A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs

Jung Hee Cheon(✉), Taechan Kim, and Yong Soo Song

Department of Mathematical Sciences and ISaC-RIM,
Seoul National University, Seoul, South Korea
{jhcheon,yoshiki1,lucius05}@snu.ac.kr

Abstract. The Discrete Logarithm Problem with Auxiliary Inputs (DLPwAI) is an important cryptographic hard problem to compute $\alpha \in \mathbb{Z}_p$ for given $g, g^\alpha, \cdots, g^{\alpha^d}$ where g is a generator of a group of order p. In this paper, we introduce a generalized version of this problem, so called the generalized DLPwAI (GDLPwAI) problem which is asked to compute α for given $g, g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_d}}$, and propose an efficient algorithm when $K := \{e_1, \cdots, e_d\}$ is a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$. Although the previous algorithms can only compute α when $p \pm 1$ has a small divisor d, our algorithm resolves the problem when neither $p+1$ or $p-1$ has an appropriate small divisor. Our method exploits a group action of K on $\mathbb{Z}_p^\times$ to partition $\mathbb{Z}_p^\times$ efficiently.

Keywords: The discrete logarithm problem · The discrete logarithm problem with auxiliary inputs · Cheon's algorithm

1 Introduction

The Discrete Logarithm Problem (DLP) is a cryptographic hard problem which is asked to find $\alpha \in \mathbb{Z}_p$ for given g and g^α where g is a generator of a group G of prime order p. In recent decades, many variants of this hard problem such as the Bilinear Diffie-Hellman Problem (BDHP) [6], the ℓ-Strong Diffie-Hellman Problem (ℓ-SDHP) [2], the Bilinear Diffie-Hellman Exponent Problem [7], and the Bilinear Diffie-Hellman Inverse Problem [1] have been introduced to support the security of many cryptographic applications using pairing groups such as ID-based encryption (IBE) [1,6], the short signatures [2], the broadcast encryption [7], and so on [3–5,8]. In spite of the importance of these computational problems, there have been only few researches on these assumptions to the best of our knowledge. The first realization of this importance was done by Brown and Gallant [9] and Cheon [10,11]. Brown and Gallant presented an algorithm to compute α for given $g, g^\alpha, g^{\alpha^d}$ when d divides $p-1$. Cheon generalized this problem into the Discrete Logarithm Problem with Auxiliary Inputs (DLPwAI), which finds the value α for given $g, g^\alpha, \cdots, g^{\alpha^d}$, and solved it when either $p-1$ or $p+1$ has a small divisor d. Jao and Yoshida [14] gave an algorithm to forge the Boneh-Boyen signatures using the Cheon's algorithm.

T. Lange, K. Lauter, and P. Lisoněk (Eds.): SAC 2013, LNCS 8282, pp. 121–135, 2014.
DOI: 10.1007/978-3-662-43414-7_6,

The idea of Cheon is to utilize the embedding to an auxiliary group such as $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$. The similar technique to embed into auxiliary groups such as an elliptic curve group or a finite field can also be found in the famous reduction algorithms from the DL problem to the DH problem [13,18,19]. After the Cheon's algorithm, Satoh [21] tried to generalize the attack using an embedding $\mathbf{F}_p$ into a subgroup of order $\Phi_k(p)$ in $GL(n, \mathbf{F}_p)$, where $\Phi_k(x)$ is the k-th cyclotomic polynomial for $k \geq 3$, but the efficiency of the algorithm was not clear. Finally, Kim [15] realized that the Satoh's algorithm essentially uses an embedding from $\mathbf{F}_p$ into $\mathbf{F}_{p^n}$ and proved that the algorithm can never be faster than the ordinary algorithm for the DLP when $d|\Phi_k(p)$ for $k \geq 3$. All these algorithms are developed by embedding an element in $\mathbf{F}_p$ into a certain auxiliary group. More recently, Kim and Cheon [16] suggested rather different approach. Their result reduced the problem to find a polynomial with small value sets. However, finding a good polynomial with small value sets is not easy and still open.

In this paper, we introduce the generalized version of the DLPwAI called the GDLPwAI. The GDLPwAI is a problem to compute $\alpha \in \mathbb{Z}_p$ for given $g, g^{\alpha^{e_1}}, \cdots g^{\alpha^{e_d}}$. The rest of the paper is devoted to recover α efficiently but heuristically when $K := \{e_i : 1 \leq i \leq d\}$ is a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$ (Theorem 2). Note that in our algorithm e_i's do not divide $p-1$ while the Cheon's algorithm requires g^{α^d} as an instance for a small divisor d of $p \pm 1$.

The outline of the proof is as follows: (1) For a multiplicative subgroup $K \leq \mathbb{Z}_{p-1}^{\times}$, we define the K-group action on $\mathbb{Z}_p^{\times}$ to partition $\mathbb{Z}_p^{\times}$ into orbits generated by group action. (2) Then we define a polynomial $f(x)$ over $\mathbb{Z}_p$ which takes the same value for all elements in an orbit but takes different values for those elements in different orbits. (3) Finally, for randomly chosen β from $\mathbb{Z}_p^{\times}$, we find an orbit containing β by computing $g^{f(\beta)}$ and finding a collision with $g^{f(\alpha_j)}$ where $\alpha_j = \zeta^{-j}\alpha$'s are the representatives of distinct orbits. By solving the equation $f(\beta) = f(\alpha_j)$, we can find the desired value α.

For a multiplicative subgroup K of $\mathbb{Z}_p^{\times}$ we define a K-group action on $\mathbb{Z}_p^{\times}$ by $(k, x) \mapsto x^k$ for $x \in \mathbb{Z}_p^{\times}$ and $k \in K$. Then the orbit generated by x is a set $\{x^k : k \in K\}$. In particular, an orbit containing just one element is called a fixed point. We show that the set of fixed points is generated by an element ζ, a primitive λ-th root of unity for $\lambda := \gcd(K-1)$, which is defined to be the greatest common divisor of $(k-1)$'s for all integers k such that $k \bmod (p-1)$ belongs to K. Moreover, the collection of orbits $(\zeta^i\alpha)^K$ is pairwise disjoint for $0 \leq i < \lambda$ and each orbit contains exactly $|K|$ elements, if α^k are distinct for all $k \in K$. Hence $\lambda|K|$ elements of $\mathbb{Z}_p^{\times}$ belong to one of orbits $(\zeta^i\alpha)^K$ for some i.

Now define a polynomial $f_K(x)$ by $\sum_{k\in K} x^k$ for K. Then f_K takes the same value for the elements in the same orbit and $f_K(\zeta^i x) = \zeta^i f_K(x)$ for a fixed point ζ. For given g^{α^k} for all $k \in K$, we compute $g^{f(\alpha)}$ in $|K|$ group multiplications and compute $g^{f(\beta)}$ for randomly chosen $\beta \in \mathbb{Z}_p^{\times}$. If β belongs one of orbits $(\zeta^i\alpha)^K$, then we can find $t \in [0, \lambda)$ such that $g^{f(\alpha)} = g^{\zeta^t f(\beta)}$ in $O(\sqrt{\lambda})$ exponentiations using the baby-step giant-step technique. Finally by finding $k \in K$ satisfying $\alpha^k = \zeta^t\beta$, we can recover the value α. Since the probability that a

random $\beta \in \mathbb{Z}_p^\times$ belongs to one of the orbits is $\lambda|K|/(p-1)$, the total complexity is $O\left(\frac{p}{\lambda|K|}(\sqrt{\lambda}+|K|)\right)$ exponentiations in $\mathbb{Z}_p$ and G. Under the assumption that the cost of a group operation in G is a constant times of the cost of a multiplication in $\mathbb{Z}_p$, the total complexity can be lowered down $O(p^{1/3}\log p)$ multiplications in $\mathbb{Z}_p$ when $\sqrt{\lambda} \approx |K| \approx p^{1/3}$.

