Research Article

Research on Attacking a Special Elliptic Curve Discrete Logarithm Problem

Jiang Weng,^{1,2} Yunqi Dou,¹ and Chuangui Ma³

¹State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

²Air Force Engineering University, Xi'an 710038, China

³Basic Department, Army Aviation Institution, Beijing 101123, China

Correspondence should be addressed to Jiang Weng; wengjiang858@163.com

Received 17 December 2015; Revised 15 May 2016; Accepted 31 May 2016

Academic Editor: Nazrul Islam

Copyright © 2016 Jiang Weng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cheon first proposed a novel algorithm for solving discrete logarithm problem with auxiliary inputs. Given some points $P, \alpha P, \alpha^2 P, \dots, \alpha^d P \in \mathbb{G}$, an attacker can solve the secret key efficiently. In this paper, we propose a new algorithm to solve another form of elliptic curve discrete logarithm problem with auxiliary inputs. We show that if some points $P, \alpha P, \alpha^k P, \alpha^{k^2} P, \alpha^{k^3} P, \dots, \alpha^{k^{\varphi(d)-1}} P \in \mathbb{G}$ and a multiplicative cyclic group $K = \langle k \rangle$ are given, where d is a prime, $\varphi(d)$ is the order of K . The secret key $\alpha \in \mathbb{F}_p^*$ can be solved in $\mathcal{O}(\sqrt{(p-1)/d} + d)$ group operations by using $\mathcal{O}(\sqrt{(p-1)/d})$ storage.

1. Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where $q = p^n$ and p is prime. Given points $P, Q \in E(\mathbb{F}_q)$ to find an integer α , if it exists, such that $Q = \alpha P$. The computational problem is called elliptic curve discrete logarithm problem (ECDLP). This problem is the fundamental building block for elliptic curve cryptography (ECC) and pairing-based cryptography and has been a major area of research in computational number theory and cryptography for several decades.

The security of elliptic curve cryptography is based on the difficulty of the ECDLP. Like any other discrete logarithm problem, ECDLP can be solved by generic algorithms such as the Baby-Step Giant-Step method [1] and Pollard rho method [2]. At present, parallelized Pollard rho algorithm [3] is the fastest general-purpose method for solving the ECDLP. So far, Pollard rho method has been implemented on a variety of accelerator platforms including FPGAs, Playstation 3 Cell Processors, and GPUs.

Many bilinear maps were applied to establish efficient cryptographic schemes, whose security relies on the infeasibility of newly proposed mathematical problems such as Bilinear Diffie-Hellman Problem (BDHP) [4], Strong

Diffie-Hellman Problem (SDHP) [5], Bilinear Diffie-Hellman Inversion Problem (BDHIP) [6], and Bilinear Diffie-Hellman Exponent Problem (BDHEP) [7].

A variant of the Diffie-Hellman problem introduced by Boneh and Boyen [5] is to compute that when given $P, \alpha P, \alpha^2 P, \dots, \alpha^d P$. Problems of this type (including the simpler case of being given $P, \alpha P, \alpha^d P$) are sometimes called discrete logarithm problems with auxiliary inputs.

In Eurocrypt 2006, Cheon [8, 9] first proposed an algorithm for solving discrete logarithm problem with auxiliary inputs (DLP-wAI). Auxiliary inputs are some additional information which is provided for solving DLP, such that some elements $(P, \alpha P, \alpha^2 P, \dots \in \mathbb{G})$ instead of only two elements $(P, \alpha P \in \mathbb{G})$.

Let $G = \langle P \rangle$ be an additive cyclic group generated by an element P of prime order p . The time complexity of Cheon's algorithm is $\mathcal{O}(\sqrt{(p-1)/d} + \sqrt{d})$ with $\mathcal{O}(\max\{\sqrt{(p-1)/d}, \sqrt{d}\})$ storage in the case of $d \mid (p-1)$. In particular, when $d \approx \sqrt{p}$, it only needs $\mathcal{O}(\sqrt[4]{p})$ in time and space. Cheon also presents a variant for the case when $d \mid (p+1)$. The idea of Cheon's algorithm is to embed a discrete logarithm α from $\mathbb{F}_p^*$ to an auxiliary group $\mathbb{F}_p^*$ (or $\mathbb{F}_{p^2}^*$) for $p-1$ (or $p+1$ case, resp.).

In 2009, Satoh [10] proposed a possible generation of Cheon's algorithm when d is a divisor of $\varphi_n(p)$ when $n \geq 2$, where $\varphi_n(p)$ is the n th cyclotomic polynomial. Although Satoh described the algorithm in the context of general linear groups, essentially Satoh's algorithm used embedding from $\mathbb{F}_p^*$ to an auxiliary group $\mathbb{F}_{p^n}^*$. In the case of $n = 2$, Satoh's algorithm reduced the number of input data pieces by the half of Cheon's original algorithm. However, the efficiency of the algorithm was not well-studied. Kim [11, 12] studied Satoh's generalization of the $p+1$ algorithm for solving the DLP-wAI. The result showed that the complexity of Satoh's algorithm was not faster than Cheon's algorithm when $d \mid \varphi_n(p)$ and $n \geq 3$. One of the main problems when using this mapping is the occurrence of high degree polynomials.

In 2012, Kim and Hee [13] proposed a new approach to solve the DLP-wAI focusing on the behavior of the function mapping rather than embedding the secret key to an auxiliary group. Kim's algorithm reduced solving DLP-wAI into finding a polynomial whose substitution polynomial has many absolutely irreducible factors. In $p+1$ case, the complexity of Kim's algorithm is $\mathcal{O}(\sqrt{p^2/R} \log^2 d \log p)$ with d auxiliary elements, where R is the number of pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ such that $f(x) = f(y)$, while Cheon's algorithm required $2d$ auxiliary elements for the same problem. However, it would be more difficult to design such a polynomial with small value sets.

Sakemi et al. [14] investigated useful techniques for speeding up Cheon's algorithm and demonstrated that it is possible to solve 160-bit DLP-wAI over a pairing-friendly elliptic curve within a practical time.

