for any set of polynomial size* $|A| = p(k)$ *(where* p *is a polynomial and* k *is a security parameter), and any probabilistic polynomial-time algorithm* $\mathcal{A}$ *in* k*, the following holds. Let* $\lambda \in \Lambda(k)$ *be a randomly chosen group index. Let* $\alpha_1, \alpha_2, \ldots, \alpha_{p(k)}$ *be* $|A|$ *group elements chosen independently at random according to the computational group sampling procedure. Then, the probability that* $\mathcal{A}(G_\lambda, \alpha_1, \alpha_2, \ldots, \alpha_{p(k)}) = (E, \gamma_1, \gamma_2, \ldots, \gamma_{p'(k)})$ *(where* p' *is a polynomial) outputs an unsatisfiable equation*

$$E = E(a_1, a_2, \ldots, a_{p(k)}; z_1, z_2, \ldots, z_{p'(k)})$$

over $F(A)$ *(where* $a_1, a_2, \ldots, a_{p(k)} \in A$ *and* $z_1, z_2, \ldots, z_{p'(k)} \in X_{\mathbb{Z}}$ *are generators and integer-valued variables, respectively, over* $F(A)$*) together with a solution* $\gamma_1, \gamma_2, \ldots, \gamma_{p'(k)} \in \mathbb{Z}$ *to the equation*

$$E' = E'(\alpha_1, \alpha_2, \ldots, \alpha_{p(k)}; z_1, z_2, \ldots, z_{p'(k)})$$

over G_λ*, is negligible in* k*.*

Remark 3.2. *If a weakly pseudo-free group* G *is abelian, then the equation can be always rewritten in the form:*

$$a_1^{z_1} a_2^{z_2} \cdots a_n^{z_n} = 1.$$

Similarly, we compare Definition 4.1 with the definition above. Then, we obtain the following proposition:

Theorem 3.2. *If a finite group* G *is pseudo-free with generalized exponential expression,* G *implies weakly pseudo-free.*

Proof. If G is pseudo-free with generalized exponential expression, any probabilistic polynomial-time adversary never outputs an equation E together with a solution. Therefore, the adversary never solves the equation with a non-trivial restriction $(x_1, x_2, \ldots, x_{p_1(k)}) = (1, 1, \ldots, 1)$, where 1 is the identity in G (i.e. set every variables ranging over group elements as the identity 1). The equation with above restriction is just the equation for weakly pseudo-free. Hence, if G is a pseudo-free with generalized exponential expression, no probabilistic polynomial-time adversary solves the equation for weakly pseudo-free. That is, a pseudo-free group with generalized exponential expression implies a weakly pseudo-free group. □

4 Properties on Variants of Pseudo-Free Groups

In this section, we describe many cryptographic assumptions for pseudo-free groups with generalized exponential expression. First, we describe several properties of weakly pseudo-free groups.

4.1 Cryptographic Problems for Weakly Pseudo-Free Groups

The following Proposition 4.1 and Proposition 4.2 ware proved in [Riv04b].

Proposition 4.1. *In a weakly pseudo-free group* G*, it is infeasible for any probabilistic polynomial-time adversary to determine the order of a randomly chosen element* α *from* G*.*

Proposition 4.2. *In a weakly pseudo-free group* G*, it is infeasible for any probabilistic polynomial-time adversary to solve the discrete logarithm for randomly chosen elements* α_1 *and* α_2 *from* G*.*

Theorem 4.1. *In a pseudo-free group with generalized exponential expression* G*, it is infeasible for any probabilistic polynomial-time adversary to determine the order of a randomly chosen element* α *from* G*.*

Proof. Using Theorem 3.2, we can prove the theorem. □

Theorem 4.2. *In a pseudo-free group with generalized exponential expression G, it is infeasible for any probabilistic polynomial-time adversary to solve the discrete logarithm for randomly chosen elements α_1 and α_2 from G.*