It also remains an open question to solve the usual DLPwAI by using our algorithm to solve the GDLPwAI.

Organization. In Sect. 2, we introduce a new representation for multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$. In Sect. 3, we define a group action on $\mathbb{Z}_p^\times$ and develop how all elements in $\mathbb{Z}_p^\times$ can be represented with only a few elements. In Sect. 4, we construct a polynomial over $\mathbb{Z}_p$ which takes the same value on the same orbit. Finally, we prove our theorem in Sect. 5 and conclude in Sect. 6.

2 Multiplicative Subgroups of $\mathbb{Z}_n^\times$

Before the state of our main theorem, we first introduce somewhat new representation for multiplicative subgroup K of $\mathbb{Z}_n^\times$. From our observation, elements of a multiplicative subgroup $K \leq \mathbb{Z}_n^\times$ seem to form an arithmetic sequence in many cases.

2.1 Representation of a Multiplicative Subgroup of $\mathbb{Z}_n^\times$

Definition 1. *For any positive integer n, let S be a subset of $\mathbb{Z}_n$. We define* $\gcd(S;\mathbb{Z}_n)$ *or* $\gcd(S)$ *unless confused, to be the greatest common divisor of all integers x such that x mod n belongs to S. Given a divisor λ of n, we define a subset K_λ of $\mathbb{Z}_n^\times$ by $K_\lambda := (1+\lambda\mathbb{Z}_n)\cap\mathbb{Z}_n^\times$, where $1+\lambda\mathbb{Z}_n := \{1+\lambda m : m \in \mathbb{Z}_n\}$.*

We can see that K_λ is a multiplicative subgroup of $\mathbb{Z}_n^\times$ because it is closed under the multiplication and inverse. If K is a multiplicative subgroup of $\mathbb{Z}_n^\times$, then K is a subgroup of K_λ for $\lambda = \gcd(K-1)$ where $K-1 = \{k-1 : k \in K\} \subseteq \mathbb{Z}_n$.

Remark 1. For an even integer n and any multiplicative subgroup $K \leq \mathbb{Z}_n^\times$, every element of K is an odd integer so that $\gcd(K-1)$ is even. It shows that

$$K_\lambda = (1+\lambda\mathbb{Z}_n)\cap\mathbb{Z}_n^\times = (1+2\lambda\mathbb{Z}_n)\cap\mathbb{Z}_n^\times = K_{2\lambda}$$

for odd λ. For this reason, we only treat the case that λ is even.

From now on, we restrict the case to $n = p-1$ for odd prime p. The next proposition determines the size of K_λ in $\mathbb{Z}_{p-1}^\times$ for given divisor λ of $p-1$.

Proposition 1. *Let λ be a divisor of $p-1$. Then $|K_\lambda| = \frac{p-1}{\lambda}\cdot\prod_{q\in Q}\left(1-\frac{1}{q}\right)$, where Q is the set of prime divisors of $p-1$ which do not divide λ. In particular, if $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$, then $|K_\lambda| = \phi(\frac{p-1}{\lambda})$, where ϕ denotes the Euler-totient function.*

Proof. Note that $1 + \lambda m \in K_\lambda$ if and only if $\gcd(1 + \lambda m, p - 1) = 1$, which is equivalent to $\gcd(1 + \lambda m, q) = 1$ for all $q \in Q$. Consider a surjective homomorphism

$$\begin{aligned} \pi : \mathbb{Z}_{p-1} &\longrightarrow \mathbb{Z}_\lambda \times \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_\ell} \\ x &\longmapsto (x \bmod \lambda, x \bmod q_1, \cdots, x \bmod q_\ell), \end{aligned}$$

where $Q = \{q_1, \cdots, q_\ell\}$. Then each element λm is in the set $K_\lambda - 1 \subseteq \mathbb{Z}_{p-1}$ if and only if $\pi(\lambda m)$ is contained in $\{0\} \times T$, where $T = (\mathbb{Z}_{q_1} \backslash \{-1\}) \times (\mathbb{Z}_{q_2} \backslash \{-1\}) \times \cdots \times (\mathbb{Z}_{q_\ell} \backslash \{-1\})$. Hence

$$\begin{aligned} |K_\lambda| = |K_\lambda - 1| &= |\pi^{-1}(\{0\} \times T)| \\ &= |T| \cdot |\ker(\pi)| \\ &= \prod_{i=1}^{\ell} (q_i - 1) \cdot \left(\tfrac{p-1}{\lambda \cdot \prod_{i=1}^{\ell} q_i} \right) \\ &= \tfrac{p-1}{\lambda} \cdot \prod_{i=1}^{\ell} \left(1 - \tfrac{1}{q_i}\right) \end{aligned}$$

Moreover, if $\gcd\left(\lambda, \frac{p-1}{\lambda}\right) = 1$, then Q is the set of all prime divisors of $\frac{p-1}{\lambda}$. Thus, we have $|K_\lambda| = \phi\left(\frac{p-1}{\lambda}\right)$. □

Proposition 2. *If λ is an even divisor of $p - 1$, then* $\gcd(K_\lambda - 1; \mathbb{Z}_{p-1}) = \lambda$.

Proof. Let us use the same notations in the proof of Proposition 1. First, we note that an integer x such that $x \pmod{p-1} \in K_\lambda - 1 = \pi^{-1}(\{0\} \times T)$ is a multiple of λ, and $\gcd(K_\lambda - 1; \mathbb{Z}_{p-1})$ is a multiple of λ by definition.

Let $P = \{p_j : 1 \le j \le k\}$ be the set of common prime divisors of λ and $\frac{p-1}{\lambda}$. Then $P \dot\cup Q$ is the set of prime divisors of $\frac{p-1}{\lambda}$. Every element q of Q is greater than 2, and there exist integers m_i for $1 \le i \le \ell$ satisfying $\lambda m_i \pmod{q_i}$ is not equal to 0 or -1. Using the Chinese Remainder Theorem, we can find an integer m such that $m \equiv m_i \pmod{q_i}$ for all $1 \le i \le \ell$ and $m \equiv 1 \pmod{p_j}$ for all $1 \le k \le j$.

We can check that $1 + \lambda m$ is not divisible by $q \in Q$ and $1 + \lambda m \pmod{p-1}$ is contained in K_λ. In addition, $\gcd(\lambda m; \mathbb{Z}_{p-1}) = \lambda \gcd(m; \mathbb{Z}_{\frac{p-1}{\lambda}}) = \lambda$ since m is not divisible by every prime divisor of $\frac{p-1}{\lambda}$. Hence, $\gcd(K_\lambda - 1; \mathbb{Z}_{p-1})$ is equal to λ. □

Example 1. Consider a prime $p = 29$ and $\lambda = 4$ be an even divisor of $p - 1$. Then, we have

$$K_\lambda = K_4 = \{1, 5, 9, 13, 17, 21, 25\} \cap \mathbb{Z}_{28}^\times,$$

and 21 is the only element which is not in $\mathbb{Z}_{28}^\times$. Since $\frac{p-1}{\lambda} = 7$, we can see that the cardinality of K_4 is $\phi(7) = 6$ as shown in Proposition 1. Also we can check that $\gcd(K_4 - 1) = 4$.

3 A Group Action on $\mathbb{Z}_p^\times$

In this section, we consider a K-group action on $\mathbb{Z}_p^\times$ and partition $\mathbb{Z}_p^\times$ into disjoint orbits generated by group action. A group action on a set clearly induces a

partition of the set with orbits. However, what we are dealing here is to partition $\mathbb{Z}_p^\times$ with only a few information. Namely, for a certain case, we can represent almost all elements of $\mathbb{Z}_p^\times$ with only two elements, one fixed point (*i.e.* an orbit with just one element) and the other point not a fixed point. We begin with defining the group action on $\mathbb{Z}_p^\times$. For more information on group theory, refer to [12,17].