In this paper, we introduce a new algorithm for solving ECDLP-wAI. If $P, \alpha P, \alpha^k P, \alpha^{k^2} P, \alpha^{k^3} P, \dots, \alpha^{k^{\varphi(d)-1}} P \in \mathbb{G}$ are given, specify that d is a prime number and that φ is the Euler totient function and that k is a generator of multiplicative cyclic group with order $\varphi(d)$; we can solve $\alpha \in \mathbb{Z}_p^*$ by using $\mathcal{O}(\sqrt{(p-1)/d} + d)$ group operations and $\mathcal{O}(\sqrt{(p-1)/d})$ storage.

The rest of this paper is organized as follows. In Section 2, we describe Cheon's algorithm. We define a group partition and show how group elements can be represented with only a few elements in Sections 3 and 4. In Section 5, we propose an algorithm for the ECDLP-wAI and analyze the complexity. Then our experimental results are reported in Section 6. Finally, we conclude this paper in Section 7.

2. Preliminary

In this section we introduce some notations and concepts used throughout this paper.

2.1. Discrete Logarithm Problem with Auxiliary Inputs. The DLP-wAI was first proposed by Cheon in [8, 9] as a variant of DLP. Let $\mathbb{G} = \langle P \rangle$ be an additive cyclic group generated by the base point P of prime order p . The DLP-wAI in $\mathbb{G}$ is to solve $\alpha \in \mathbb{F}_p^*$ from some additional information such as $\alpha^i P \in \mathbb{G}$ for some integer i .

Cheon proposed two types ($p-1$ and $p+1$ case) of DLP-wAI. Both of the two algorithms transform the discrete logarithm in $\mathbb{F}_p^*$ into an auxiliary group, and solving the DLP in the auxiliary group is more efficient than original group.

We now sketch the technique due to Brown and Gallant [15] for solving ECDLP instances $P, \alpha P, \alpha^d P$, where P has order p and $d \mid (p-1)$. Fix $\zeta \in \mathbb{Z}_p^*$ of order equal to $(p-1)$, so that ζ^d has order $(p-1)/d$. Since α^d has order modulo p dividing $(p-1)/d$, we have $\alpha^d \equiv (\zeta^d)^x \pmod{p}$ for some integer $0 \leq k_1 < (p-1)/d$. Writing $m \leftarrow \lceil \sqrt{(p-1)/d} \rceil$ and $k_1 = u + mv$ with $0 \leq u, v < m$ we have $\alpha^d P = (\zeta^d)^u (\zeta^{md})^v P$. Hence one can compute a list of values $(\zeta^{-du})P_d$ and a list of values $(\zeta^{dm})^v P$ and find in $\mathcal{O}(\sqrt{(p-1)/d})$ steps the matching pair (u, v) . Writing $k_1 = u + mv$ we have $\alpha^d \equiv (\zeta^d)^{k_1} \pmod{p}$. To find α we write $\alpha = \zeta^k$ and note that $k = k_1 + k_2 \sqrt{(p-1)/d}$ for some $0 \leq k_2 < d$. By a similar method based on αP one computes k_2 in $\mathcal{O}(\sqrt{d})$ steps and hence computes α . Overall we compute α in $\mathcal{O}(\max\{\sqrt{(p-1)/d}, \sqrt{d}\})$ group operations.

The $p-1$ case is that $P, \alpha P, \alpha^d P$ are given for a positive divisor d of $p-1$. This case maps α to α^d and the subgroup of $\mathbb{F}_p^*$ with order $(p-1)/d$ as the auxiliary group. We give Cheon's algorithm with $p-1$ case as follows:

Algorithm 1.

Input: $\{P, P_1 = \alpha P, P_d = \alpha^d P \in G\}, d \mid p-1$;

Output: $\alpha \in \mathbb{Z}_p^*$;

(1) Find a generator $\zeta \in \mathbb{Z}_p^*$,

(2) Set $\zeta_d \leftarrow \zeta^d$,

(3) $m \leftarrow \lceil \sqrt{(p-1)/d} \rceil, \widehat{m} \leftarrow \lfloor (p-1)/md \rfloor$,

(4) Find $0 \leq u < m, 0 \leq v \leq \widehat{m}$ such that $\zeta_d^{-u} P_d = \zeta_d^{mv} P$,

(5) $k_1 \leftarrow u + mv$,

(6) Set $\zeta_e = \zeta^{(p-1)/d}$,

(7) $m' \leftarrow \lceil \sqrt{d} \rceil, \widehat{m}' \leftarrow \lfloor d/m' \rfloor$,

(8) Find $0 \leq u' < m', 0 \leq v' \leq \widehat{m}'$ such that $\zeta_e^{-u'} \zeta^{-k_1} P_1 = \zeta_e^{m'v'} P$,

(9) $k_2 \leftarrow u' + m'v'$,

(10) Output $\alpha = \zeta^{k_1 + k_2(p-1)/d}$.

The secret key $\alpha \in \mathbb{F}_p^*$ can be recovered in time complexity $\mathcal{O}(\sqrt{(p-1)/d} + \sqrt{d})$ by using $\mathcal{O}(\max\{\sqrt{(p-1)/d}, \sqrt{d}\})$ storage. In the extreme case where there is a factor $d \mid (p-1)$ with $d \approx \sqrt{p}$, then one can solve the ECDLP in $\mathcal{O}(\sqrt{p})$ steps, which is much efficient than that for solving DLP in general groups (which requires $\mathcal{O}(\sqrt{p})$).

The $p+1$ case is that $P, \alpha P, \alpha^2 P, \dots, \alpha^{2d} P$ are given for a positive divisor d of $p+1$. This case maps α to $(\alpha + \theta)^{(p-1)/d}$, where $\theta \in \mathbb{F}_p^* \setminus \mathbb{F}_p$, and the subgroup of $\mathbb{F}_p^*$ with order $(p+1)/d$

as the auxiliary group. We give Cheon's algorithm with $p + 1$ case as follows:

Algorithm 2.