Proof. Using Theorem 3.2, we can prove the theorem. □

Theorem 4.3. *In a weakly pseudo-free group G, it is infeasible for any probabilistic polynomial-time adversary to solve the generalized power problem for randomly chosen elements α_1 and α_2 from G.*

Proof. In a weakly pseudo-free group G, any probabilistic polynomial-time adversary cannot output the equation together with a solution to G. So, it is infeasible for the adversary to solve an equation with the following restriction: $(z_3, z_4, \ldots, z_{p'(k)}) = (0, 0, \ldots, 0)$. Then, since the equation $E : a_1^{z_1} a_2^{z_2} = \epsilon$ is unsatisfiable over $F(a_1, a_2)$, the adversary cannot solve the equation $E' : \alpha_1^{z_1} \alpha_2^{z_2} = e$ for randomly chosen elements α_1, α_2 from G. Therefore, it is infeasible for the adversary to solve the generalized power problem. □

Theorem 4.4. *In a pseudo-free group with generalized exponential expression G, it is infeasible for any probabilistic polynomial-time adversary to solve the generalized power problem for randomly chosen elements α_1 and α_2 from G.*

Proof. Using Theorem 3.2, we can prove the theorem. □

4.2 The Intersection Problem for Cyclic Subgroups in Pseudo-Free Groups

In the [Riv04a], he showed that the RSA problem and the strong RSA problem hold in pseudo-free groups. Now, in six cryptographic problems, it remains only the intersection problem for cyclic subgroups. In order to describe the problem, we consider whether the following proposition is true: Is the subgroup of a pseudo-free group (with generalized exponential expression) also pseudo-free (with generalized exponential expression)? That is, in order to describe the intersection problem for cyclic subgroups, we must solve the proposition. However, we remain the proposition as conjecture. Although we believe that it is intuitively true, proving the proposition is not easy.

Conjecture 4.1. *A finite group G is pseudo-free (with generalized exponential expression) if and only if $\langle g \rangle := \{g^i | i \in \mathbb{Z}\}$ is pseudo-free (with generalized exponential expression), for a randomly chosen element g from G.*

If the above conjecture is proved, then we obtain that the intersection problem for cyclic subgroups hold in a pseudo-free group.

Now, we give the following interesting lemma closely related to the conjecture.

Lemma 4.1. *We assume that a finite group G is abelian. For randomly chosen elements g_1, g_2 from G, if $\langle g_1 \rangle := \{g_1^i \mid i \in \mathbb{Z}\}$ is pseudo-free with generalized exponential expression, then $\langle g_1, g_2 \rangle := \{g_1^i g_2^j \mid i, j \in \mathbb{Z}\}$ is weakly pseudo-free.*

Proof. Let k be a security parameter and p be a polynomial. By hypothesis, for $h_1, h_2, \ldots, h_{p(k)} \in_R \langle g_1 \rangle$, the probability that any probabilistic polynomial-time adversary $\mathcal{A}_{g_1}$ outputs an equation together with a solution is negligible in k.

We assume that $\langle g_1, g_2 \rangle$ is not weakly pseudo-free. Then, there exists a probabilistic polynomial-time adversary $\mathcal{A}_{g_1 g_2}$ and a polynomial p' such that for $\alpha_1, \alpha_2, \ldots, \alpha_n \in_R \langle g_1, g_2 \rangle$, $\mathcal{A}_{g_1 g_2}(\langle g_1, g_2 \rangle, \alpha_1, \alpha_2, \ldots, \alpha_n)$ outputs an equation E together with a solution $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbb{Z}$, with non-negligible probability (where $n = p'(k)$). For simplicity of exposition and without loss of generality, we assume that every $\gamma_j \neq 0$ $(1 \leq j \leq n)$.

