Discrete Logarithm with Auxiliary Inputs (Special Semester Workshop 4)

Jung Hee Cheon
(partly joint work with Taechan Kim and Yongsu Song)

Department of Mathematical Sciences and ISaC-RIM
Seoul National University

December 13, 2013

Outline

Discrete Logarithm Problem (DLP)

- Let $G = \langle g \rangle$ be a cyclic group of prime order p.
- Discrete Logarithm Problem(DLP): Find $\alpha \in \mathbb{F}_p$ when g, g^α are given.
  - CDHP: given (g, g^α, g^β), compute $g^{\alpha\beta}$
  - DDHP: given $(g, g^\alpha, g^\beta, g^\gamma)$, decide if $g^\gamma = g^{\alpha\beta}$
- Pubelic Key Encryption, Digital Signature, Authentication, etc
- Baby-Step Giant-Step (BSGS)
  - Let $L = \lceil \sqrt{p} \rceil$. Find a collision between two lists

$$L_1 = \{g^{-i} : i \in [0, L)\}, \quad L_2 = \{g^{Lj} : j \in [0, L)\}$$

  - $O(\sqrt{p})$ computations and storage
- Pollard's ρ, Pohlig-Hellman, Index calculus (NFS, FFS)

Relax the problems

- Why?
  - To design a new system with additional properties
  - To prove the security without random oracles
- How to get a good grade in an exam?
  - Flexible grading
  - More Hints before the test

Relax the problems: *Flexible Grading*

- Flexible RSA Problem (BP97,CS99,GHR99):
  Given a composite n and a message $m \in \mathbb{Z}_n$ find $(e, m^{1/e})$ for some $e > 2$

- (Decisional) Linear Assumption (BBS04):
  Given $g, g_1, g_2, g_1^c, g_2^d, v \in G$, decide if $v = g^{c+d}$
  - Let $d = 0$, $a = x^{-1}$, $ac = y$.
  - Given $g^{x^{-1}}, g^y, v$ decide if $v = g^{c+d} = g^{xy}$

Relax the problems: *More Hints (1/2)*

- ℓ-Weak DHP: Given $g, g^{\alpha}, \cdots, g^{\alpha^{\ell}}$, compute $g^{1/\alpha}$
  - Traitor Tracing [Mitsunari-Sakai-Kasahara02]
- ℓ-Strong DHP: Given $g, g^{\alpha}, \cdots, g^{\alpha^{\ell}}$, compute $g^{\alpha^{\ell+1}}$
  - Short Signatures without Random Oracle[BB04s]
  - Short Group Signatures[BBS04]
- One More DL: With n-queries to DL oracle, solve $(n+1)$ DL problems.
  - GQ/Schnorr Identification
  - One More DH

Relax the problems: *More Hints (2/2)*

- $e : G_1 \times G_2 \to G'$: a bilinear map
- ℓ-Bilinear DHI: Given $g, g^{\alpha}, \cdots, g^{\alpha^{\ell}}$, compute $e(g,g)^{1/\alpha}$
  - Identity-based Encryptions[BB04e]
  - Verifiable Random Functions[DY05]
- ℓ-Bilinear DHE: Given $h, g, \cdots, g^{\alpha^{\ell-1}}, g^{\alpha^{\ell+1}}, \cdots, g^{\alpha^{2\ell}}$, compute $e(g,h)^{\alpha^{\ell}}$
  - HIBE with constant-size ciphertext[BBG05]
  - Public Key Broadcast Encryption[BGW05]

Variants of DL problems on Pairing Groups

- Refer to `http://www.ecrypt.eu.org/wiki`
  - Find 36 variants of DL in `http://www.ecrypt.eu.org/wiki/index.php/Discrete_Logarithms`
  - Find 8 variants of BDL in `http://www.ecrypt.eu.org/wiki/index.php/Pairings`
- Are they secure?
  - Assume it is as secure as DL
  - Find reductions or dedicated attacks
  - Estimate the complexity in the generic group model
- Attacks or Reductions: very few results

Discrete Logarithm with Auxiliary Inputs (DLPwAI)

- Many of DL variants has auxiliary inputs $g, g^{\alpha}, \ldots, g^{\alpha^d}$
- Question: are they as hard as DL?
  - In the generic group model, the complexity of SDL is lower bounded by $O(\sqrt{p/d})$ group operations when $d < p^{1/3}$.
  - $O(\sqrt{p})$ for the DL
- d-DLPwAI: Given $g, g^{\alpha}, \ldots, g^{\alpha^d}$, compute $\alpha \in \mathbb{F}_p$.

