Generailized DLP with Auxiliary Inputs (SAC 2013)

Jung Hee Cheon, Taechan Kim, and Yongsoo Song

Department of Mathematical Sciences and ISaC-RIM
Seoul National University

August 15, 2013

Classical Hard Problems

G is a group of prime order p with a generator g

- DLP : given (g, g^{α}), compute $\alpha \in \mathbb{F}_p$
  - CDHP: given (g, g^x, g^y), compute g^{xy}
  - DDHP: given (g, g^x, g^y, g^z), decide if $g^z = g^{xy}$

- Variants of the DLP?
  - Cryptographic schemes with additional properties
  - Security proof without random oracles

- Public Key Encryption, Digital Signature, Authentication, etc

Variants of the DLP

- DLPwAI: given $(g, g^{\alpha}, \ldots, g^{\alpha^d})$, compute $\alpha \in \mathbb{F}_p$
- GDLPwAI: given $(g, g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_d}})$, compute $\alpha \in \mathbb{F}_p$
- Applications
  - Short Group Signatures[BBS04]
  - Identity-based Encryptions[BB04e]
  - Public Key Broadcast Encryption[BGW05]
- $(g_1, g_1^{\alpha}, \cdots, g_1^{\alpha^d})$ can be obtained from g, g^{α} and a d-multilinear map $e : G \times G \times \cdots \times G \to G_T$

Previous Works for the DLPwAI

Previous Work: $p \pm 1$ Cases

- $p-1$ has a small divisor d [Brown-Gallant'05], [C'06]
  - Parameter : $g, g^{\alpha}, g^{\alpha^d}$
  - Apply BSGS twice
  - Total complexity : $\log p \cdot O\left(\sqrt{\frac{p-1}{d}} + \sqrt{d}\right)$
- $p+1$ has a small divisor d [C'06]
  - Parameter : $g, g^{\alpha}, \cdots, g^{\alpha^d}$
  - Embed $\mathbb{F}_p$ into an order-$(p+1)$ subgroup of $\mathbb{F}_{p^2}$
  - Total complexity : $\log p \cdot O\left(\sqrt{\frac{p+1}{d}} + d\right)$

[C'06] Cheon,J.H.: Security Analysis of the Strong Diffie-Hellman Problem. EUROCRYPT 2006.

Previous Work: Embedding to $\mathbb{F}_{p^n}$

- d is a divisor of $\Phi_n(p)$ [Satoh'09]
  - Embed $\mathbb{F}_p$ into $GL_n(\mathbb{F}_p)$
  - $n = 1$ (or $n = 2$) case falls into the $p - 1$ (or $p + 1$) case of the previous algorithm
  - The complexity is greater than $p^{1/2}$ when $n \geq 3$

- d is a divisor of $p^n - 1$ [C.-Kim-Lee'12]
  - $D < p$ is an divisor of $p^n - 1$, and $E = (p^n - 1)/D$
  - Embedding $\mathbb{F}_p \to \mathbb{F}_{p^n}, \quad x \mapsto (x + \zeta_\tau)^{(p^n-1)/D}$
  - Find r such that $S_p(rE) \leq d$
  - Total complexity : $O(\sqrt{D} + S_p(rE))$

[C.-Kim-Lee'12] Minkyu Kim, Jung Hee Cheon and In-Sok Lee: Analysis on a Generalized Algorithm for the Strong Discrete Logarithm Problem with Auxiliary Inputs, 2012.

Previous Work: Polynomials with Small Value Sets

- $f(x) = f_0 + \cdots + f_d x^d$ has a small image size $|Im(f)| = q$
- Multipoint evaluation $\{f(r_i\alpha)\}, \{f(s_j)\}$ for random r_i, s_j's using exponent FFT
- Find a collision $f(r_i\alpha) = f(s_j)$ and solve this equation
- However, $|Im(f)| \approx p/e$ in general
- $f(x) = x^d, d|p-1$ ($p-1$ case)
- The Dickson polynomial $D_d(x, a)$ ($p+1$ case)

[C.-Kim'12] Taechan Kim and Jung Hee Cheon: A New Approach to Discrete Logarithm Problem with Auxiliary Inputs, IACR Cryptology ePrint Archive, 2012.

New Approach using Group Actions

Motivation

- Consider $f(x) = x + x^k + \cdots + x^{k^{d-1}} \in \mathbb{F}_p[x]$, where $k \in \mathbb{Z}_{p-1}$ and $k^d = 1$
- $f(x) = f(x^k) = \cdots = f(x^{k^{d-1}})$, and f has the small value set
- The degree of $f(x) = x + x^k + \cdots + x^{k^{d-1}} \in \mathbb{F}_p[x]$ is high, the FFT cannot be applied
- Considering $\zeta \in \mathbb{F}_p$ s.t. $\zeta^k = \zeta$, then $f(\zeta^i x) = \zeta^i f(x)$ for any i and $x \in \mathbb{F}_p$
- Solve the DLP with inputs $g, g^{\alpha}, \cdots, g^{\alpha^{k^{d-1}}}$

Generalizations

- GDLPwAI: given $(g, g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_d}})$, compute $\alpha \in \mathbb{F}_p$
- Replace $\{1, k, \cdots k^{d-1}\}$ by any multiplicative subgroup K of $\mathbb{Z}_{p-1}^{\times}$ of order d
- $f(x) = \sum_{k \in K} x^k$ is d-to-1 since $f(x) = f(x^k)$ for any $k \in K$
- $f(\zeta^i x) = \zeta^i f(x)$ if $\zeta^k = \zeta$ for any $k \in K$