Now, we take two randomly chosen elements r_{11}, r_{21} from $\mathbb{Z}$, and let α_1 be $hg_1^{r_{11}}g_2^{r_{21}}$, where h is a randomly chosen element from $\langle g_1 \rangle$. Then, it is clear that α_1 is a randomly element on $\langle g_1, g_2 \rangle$. In the same way, we set α_i $(2 \leq i \leq n)$ as above: $\alpha_i = hg_1^{r_{1i}}g_2^{r_{2i}}$ $(r_{1i}, r_{2i} \in_R \mathbb{Z})$. Thus, using an adversary $\mathcal{A}_{g_1g_2}$ we obtain the following equation E together with a solution:

$$\alpha_1^{\gamma_1}\alpha_2^{\gamma_2}\cdots\alpha_n^{\gamma_n} = 1.$$

Since G is abelian, we transform the above equation into as follows:

$$h^{\gamma}g_1^{R_1}g_2^{R_2} = 1,$$

where, $\gamma = \gamma_1 + \gamma_2 + \cdots + \gamma_n$, $R_i = r_{i1}\gamma_1 + r_{i2}\gamma_2 + \cdots + r_{in}\gamma_n$ $(i = 1, 2)$. Then, it follows that $g_2^{-R_2}$ is a element of $\langle g_1 \rangle$.

Here, we consider relationship between g_1 and g_2: we find integers $|s|, |t| \geq 1$ such that $g_1^s = g_2^t$. In order to solve above, we can use the adversary $\mathcal{A}_{g_1g_2}$: for $1 \leq j \leq n$, we take randomly chosen elements d_{1j}, d_{2jj} from $\mathbb{Z}$, and set $\beta_j = g_1^{d_{1j}}g_2^{d_{2j}}$. Then, using $\mathcal{A}_{g_1g_2}$ we obtain the following equation together with a solution:

$$\beta_1^{l_1}\beta_2^{l_2}\cdots\beta_n^{l_n} = 1,$$

where $l_1, l_2, \ldots, l_n$ are non-zero integers. From $\beta_j = g_1^{d_{1j}}g_2^{d_{2j}}$, we can rewrite as follows:

$$g_1^s = g_2^t$$

where $s = d_{11}l_1 + d_{12}l_2 + \cdots + d_{1n}l_n$ and $t = -(d_{21}l_1 + d_{22}l_2 + \cdots + d_{2n}l_n)$. Thus, we can find integers s, t. If $\gcd(s, t) = d_1 > 1$, we can take $s = s'$ and $t = t'$ again, where $s' = s/d_1$ and $t' = t/d_1$. Then $\gcd(s, t) = 1$.

Now, we show that for a randomly chosen element h from $\langle g_1 \rangle$, an adversary $\mathcal{A}_{g_1}$ outputs an equation E together with a solution, with non-negligible probability.

The adversary $\mathcal{A}_{g_1}(\langle g_1 \rangle, h)$ executes as follows.

- set $\alpha_1, \alpha_2, \ldots, \alpha_n$ as above ($\mathcal{A}_{g_1}$ knows such r_{1i}, r_{2i}, $(1 \leq i \leq n)$).
- find $|s|, |t| \geq 1$ such that $g_1^s = g_2^t$ and $\gcd(s, t) = 1$ by using an adversary $\mathcal{A}_{g_1g_2}$.
- obtain an equation E together with a solution as above by using an adversary $\mathcal{A}_{g_1g_2}$.
- put an equation E_1 as $h^z = x_1^{z_1}x_2^{z_2}$, where x_1, x_2 are variables over $\langle g_1 \rangle$ and z, z_1, z_2 are integer-valued variables.

Here, we see that $x_1 = g_1, x_2 = g_2^{-R_2}, z = \gamma, z_1 = -R_1$, and $z_2 = 1$ are solutions to the equation E'. However, the equation is not unsatisfiable over free groups because $z_2 = 1$. Here

$$\begin{aligned} h^{t\gamma} &= g_1^{-tR_1}g_2^{-tR_2} \\ &= g_1^{-tR_1}(g_2^t)^{-R_2} \\ &= g_1^{-tR_1}(g_1^s)^{-R_2} \\ &= g_1^{-tR_1}g_1^{-sR_2} \\ &= g_1^{-tR_1-sR_2} \end{aligned}$$

Let $u = t\gamma$ and $v = -tR_1 - sR_2$, and compute $\gcd(u, v) = d_2$. Then, we take $e = u/d_2$ and $f = v/d_2$ then $\gcd(e, f) = 1$, and set an equation E_2 as $h^{z'} = x^{z'_1}$. From Remark A.1, the equation E_2 with a restriction that $z'_1 > 1$ and $\gcd(z', z'_1) = 1$, is an unsatisfiable equation, where x is a variable over group and z', z'_1 are integer-valued variables. Then, $x = g_1, z' = e, z'_1 = f$ are solutions to E_2.