Outline

$p-1$ has a small divisor d [Brown-Gallant05], [JoC'10,C.]

- Assume $(g, g_1 = g^{\alpha}, g_d = g^{\alpha^d})$ are given for $d|p-1$
- Let ξ be a generator of $\mathbb{Z}_p^*$ and $\zeta := \xi^d$
- Idea: Put $\alpha = \xi^{z_1 + z_2 \frac{p-1}{d}}$ for $0 \leq z_1 < \frac{p-1}{d}, 0 \leq z_2 < d$. Then compute z_1 s.t. $g^{\alpha^d} = g^{\zeta_1^z}$ and then z_2 independently.
- $\alpha^d = \zeta^{z_1}$ contained in a subgroup of order $\frac{p-1}{d}$
  - Apply BSGS: $\alpha^d \zeta^{-u} = \zeta^{Lv}$ for $0 \leq u, v < L := \left\lceil \sqrt{\frac{p-1}{d}} \right\rceil$
  - Check the equality: $g_d = g^{\zeta^{z_1}}$
  - $O(\left\lceil \sqrt{\frac{p-1}{d}} \right\rceil)$ complexity and memory

$p-1$ has a small divisor d [Brown-Gallant05], [JoC'10,C.]

- $\alpha = \xi^{z_1 + z_2 \frac{p-1}{d}}$. Once we know $z_1 \in [0, \frac{p-1}{d})$ and $\alpha^d = \zeta^{z_1}$, find $z_2 \in [0, d)$ such that $\alpha \xi^{-z_1} = \xi^{z_2 \frac{p-1}{d}}$
  - Check the equality: $g_1^{\xi^{-z_1}} = (g^{\xi^{\frac{p-1}{d}}})^{z_2}$
  - Apply BSGS: $O(\sqrt{d})$ computations and storage
- Total: $\log p \cdot O\left(\sqrt{\frac{p-1}{d}} + \sqrt{d}\right)$ multiplications in $\mathbb{Z}_p$
- It has the minimum $O(p^{1/4})$ when $d = p^{1/2}$
- What can you do when given $\{g^{\alpha^i} | 0 \le i \le \ell, \ell \nmid p-1\}$

Outline

Use a field embedding [C.-Kim-Lee'12]

- Let $p^n - 1 = DE$ for $0 < D < p$, and $d = \Phi_n(p)/D$
- ξ: a generator of $\mathbb{F}_{p^n}^*$, 1_n: the identity of $\mathbb{F}_{p^n}^*$
- H: the subgroup of order D generated by $\zeta = \xi^E$.
- The idea of (generalized) Cheon's algorithm $\Phi_n(p)$ cases: use the embedding for $\theta \in \mathbb{F}_{p^n}$,

$$\begin{array}{ccc} \mathbb{F}_p & \longrightarrow & H \subseteq \mathbb{F}_{p^n} \\ \alpha & \longmapsto & \beta = (\alpha + \xi_\tau)^{rE}, \end{array}$$

  where H is a (small) subgroup of order $\frac{p^n-1}{E}$.
- Find $z \in [0, D)$ such that $\beta = \zeta^z$ in $H \subset \mathbb{F}_{p^n}$