Input: let $\{P, P_1 = \alpha P, P_2 = \alpha^2 P, \dots, P_{2d} = \alpha^{2d} P \in G\}$, $d \mid p + 1$, a a quadratic nonresidue of $\mathbb{Z}_p$, and θ a root of $X^2 - a$ in $\mathbb{F}_p$, $H \leq \mathbb{F}_p[\theta]^*$, $\beta = \beta_0 + \beta_1\theta$, and $|H| = p + 1$;

Output: $\alpha \in \mathbb{Z}_p^*$:

- (1) Find a generator $\zeta \in H$,
- (2) Set $\zeta_d \leftarrow \zeta^d$, $\bar{\zeta}_d \leftarrow \zeta_d^{-1}$,
- (3) $m \leftarrow \lceil \sqrt{(p+1)/d} \rceil$, $\hat{m} \leftarrow \lfloor (p+1)/md \rfloor$,
- (4) $P_1(x) \leftarrow \sum_{i=0}^d \binom{2d}{2i} a^i x^{2i} P$, $P_2(x) \leftarrow \sum_{i=0}^{d-1} \binom{2d}{2i+1} a^i x^{2i+1} P$, $P_3(x) \leftarrow \sum_{i=0}^d \binom{d}{i} (-a)^i x^{2i} P$, and $\beta^d \leftarrow (P_1(x) + P_2(x)\theta)/P_3(x)$,
- (5) Find $0 \leq u < m$, $0 \leq v \leq \hat{m}$ such that $\zeta_d^{-u} \beta^d = \zeta_d^{mv}$,
- (6) $k_1 \leftarrow u + mv$,
- (7) Set $\zeta_e = \zeta^{(p+1)/d}$,
- (8) $m' \leftarrow \lceil \sqrt{d} \rceil$, $\hat{m}' \leftarrow \lfloor d/m' \rfloor$,
- (9) Find $0 \leq u' < m'$, $0 \leq v' \leq \hat{m}'$ such that $\beta \zeta_e^{-u'} \zeta^{-k_2} = \zeta_e^{m'v'}$,
- (10) $k_2 \leftarrow u' + m'v'$,
- (11) $\beta \leftarrow \zeta^{k_1+k_2(p+1)/d}$,
- (12) Output $\alpha = \beta_1/(\beta_0 + 1)$.

The secret key $\alpha \in \mathbb{F}_p^*$ can be recovered in time complexity $\mathcal{O}(\sqrt{(p+1)/d} + d)$ by using $\mathcal{O}(\max\{\sqrt{(p+1)/d}, \sqrt{d}\})$ storage.

3. Partitions of Group Elements

In this section, we introduce a representation of a multiplicative subgroup and then give a group action on $\mathbb{F}_p^*$. For more information about group theory, one refers to [16, 17].

3.1. Multiplicative Cyclic Subgroup of $\mathbb{Z}_{p-1}^*$ Construction. A representation of the subgroup can help to analyze the structure of the subgroup. In this paper, we introduce a new representation for multiplicative subgroup of $\mathbb{Z}_{p-1}^*$, where p is an odd prime.

Let S be a subset of $\mathbb{Z}_p$. The greatest common divisor of all integers s is denoted by $\gcd(S)$, where $s \bmod (p-1)$ belongs to S . We define a subset K of $\mathbb{Z}_{p-1}^*$ by $K = (1 + \lambda \mathbb{Z}_{p-1}) \cap \mathbb{Z}_{p-1}^*$, where $p-1 = d\lambda$, λ is an even integer, and d is an odd prime number.

Lemma 3. Let $K = \{n\lambda + 1 : n \in [0, (p-1)/\lambda)\} \cap \mathbb{Z}_{p-1}^*$. Thus K is a multiplicative subgroup of $\mathbb{Z}_{p-1}^*$.

Proof. Let $1+i\lambda, 1+j\lambda \in K$; then $(1+i\lambda)(1+j\lambda) \bmod (p-1) \equiv 1 + (i+j+ij\lambda)\lambda \bmod (p-1)$. Since $\gcd(1+i\lambda, p-1) = 1$ and $\gcd(1+j\lambda, p-1) = 1$, this means $\gcd((1+i\lambda)(1+j\lambda), p-1) = 1$. So $(1+i\lambda)(1+j\lambda) \in K$.

Let $1+i\lambda \in K$; we assume $(1+i\lambda)(1+j\lambda) \equiv 1 \bmod (p-1)$. Since $1+(i+j+ij\lambda)\lambda \equiv 1 \bmod (p-1) \Rightarrow i+j(1+\lambda) \equiv 0 \bmod d$ and $\gcd(d, 1+i\lambda) = 1$, then there exists j such that $1+j\lambda$ is the inverse of $1+i\lambda$.

It is closed under multiplication and inversion. Therefore K is a multiplicative subgroup of $\mathbb{Z}_{p-1}^*$. $\square$

Since λ is an even integer, every element of K is as form $1+n\lambda$ so that $\lambda = \gcd(K-1)$, where $K-1 = \{k-1 : k \in K\}$.

3.2. Group Action

Definition 4 (see [16]). An action of group G on a set S is a function $G \times S \rightarrow S$ (usually denoted by $(g, x) \mapsto g \circ x$) such that for all $g_1, g_2 \in G$, $x \in S$ satisfies:

$$(g_1 g_2) \circ x = g_1 \circ (g_2 \circ x), \quad (1)$$

$$e \circ x = x,$$

where e is a unit element of G . When such an action is given, we say that G acts on set S .

Since there may be many different actions of group G on given set S , the notation gx is ambiguous. A group action on a set induces a partition of this set, which is called the orbit of the set under this group action.

Let G be a group that acts on a set S . The relation on S defined by $x \sim x' \Leftrightarrow gx = x'$ for some $g \in G$ is an equivalence relation. The equivalence classes of the equivalence relation are called the orbits of the set under this group action; usually the orbit of $x \in S$ is denoted as $\langle x \rangle$.

A group action of G on a set S induces a partition of S via the equivalence relation defined by $x \sim x' \Leftrightarrow g \circ x = x'$ for some $g \in G$. The equivalence classes are called orbits of S under the action of G ; usually the orbit of $x \in S$ is denoted as $\langle x \rangle$. We define the set of fixed points of S under the action of G by $\text{Fix}(G) = \{x \in S : g \circ x = x \text{ for all } g \in G\}$ and the set of nonfixed points $\text{nFix}(G)$ by $S \setminus \text{Fix}(G)$. Hence all elements of group G can be represented by only two types of elements, *fixed points* and *nonfixed points*.