Definition 2. *Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$. Define a K-action on $\mathbb{Z}_p^\times$ by $(k, x) \mapsto x^k$ for $k \in K$ and $x \in \mathbb{Z}_p^\times$. The K-orbit of x is a set $x^K := \{x^k : k \in K\}$. The set of fixed point $(\mathbb{Z}_p^\times)_K$ is a set $\{x \in \mathbb{Z}_p^\times : x^k = x \text{ for all } k \in K\}$*

We can easily check that Definition 2 satisfies the definition of group action. Note that we have $|x^K| = |K|/|K_x|$ where K_x is a stabilizer of x which is a set defined by $K_x := \{k \in K : x^k = x\}$, thus $|x^K| = |K|$ if and only if $|K_x| = 1$. The next proposition states that if two multiplicative subgroups H and K of $\mathbb{Z}_{p-1}^\times$ satisfies $\gcd(H-1) = \gcd(K-1)$, then the two sets of fixed points by H-action and K-action respectively are the same. Furthermore, the set of fixed points forms a cyclic group of order $\lambda = \gcd(H-1) = \gcd(K-1)$.

Proposition 3. *Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$ and $\lambda = \gcd(K-1)$. Then, $(\mathbb{Z}_p^\times)_K = (\mathbb{Z}_p^\times)_{K_\lambda} = \{z \in \mathbb{Z}_p^\times : z^\lambda = 1\}$.*

Proof. The set of fixed point by K-action is denoted by $(\mathbb{Z}_p^\times)_K = \{z \in \mathbb{Z}_p^\times : z^{k-1} = 1 \text{ for all } k \in K\}$. Now it is easy to see that $z^{k-1} = 1$ for all $k \in K$ if and only if $z^\lambda = 1$ where $\lambda = \gcd\{k-1 : k \in K\}$. Since $\lambda = \gcd(K-1) = \gcd(K_\lambda - 1)$, we have $(\mathbb{Z}_p^\times)_K = (\mathbb{Z}_p^\times)_{K_\lambda}$ by the same argument. □

Let ξ be a primitive element in $\mathbb{Z}_p$, then $\zeta = \xi^{\frac{p-1}{\lambda}}$ is a generator of a cyclic group of fixed points $(\mathbb{Z}_p^\times)_K = \langle\zeta\rangle = \{z \in \mathbb{Z}_p^\times : z^\lambda = 1\}$. Note that the orbit generated by $\zeta^i x$ satisfies $(\zeta^i x)^K = \zeta^i x^K$ for all $1 \le i \le \lambda$, since $\zeta^k = \zeta$ for all $k \in K$. The following proposition considers two orbits generated by $\zeta^i x$ and $\zeta^j x$ are disjoint for $0 \le i, j < \lambda$ and $i \ne j$.

Proposition 4. *(Disjoint Orbit Condition) Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$, ζ a generator of a cyclic group of fixed points $\{z \in \mathbb{Z}_p^\times : z^\lambda = 1\}$ for $\lambda = \gcd(K-1)$. If $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$, then two orbits $\zeta^i x^K$ and $\zeta^j x^K$ are disjoint i.e. $(\zeta^i x^K) \cap (\zeta^j x^K) = \emptyset$ for $0 \le i, j < \lambda, i \ne j$, and $x \in \mathbb{Z}_p^\times$.*

Proof. Note that two orbits are identical or disjoint. Suppose that $(\zeta^i x^K) \cap (\zeta^j x^K) \ne \emptyset$ for some i, j. Then, $\zeta^i x^K = \zeta^j x^K$ and $y := \zeta^{i-j} = x^{k_1 - k_2}$ for some $k := k_1 - k_2 \in K$. Since $\left(\zeta^{i-j}\right)^\lambda = 1$ and $\left(x^{k_1-k_2}\right)^{\frac{p-1}{\lambda}} = 1$ for a non-fixed point $x \in \mathbb{Z}_p^\times$, the order of y divides both λ and $\frac{p-1}{\lambda}$. In other words, it divides $\gcd(\lambda, \frac{p-1}{\lambda})$ which equals to 1, following that y must be equal to 1. □

Example 2. Let $K := K_4 = \{1, 5, 9, 13, 17, 25\} \leq \mathbb{Z}_{28}^{\times}$ and consider the K-action on $\mathbb{Z}_{29}^{\times}$. Then we have 4 disjoint orbits of length 6,

$$\begin{aligned} 2^K &= \{2, 2^5, 2^9, 2^{13}, 2^{17}, 2^{25}\} = \{2, 3, 19, 14, 21, 11\} \\ 4^K &= \{4, 9, 13, 22, 6, 5\} \\ 7^K &= \{7, 16, 20, 25, 24, 23\} \\ 8^K &= \{8, 27, 15, 18, 10, 26\}, \end{aligned}$$

and 4 fixed points $\{1, 12, 17, 28\}$. Note that $1^4 \equiv 12^4 \equiv 17^4 \equiv 28^4 \equiv 1 \bmod 29$.

Since there is an one-to-one correspondence between $\zeta^i x^K$ and $\zeta^j x^K$ for all i, j, they have the same number of elements. If we define

$$\mathcal{O}_{x,K} := x^K \,\dot\cup\, \zeta x^K \,\dot\cup\, \cdots \,\dot\cup\, \zeta^{\lambda-1} x^K,$$

where $\dot\cup$ denotes the disjoint union, we have $|\mathcal{O}_{x,K}| = |x^K|\lambda$ for $x \in \mathbb{Z}_p^{\times}$. Along with the set of fixed points, we have $|\mathcal{O}_{x,K} \cup \langle\zeta\rangle| = (|x^K| + 1)\lambda$ number of elements in $\mathbb{Z}_p^{\times}$ for a non-fixed point $x \in \mathbb{Z}_p^{\times}$. From now on, $\mathrm{ord}_p(x)$ denotes the order of x modulo p.

Remark 2. The set $\mathcal{O}_{x,K}$ behaves just like an extended orbit, which means that for $x, y \in \mathbb{Z}_p^{\times}$, $\mathcal{O}_{x,K}$ and $\mathcal{O}_{y,K}$ are disjoint or identical. In other words, $\mathcal{O}_{x,K} \cap \mathcal{O}_{y,K} \neq \emptyset$ implies $y = \zeta^i x^k$ and $\mathcal{O}_{x,K} = \mathcal{O}_{y,K}$. Therefore, $\mathbb{Z}_p^{\times}$ can be expressed by the disjoint union of distinct $\mathcal{O}_{x,K}$'s. Moreover, if $\mathcal{O}_{x,K} = \mathcal{O}_{y,K}$, then $y = \zeta^i x^k$ for some $0 \leq i < \lambda, k \in K$ and $y^\lambda = x^{\lambda k}$. It implies that $\mathrm{ord}_p(x^\lambda) = \mathrm{ord}_p(y^\lambda)$.

The next proposition gives a condition to satisfy $|x^K| = |K|$.

Proposition 5. *Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$, $\lambda = \gcd(K-1)$ and $x \in \mathbb{Z}_p$. If $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$, then $|x^K| = |K|$ for x satisfying $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$. In particular, if $\frac{p-1}{\lambda}$ is prime, then $|x^K| = |K|$ for $x \notin (\mathbb{Z}_p^{\times})_K$.*

Proof. Note that $|x^K| = |K|$ if and only if $|K_x| = |\{k \in K : x^k = x\}| = 1$. Suppose that $x^k = x$ for some $k = 1 + \lambda n \in K$ and $0 \leq n < \frac{p-1}{\lambda}$. It implies that $(x^\lambda)^n = 1$ for some $0 \leq n < \frac{p-1}{\lambda}$. However, since $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$, n must be zero. It follows that K_x contains only one element, $k = 1$.

