Discrete logarithm problem VI

Building up to Pohlig–Hellman attack

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Compute $a_2 = \log_R S \equiv a \bmod 53$. This is a DLP in a group of size 53.

Back to our running example

$y^2 = x^3 - x$ over $\mathbf{F}_p$, $p = 1000003$.

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

Given $Q = aP = (670366, 740819)$, find $a = \log_P Q$

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.

Easy to compute $a_1 = \log_R S \equiv a \bmod 2$.
Note $S = (53^2 \cdot 89)Q = (53^2 \cdot 89)aP$ and $(2 \cdot 53^2 \cdot 89)P = \infty$.

- a even, i.e., $a = 2a'$: $S = (53^2 \cdot 89)2a'P = a'\infty = \infty$
- a odd, i.e., $a = 2a' + 1$: $S = (53^2 \cdot 89)(2a' + 1)P = (53^2 \cdot 89)P \neq \infty$

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.

Compute $a_2 = \log_R S \equiv a \bmod 53$. This is a DLP in a group of size 53.

Takes more effort than size 2, but much easier than size 500002.

Can use Pollard rho to attack this subgroup problem in $\sqrt{53\pi/2}$ steps.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo $2 \cdot 53 \cdot 89$.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.

Note that cost counts steps, ignores computation of R and S.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.

Note that cost counts steps, ignores computation of R and S.

But this misses a 53.

Running example continued

$P = (101384, 614510)$ has order $2 \cdot 53^2 \cdot 89$.

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 \bmod 53,$$
$$a \equiv a_4 \bmod 89,$$

to determine a modulo $2 \cdot 53 \cdot 89$. Cost: $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2}$.

Note that cost counts steps, ignores computation of R and S.

But this misses a 53. Brute force search in residue class: cost $+53$.

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Are we there, yet?

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + \sqrt{53^2\pi/2} + \sqrt{89\pi/2} = 79.24$ instead of
cost $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2} + 53$

Are we there, yet? This is not Pohlig–Hellman

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 89)P$ has order 53^2, and
$S = (2 \cdot 89)Q$ is multiple of R.
Compute $a_5 = \log_R S \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_5 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + \sqrt{53^2\pi/2} + \sqrt{89\pi/2} = 79.24$ instead of
cost $1 + \sqrt{53\pi/2} + \sqrt{89\pi/2} + 53 = 74.94$.

Ratio would look worse without Pollard rho (no square roots):
$1 + 2 \cdot 53 + 89 = 196$ vs $1 + 53^2 + 89 = 2899$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T$

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 + 53a_3 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Pohlig–Hellman for running example

$R = (53^2 \cdot 89)P$ has order 2, and
$S = (53^2 \cdot 89)Q$ is multiple of R.
Compute $a_1 = \log_R S \equiv a \bmod 2$.

$R = (2 \cdot 53 \cdot 89)P$ has order 53, and
$S = (2 \cdot 53 \cdot 89)Q$ is multiple of R.
Compute $a_2 = \log_R S \equiv a \bmod 53$.

$T = (2 \cdot 89)(Q - a_2 P) = (2 \cdot 89)(a - a_2)P$ is multiple of R
because $a - a_2 \equiv 0 \bmod 53$, i.e. $a - a_2 = 53a'$ and $T = (2 \cdot 89 \cdot 53)a'P$.
Compute $a_3 = \log_R T \equiv a' \bmod 53$.
Note $a_2 + 53a_3 \equiv a \bmod 53^2$.

$R = (2 \cdot 53^2)P$ has order 89, and
$S = (2 \cdot 53^2)Q$ is multiple of R.
Compute $a_4 = \log_R S \equiv a \bmod 89$.

Use Chinese Remainder Theorem to determine a modulo $2 \cdot 53^2 \cdot 89$.

$$a \equiv a_1 \bmod 2,$$
$$a \equiv a_2 + 53a_3 \bmod 53^2,$$
$$a \equiv a_4 \bmod 89,$$

Cost $1 + 2\sqrt{53\pi/2} + \sqrt{89\pi/2} = 31.07 < 74.94$.