We define the action of subgroup K on $\mathbb{F}_p^*$ such that $K \times \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$ satisfies $(k, x) \mapsto x^k$ for all $k \in K$ and $x \in \mathbb{F}_p^*$. This map induces a set $x^K = \{x^k : k \in K\}$ that is called a K -orbit of x . In particular, $\text{Fix}(K) = \{x \in \mathbb{F}_p^* \mid x^k \equiv x \bmod (p-1), \text{ for every } k \in K\}$ is a subgroup of $\mathbb{F}_p^*$, which is the set of fixed points.

Let ξ be a primitive element in $\mathbb{Z}_p$; then $\zeta = \xi^{(p-1)/\lambda}$ is a generator of a cyclic group. Obviously, the fixed point set is generated by ζ , where $\langle \zeta \rangle = \{x \in \mathbb{F}_p^* : x^\lambda \equiv 1 \bmod (p-1)\}$ and $\lambda = \gcd\{k-1 : k \in K\}$.

By using this group action on $\mathbb{F}_p^*$, we can efficiently partition $\mathbb{F}_p^*$. Thus the elements of $\mathbb{F}_p^*$ can be represented with only a few subsets.

4. A Group Represented by Disjoint Orbits

In this section, we introduce how to partition group elements by disjoint orbits.

4.1. A Group Partition. Let $p - 1 = 2^{e_1} \prod_{i \in I} p_i^{e_i}$, where $I = \{2, 3, \dots, t\}$ is an index set, $p_2, \dots, p_t$ are distinct odd prime numbers, and each $e_i \geq 1$. We choose a prime divisor p_j of $p - 1$ with $e_j = 1$, denoted as $p_j = d$. Let $\lambda = 2^{e_1} \prod_{i \in I \setminus j} p_i^{e_i} = (p - 1)/d$. It is equivalent to $\gcd(\lambda, d) = 1$. We generate a set K that is defined by $K := \{1 + n\lambda : n \in [0, d)\}$.

Proposition 5. Let $K = \{1 + n\lambda : n \in [0, d)\} \cap \mathbb{Z}_{p-1}^*$ be a multiplicative subgroup of $\mathbb{Z}_{p-1}^*$. Thus the order of K is $\varphi(d)$, where φ denotes Euler's totient function.

Let $(p - 1)/\lambda = d$ be prime; then $|K| = d - 1$. We note that $\gcd(\lambda, d) = 1$ and $1 + n\lambda$, where $0 \leq n < d$. Obviously, $1 + n\lambda$ is a complete residue modulo d for $0 \leq n < d$. Thus, there exists unique $0 \leq n' < d$ such that $d \mid 1 + n'\lambda$. So all the elements of K can be expressed by $K = \{1 + n\lambda : n \in [0, d) \setminus n'\}$. Thus we know that $|K| = \varphi(d) = d - 1$.

Proposition 6. Let $K = \{1 + n\lambda : n \in [0, d) \setminus n'\}$ be a multiplicative subgroup of $\mathbb{Z}_{p-1}^*$. If $\gcd(\lambda, d) = 1$, then K is a cyclic group.

Proof. We define a map $f: K \rightarrow \mathbb{Z}_d^*$, where $\mathbb{Z}_d^*$ is a multiplicative cyclic group of order $d - 1$. The map f is defined by $f: 1 + n\lambda \rightarrow (1 + n\lambda) \bmod d$ for every $1 + n\lambda \in K$.

Let $1 + n\lambda = k_1d + t_1$ and $1 + m\lambda = k_2d + t_2$, where $0 \leq t_1, t_2 < d$:

$$\begin{aligned} & (1 + n\lambda)(1 + m\lambda) \bmod d \\ &= (k_1d + t_1)(k_2d + t_2) \bmod d \\ &= k_1k_2d^2 + (k_1t_2 + t_1k_2)d + t_1t_2 \bmod d \\ &= t_1t_2 \bmod d, \\ & (1 + n\lambda) \bmod d \cdot (1 + m\lambda) \bmod d \\ &= (k_1d + t_1) \bmod d \cdot (k_2d + t_2) \bmod d \\ &= t_1 \bmod d \cdot t_2 \bmod d = t_1t_2 \bmod d. \end{aligned} \quad (2)$$

Hence $(1 + n\lambda)(1 + m\lambda) \bmod d \equiv (1 + n\lambda) \bmod d \cdot (1 + m\lambda) \bmod d$; it implies that the map f is a group-homomorphism for the multiplicative structures on K and $\mathbb{Z}_d^*$. In order to prove the map is bijective, we only need to prove the map f is injective.

If $1 + n\lambda \neq 1 + m\lambda$, then $(1 + n\lambda) \bmod d \neq (1 + m\lambda) \bmod d$ for all $0 \leq n, m < d$ and $n \neq m$. Suppose $(1 + n\lambda) \bmod d = (1 + m\lambda) \bmod d$; then $d \mid (n - m)\lambda$. Since $\gcd(\lambda, d) = 1$, we have $d \mid n - m$. This is a contradiction. Therefore, the map f is injective. It is natural that f is bijective. Hence the groups K and $\mathbb{Z}_d^*$ are isomorphism (written as $K \cong \mathbb{Z}_d^*$).

Therefore the group K is a cyclic group. $\square$

Then we need to find a generator of K . Since K is a cyclic group and $K \cong \mathbb{Z}_d^*$, the homomorphism f maps the generator of K to the generator of $\mathbb{Z}_d^*$. Let γ be a generator of $\mathbb{Z}_d^*$; then $K = \langle f^{-1}(\gamma) \rangle$. The following proposition implies that $x, x^k, x^{k^2}, \dots, x^{k^{\varphi(d)-1}}$ are all the distinct elements for $x \in \mathbb{F}_p^* \setminus \langle \zeta \rangle$, where k is a generator of K .

Proposition 7. Let K be defined as above and ζ a generator of $\text{Fix}(K)$; then all elements $x, x^k, \dots, x^{k^{\varphi(d)-1}}$ in the same orbit are distinct for every $x \in \mathbb{F}_p^* \setminus \langle \zeta \rangle$.