Since $(x^\lambda)^{\frac{p-1}{\lambda}} \equiv 1 \pmod p$ for all $x \in \mathbb{Z}_p$, we have $\mathrm{ord}_p(x^\lambda)$ divides $\frac{p-1}{\lambda}$. In addition, $\mathrm{ord}_p(x^\lambda) = 1$ if and only if $x \in (\mathbb{Z}_p^{\times})_K$. Thus, if $\frac{p-1}{\lambda}$ is a prime, it follows that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$ if and only if $x \notin (\mathbb{Z}_p^{\times})_K$. □

Example 3. Note that for $p = 29$ and $\lambda = 4$, we have $|K| = |2^K| = |4^K| = |7^K| = |8^K| = 6$ for $K = K_4$, and $\langle 17\rangle = \{17, 28, 12, 1\}$ forms a cyclic group of fixed points. It is easily verified that $17 \cdot 2^K = 4^K$, $28 \cdot 2^K = 8^K$ and $12 \cdot 2^K = 7^K$, thus $\mathcal{O}_{2,K} = 2^K \,\dot\cup\, 4^K \,\dot\cup\, 8^K \,\dot\cup\, 7^K = \mathbb{Z}_{29}^{\times} \backslash \langle 17\rangle$.

The following proposition shows how many x's in $\mathbb{Z}_p^{\times}$ satisfy $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$.

Proposition 6. *Assume that λ is a divisor of $p-1$. Then there are exactly $\lambda\phi(\frac{p-1}{\lambda})$ elements x in $\mathbb{Z}_p^\times$ such that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$.*

Proof. Let ξ be a primitive element of $\mathbb{Z}_p$. There exists a unique $0 \le j < p$ satisfying $x = \xi^j$ for any $x \in \mathbb{Z}_p^\times$. We will use the fact that $\mathrm{ord}_p(\xi^i) = \frac{p-1}{\gcd(i,p-1)}$ for all i.

From $\mathrm{ord}_p(x^\lambda) = \mathrm{ord}_p(\xi^{\lambda j}) = \frac{p-1}{\gcd(\lambda j, p-1)} = \frac{p-1}{\lambda}\frac{1}{\gcd(j, \frac{p-1}{\lambda})}$, we show that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$ if and only if $\gcd(j, \frac{p-1}{\lambda}) = 1$. Therefore, there are exactly $\phi(\frac{p-1}{\lambda})$-number of j's modulo $\frac{p-1}{\lambda}$ satisfying $\gcd(j, \frac{p-1}{\lambda}) = 1$, thus $\lambda\phi(\frac{p-1}{\lambda})$-number of x's in $\mathbb{Z}_p^\times$ satisfying $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$. □

Note that $\lambda\phi(\frac{p-1}{\lambda}) = \lambda\frac{p-1}{\lambda}\prod_{q\in Q}(1-\frac{1}{q}) = (p-1)\prod_{q\in Q}(1-\frac{1}{q})$ where Q is the set of prime divisors of $\frac{p-1}{\lambda}$. Hence, if we randomly take x in $\mathbb{Z}_p^\times$, then the probability that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$ is $\prod_{q\in Q}(1-\frac{1}{q})$. Moreover, if $\frac{p-1}{\lambda}$ has only large prime divisors, then the probability $\prod_{q\in Q}(1-\frac{1}{q})$ will be almost equal to 1.

Combining these results with Proposition 1, we surprisingly obtain an immediate partition of $\mathbb{Z}_p^\times$. Recall that for an even divisor λ of $p-1$, we defined a multiplicative subgroup $K_\lambda = \{1+\lambda n : n \in [0, \frac{p-1}{\lambda}) \cap \mathbb{Z}\} \cap \mathbb{Z}_{p-1}^\times$.

Theorem 1. *Let λ be an even divisor of $p-1$ satisfying $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$ and K_λ be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$ defined as above. Consider the K_λ-action on $\mathbb{Z}_p^\times$. Let ζ be a generator of a cyclic group of fixed points by the K_λ-action, $\{z \in \mathbb{Z}_p^\times : z^\lambda = 1\}$. Then the followings hold:*

1. *If $\frac{p-1}{\lambda} = \mu$ is prime, then $\mathbb{Z}_p^\times = \mathcal{O}_{x,K_\lambda} \dot\cup (\mathbb{Z}_p^\times)_{K_\lambda}$ for $x \notin (\mathbb{Z}_p^\times)_{K_\lambda}$.*
2. *If $\frac{p-1}{\lambda} = \mu_1 \cdots \mu_\ell$ is square-free for prime $\mu_1, \cdots, \mu_\ell$, then $\mathbb{Z}_p^\times = \dot\cup_{J\subseteq I} \mathcal{O}_{x^{\mu_J},K_\lambda}$ for $x \in \mathbb{Z}_p^\times$ such that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$, where $I = \{1, 2, \cdots, \ell\}$ is an index set and $\mu_J = \prod_{j\in J}\mu_j$ for $J \subseteq I$ (For the convenience, define $\mu_\emptyset = 1$ for the empty subset $\emptyset \subseteq I$). In particular, $\mathcal{O}_{x^{\mu_I},K_\lambda} = (\mathbb{Z}_p^\times)_{K_\lambda}$.*

Proof. If $\frac{p-1}{\lambda} = \mu$ is prime, then $|K_\lambda| = \phi(\frac{p-1}{\lambda}) = \phi(\mu) = \mu - 1$ by Proposition 1. Note that $\mathcal{O}_{x,K_\lambda}$ and $(\mathbb{Z}_p^\times)_{K_\lambda}$ are disjoint subsets of $\mathbb{Z}_p^\times$ for $x \notin (\mathbb{Z}_p^\times)_{K_\lambda}$. Thus we have $|\mathcal{O}_{x,K_\lambda} \dot\cup (\mathbb{Z}_p^\times)_{K_\lambda}| = |\mathcal{O}_{x,K_\lambda}| + |(\mathbb{Z}_p^\times)_{K_\lambda}|$. By Proposition 5, we obtain $|\mathcal{O}_{x,K_\lambda}| = |x^{K_\lambda}|\lambda = |K_\lambda|\lambda = (\mu-1)\lambda$ and $|(\mathbb{Z}_p^\times)_{K_\lambda}| = \lambda$. Therefore, $|\mathcal{O}_{x,K_\lambda} \dot\cup (\mathbb{Z}_p^\times)_{K_\lambda}| = p-1$ deduces that $\mathcal{O}_{x,K_\lambda} \dot\cup (\mathbb{Z}_p^\times)_{K_\lambda} = \mathbb{Z}_p^\times$.