Baby-step Giant-step phase

- Given $rE = \sum_{i=0}^{n-1} e_i p^i$, $|e_i| < p/2$, $S_p(rE) = \max\{\sum_{e_i>0} e_i, \sum_{e_i<0} e_i\}$ is called the **sum of signed digits**, denoted by e.
- $\beta = (\alpha \cdot 1_n + \xi_\tau)^{rE} = \prod_{i=0}^{n-1}(\alpha \cdot 1_n + \xi_\tau^{p^i})^{e_i} = \frac{\sum_{j=0}^{\tau-1} f_j(\alpha)\xi_\tau^j}{\sum_{j=0}^{\tau-1} \bar{f}_j(\alpha)\xi_\tau^j}$ where f_j and $\bar{f}_j$ are polynomials over $\mathbb{F}_p$ with degree $\leq e$
- Need g^{α^i} for $1 \leq i \leq e = S_p(rE)$ for $O(\sqrt{D})$ attack
- Find $z \in [0, D)$ s.t. $g^\beta = g^{\zeta^z}$ or $(g^\beta)^{\zeta^{-u\lceil\sqrt{D}\rceil}} = g^{\zeta^v}$ for $0 \leq u, v < \lceil\sqrt{D}\rceil$.

Attack Scenario

- Suppose a prime p and $g, g^{\alpha}, \cdots, g^{\alpha^d}$ are given.
- Find an appropriate divisor $D < p$ of $\Phi_n(p)$ for some n for the n-th cyclotomic polynomial $\Phi_n(x)$
- Find r s.t. $S_p(rE) \leq d$ and $\gcd(r, D) = 1$.
- Apply the algorithm to recover α
- The complexity of the attack is about $O(\sqrt{D} + S_p(rE))$

However...

- (Minkowski Thm) Lattice reductions gives r with

$$S_p(rE) \leq E^{1/\phi(n)} \approx p/D^{1/\phi(n)}$$

  when $DE = \Phi_n(p)$
- It is optimal except when every prime divisor of D divides $n(p^2 - 1)$.
- Investigate the exceptional case
- C.-Kim-Lee'12: $(n \geq 3)$ In most cases, the compleixty is greater than $\sqrt{p}$

n=2 case

- $\Phi_2(p) = p + 1$ has a small divisor d
- Total compleixty: $\log p \cdot O\left(\sqrt{\frac{p+1}{d}} + d\right)$,

  can be lowered down to $O(p^{1/3})$ when $d \approx p^{1/3}$
- This algorithm requires all of g^{α^i}'s for all $0 \leq i \leq d$
  - What can you do if one is missing? e.g. g^{α^2}

Outline

Examples

- NIST Curves
  - B-163: $p-1 = 2 \cdot 53 \cdot 383 \cdot 21179 \cdot$ (a 132 bit prime)
  - K-163: $p-1 = 24 \cdot 43 \cdot 73 \cdot$ (a 16 bit prime) (an 18 bit prime) (a 112 bit prime)
  - P-192: $p-1 = 24 \cdot 5 \cdot 2389 \cdot$ (an 83 bit prime) (a 92 bit prime)
- BGW Broadcast Encryption for n users is based on $2n$-BDHE
  - $E^+(\mathbb{F}_{3^{97}})$ has a subgroup G of 151 bit prime order
  - Pollard rho: $O(2^{76})$ elliptic curve operations
  - Proposed attack: $O(2^{59})$ Exponentiations for $n = 2^{32}$
  - Need 220 bit prime for 2^{80} security with 2^{64} users
- Implementation on $E(F_{3^{127}})$ with 41-bit d took 14 hours on a PC (Izu-Takenaka-Yasuda, ARES2010)
- Sakemi et al, Solving a Discrete Logarithm Problem with Auxiliary Input on a 160-bit Elliptic Curve, PKC 2012

Boneh-Boyen Signature and Strong DL (Jao and Yoshida)

- Boneh-Boyen signature is of form $(m, g^{1/(\alpha-m)})$, where m is a message.
- If $(m_1, g^{1/(\alpha-m_1)}), \cdots, (m_d, g^{1/(\alpha-m_d)})$ are given.
- Let $g_1 = g^{1/\prod_{i=1}^{d}(\alpha-m_i)}$, then one obtains $g_1, g_1^{\alpha}, \cdots, g_1^{\alpha^d}$ using partial fraction decomposition.
- Then α is recovered by using Previous algorithm.