Proof. Suppose that $x^{k^i} = x^{k^j}$ for $0 \leq i, j < d, i \neq j$. Writing this as $x^{k^i - k^j} = 1$, we know $p - 1 \mid k^i - k^j$. Since $k^i - k^j = \lambda l$, where $0 \leq l < (p - 1)/\lambda$, notice that $\text{ord}(x) = p - 1$; we have $(p - 1) \mid \lambda l$. However, $p - 1 > \lambda l$; this is a contradiction. Thus $x, x^k, \dots, x^{k^{\varphi(d)-1}}$ are distinct for $0 \leq i, j < d, i \neq j$. $\square$

Let ζ be a generator of a cyclic group of fixed point. In the following we mainly discuss the relation between $\zeta^i x^K$ and $\zeta^j x^K$ under the condition $\gcd(\lambda, d) = 1$ for all $0 \leq i, j \leq \lambda - 1$ and $i \neq j$, where ζ is a fixed point and x is a nonfixed point.

Proposition 8. Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^*$ and ζ a generator of fixed point for $\lambda = \gcd(K - 1)$. If $\gcd(\lambda, d) = 1$, then any two orbits $\zeta^i x^K$ and $\zeta^j x^K$ are disjoint for $0 \leq i, j \leq \lambda - 1, i \neq j$.

Proof. Any two orbits $\zeta^i x^K$ and $\zeta^j x^K$ are disjoint for $0 \leq i, j \leq \lambda - 1, i \neq j$. It is equivalent to $(\zeta^i x^K) \cap (\zeta^j x^K) = \emptyset$. Suppose that $(\zeta^i x^K) \cap (\zeta^j x^K) \neq \emptyset$ for some i, j . This means that $\zeta^i x^K = \zeta^j x^K$ and $y = \zeta^{i-j} = x^{k^m - k^n}$, where $k^m, k^n \in K$. Since $(\zeta^{i-j})^\lambda = 1$ and $(x^{k^m - k^n})^d = 1$ for $x \in \mathbb{F}_p^*$, the order of y divides both λ and d . Then it divides $\gcd(\lambda, d) = 1$, from which it follows that y must be equal to 1. This is a contradiction, so $\zeta^i x^K$ and $\zeta^j x^K$ are disjoint. On the other hand, if $i = j$, there is natural $\zeta^i x^K = \zeta^j x^K$. $\square$

From the above discussion, we conclude that two orbits $\zeta^i x^K$ and $\zeta^j x^K$ are identical or disjoint. Therefore, group elements can be expressed by disjoint orbits. We may divide the group G into two classes, the nonfixed points (denoted as G_{nfp}) and the fixed points (denoted as G_{fp}). The group G can be expressed by $G = G_{nfp} \cup G_{fp}$, where $\cup$ denotes the disjoint union.

The nonfixed points part G_{nfp} behaves just like an extended orbit. G_{nfp} can be partitioned by the disjoint union of distinct $G_{x,nfp}$, such as $G_{x,nfp} = x^K \cup \zeta x^K \cup \dots \cup \zeta^{\lambda-1} x^K$ where we choose $x \in G$ as a nonfixed point representative element, and $\zeta \in G$ is a fixed point.

The above discussion gives a decomposition of group elements as union of distinct orbits, which we call the orbit decomposition formula. Furthermore, we can take these elements $x, \zeta x, \dots, \zeta^{\lambda-1} x$ as the different representatives for distinct orbits. Obviously, any two orbits $\zeta^i x^K$ and $\zeta^j x^K$ are one-to-one correspondence, where $0 \leq i, j < \lambda$. Thus any two orbits have the same cardinality.

Hence, the cardinality of $G_{x,nfp}$ can be expressed by $|K|\lambda$ for $x \in G$. The order of G can be expressed by $|G| = |G_{x,nfp} \cup G_{fp}| = (|K| + 1)\lambda$ for a non-fixed point $x \in G$ and a fixed point $\zeta \in G$.

Example 9. Let $K = \{1, 5, 9, 13, 17, 25\} \subseteq \mathbb{Z}_{28}^*$; define a map $x \mapsto x^{k^i}$ for $k = 5$ and $0 \leq i \leq 5$. We consider a group partition method on $\mathbb{Z}_{71}^*$. Then we have $\lambda = 4$ disjoint orbits of length $\varphi(d) = 6$. Since there is one-to-one correspondence between any two orbits, the group $\mathbb{Z}_{29}^*$ can be divided as follows:

$$\begin{aligned} 2^K &= \{2, 3, 19, 14, 21, 11\}, \\ 4^K &= 25 \times 2^K = \{4, 9, 13, 22, 6, 5\}, \\ 7^K &= 70 \times 2^K = \{7, 16, 20, 25, 24, 23\}, \\ 8^K &= 57 \times 2^K = \{8, 27, 15, 18, 10, 26\}. \end{aligned} \quad (3)$$

So the cardinality of every orbit is $|K| = |2^K| = |4^K| = |7^K| = |8^K| = 6$. We have 4 fixed points $G_{fp} = \langle 12 \rangle = \{1, 12, 17, 28\}$ and note that $1^4 \equiv 12^4 \equiv 17^4 \equiv 28^4 \equiv 1 \pmod{29}$. Obviously, G_{nfp} can be represented as $G_{nfp} = 2^K \cup 4^K \cup 7^K \cup 8^K$. Thus $\mathbb{Z}_{29}^*$ can be partitioned by $\mathbb{F}_{71}^* = \text{Fix}(K) \cup n\text{Fix}(K)$.

5. A Special Polynomial Construction

In [13], Kim and Hee proposed a fast multipoint evaluation method to solve DLP-wAI focusing on the behavior of function mapping between the finite fields rather than using embedding for auxiliary groups. This method reduced solving DLP-wAI into finding a polynomial whose substitution polynomial has many absolutely irreducible factors.