In the case that $\frac{p-1}{\lambda} = \mu_1 \cdots \mu_\ell$ is square-free and $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$, we have $|x^{K_\lambda}| = |K_\lambda| = \phi(\frac{p-1}{\lambda}) = \phi(\mu_I) = \prod_{1\le j\le \ell}(\mu_j - 1)$ by Proposition 1. For a subset J of I and $y = x^{\mu_J}$, we first calculate $|y^{K_\lambda}|$ and $|\mathcal{O}_{y,K_\lambda}|$ by using the fact that $|y^{K_\lambda}| = |K_\lambda|/|(K_\lambda)_y|$, where $(K_\lambda)_y = \{k \in K_\lambda : y^k = y\}$. Since $k = 1+\lambda n \in (K_\lambda)_y$ if and only if $y^{k-1} = (x^{\mu_J})^{\lambda\cdot n} = 1$ if and only if $\mu_{I\setminus J} = \mu_I/\mu_J$ divides n, the size of $(K_\lambda)_y$ is equal to the number of n satisfying that $1+\lambda n \in \mathbb{Z}_{p-1}^\times$, $0 \le n < \mu_I$ and $\mu_{I\setminus J}$ divides n. Therefore, by the similar argument in Proposition 1, we get

$$
\begin{aligned}
|(K_\lambda)_y| &= \left|\left\{n \in [0,\mu_I) \cap \mathbb{Z} : 1+\lambda n \in \mathbb{Z}_{p-1}^\times \text{ and } \mu_{I\setminus J} | (\lambda n)\right\}\right| \\
&= \left|\left\{n \in [0,\mu_I) \cap \mathbb{Z} : \mu_j \nmid (1+\lambda n) \text{ for each } j \text{ and } \mu_{I\setminus J} | n\right\}\right| \\
&= \frac{\mu_I}{\mu_{I\setminus J}} \cdot \prod_{j\in J}\left(1-\frac{1}{\mu_j}\right) \\
&= \mu_J \cdot \prod_{j\in J}\left(1-\frac{1}{\mu_j}\right) = \phi(\mu_J),
\end{aligned}
$$

resulting $|y^{K_\lambda}| = \frac{|K_\lambda|}{|(K_\lambda)_y|} = \frac{\phi(\mu_I)}{\phi(\mu_J)} = \phi(\mu_{I\setminus J})$ and $|\mathcal{O}_{y,K_\lambda}| = \lambda |y^{K_\lambda}| = \lambda\phi(\mu_{I\setminus J})$.

Since $\mathcal{O}_{x^{\mu_J},K_\lambda}$'s are pairwise disjoint for all $J \subseteq I$, we have $|\dot\cup_{J\subseteq I}\, \mathcal{O}_{x^{\mu_J},K_\lambda}| = \sum_{J\subseteq I} |\mathcal{O}_{x^{\mu_J},K_\lambda}| = \lambda \sum_{J\subseteq I} \phi(\mu_{I\setminus J})$. Finally, using elementary number theory, we have $\sum_{J\subseteq I} \phi(\mu_{I\setminus J}) = \sum_{d|\mu_I} \phi(d) = \mu_I$ and $|\dot\cup_{J\subseteq I}\, \mathcal{O}_{x^{\mu_J},K_\lambda}| = \lambda \cdot \mu_I = p-1$ deducing that $\mathbb{Z}_p^\times = \dot\cup_{J\subseteq I}\, (\mathcal{O}_{x^{\mu_J},K_\lambda})$. □

Note that for any given $x \in \mathcal{O}_{y,K_\lambda}$, there exist $0 \le i < \lambda$ and $k \in K_\lambda$ satisfying $x = \zeta^i y^k$. By virtue of Theorem 1, all elements in $\mathbb{Z}_p^\times$ can be expressed with only a few information. For example, we can simply partition $\mathbb{Z}_p^\times$ with only two elements $x \in \mathbb{Z}_p^\times - (\mathbb{Z}_p^\times)_{K_\lambda}$ and $\zeta \in (\mathbb{Z}_p^\times)_{K_\lambda}$, when $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$ and $q = \frac{p-1}{\lambda}$ is prime, so that any of element in $\mathbb{Z}_p^\times$ is of form $\zeta^i x^k$ for $0 \le i < \lambda$ and $k \in K$. In our example, with only $x = 2$ and $\zeta = 17$, we can express all elements in $\mathbb{Z}_{29}^\times$.

In the case of $\frac{p-1}{\lambda} = \mu_1 \cdots \mu_\ell$ is square-free and $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$, Remark 2 says that $\mathrm{ord}_p(y^\lambda) = \mu_{I\setminus J}$ if $y \in \mathcal{O}_{x^{\mu_J},K_\lambda}$. The converse is also true because $\mathbb{Z}_p^\times = \dot\cup_{J\subseteq I}\, \mathcal{O}_{x^{\mu_J},K_\lambda}$ and y cannot be contained in $\mathcal{O}_{x^{\mu_{J'}},K_\lambda}$ for $J \ne J' \subseteq I$.

4 Polynomial Construction

In this section, we will define a polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree d having small value sets. Recently, the similar idea was developed by Kim and Cheon [16] to solve the DLPwAI. Their approach exploited the fast multipoint evaluation method, so the degree of their polynomial was restricted to at most $d \approx p^{1/3}$ due to the efficiency issue.

The polynomial we will use in this paper is of very large degree which might be greater than $p^{1/3}$ but is sparse (all but d coefficients are zero) and have small value sets. Thus the fast multipoint evaluation method as in [16] seems hardly to be applied in our case. Instead, we take somewhat different approach with the idea developed in Sect. 3. We will define a polynomial so that it takes the same value for all elements in an orbit. In the proof of our main theorem, we will make some lists of $f(\alpha_1), \cdots, f(\alpha_\ell)$ from $f(\alpha)$ where α_i's are the representatives of distinct orbits and α is a discrete log to find. Then we find an index j such that $f(\alpha_j) = f(\beta)$ for randomly chosen $\beta \in \mathbb{Z}_p^\times$ *i.e.* we find an orbit in which β is contained. For this process, $f(\alpha)$ should be nonzero.

Definition 3. *Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$. Define a polynomial $f_K(x)$ over $\mathbb{Z}_p$ by $f_K(x) := \sum_{k\in K} x^k$. We will simply write $f_K = f$ if there is no ambiguity in the meaning.*

By the definition, it is clear that f_K takes the same value for the elements in the same orbit defined by K-action.

Proposition 7. *For any $k \in K$ and $x \in \mathbb{Z}_p^\times$, we have $f(x^k) = f(x)$. If $\zeta^i \in (\mathbb{Z}_p^\times)_K$ is a fixed point, then $f(\zeta^i x) = \zeta^i f(x)$.*

Since the degree of $f = f_K$ might be large (approximately p), it looks hard to evaluate $f(\alpha_1), \cdots, f(\alpha_\ell)$ in $O(\ell)$ time complexity for random α_i's with fast multipoint evaluation method. However, for a non-fixed point $\alpha \in \mathbb{Z}_p^\times$ and a fixed point (not necessarily generator) $\zeta \in (\mathbb{Z}_p)_K$, we can compute $f(\alpha), f(\zeta\alpha) = \zeta f(\alpha), \cdots, f(\zeta^\ell\alpha) = \zeta^\ell f(\alpha)$ in ℓ multiplications by ζ with $O(|K|)$ exponentiations for computing $f(\alpha)$. Furthermore, if $f(\alpha)$ is nonzero, then we can deduce that all $\alpha, \zeta\alpha, \cdots, \zeta^\ell\alpha$ are the different representatives for distinct orbits. The following proposition calculates $f(x)$ explicitly in special cases.

Proposition 8. *Assume that λ is an even divisor of $p-1$ satisfying $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$. Let $K = K_\lambda$ and $f = f_K$ be defined as aforementioned. Then the followings hold:*

1. *If $\frac{p-1}{\lambda} = \mu$ is prime, then $f(x) \neq 0$ for $x \in \mathbb{Z}_p^\times$.*
2. *If $\frac{p-1}{\lambda} = \mu_1 \cdots \mu_\ell$ is square-free for prime $\mu_1, \ldots, \mu_\ell$, then $f(x) \neq 0$ for $x \in \mathbb{Z}_p^\times$.*

Proof. If $\frac{p-1}{\lambda} = \mu$ is prime, then $|K| = \mu - 1$ by Proposition 1. Consider a map from $\mathbb{Z}_\mu$ to itself defined by $n \mapsto (1 + \lambda n)$. Since λ and μ are relatively prime, this map is bijective. In other words, $1 + \lambda n$ for $0 \leq n < \mu$ induces complete residue modulo μ. Thus, there exists a unique $0 \leq n_0 < \mu$ such that $1 + \lambda n_0$ is divisible by μ. Therefore,

$$f(x) = \sum_{k\in K} x^k = \sum_{0\leq n<\mu} x^{1+\lambda n} - x^{1+\lambda n_0} = x \cdot \frac{x^{p-1} - 1}{x^\lambda - 1} - x^{1+\lambda n_0} = -x^{1+\lambda n_0}$$

for $x \notin (\mathbb{Z}_p^\times)_K$. Otherwise, if $x^\lambda = 1$ then $x^k = x$ for all $k \in K$ and $f(x) = (\mu - 1)x \neq 0$.