Partial Fraction Decomposition

- Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree d.
- Partial fraction decomposition says

$$\frac{f(x)}{(x-m_1)\cdots(x-m_k)} = q(x) + \sum_{i=1}^{k} \frac{A_i}{x-m_i}$$

with $\deg q(x) = d-k$ and $A_i \in \mathbb{F}_p$.

Boneh-Boyen Signature and Strong DL

- Futhermore, if $(m_i, g^{1/(\alpha - m_i)})$ for $i = 1, \cdots, k$ and g^{α^j} for $j = 1, \cdots, d - k$ are given.
- We also obtain an instance of SDL, $g_1, g_1^{\alpha}, \cdots, g_1^{\alpha^d}$ for $g_1 = g^{1/\prod_{i=1}^{k}(\alpha - m_i)}$.

Summary

- $\log p$ factor can be removed by precomputation table (Kozaki-Kutsuma-Matsuo, Pairing 2007)
- Given $\{g^{\alpha^i} | 0 \leq i \leq \ell\}$ and $\{g^{1/(\alpha - m_i)} | 0 \leq i \leq k\}$
  - If $d | p-1$ and $d \leq k\ell$, DL is solved in $O(\sqrt{(p-1)/d} + \sqrt{d})$
  - If $d | p+1$ and $d \leq k\ell$, DL is solved in $O(\sqrt{(p+1)/d} + d)$
  - The complexity is reduced by $\sqrt{d}$ from $O(\sqrt{q})$
- Is there any prime p s.t. both $p-1$ and $p+1$ are almost prime?

Outline

Attack Scenario

- Suppose a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d has a small image size $|Im(f)| = v$
- Take two lists $L = \{r_1, \cdots, r_m\}, L' = \{s_1, \cdots, s_m\}$ for randomly chosen r_i and s_j from $\mathbb{F}_p$
- Compute and find a collision between following two lists:

$$g^L = \{g^{f(r_i\alpha)} : 1 \leq i \leq m\}, \quad g^{L'} = \{g^{f(s_j)} : 1 \leq j \leq m\}$$

- One solves the equation $f(r_i\alpha) = f(s_j)$ in α from a collision
- Obstacles:
  - Compute g^L efficiently with $g, g^{\alpha}, \cdots, g^{\alpha^d}$
  - Decide an appropriate size m of lists
  - Find suitable polynomials f

Compute g^L: Exponent FFT

- Suppose $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{F}_p[x]$ and denote $g^{f(x)} := (g^{a_0}, \cdots, g^{a_d})$.
- Let $w \in \mathbb{F}_p$ be a primitive d-th root of unity.
- If we are given $g^{f(x)}$, $h(x)$, and w, then we can compute;
  - $g^{DFT_w(f)} := (g^{f(1)}, g^{f(w)}, \cdots, g^{f(w^{d-1})})$ in $O(d \log d)$ group exponentiations.
  - $g^{f(x)h(x)}$ in $O(d \log d)$ group exponentiations using the exponent FFT.
  - $g^{f(x) \mod h(x)}$ in $O(d \log d)$ group exponentiations. Here $\deg(f) = 2d, \deg(h) = d$. (via Newton Method)

Compute g^L: Exponent FFT

- Thus for given $g^{f(x)}$, computing $g^{f(1)}, \cdots, g^{f(d)}$ is done in $O(d \log^2 d)$ group exponentiation.
- If the primitive d-th root $w \notin \mathbb{F}_p$, then use Schonhage-Strassen multiplication.

Length of lists: Birthday Problem

- Consider $V(f) := \{f(x) : x \in \mathbb{F}_p\} = \{f_1, \ldots, f_v\}$.
- p_i: the probability that $f(x) = f_i$ for randomly chosen $x \in \mathbb{F}_p$
  - Assume that $p_1 = \cdots = p_v = \frac{1}{v}$.
- By the birthday paradox, we have a collision after $\approx \sqrt{\frac{\pi}{2} v}$ elements are picked up.
- We can set the size of the lists to be $m = \lceil \sqrt{\frac{\pi}{2} v} \rceil$.
- The problem reduces to find a polynomial with small value set.

