Discrete logarithm problem VIII

Summary of DL systems

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Generic attacks against DLP

All attacks in this unit are generic attacks, i.e., they work in any group.
Pohlig-Hellman reduces security of DLP to security of largest prime order subgroup. Many groups are much weaker than their size n predicts!

Generic attacks against DLP

All attacks in this unit are generic attacks, i.e., they work in any group. Pohlig-Hellman reduces security of DLP to security of largest prime order subgroup. Many groups are much weaker than their size n predicts!

Let $n = \prod p_i^{e_i},\ \ell = \max\{p_i\}$.

Breaking DLP costs $O(\sqrt{\ell})(\log n)^{O(1)}$ bit operations.

O ignores all constants and lower order terms. $(\log n)^{O(1)}$ covers e_i repetitions in PH, scalar multiplications, and cost of group operations.

Generic attacks against DLP

All attacks in this unit are generic attacks, i.e., they work in any group. Pohlig-Hellman reduces security of DLP to security of largest prime order subgroup. Many groups are much weaker than their size n predicts!

Let $n = \prod p_i^{e_i},\ \ell = \max\{p_i\}$.

Breaking DLP costs $O(\sqrt{\ell})(\log n)^{O(1)}$ bit operations.

O ignores all constants and lower order terms. $(\log n)^{O(1)}$ covers e_i repetitions in PH, scalar multiplications, and cost of group operations.

Remember? Warning #1: Many p are unsafe!
(from ecc-2.pdf, talking about the clock group)

The clock over $\mathbf{F}_p$ has

- $p+1$ points for $p \equiv 3 \bmod 4$,
- $p-1$ points for $p \equiv 1 \bmod 4$.

Thus clock over $\mathbf{F}_{17}$ has $16 = 2^4$ points, very weak DLP.
Fermat $p = 2^{2^m}+1$ & Mersenne $p = 2^m - 1$ primes have weak clock DLP.

Generic attacks against DLP

All attacks in this unit are generic attacks, i.e., they work in any group. Pohlig-Hellman reduces security of DLP to security of largest prime order subgroup. Many groups are much weaker than their size n predicts!

Let $n = \prod p_i^{e_i}, \ \ell = \max\{p_i\}$.

Breaking DLP costs $O(\sqrt{\ell})(\log n)^{O(1)}$ bit operations.

O ignores all constants and lower order terms. $(\log n)^{O(1)}$ covers e_i repetitions in PH, scalar multiplications, and cost of group operations.

Remember? Warning #1: Many p are unsafe!
(from ecc-2.pdf, talking about the clock group)

The clock over $\mathbf{F}_p$ has

- $p+1$ points for $p \equiv 3 \bmod 4$,
- $p-1$ points for $p \equiv 1 \bmod 4$.

Thus clock over $\mathbf{F}_{17}$ has $16 = 2^4$ points, very weak DLP.
Fermat $p = 2^{2^m}+1$ & Mersenne $p = 2^m - 1$ primes have weak clock DLP.

Similar story for elliptic curves, but no general statements on group order. Important to count points to avoid hitting weak group orders n.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

If $c \equiv ab \bmod n$ then also $c_i \equiv a_i b_i \bmod p_i$ because p_i divides n.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

If $c \equiv ab \bmod n$ then also $c_i \equiv a_i b_i \bmod p_i$ because p_i divides n.

If $c \not\equiv ab \bmod n$ then $c_i \equiv a_i b_i \bmod p_i$ only with probability $1/p_i$.

Thus, compute a_i, b_i, c_i for smallest prime p_i.

- If $c_i \not\equiv a_i b_i \bmod p_i$ we know this is not a valid DH triple.
- Else try next larger prime, or p_i^2, or accept higher risk of false positive and output that it is a valid DH triple.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

If $c \equiv ab \bmod n$ then also $c_i \equiv a_i b_i \bmod p_i$ because p_i divides n.

If $c \not\equiv ab \bmod n$ then $c_i \equiv a_i b_i \bmod p_i$ only with probability $1/p_i$.

Thus, compute a_i, b_i, c_i for smallest prime p_i.

- If $c_i \not\equiv a_i b_i \bmod p_i$ we know this is not a valid DH triple.
- Else try next larger prime, or p_i^2, or accept higher risk of false positive and output that it is a valid DH triple.

We correctly solve the DDHP with probability $(2p_i - 1)/(2p_i)$
at the cost of 3 DLPs in group of size p_i

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

If $c \equiv ab \bmod n$ then also $c_i \equiv a_i b_i \bmod p_i$ because p_i divides n.

If $c \not\equiv ab \bmod n$ then $c_i \equiv a_i b_i \bmod p_i$ only with probability $1/p_i$.

Thus, compute a_i, b_i, c_i for smallest prime p_i.

- If $c_i \not\equiv a_i b_i \bmod p_i$ we know this is not a valid DH triple.
- Else try next larger prime, or p_i^2, or accept higher risk of false positive and output that it is a valid DH triple.

We correctly solve the DDHP with probability $(2p_i - 1)/(2p_i)$
at the cost of 3 DLPs in group of size p_i

Example: $p_i = 2$.
Trivial DLPs, correct with $3/4$ probability. Advantage over guessing: $1/4$.

DDHP, CDHP, and DLP

So far: DLP attacks; typically also best approach for CDHP.

DDHP in group of $n = \prod p_i^{e_i}$ elements:
Given P, aP, bP, and cP decide whether $cP = abP$.

For small p_i can easily get a_i, b_i, c_i.

If $c \equiv ab \bmod n$ then also $c_i \equiv a_i b_i \bmod p_i$ because p_i divides n.

If $c \not\equiv ab \bmod n$ then $c_i \equiv a_i b_i \bmod p_i$ only with probability $1/p_i$.

Thus, compute a_i, b_i, c_i for smallest prime p_i.

- If $c_i \not\equiv a_i b_i \bmod p_i$ we know this is not a valid DH triple.
- Else try next larger prime, or p_i^2, or accept higher risk of false positive and output that it is a valid DH triple.

We correctly solve the DDHP with probability $(2p_i - 1)/(2p_i)$
at the cost of 3 DLPs in group of size p_i

Example: $p_i = 2$.
Trivial DLPs, correct with $3/4$ probability. Advantage over guessing: $1/4$.

For DDHP to be hard make sure n is prime.