In the case of $\frac{p-1}{\lambda} = \mu_1 \cdots \mu_\ell$ is square-free, $|K| = \phi(\mu_1 \cdots \mu_\ell)$ by Proposition 1. By similar argument as above, for a subset J of an index set $I = \{1, 2, \cdots \ell\}$, let $\mu_J = \prod_{j\in J} \mu_j$, and define a map from $\mathbb{Z}_{\mu_J}$ to itself by $n \mapsto (1 + \lambda n)$. Since λ and μ_J are relatively prime, it also induces the complete residue modulo μ_J. Thus, there exists a unique $0 \leq n_J < \mu_J$ such that $1 + \lambda n_J$ is divisible by μ_J (For convenience, define $\mu_J = 1$ and $n_J = 0$ for empty set $J = \emptyset$). We easily check that $n_J \equiv n_I \pmod{\mu_J}$ for all $J \subseteq I$. Now, $\mathrm{ord}_p(x^\lambda) = \mu_{I_0}$ for some $I_0 \subseteq I$ since $\mathrm{ord}_p(x^\lambda)$ is a divisor of $\frac{p-1}{\lambda} = \mu_I$. For $J \subseteq I$, $x^{\lambda\mu_J} = 1$ if and only if $I_0 \subseteq J$.

Using the inclusion–exclusion principle, we have

$$f(x) = \sum_{k \in K} x^k = \sum_{J \subseteq I} (-1)^{|J|} \sum_n x^{1+\lambda n},$$

where n in summation runs through $0 \le n < \mu_I$ satisfying $n \equiv n_J \pmod{\mu_J}$.

If $I_0 \not\subseteq J \subseteq I$, then $x^{\lambda \mu_J} \neq 1$ and $\sum_n x^{1+\lambda n} = x^{1+\lambda n_J} \frac{x^{p-1}-1}{x^{\lambda \mu_J}-1} = 0$. Otherwise $I_0 \subseteq J \subseteq I$, then $x^{\lambda \mu_J} = 1$ and $\sum_n x^{1+\lambda n} = \sum_n x^{1+\lambda n_J} = \frac{\mu_I}{\mu_J} x^{1+\lambda n_J} = \mu_{I \setminus J} x^{1+\lambda n_I}$ since n in summation is equivalent to n_J modulo μ_J, and $n_J \equiv n_I \pmod{\mu_J}$.

Finally, we have

$$\begin{aligned} f(x) =& \sum_{J \subseteq I} (-1)^{|J|} \sum_n x^{1+\lambda n} = \sum_{I_0 \subseteq J \subseteq I} (-1)^{|J|} \sum_n x^{1+\lambda n} \\ =& x^{1+\lambda n_I} \sum_{I_0 \subseteq J \subseteq I} (-1)^{|J|} \mu_{I \setminus J} = x^{1+\lambda n_I} \sum_{J \subseteq I \setminus I_0} (-1)^{|I \setminus J|} \mu_J \\ =& x^{1+\lambda n_I} (-1)^{\ell} \prod_{j \in I \setminus I_0} (1 - \mu_j) \neq 0. \end{aligned}$$

In particular, if $\mathrm{ord}_p(x^\lambda) = \mu_I$, then $f(x) = (-1)^\ell x^{1+\lambda n_I}$. □

The above proposition says that $f_K(x)$ is not identically zero for $K_\lambda = K$ for even divisor λ of $p-1$. Actually, it appears to be of form $f_K(x) = -x^d$ where $\gcd(d, p-1)$ is large, however in our application, it is desirable that $f_K(x) \neq 0$ but is not of simple form such as x^d, where d has large common divisor with $p-1$, since this simple form leads us to the already known Cheon's $p-1$ algorithm. In many cases, for a non proper subgroup K of K_λ, $f_K(x)$ also tends to not to be identically zero, although it seems hard to show it.

Example 4. For $K = K_4 = \{1, 5, 9, 13, 17, 25\} \le \mathbb{Z}_{28}^\times$, define $f_K(x) = x + x^5 + x^9 + x^{13} + x^{17} + x^{25} = -x^{21} \in \mathbb{Z}_{29}[x]$, where 21 and 28 have common divisor 7. For a subgroup $K' = \langle 9 \rangle = \{9, 25, 1\}$ of K, we have $K/\langle 9 \rangle = \{1, 5\}$. Now consider $f_{K'}(x) = x + x^9 + x^{25}$. Then $f_{K'}(x)$ takes same value for x in the same orbit. We have 8 disjoint orbits of length 3 and 4 fixed points. Note that the fixed points for K and K' are same as shown in Proposition 3.

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

The polynomial $f_{K'}(x)$ takes nonzero value $2 + 19 + 11 \equiv 3 \bmod 29$ for all $x \in 2^{K'}$, and we can check that $f_{K'}(x)$ take distinct values for disjoint orbits.

Proposition 9. *Assume that λ is an even divisor of $p-1$ satisfying $\gcd(\lambda, \frac{p-1}{\lambda}) = 1$. Let $K = K_\lambda$ and $f = f_K$. If $\frac{p-1}{\lambda} = q^e$ for some prime q and $e \ge 2$, then $f(x) = 0$ unless $x^{\lambda q} = 1$ in $\mathbb{Z}_p^\times$.*

Proof. Since $\frac{p-1}{\lambda}$ has only one prime divisor q, we can efficiently express elements of K and compute $f(x)$. For $n \in \mathbb{Z}_\mu$, $1+\lambda n$ is contained in K if and only if $\gcd(1+\lambda n, q) = 1$. Since $1+\lambda n \equiv 0 \pmod{q}$ has exactly one solution $n_0 \equiv -\lambda^{-1}$ in modulo q, there exist q^{e-1}-number of solutions $\{n_0 + qm : 0 \le m < q^{e-1}\}$ in $\mathbb{Z}_\mu$. Therefore, $f(x)$ is computed by

$$\begin{aligned} f(x) = &\sum_{n \in [0, \frac{p-1}{\lambda}) \cap \mathbb{Z}, 1+\lambda n \in K} x^{1+\lambda n} = \sum_{0 \le n < q^e} x^{1+\lambda n} - \sum_{0 \le m < q^{e-1}} x^{1+\lambda(n_0+qm)} \\ =&x \left(\sum_{0 \le n < q^e} x^{\lambda n} \right) - x^{1+\lambda n_0} \left(\sum_{0 \le m < q^{e-1}} x^{\lambda q m} \right), \end{aligned}$$

and it is equal to zero unless $x^{\lambda q} = 1$. However, there are only $\lambda q = \frac{p-1}{q^{e-1}}$-number of such elements x in $\mathbb{Z}_{p-1}^\times$. □

In general, if $\frac{p-1}{\lambda}$ is not square-free, then $f_{K_\lambda}(x) = 0$ for most of the elements in $\mathbb{Z}_{p-1}^\times$. Modifying the proofs of Propositions 8 and 9 easily show it. We will omit details here.

5 Main Theorem

By using a group action on $\mathbb{Z}_p^\times$, we can efficiently partition $\mathbb{Z}_p^\times$ with only a few elements. This leads us to a new algorithm that solves the GDLPwAI efficiently. Now we can state our main theorem as follows.