Polynomial finding: General Theory

- $v := |Im(f)| \geq \lfloor \frac{p-1}{d} \rfloor + 1$
  - $v = \lfloor \frac{p-1}{d} \rfloor + 1$ iff $d|p-1$ and $f(x) = (x+\beta)^d + \gamma$
- Mean value of the image set size: Expected value $E(v)$ over all polynomials f of degree d is

$$p \cdot \left(1 - \frac{1}{2!} + \cdots + (-1)^d \frac{1}{d!}\right) \approx p/e$$

- Very few candidates for our algorithm

Polynomial finding: Monomial

- If $f(x) = x^d$ with $d|(p-1)$, $|Im(f)| = \frac{p-1}{d} = L^2$
- Collision finds $(g^{\alpha^d})^{u^d} = g^{v^d}$ and $\alpha = v/u$.
- Complexity is $O\left(d \log d \times \frac{L}{d}\right) = O\left(\sqrt{\frac{p-1}{d}} \log d\right)$ exponentiations

Polynomial finding: Extension Field case

- If $D|\Phi_n(p)$, let $f(x) = (x \cdot 1 + \zeta)^E$ for $\zeta \in \mathbb{F}_{p^n}$, $\Phi_n(p) = DE$.
- Suppose that we can write $f(x) = f_1(x)\theta_1 + \cdots + f_n(x)\theta_n$ where $(\theta_1, \cdots, \theta_n)$ is a basis for $\mathbb{F}_{p^n}$.
- For $x \in \mathbb{F}_p$, $|Im(f)| \leq D$, we have $|Im(f_k)| \leq D$ where $k = 1, \cdots, n$.
- Compute $g^{f_k(i\alpha)}$ and $g^{f_k(j)}$ for $i, j = 1, \cdots, \sqrt{D}$ using the exponent FFT.
- We find a collision and have α by solving the equation.
- However, the degree of f is not small enough.

Rational function: Elliptic Curves

- If $f(x) = \frac{\phi_m(x)}{\psi_m^2(x)}$ and $m|\#E(\mathbb{F}_p)$, $|Im(f)| = \frac{\#E(\mathbb{F}_p)}{m} \approx \frac{p}{m}$.
- Compute $g^{\phi_m(\alpha)}, \ldots, g^{\phi_m(q'\alpha)}$ and $g^{\psi_m^2(\alpha)}, \ldots, g^{\psi_m^2(q'\alpha)}$ in $O(q' \log d)$ Expo.
- We obtain $g^{f(\alpha)}, \ldots, g^{f(q'\alpha)}, g^{f(1)}, \ldots, g^{f(q')}$ if
  - $e(g^a, g^b) = h^{a/b}$ or $IE(g^b) = h^{1/b}$ oracle queries are allowed.
- If $f(x) = \psi_m^2(x)$, then $|ker(f)| = m$ and $|Im(f)| = ?$

Application to the Dickson Polynomial

- Dickson Polynomial: For $a \in \mathbb{F}_p$ and $d \geq 1$ an integer, let

$$D_d(x, a) = \sum_{k=0}^{\lfloor d/2 \rfloor} \frac{d}{d-k} \binom{d-k}{k} (-a)^k x^{d-2k} \in \mathbb{F}_p[x].$$

- Value set of Dickson Polynomial: If a is a quadratic non-residue and d is odd, then

$$R_{(d,p-1)} = \frac{p-1}{2(d, p-1)} \text{ and } R_{(d,p+1)} = \frac{p+1}{2(d, p+1)}.$$

- If $d|(p+1)$, then $R_1 = \frac{p-1}{2}$ and $R_d = \frac{p+1}{2d}$.