Therefore, if $\mathcal{A}_{g_1g_2}$ returns an equation together with a solution whose the probability is non-negligible, then $\mathcal{A}_{g_1}$ also returns as above with non-negligible probability. This is by contradiction that $\langle g_1 \rangle$ is pseudo-free with generalized exponential expression. Hence, $\langle g_1, g_2 \rangle$ is weakly pseudo-free. □

5 Conclusion and Open Problems

We have seen variations on the definition, and shown that many cryptographic assumptions never hold. Furthermore, we have proved several properties for the pseudo-free group, which we summarize using a table. The table is for relationship between pseudo-free groups and cryptographic assumptions.

	OP	**DLP**	**RSAP**	**SRSAP**	**GPP**	**IPCS**
PFG	×	×	○	×	×	×
PFGwGEE	○	○	○	○	○	△
WPFG	○	○	×	×	○	△

Table 1: Relationship between Pseudo-Free Groups and Cryptographic Problems.

In addition to the intersection problem for cyclic subgroups in pseudo-free groups, many open problems remain. We describe some of them.

The following problem, already posed in [Riv04a], is the most important in the theory of pseudo-free groups.

- Show that it is decidable whether given an equation with generalized exponential expression is satisfiable over a free group.

We have to solve this open problem under the present definition. Naturally, the equation with no integer-valued exponent variables are well-studied (see [LS77]). However, we must use like generalized exponential expression, which is allow the equation to contain exponent variables.

The next open problem is also in [Riv04a]:

- Show that the computational and decisional Diffie-Hellman problem in pseudo-free groups is computationally infeasible.

In this connection, it is an interesting problem that we apply the theory of pseudo-free groups to some groups which is already known some side informations. For example, $(\mathbb{Z}/p\mathbb{Z})^\times$, where p is a prime, is not typically pseudo-free because we can find the order of it easily.

The following problem is also an interesting problem.

- Find examples of pseudo-free groups under the definition (i.e. for pseudo-free group or weakly pseudo-free group).

In Definition 3.1, Micciancio [Mic05] showed that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a pseudo-free under the strong RSA problem, at least when n is the product of two safe primes. Unfortunately, we cannot apply his proof using Definition 3.2 or 3.3. Nevertheless, we believe that $(\mathbb{Z}/n\mathbb{Z})^\times$ is pseudo-free.

References

[CS00] Ronald Cramer and Victor Shoup. Signature schemes based on the strong rsa assumption. *ACM Transactions on Information and System Security*, 3(3):161–185, 2000.

[Gut00] Claudio Gutiérrez. Satisfiability of equations in free groups is in pspace. *STOC 2000*, pages 21–27, 2000.

[Hoh03] Susan Hohenberger. The cryptographic impact of groups with infeasible inversion. Master's thesis, EECS Dept., MIT, June 2003.

[LI71] Seymour Lipschutz and Charles F. Miller III. Groups with certain solvable and unsolvable decision problems. *Communications on Pure and Applied Mathematics*, XXIV:7–15, 1971.

[LS77] Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory.* Springer, 1977.

[Mak82] Gennady S. Makanin. Equations in free groups. *Izvestiya NA SSSR*, 46:1199–1273, 1982. English translation in Math USSR Izvestiya, 21, 483-546, 1983.

[Mic05] Daniele Micciancio. The RSA group is pseudo-free. *EUROCRYPT 2005, LNCS*, 3494:387–403, 2005.