Theorem 2. *Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^\times$ with $\lambda = \gcd(K-1)$. Assume that we are given $\left\{ \left(k, g^{\alpha^k} \right) : k \in K \right\}$ and $|\alpha^K| = |K|$. Then, we can solve $\alpha \in \mathbb{Z}_p$ in $O\left(\frac{p}{\lambda}\right)$ exponentiations in $\mathbb{Z}_p$ and $O\left(\frac{p}{|K|\sqrt{\lambda}} + |K|\right)$ exponentiations in G unless $\sum_{k \in K} \alpha^k = 0$.*

Proof. We give a sketch of the proof following the next steps.

1. For given g^{α^k} for all $k \in K$, one computes $g^{f(\alpha)} = \prod_{k \in K} g^{\alpha^k} \in G$ in $|K|$ multiplications in G. Note that $g^{f(\alpha)} \neq 1$, since $f(\alpha) \neq 0$.
2. Take a random element β from $\mathbb{Z}_p^\times$ and compute $f(\beta) = \sum_{k \in K} \beta^k \in \mathbb{Z}_p$ in $|K|$ exponentiations in $\mathbb{Z}_p$. If $\beta \in \mathcal{O}_{\alpha,K}$, then there exists a unique $0 \le t < \lambda$ satisfying $\alpha^K = \zeta^t \beta^K$ and $f(\alpha) = \zeta^t f(\beta)$.
3. To find such t, we use Baby-Step Giant-Step method. Let $L := \lceil \sqrt{\lambda} \rceil$. Make two lists $\{g^{f(\zeta^{L \cdot i}\beta)} = (g^{f(\beta)})^{\zeta^{L \cdot i}} \in G : 0 \le i < L\}$ and $\{g^{f(\zeta^{-j}\alpha)} = (g^{f(\alpha)})^{\zeta^{-j}} \in G : 0 \le j < L\}$ in $2\sqrt{\lambda}$ exponentiations in G. If $\beta \in \mathcal{O}_{\alpha,K}$, these two lists must have a collision since there exist $0 \le i, j < L$ satisfying $t = Li + j$.
4. Repeat the steps 2 and 3 until finding a collision. The expected number of repetitions is $\frac{p}{|K|\lambda}$, since the probability that $\beta \in \mathcal{O}_{\alpha,K}$ is $\frac{|\mathcal{O}_{\alpha,K}|}{p} = \frac{|\alpha^K|\lambda}{p} = \frac{|K|\lambda}{p}$.

5. Locate $g^{\zeta^t\beta}$ from the set $\left\{g^{\alpha^k} : k \in K\right\}$ to find $k_0 \in K$ such that $g^{\alpha^{k_0}} = g^{\zeta^t\beta}$. This gives $\alpha = (\zeta^t\beta)^{k_0^{-1}}$ in $|K|$ comparisons in G.

We carry out the above process in

$|K|$ multiplications in G in Step 1, $O\left(\frac{p}{|K|\lambda} \cdot |K|\right) = O\left(\frac{p}{\lambda}\right)$ exponentiations in $\mathbb{Z}_p$ in Steps 2 and $O\left(\frac{p}{|K|\sqrt{\lambda}}\right)$ exponentiations in G in Step 3 and 4, and $|K|$ comparisons in G in Step 5. The overall complexity is as in the theorem. □

Remark 3. In the proof of Theorem 2, we may find a fake collision. That is, some element $\beta \in \mathbb{Z}_p$ could satisfy $f(\alpha) = \zeta^t f(\beta)$ but $\zeta^t\beta \notin \alpha^K$. If a fake collision occurs in Step 3 and 4, there would be no element $k_0 \in K$ such that $\alpha^{k_0} = \zeta^t\beta$ and we can check it in Step 5. They do not affect the total complexity.

For any multiplicative subgroup K of $\mathbb{Z}_{p-1}^\times$, K is a multiplicative subgroup of K_λ where $\lambda = \gcd(K-1)$. Hence we can define $\kappa = [K_\lambda : K]$.

Corollary 1. *For a multiplicative subgroup K of $\mathbb{Z}_p^\times$, set $\lambda = \gcd(K-1)$ and define $\kappa = [K : K_\lambda]$. Assume that the computational cost for the multiplications in G is a constant times of the cost for the multiplications in $\mathbb{Z}_p$. Then we can solve the GDLPwAI in $O\left(\left(\kappa\sqrt{\lambda} + \frac{p}{\lambda}\right)\log p\right)$ multiplications in $\mathbb{Z}_p$.*

Proof. In Proposition 1, we showed that $|K_\lambda| = \frac{p-1}{\lambda}\prod_{q\in Q}(1-\frac{1}{q})$ where Q is the set of prime divisors of $p-1$ not dividing λ. We may assume that $\prod_{q\in Q}(1-\frac{1}{q})$ is a constant greater than zero since $\prod_{q\in Q}(1-\frac{1}{q}) \geq \frac{\phi(\frac{p-1}{\lambda})}{\frac{p-1}{\lambda}} \geq \frac{1}{6\log\log\frac{p-1}{\lambda}}$ and $\log\log\frac{p-1}{\lambda}$ is not so large for usual size of p. In fact, $\prod_{q\in Q}(1-\frac{1}{q})$ is much greater than this lower bound in almost cases. Then we have $|K| = \frac{|K_\lambda|}{\kappa} = O\left(\frac{p}{\lambda\kappa}\right)$ and $\frac{p}{|K|\sqrt{\lambda}} = O\left(\kappa\sqrt{\lambda}\right)$.

By Theorem 2, the overall complexity is $O(|K|\log p) = O\left(\frac{p}{\lambda}\log p\right)$ multiplications in $\mathbb{Z}_p$ and $O\left(\left(|K| + \frac{p}{|K|\sqrt{\lambda}}\right)\log p\right) = O\left(\left(\kappa\sqrt{\lambda} + \frac{p}{\lambda}\right)\log p\right)$ multiplications in G. By the assumption, we can put them together in one notation. □

Example 5. Consider a multiplicative group $\mathbb{Z}_q^\times$ for prime $q = 1984044749$. The element $g = 268435456 \in \mathbb{Z}_q^\times$ generates the multiplicative subgroup $G = \langle g\rangle$ of 20-bit prime order $p = 70858741$. Suppose that we are given $\left\{\left(k, g^{\alpha^k}\right) : k \in K\right\}$ $= \{(1, 368141755), (9447833, 908277040), (14171749, 1018628336), (51963077, 651549246)\}$ for the multiplicative subgroup K of $\mathbb{Z}_{p-1}^\times$ with $\lambda = \gcd(K; \mathbb{Z}_{p-1}) = 4723916$. Following Theorem 2, we have $g^{f(\alpha)} = 104646375$ and $f(\beta) = 29994755$ for randomly chosen $\beta = 27015355$ in G. Using the BSGS technique, we find $t = 993142$ satisfying $g^{f(\alpha)} = g^{\zeta^t f(\beta)}$ for a primitive element ξ and a fixed point $\zeta = \xi^{\frac{p-1}{\lambda}}$. Then we find out that $\alpha^{k_0} = \zeta^t\beta$ for $k_0 = 51963077$ by comparing $g^{\zeta^t\beta}$ with $\{g^{\alpha^k} : k \in K\}$. Finally, we have $\alpha = (\zeta^t\beta)^{k_0^{-1}} = 37217684$.

Example 6. We use the same notations with Example 5. Set $q = 8307519720650407$, $g = 3814697265625 \in \mathbb{Z}_q^\times$. The element g has the order $p = 461528873369467$ of 50-bit prime. We are given our instance for a multiplicative subgroup K of K_λ such that $\lambda = 4742043558, |K_\lambda| = 97326, |K| = 16221$. Our algorithm finds that

$$\alpha = \zeta^t \beta = 55526261320836$$

for $\zeta = 265871590696697$, $\beta = 257387303120427$ and $t = 275438533$.