In this section, we construct a polynomial $f(x) \in \mathbb{F}_p[x]$ having the same value for the elements in the same orbit. We define a function $f(x)$ by

$$f(x) := x + x^{k^1} + x^{k^2} \cdots + x^{k^{d-2}} + x^{k^{d-1}} \in \mathbb{F}_p[x], \quad (4)$$

where $k^{\varphi(d)} \equiv 1 \pmod{p-1}$. It implies that $x, x^k, \dots, x^{k^{\varphi(d)-1}}$ are all distinct elements and that this sequence is repeated for further powers. Furthermore, we define the equivalence relation $\sim$ on $\mathbb{F}_p^*$ as follows:

$$\begin{aligned} \langle x \rangle &\sim \{x, x^k, \dots, x^{k^{\varphi(d)-1}}\} \mapsto f(x) \\ \langle \zeta x \rangle &\sim \{\zeta x, \zeta x^k, \dots, \zeta x^{k^{\varphi(d)-1}}\} \mapsto \zeta f(x) \\ &\vdots \\ \langle \zeta^{\lambda-1} x \rangle &\sim \{\zeta^{\lambda-1} x, \zeta^{\lambda-1} x^k, \dots, \zeta^{\lambda-1} x^{k^{\varphi(d)-1}}\} \mapsto \\ &\quad \zeta^{(\lambda-1)} f(x), \end{aligned} \quad (5)$$

where ζ is a fixed point and $\zeta^i x$ are the representatives of distinct orbits.

This relation partitions the group $\mathbb{F}_p^*$ into different equivalence classes, and each class contains $\varphi(d)$ elements. Obviously, any two equivalence classes, that is, $\langle \zeta^i x \rangle$ and $\langle \zeta^j x \rangle$, have one-to-one correspondence for all i, j and $i \neq j$.

Proposition 10. Let K be multiplicative subgroup of $\mathbb{Z}_{p-1}^*$ and ζ a generator of fixed point. Then we have $f(x) \equiv f(x^k) \equiv \dots \equiv f(x^{k^{\varphi(d)-1}}) \pmod{p}$ and $f(\zeta^i x) \equiv \zeta^i f(x) \pmod{p}$, where $x \in \mathbb{F}_p^* \setminus \langle \zeta \rangle$, $k \in K$, and $0 \leq i \leq \lambda - 1$.

Proof. One has $\zeta^k \equiv \zeta \pmod{p}$ for all $k \in K$; the orbit generated by $\zeta^i x$ satisfies $(\zeta^i x)^K = \zeta^i x^K$ for all $0 \leq i \leq \lambda - 1$. $\square$

5.1. The Proposed Algorithm

Theorem 11. Let $\mathbb{G} = \langle P \rangle$ be an additive cyclic group of prime order p with a generator P . Let K be a multiplicative subgroup of $\mathbb{F}_{p-1}^*$ with $\lambda = \gcd(K - 1)$. Suppose that a generator ζ of $\mathbb{F}_{p-1}^*$ and $P, \alpha P, \alpha^k P, \dots, \alpha^{k^{\varphi(d)-1}} P$ are given. Then $\alpha \in \mathbb{F}_p^*$ can be computed in time $2\lceil \sqrt{(p-1)/d} \rceil + (d-1)$ group operations by using storage for $\lceil \sqrt{(p-1)/d} \rceil$ elements of $\mathbb{G}$.

Proof. Let $\mathbb{G} = \langle P \rangle$ be an additive cyclic group generated by an element P of prime order p . Polynomial $f(x) = x + x^k + x^{k^2} + \dots + x^{k^{\varphi(d)-1}} \pmod{p}$ has the same value for all elements in an orbit, and it is to say that $f(\alpha) \equiv f(\alpha^k) \equiv \dots \equiv f(\alpha^{k^{\varphi(d)-1}}) \pmod{p}$, where $k, k^2, \dots, k^{\varphi(d)-1} \in K$ and $\alpha \in \mathbb{F}_p^*$.

Given $P, \alpha P, \alpha^k P, \dots, \alpha^{k^{\varphi(d)-1}} P \in \mathbb{G}$, we first compute $f(\alpha)P = \alpha P + \alpha^k P \cdots + \alpha^{k^{\varphi(d)-1}} P \in \mathbb{G}$. Then we randomly choose a nonfixed element β from $\mathbb{F}_p^*$ and evaluate $f(x)$ at β . There exist nonnegative integers $0 \leq i, j \leq \lambda - 1$ such that $\zeta^i f(\alpha) = f(\beta)$.

If we take $m = \lceil \sqrt{(p-1)/d} \rceil$, t can be expressed in a unique manner as $t = mv + u$, where $0 \leq u, v < m$. This implies that

$$\zeta^{mv} f(\alpha) = \zeta^{-u} f(\beta). \quad (6)$$

Since $f(\alpha)$ is unknown value, in practice, we search for integers u and v that satisfy

$$\zeta^{mv} f(\alpha)P = \zeta^{-u} f(\beta)P. \quad (7)$$

In order to find such t , we use Baby-Step Giant-Step [1] method. We construct a lookup table, which contains all the pairs $(\zeta^{-u} f(\beta)P, u)$ for $0 \leq u < m$, and we sort the table by the first component. Then we compute $\zeta^{mv} f(\alpha)P$ for each $0 \leq v < m$ and compare with the lookup table in order to identify coincidence. Note that the terms in both sides of (7) can be computed by repeated elliptic curve scalar multiplication. Thus, we can determine a pair of (u, v) that satisfies (7) in $2m$ group operations by using storage for m elements of $\mathbb{G}$. Then t can be found.

There is $\zeta^t f(\alpha)P = f(\beta)P$ or equivalently $f(\zeta^t \alpha)P = f(\beta)P$. Since the k th power of any point is still in the same

orbit, there exists an integer $k^l \in K$ such that $\zeta^t \alpha P = \beta^{k^l} P$. We compute $\beta^{k^l} P$ and compare with $\zeta^t \alpha P$ in $\mathbb{G}$, where $0 \leq i \leq \lambda - 1$. This gives $\alpha = \zeta^{-t} \cdot \beta^{k^l}$. $\square$

We briefly describe this method in Algorithm 12. The algorithm is probabilistic, in which $\beta \in \mathbb{F}_p^*$ satisfies $\zeta^t f(\alpha)P = f(\beta)P$ for our attack. Since all elements of group $\mathbb{F}_p^*$ can be represented by fixed point and nonfixed point, the probability that a random element $\beta \in \mathbb{F}_p^*$ is a nonfixed point is $\varphi(d)\lambda/p = 1 - \lambda/p$, which is sufficiently large.