Application to the Dickson Polynomial

- d-to-1 for $\frac{p+1}{2}$ elements of $\mathbb{F}_p$
- Complexity: $O\left(\sqrt{\frac{p+1}{d}}\log^2 d\right)$ exponentiations
- Note that $|Im(D_d(x,a))| = \frac{p-1}{2} + \frac{p+1}{2d}$ is not small enough

Outline

Application with Sparse Polynomial [C-Kim-Song13]

- Consider $f(x) = x + x^r + \cdots x^{r^{d-1}} \in \mathbb{F}_p[x]$, where $r^d = 1 \mod (p-1)$.
- Then $f(x) = f(x^r) = \cdots = f(x^{r^{d-1}})$, so it is d-to-1 map.
- Due to its high degree, hard to compute $f(r_1), \cdots, f(r_m)$ efficiently for random r_i's.
- $f(\zeta^i x) = \zeta^i f(x)$ if $\zeta^r = \zeta \mod (p-1)$.
- In this case, the multipoint evaluation can be replaced by simple scalar multiplications.

Application with Sparse Polynomial [C-Kim-Song13]

- Consider subsets of $\mathbb{Z}_p$ for the discrete log α:

$$\begin{aligned}
\langle \alpha \rangle &:= \{\alpha, \alpha^r, \ldots, \alpha^{r^{d-1}}\} \mapsto f(\alpha), \\
\langle \zeta\alpha \rangle &:= \{\zeta\alpha, \zeta\alpha^r, \ldots, \zeta\alpha^{r^{d-1}}\} \mapsto \zeta f(\alpha), \\
&\vdots \\
\langle \zeta^{r-1}\alpha \rangle &:= \{\zeta^{r-1}\alpha, \zeta^{r-1}\alpha^r, \ldots, \zeta^{r-1}\alpha^{r^{d-1}}\} \mapsto \zeta^{r-1} f(\alpha).
\end{aligned}$$

- The sets are disjoint unless $f(\alpha) = 0$.
- The table size is dr.
- A random $\beta \in \mathbb{F}_p$ is in $\langle \zeta^i \alpha \rangle$ for some i w.h.p. if $dr \approx p$.

Application with Sparse Polynomial [C-Kim-Song13]

- For given $g, g^{\alpha}, g^{\alpha^r}, \cdots, g^{\alpha^{r^{d-1}}}$, compute $g^{f(\alpha)} = \prod_{i=1}^{d} g^{\alpha^{r^i}}$.
- For random β, find $k = i \cdot \lceil \sqrt{r} \rceil + j$ such that $f(\beta) = \zeta^k f(\alpha)$,

$$\left(g^{f(\beta)}\right)^{(\zeta^{-\lceil \sqrt{r} \rceil})^i} = \left(g^{f(\alpha)}\right)^{\zeta^j}.$$

  Then $\beta \in \zeta^k \{\alpha, \alpha^r, \ldots, \alpha^{r^{d-1}}\}$.
- Find $\ell \in [0, d-1]$ s.t. $\beta = \zeta^k \alpha^{r^\ell}$
- Recover $\alpha = (\beta \zeta^{-i})^{r^{-\ell}}$ in $O(\sqrt{r} + d) \geq O(p^{1/3})$ where $dr \approx p$

Generalized DLPwAI

- Generalized DLPwAI (GDLPwAI): Find $\alpha \in \mathbb{F}_p$ when $g^{\alpha^{e_1}}, \ldots, g^{\alpha^{e_d}}$ are given.
- We can solve the GDLPwAI when $e_i \in K$ for a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$.
- The time complexity is $O\left(\frac{p}{|K|\sqrt{\lambda}} + |K|\right)$, where $\lambda = \gcd(x - 1 : x \in K)$.

Summary and Open Problem

- We can solve the DLwAI more *efficiently* if there is a polynomial $f : \mathbb{F}_p \to \mathbb{F}_p$ of low degree with small value set.
- We have such f's if
  - $p-1$ or $p+1$ has an appropriate divisor
  - f is rational
  - f has large degree
  - p is a power of prime
- Except these cases, not known if there is such a polynomial.
- Substitutional Polynomials: If $f(x) - f(y) = 0$ has r absolutely irreducible factors, many elements has r preimages under f which yields $O(\sqrt{p/r})$ algorithm. (More precisely, $\sum_{i=1}^{d} i^2 R_i = rp + O(d^2 p)$)