In summary, if we are given g^{α^k} for all $k \in K_\lambda$, then $\kappa = 1$ and we can solve the GSDL problem in $O\left(\left(\sqrt{\lambda} + \frac{p}{\lambda}\right)\log p\right)$. However, in this case, $g^{f_{K_\lambda}(\alpha)} = g^{-d}$ with nontrivial $\gcd(d, p-1)$, which falls into the Cheon's $p-1$ algorithm. When we are working with $|K| < |K_\lambda|$, then we need to carry out $O\left(\left(\kappa\sqrt{\lambda} + \frac{p}{\lambda}\right)\log p\right)$ multiplications, so we want $\kappa > 1$ to be sufficiently small. The computation amount can be reduced to $O\left(p^{1/3}\log p\right)$, when κ is small enough and $\lambda \approx p^{2/3}$.

Remark 4. If we assume that α is chosen randomly in $\mathbb{Z}_p^\times$, the condition $|\alpha^K| = |K|$ is satisfied with high probability. As we mentioned in Proposition 5 and Proposition 6, there are $\lambda\phi(\frac{p-1}{\lambda})$-number of x's in $\mathbb{Z}_p^\times$ such that $\mathrm{ord}_p(x^\lambda) = \frac{p-1}{\lambda}$, and they satisfy $|x^K| = |K|$. Therefore, the probability is greater than $\frac{1}{6\log\log(p-1)}$, since $\frac{\lambda\phi(\frac{p-1}{\lambda})}{p-1} \geq \frac{\phi(p-1)}{p-1}$ and $\frac{\phi(n)}{n} \geq \frac{1}{6\log\log n}$ for all $n \geq 5$ [20].

Remark 5. It is hard to compute the probability of $\sum_{k\in K}\alpha^k = 0$ in general, but we can predict that $f_K(x) = 0$ has not so many roots in $\mathbb{Z}_p$ if $\frac{p-1}{\lambda}$ is a square-free which is relatively prime to λ. Let $\kappa = [K_\lambda : K]$ and $\{k_1, \cdots k_\kappa\}$ be elements of distinct left cosets of K in K_λ. Then we have $f_{K_\lambda}(x) = \sum_{i=1}^{\kappa} f_K(x^{k_i})$. We saw in Proposition 8 that if $\frac{p-1}{\lambda}$ is a square-free which is relatively prime to λ, then f_{K_λ} is a monomial and hence it is never zero on $\mathbb{Z}_p$. Therefore, we can say that the condition $f_K(\alpha) \neq 0$ in Theorem 2 is not so unnatural in this case. In the contrary, it may be harder to satisfy the condition $f_K(\alpha) \neq 0$ if $\frac{p-1}{\lambda}$ has prime powers. The case of Proposition 9 is a typical example.

We have another strategy to avoid 'bad cases' aforementioned by randomizing α. In the case of $|\alpha^K| \neq |K|$, take a random element γ in $\mathbb{Z}_p^\times$ and compute new parameters $\{(g^{\alpha^k})^{\gamma^k} : k \in K\}$, which can be done in $|K|$ exponentiations in $\mathbb{Z}_p$ and G. We repeat this process until finding γ which satisfies $|(\alpha\gamma)^K| = |K|$, and the expected number of repetition is less than $6\log\log(p-1)$. Finally, we can compute $\alpha\gamma$ in $O\left(\frac{p}{\lambda|K|}(\sqrt{\lambda} + |K|)\right)$ exponentiations by Theorem 2, and get $\alpha = (\alpha\gamma)\cdot\gamma^{-1}$. The total number of computations is $O\left(|K|\log\log p + \frac{p}{\lambda|K|}(\sqrt{\lambda} + |K|)\right)$, which does not have significant difference with $O\left(\frac{p}{\lambda|K|}(\sqrt{\lambda} + |K|)\right)$.

This strategy can be also used in the case of $f_K(\alpha) = 0$. We can compute new parameters $\{(g^{\alpha^k})^{\gamma^k} : k \in K\}$ in $|K|$ exponentiations in $\mathbb{Z}_p$, and check

whether $f_K(\alpha\gamma)$ is equal to zero or not in $|K|$ multiplications in G. The expected number of repetition depends on the number of roots of $f_K(x) = 0$ in $\mathbb{Z}_{p-1}$. This algorithm must be more efficient than the above, but the exact complexity is not resolved yet.

6 Conclusion

In this paper, we generalized the discrete logarithm problem with auxiliary inputs and proposed an algorithm to solve this problem efficiently. Precisely, our algorithm takes $g, g^{\alpha}, g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_{d-1}}}$ as an instance where e_i's form a multiplicative subgroup in $\mathbb{Z}_{p-1}^{\times}$. If $d \approx p^{1/3}$ is a prime (or square-free) divisor of $p-1$ and $e_i = 1 + \frac{p-1}{d} \cdot n_i \in \mathbb{Z}_{p-1}^{\times}$ for some $0 \leq n_i < d$, then our algorithm solves $\alpha \in \mathbb{Z}_p$ in $O(p^{1/3})$ group operations.

The main part of our technique is to partition the set $\mathbb{Z}_p^{\times}$ using a group action. In particular, if d is square-free with ℓ prime factors, then all elements in $\mathbb{Z}_p^{\times}$ can be represented by using only 2^{ℓ} elements.

It would be of interest to find an algorithm to solve the DLPwAI using our algorithm, that is, to convert an instance of the form $g, g^{\alpha}, \cdots, g^{\alpha^d}$ for $d < p^{1/3}$ into g^{α^k}'s with $k \in K$ for a multiplicative subgroup K of $\mathbb{Z}_{p-1}^{\times}$.

Acknowledgement. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2011-0018345). Yongsoo Song was partially supported by NRF-12-Global Ph.D. Fellowship Program.

References

1. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, Ch., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
2. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, Ch., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
3. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol. **21**(2), 149–177 (2008)
4. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
5. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
6. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
7. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005)

8. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004)
9. Brown, D.R.L., Gallant, R.P.: The static Diffie-Hellman problem. IACR Cryptology ePrint Archive. http://eprint.iacr.org/2004/306 (2004)
10. Cheon, J.H.: Security analysis of the strong Diffie-Hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006)
11. Cheon, J.H.: Discrete logarithm problems with auxiliary inputs. J. Cryptol. **23**(3), 457–476 (2010)
12. Conrad, K.: Group theory. http://www.math.uconn.edu/~kconrad/blurbs/
13. den Boer, B.: Diffie-Hellman is as strong as discrete log for certain primes. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 530–539. Springer, Heidelberg (1990)
14. Jao, D., Yoshida, K.: Boneh-Boyen signatures and the strong Diffie-Hellman problem. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 1–16. Springer, Heidelberg (2009)
15. Kim, M.: Integer factorization and discrete logarithm with additional information. Ph.D. dissertation, Seoul National University (2011)
16. Kim, T., Cheon, J.H.: A new approach to discrete logarithm problem with auxiliary inputs. IACR Cryptology ePrint Archive. http://eprint.iacr.org/2012/609 (2012)
17. Lang, S.: Algebra, 3rd edn. Springer, New York (2002)
18. Maurer, U.M.: Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 271–281. Springer, Heidelberg (1994)
19. Maurer, U.M., Wolf, S.: The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. SIAM J. Comput. **28**(5), 1689–1721 (1999)
20. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
21. Satoh, T.: On generalization of Cheon's algorithm. IACR Cryptology ePrint Archive. http://eprint.iacr.org/2009/058 (2009)