Algorithm 12 (a new algorithm to ECDLP with auxiliary inputs). Consider the following:

Input: let $\{P, \alpha P, \alpha^k P, \dots, \alpha^{k^{\varphi(d)-1}} P \in G\}$, $\{k, k^2, \dots, k^{\varphi(d)-1} \in K\}$, and ξ a primitive element in $\mathbb{F}_p$, $f(x) = x + x^k + x^{k^2} \dots + x^{k^{\varphi(d)-1}}$;

Output: $\alpha \in \mathbb{F}_p^*$:

- (1) Set $\zeta \leftarrow \xi^d$,
- (2) [Step 1] Compute $f(\alpha)P = \alpha P + \alpha^k P \dots + \alpha^{k^{\varphi(d)-1}} P$,
- (3) Randomly choose $\beta \in \mathbb{F}_p^*$ and compute $f(\beta)P = (\beta + \beta^k \dots + \beta^{k^{\varphi(d)-1}})P$,
- (4) [Step 2] $m \leftarrow \lceil \sqrt{\lambda} \rceil$,
- (5) Find $0 \leq u, v < m$, such that $\zeta^{mv} f(\alpha)P = \zeta^{-u} f(\beta)P$,
- (6) In case of failure, return to line 3 until $t \leftarrow mv + u$,
- (7) [Step 3] Find $k^l \in K$, $0 < l < \varphi(d)$ such that $\zeta^t \alpha P = \beta^{k^l} P$,
- (8) Output $\alpha = \zeta^{-t} \cdot \beta^{k^l}$.

In summary, if $P, \alpha P, \alpha^k P, \dots, \alpha^{k^{\varphi(d)-1}} P$ and multiplicative group K are given, the proposed algorithm computes α approximately in $\mathcal{O}(\sqrt{(p-1)/d} + d)$ group operations with storage $\mathcal{O}(\sqrt{(p-1)/d})$ in $\mathbb{G}$.

6. Experimental Results

This section describes our experimental results of our new algorithm for an elliptic curve. We successfully solved ECDLP-wAI by our implementation in a group $\mathbb{G}$ with 61-bit order.

6.1. Parameters. We use an addition cyclic group $\mathbb{G} = \langle P \rangle$ with order p on an elliptic curve $y^2 + xy = x^3 + x^2 + 415485412408256448$ defined over a binary finite field $\mathbb{F}_{2^{61}}$. Concrete values of these parameters are summarized in the following:

$$(i) \ q = 0x2000000000000000 \ (61 - \text{bit})$$

$$= 2^{61},$$

$$(ii) \ #E = 0x1FFFFFFFFF35AB90A \ (61 - \text{bit})$$

$$= 2305843009001535754$$

$$= 2 \times 1152921504500767877,$$

$$(iii) \ p = 0xFFFFFFFFF9AD5C85 \ (61 - \text{bit})$$

$$= 1152921504500767877,$$

$$(iv) \ p - 1 = 0xFFFFFFFFF9AD5C84 \ (61 - \text{bit})$$

$$= 2^2 \times 7 \times 1213 \times 33945398201059,$$

where $\#E$ denotes the number of points in $E(\mathbb{F}_{2^{61}})$. In the implementation of our new algorithm, we use the following parameters:

$$(i) \ \lambda = 950471149629652 \ (50 - \text{bit}),$$

$$(ii) \ \lceil \sqrt{\lambda} \rceil = 30829713 \ (25 - \text{bit}),$$

$$(iii) \ k = 1900942299259305,$$

$$(iv) \ d = 1213, |K| = 1212, K = \{k^i \mid i \in [0, 1211]\},$$

$$(v) \ G_{fp} = \langle \zeta \rangle = \langle 917376305973559977 \rangle \text{ and } |G_{fp}| = \lambda.$$

Here, d is chosen to minimize the time complexity of our algorithm. The element ζ is chosen as the generator of the multiplicative group G_{fp} . A base point P is randomly chosen from points in $E(\mathbb{F}_q)$ with order p . Given the coordinate of $P, P_1 = \alpha P, P_2 = \alpha^k P, P_3 = \alpha^{k^2} P, \dots, P_{1212} = \alpha^{k^{1211}} P$, the corresponding values for x and y are as follows:

$$x(P) = 0x15934FDA439710FD,$$

$$y(P) = 0x23394044E191AD5$$

$$x(P_1) = 0x1EBFBF5362EA038C,$$

$$y(P_1) = 0x1499B155A750CE2C$$

$$x(P_2) = 0x1A8DE21E255B38F8,$$

$$y(P_2) = 0x1A16E1F6A5367A3B$$

$\vdots$

$$x(P_{1212}) = 0x2C878114BD6109E,$$

$$y(P_{1212}) = 0x11C28EA554F98437.$$

6.2. Results. In this experiment, we randomly choose an element $\beta = 916588465071928542$.

Step 1. We compute $f(\alpha)P = \alpha P + \alpha^k P + \dots + \alpha^{k^{1211}} P$ and $f(\beta)P = (\beta + \beta^k + \dots + \beta^{k^{1211}})P$ as follows:

$$x(f(\alpha)P) = 0xF18BC6972DD660F,$$

$$y(f(\alpha)P) = 0x103F35553C14D081,$$

$$x(f(\beta)P) = 0x16983D29CE603AF0,$$

$$y(f(\beta)P) = 0x13E3CF104F63D01D.$$

(9)

Step 2. We search for the integer $0 \leq t < \lambda$ such that

$$\zeta^t \cdot f(\alpha)P = f(\beta)P. \quad (10)$$

It is equivalent to searching for integer $0 \leq u, v < \lceil \sqrt{\lambda} \rceil$, such that

$$\zeta^{\lceil \sqrt{\lambda} \rceil v} \cdot f(\alpha)P = \zeta^{-u} \cdot f(\beta)P. \quad (11)$$

We establish two databases $DB_L = \{\zeta^{i\lceil \sqrt{\lambda} \rceil} \cdot f(\alpha)P\}$ and $DB_R = \{\zeta^{-j} \cdot f(\beta)P\}$. To establish database DB_R , we have to compute and store the following points:

$$\zeta^{-0} \cdot f(\beta)P, \zeta^{-1} \cdot f(\beta)P, \zeta^{-2} \cdot f(\beta)P, \dots, \zeta^{-(\lceil \sqrt{\lambda} \rceil - 1)} \cdot f(\beta)P. \quad (12)$$

In order to reduce the storage space, we use the point compression technique as [18]. Each point $\zeta^{-j} \cdot f(\beta)P$ is digested as $LSB_{64}(MD5(x(P) \parallel y(P)))$, so each point needs 8 bytes.