[Riv04a] Ronald L. Rivest. On the notion of pseudo-free groups. *TCC 2004, LNCS*, 2951:505–521, 2004.

[Riv04b] Ronald L. Rivest. On the notion of pseudo-free groups. `http://theory.lcs.mit.edu/~rivest/Rivest-TCC04-PseudoFreeGroups.ppt`, 2004.

A Six Cryptographic Problems for Free Groups

Lipschutz and Miller [LI71] considered six fundamental problems commonly appeared in many cryptographic protocols; the order problem [solving $a^e = 1$ for e], the power problem (aka the discrete logarithm problem) [solving $a^e = b$ for e], the root problem (aka the RSA problem) [solving $x^e = a$ for x], the proper power problem (aka the strong RSA problem) [solving $x^e = a$ for x and $e > 1$], the generalized power problem [solving $a^e = b^f$ for nonzero e, f], and the intersection problem for cyclic subgroups [solving $a^e = b^f \neq 1$ for e, f]. They showed that these problems are independent, i.e. for each pair of problems there is a group such that one problem is solvable (that is, satisfiability of the relevant equation is decidable) while the other problem is unsolvable. We explore their satisfiability in the free groups. In this section, we assume that the adversary has infinitely computational resources.

Definition A.1. *(The Order Problem (OP)) The order problem in G is the following: given an element $a \in G$, to determine a positive integer e (if any exist) such that*

$$a^e = 1.$$

The least positive such value e is the order of the element a in the group G.

In a free group all elements except for the identity have infinite order. Hence, there is no solution to the equation in such a group. That is, it is infeasible for any adversary to solve the order problem in free groups.

Definition A.2. *(The Discrete Logarithm Problem (DLP)) The discrete logarithm problem in G is the following: given elements a and b from G, to determine an integer e (if any exist) such that*

$$a^e = b.$$

The value e is a discrete logarithm of b, to the base a, in the group G.

In $F(a, b)$ and $FA(a, b)$ it is infeasible for any adversary to solve the above equation, for any value of e. Since a and b are distinct generators, the two sides of the equation are variable-free constant expressions that cannot be equal.

Definition A.3. *(The RSA Problem (RSAP)) The RSA problem in G is the following: given an element a from G and a positive integer $e > 1$, to find x (if any exist) such that*

$$x^e = a.$$

It is clear that the equation has no solution in $F(a)$ and $FA(a)$.

Definition A.4. *(The Strong RSA Problem (SRSAP)) The strong RSA problem in G is the following: given an element a from G, to find x and a positive integer $e > 1$ (if any exist) such that*

$$x^e = a.$$

Similarly, the above equation has no solution in $F(a)$ and $FA(a)$. A different point from the RSA problem is that an adversary can choose himself an exponent $e > 1$.

Remark A.1. *Similar equations, such as*

$$x^e = a^f,$$

where the adversary is given a and must find x, e, and f such that $e > 1$ and $\gcd(e, f) = 1$, are also infeasible for the adversary to solve in free groups, because this problem is equivalent to solving the strong RSA problem since $\hat{x}^e = a$ where $\hat{x} = x^{f'} a^{e'}$ and $ee' + ff' = 1$ (see [CS00, Lemma 1]).

Definition A.5. *(The Generalized Power Problem (GPP)) The generalized power problem is: given group elements a and b, to find nonzero integers e, f satisfying*

$$a^e = b^f.$$

There is no relationship between the element of $F(A)$ or $FA(A)$. Thus, it is infeasible for the adversary to solve the generalized power problem in free groups.

Definition A.6. *(The Intersection Problem for Cyclic Subgroups (IPCS)) The intersection problem for cyclic subgroups is: given group elements a and b, to find integers e, f such that*

$$a^e = b^f \neq 1.$$

We note that the above problem is in the cyclic subgroup of a free group. It is well-known that if a group G is free, every subgroup of G is also free. For this reason, it is infeasible for the adversary to solve the intersection problem for cyclic subgroups in free groups.