The Representation Technique
Cryptanalysis for Dlog, SubsetSum, Decoding

Alexander May

Ruhr-University Bochum

Summer School Kaliningrad, July 2019

Discrete Logarithms

DLP: Discrete Logarithm Problem

Given: Generator g for $G = \langle g \rangle$ with $2^{n-1} \leq |G| < 2^n$, $\beta = g^x$
Find: $x = \mathrm{dlog}_g \beta \in \mathbb{Z}_{|G|}$

Examples:

- $G = (\mathbb{Z}, +) = \langle 1 \rangle$, $x = \mathrm{dlog}_1 \beta = \beta$
- $G = (E(p), +)$, best algorithm $\tilde{\mathcal{O}}(\sqrt{|G|}) = \tilde{\mathcal{O}}(2^{\frac{n}{2}})$.
- $G = (\mathbb{Z}_p^*, \cdot)$, best algorithm sub-exponential
- G generic: $\Omega(\sqrt{|G|})$

Variants: small x, small Hamming weight x, faulty x, many x

DLP Enumeration

Algorithm Brute-Force DLP

Input: g, β

1. $x = 0$.
2. **While** $(g^x \neq \beta)$ **do** $x = x + 1$;

Output: $x = \mathrm{dlog}_g \beta$

Runtime:

- Need x iterations of while-loop, each costs one group operation.
- $\mathcal{O}(x) = \mathcal{O}(|G|) = \mathcal{O}(2^n)$ group operations.
- Each group operation costs usually $\mathcal{O}(\log^c n)$ bit operations.
- **Notice:** Brute-Force not bad for small x.

Reaching Square Root Complexity

Idea:

- Write $x = x_1 + x_2 2^{n/2}$ with $0 \leq x_1, x_2 < 2^{n/2}$.
- Use identity $g^{x_1} = \beta \cdot (g^{-2^{\frac{n}{2}}})^{x_2}$.

Algorithm Meet-in-the-Middle DLP

Input: g, β

1. **For** $0 \leq i < 2^{n/2}$ **do** store (i, g^i) in list L.
2. Sort list L according to second entry.
3. **For** $0 \leq i < 2^{n/2}$ **do** if $\exists (i, \beta \cdot (g^{-2^{\frac{n}{2}}})^j) \in L$, output $x = i + j2^{n/2}$.

Output: $x = \mathrm{dlog}_g \beta$

Correctness: MitM terminates iff $(i, j) = (x_1, x_2)$.
Run time: $\tilde{\mathcal{O}}(2^{\frac{n}{2}}) = \tilde{\mathcal{O}}(\sqrt{|G|})$. But also memory $\tilde{\Theta}(\sqrt{|G|})$.

Exercise: Modify MitM such that it has runtime $\tilde{\mathcal{O}}(x)$.

Multiple Discrete Logarithms

Multiple DLP

Given: Generator g for $G = \langle g \rangle$ with $2^{n-1} \leq |G| < 2^n$,
$\beta_1 = g^{x_1}, \ldots, \beta_k = g^{x_k}$

Find: $x_1, \ldots, x_k$

Easy: $\tilde{\mathcal{O}}(k \cdot \sqrt{|G|})$.

Exercise: Show that Multiple DLP can be solved in $\tilde{\mathcal{O}}(\sqrt{k \cdot |G|})$.

Small Weight Discrete Logarithms

Small weight DLP

Given: Generator g for $G = \langle g \rangle$ with $2^{n-1} \leq |G| < 2^n$,
$\beta = g^x$ with known Hamming weight $\mathrm{wt}(x) = \alpha n$, $\alpha \in [0, 1]$

Find: x

Algorithm Brute-Force Small weight DLP

Input: g, β, α

1. **For all** x with $\mathrm{wt}(x) = \alpha n$ **do** if $(g^x = \beta)$ output x;

Output: $x = \mathrm{dlog}_g \beta$

Run time: $\tilde{\mathcal{O}}(\binom{n}{\alpha n})$. How good is that?

Bounding Binomial Coefficients

Theorem Binomials

We have $\binom{n}{\alpha n} = \tilde{\Theta}(2^{H(\alpha)n})$ with $H(\alpha) = -\alpha\log(\alpha) - (1-\alpha)\log(1-\alpha)$.

By Stirling's formula $n! \sim \sqrt{2\pi n}\cdot(\frac{n}{e})^n$ we have

$$\begin{aligned}\binom{n}{\alpha n} &= \frac{n!}{(\alpha n)!((1-\alpha)n)!} = \tilde{\Theta}\left(\frac{(\frac{n}{e})^n}{(\frac{\alpha n}{e})^{\alpha n}(\frac{(1-\alpha)n}{e})^{(1-\alpha)n}}\right) \\ &= \tilde{\Theta}\left(2^{(-\alpha\log\alpha-(1-\alpha)\log(1-\alpha))n}\right) = \tilde{\Theta}(2^{H(\alpha)n})\end{aligned}$$

Corollary

For $0 \le \alpha \le \beta \le 1$: $\binom{\beta n}{\alpha n} = \binom{\beta n}{\alpha\frac{1}{\beta}\beta n} = \tilde{\Theta}(2^{H(\frac{\alpha}{\beta})\cdot\beta n})$.

Small weight Discrete Logarithms

Brute-Force Small Weight DLP: $\tilde{\mathcal{O}}(\binom{n}{\alpha n}) = \tilde{\mathcal{O}}(2^{H(\alpha)n})$, $\alpha = \frac{1}{2} : \tilde{\mathcal{O}}(2^n)$.

Exercise 1: Assume that we get the promise $x = x_1 + x_2 2^{n/2}$ with

$$0 \le x_1, x_2 < 2^{n/2} \text{ and } \mathrm{wt}(x_1) = \mathrm{wt}(x_2) = \alpha \cdot \frac{n}{2}.$$

Devise a MitM algorithm with run time $\tilde{\mathcal{O}}(2^{\frac{H(\alpha)}{2} n})$.

Exercise 2: Do Exercise 1 without promise.

Faulty Discrete Logarithms

Faulty DLP

Given: Generator g for $G = \langle g \rangle$ with $2^{n-1} \leq |G| < 2^n$,
$\beta = g^x$, faulty $\tilde{x}$ with αn, $\alpha \in [0, 1]$ many $1 \to 0$-bits of x

Find: x

Mini Exercise: Show how Faulty DLP relates to Small weight DLP.

Discrete Logarithms

Discrete Logarithms