Thus, $\lceil \sqrt{\lambda} \rceil \times 8 = 246637704$ bytes (≈ 235.2 Mbytes) is required for DB_R , and about 6.5 hours is required in total (on Pentium® Dual-Core CPU E5700 3.00 GHz). To establish database DB_L ,

$$\zeta^{0 \cdot \lceil \sqrt{\lambda} \rceil} \cdot f(\alpha)P, \zeta^{1 \cdot \lceil \sqrt{\lambda} \rceil} \cdot f(\alpha)P, \zeta^{2 \cdot \lceil \sqrt{\lambda} \rceil} \cdot f(\alpha)P, \dots, \zeta^{(\lceil \sqrt{\lambda} \rceil - 1) \cdot \lceil \sqrt{\lambda} \rceil} \cdot f(\alpha)P \quad (13)$$

were computed and stored. With the same space saving technique, $\lceil \sqrt{\lambda} \rceil \times 8 = 246637704$ bytes (≈ 235.2 Mbytes) was required for DB_L , and 6.5 hours was required in total.

Then, a collision $\zeta^{\lceil \sqrt{\lambda} \rceil v} \cdot f(\alpha)P = \zeta^{-u} \cdot f(\beta)P$ between two databases DB_L and DB_R was searched by a naive method. Since databases are small, the time for comparison is negligible. Collisions $v = 7$ and $u = 235$ were found. Thus, a solution

$$t = \lceil \sqrt{\lambda} \rceil v + u = 215808226 \quad (14)$$

can be found.

Step 3. To find α , we have known an integer t that satisfies $\zeta^t \cdot f(\alpha)P = f(\beta)P$; it is equivalent to $\zeta^t \cdot \alpha P = \beta^k P$ for $0 \leq l \leq 1211$. Locate $\zeta^t \cdot \alpha P$ from the set $\{\beta^{k^l} P\}$ to find $0 \leq l \leq 1211$ such that $\zeta^t \cdot \alpha P = \beta^{k^l} P$. Finally, we succeed in finding a solution $\alpha = \zeta^{-t} \cdot \beta^{k^l} = 1073972411177481784$ for $l = 1093$.

7. Conclusion

In this paper, we propose a new ECDLP-wAI and give an algorithm to solve the ECDLP efficiently. When given some points $P, \alpha P, \alpha^k P, \alpha^{k^2} P, \alpha^{k^3} P, \dots, \alpha^{k^{\varphi(d)-1}} P \in \mathbb{G}$ and multiplicative cyclic group K , our new algorithm can recover the secret key $\alpha \in \mathbb{F}_p^*$ in $\mathcal{O}(\sqrt{(p-1)/d} + d)$ group operations by using $\mathcal{O}(\sqrt{(p-1)/d})$ storage, where k is a generator of K and $\varphi(d)$ is the order of K . This algorithm can be used to attack these cryptographic schemes that admit an oracle returning k th power of its secret key upon an arbitrary input.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (nos. 61309016, 61379150, and 61103230), Fundamental Research Funds for the Central Universities (no. JB140302), and the National Cryptology Development Project of China (no. MMJJ201201004).

References

- [1] D. Shanks, "Class number, a theory of factorization and genera," in *Proceedings of the Symposia in Pure Mathematics*, vol. 20, pp. 415–440, 1971.
- [2] J. M. Pollard, "Monte carlo methods for index computations (mod p)," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.
- [3] P. C. Van Oorschot and M. J. Wiener, "Parallel collision search with cryptanalytic applications," *Journal of Cryptology*, vol. 12, no. 1, pp. 1–28, 1999.
- [4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
- [5] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology—EUROCRYPT 2004*, pp. 56–73, Springer, Berlin, Germany, 2004.
- [6] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT 2004*, pp. 223–238, Springer, Berlin, Germany, 2004.
- [7] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology—CRYPTO 2005*, V. Shoup, Ed., vol. 3621 of *Lecture Notes in Computer Science*, pp. 258–275, Springer, Berlin, Germany, 2005.
- [8] J. H. Cheon, "Security analysis of strong diffie-hellman problem," in *Advances in Cryptology—EUROCRYPT 2006*, vol. 4004, pp. 1–11, Springer, Berlin, Germany, 2006.
- [9] J. H. Cheon, "Discrete logarithm problems with auxiliary inputs," *Journal of Cryptology*, vol. 23, no. 3, pp. 457–476, 2010.
- [10] T. Satoh, "On generalization of Cheon's algorithm," IACR Cryptology ePrint Archive 2009:58, 2009.
- [11] T. Kim, *Integer factorization and discrete logarithm with additional information [Ph.D. thesis]*, Seoul National University, 2011.
- [12] M. Kim, J. H. Cheon, and I.-S. Lee, "Analysis on a generalized algorithm for the strong discrete logarithm problem with auxiliary inputs," *Mathematics of Computation*, vol. 83, no. 288, pp. 1993–2004, 2014.
- [13] T. Kim and C. J. Hee, "A new approach to discrete logarithm problem with auxiliary inputs," IACR Cryptology ePrint Archive 2012:609, 2012.
- [14] Y. Sakemi, G. Hanaoka, T. Izu, M. Takenaka, and M. Yasuda, "Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve," in *Public Key Cryptography—PKC 2012*, M. Fischlin, J. Buchmann, and M. Manulis, Eds., vol. 7293 of *Lecture Notes in Computer Science*, pp. 595–608, Springer, New York, NY, USA, 2012.

- [15] D. R. L. Brown and R. P. Gallant, “The static Diffie-Hellman problem,” Cryptology ePrint Archive Report 2004/306, 2004, <https://eprint.iacr.org/2004/306>.
- [16] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, 1980.
- [17] S. Lang, *Algebra*, Graduate Texts in Mathematics, Springer, New York, NY, USA, 3rd edition, 2002.
- [18] T. Izu, M. Takenaka, and M. Yasuda, “Experimental results on Cheon’s algorithm,” in *Proceedings of the 5th International Conference on Availability, Reliability, and Security (ARES '10)*, pp. 625–628, IEEE, February 2010.

Hindawi

Submit your manuscripts at
<http://www.hindawi.com>