Main Idea

- Our algorithm solves the GDLPwAI when $K = \{e_1, \cdots e_d\}$ is a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$
  - Parameter: g and $\{(k, g^{\alpha^k}) : k \in K\}$
  - Define the group action $\theta : K \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $(k, x) \mapsto x^k$
  - $f(x) = \sum_{k \in K} x^k$ has the same value on one orbit x^K
  - $f(\zeta x) = \zeta f(x)$ if ζ is a fixed point of the group action θ
  - $g^{f(\alpha)} = \prod_{k \in K} g^{\alpha^k}$ can be computed

Fixed Points

- The elements of multiplicative subgroup K seem like a part of an arithmetic sequence starting from 1
  - $\lambda = \gcd(K-1) = \gcd\{k-1 : k \in K\}$ is a divisor of $p-1$
  - Every element of K is of the form $1+\lambda m$ for some $m \in \mathbb{Z}_{p-1}$

- The set of fixed points of the group action is
  - $\{x \in \mathbb{Z}_p^* : x^k = x\} = \{x \in \mathbb{Z}_p^* : x^\lambda = 1\} = \langle \zeta \rangle$
  - ξ is a primitive root of $\mathbb{Z}_p$ and $\zeta := \xi^{(p-1)/\lambda}$

- Example: $p = 29, K = \{1, 5, 9, 13, 17, 25\} \leq \mathbb{Z}_{28}^\times$
  - $\lambda = \gcd(K-1) = 4$
  - $\xi = 2$ is a primitive element of $\mathbb{Z}_{29}$, and $\zeta = \xi^{(p-1)/\lambda} = 12$
  - $\langle 12 \rangle = \{1, 12, 17, 28\} \leq \mathbb{Z}_{29}^*$ are the fixed points

- We get $f(\zeta^t x^k) = \zeta^t f(x)$ for any $t \in [0, \lambda), k \in K$
- λd-number of elements of $\mathbb{Z}_p^*$ are obtained from $f(x)$

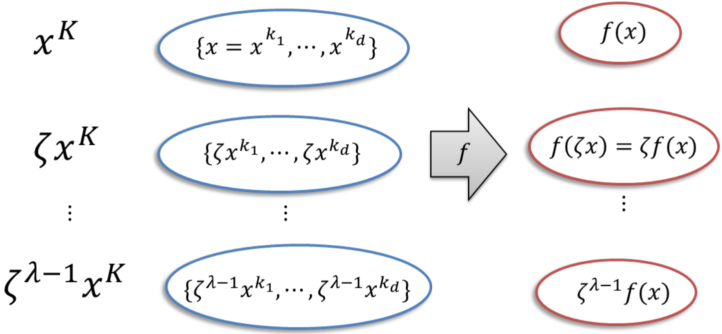

Figure : d-to-1 Evaluation

Algorithm

- For random $\beta \in \mathbb{Z}_p^*$, compute $f(\beta) = \sum_{k \in K} \beta^k$ and $g^{f(\beta)}$ in $O(d)$. The probability that $\zeta^t \alpha^k = \beta$ for some $t \in [0, \lambda), k \in K$ is equal to $\lambda d/(p-1)$
- Using the BSGS method, find $t \in [0, \lambda)$ in $O(\sqrt{\lambda})$ from the relation $g^{\zeta^t f(\alpha)} = g^{f(\beta)}$
- Determine $k \in K$ by comparing $g^{\zeta^{-t}\beta}$ with g^{α^k}'s for $k \in K$
- The expectation number of repetition is $(p-1)/\lambda d$

Main Theorem

Theorem

Let K be a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$ with $\lambda = \gcd(K-1)$. Then, one can solve the GDLPwAI in $O\left(\frac{p}{\lambda d}(\sqrt{\lambda}+d)\right)$ exponentiations in $\mathbb{Z}_p$ if $|\alpha^K| = d$ and $\sum_{k\in K}\alpha^k \neq 0$.

- In many cases, $d = O(\frac{p}{\lambda})$ and the complexity is $O(\sqrt{\lambda}+\frac{p}{\lambda})$. It can be lowered down to $O(p^{1/3})$ when $\lambda \approx p^{2/3}$.
- Additional conditions $|\alpha^K| = |K|$ and $\sum_{k\in K}\alpha^k \neq 0$ are satisfied with a high probability.

Summary

- The polynomial $f(x) = \sum_{k \in K} x^k$ has the small image set but high degree
- The multipoint evaluation of f can be done with the equation $f(\zeta^i x^k) = \zeta^i f(x)$
- The total complexity $O\left(\sqrt{\lambda} + \frac{p}{\lambda}\right)$ can be lowered down to $O(p^{1/3})$ when $\lambda \approx p^{2/3}$

Open Problems and Further Works

- The FFT cannot be applied since the degree of f is high. Can you calculate many $f(\beta) = \sum_{k \in K} \beta^k$'s efficiently?

- Is it possible to convert the parameter $(g^{\alpha}, \cdots, g^{\alpha^d})$ of the DLPwAI to $(g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_d}})$ of the GDLPwAI?

- Boneh, D. and Boyen, X.: Short Signatures Without Random Oracles. Advances in Cryptology - EUROCRYPT 2004, pp. 56–73.
- Cheon, J. H.: Security Analysis of the Strong Diffie-Hellman Problem. In: Vaude- nay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1-11. Springer, Heidelberg (2006)
- Cheon, J. H.: Discrete Logarithm Problems with Auxiliary Inputs. Journal of Cryptology 23(3), pp. 457-476. (2010)
- Satoh, T.: On Generalization of Cheon's Algorithm. http://eprint.iacr.org/2009/058.pdf (2009)
- Kim, T. and Cheon, J. H.: A New Approach to Discrete Logarithm Problem with Auxiliary Inputs. IACR Cryptology ePrint Acheive (2012). `http://eprint.iacr.org/2012/609`