Elliptic-curve cryptography XII

Speedups to Pollard rho for ECC

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Can we use any structure in ECDLP?

On Weierstrass curve $W = (x, y)$ and $-W = (x, -y)$
have same x-coordinate.
Search for x-coordinate collision.

Search space for collisions is only $\lceil \ell/2 \rceil$; this gives factor $\sqrt{2}$
speedup . . . if $f(W_i) = f(-W_i)$.

Can we use any structure in ECDLP?

On Weierstrass curve $W = (x, y)$ and $-W = (x, -y)$ have same x-coordinate.
Search for x-coordinate collision.

Search space for collisions is only $\lceil \ell/2 \rceil$; this gives factor $\sqrt{2}$ speedup ... if $f(W_i) = f(-W_i)$.

To ensure $f(W_i) = f(-W_i)$:
Define $j = h(| W_i |)$ and $f(W_i) = | W_i | + c_j P + d_j Q$, with, e.g., $| W_i |$ the lexicographic minimum of $W_i, -W_i$.
See DLP-IV for definition of the additive walk.

This negation speedup is textbook material.

Problem: fruitless cycles!

Example:
If $h(\mid W_{i+1} \mid) = j = h(\mid W_i \mid)$ and $\mid W_{i+1} \mid = -W_{i+1}$ then

$$\begin{aligned} W_{i+2} &= f(W_{i+1}) = -W_{i+1} + c_j P + d_j Q \\ &= -(\mid W_i \mid + c_j P + d_j Q) + c_j P + d_j Q \\ &= -\mid W_i \mid \end{aligned}$$

Problem: fruitless cycles!

Example:
If $h(\mid W_{i+1} \mid) = j = h(\mid W_i \mid)$ and $\mid W_{i+1} \mid = -W_{i+1}$ then

$$\begin{aligned} W_{i+2} &= f(W_{i+1}) = -W_{i+1} + c_j P + d_j Q \\ &= -(\mid W_i \mid + c_j P + d_j Q) + c_j P + d_j Q \\ &= -\mid W_i \mid \end{aligned}$$

so $\mid W_{i+2} \mid = \mid W_i \mid$
so $W_{i+3} = W_{i+1}$
so $W_{i+4} = W_{i+2}$ etc.

Problem: fruitless cycles!

Example:
If $h(|W_{i+1}|) = j = h(|W_i|)$ and $|W_{i+1}| = -W_{i+1}$ then

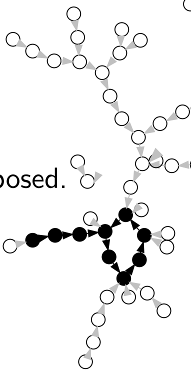
$$\begin{aligned} W_{i+2} &= f(W_{i+1}) = -W_{i+1} + c_j P + d_j Q \\ &= -(|W_i| + c_j P + d_j Q) + c_j P + d_j Q \\ &= -|W_i| \end{aligned}$$

so $|W_{i+2}| = |W_i|$
so $W_{i+3} = W_{i+1}$
so $W_{i+4} = W_{i+2}$ etc.

If h maps to r different values then expect this example to occur with probability $1/(2r)$ at each step.

Known issue, not quite textbook.

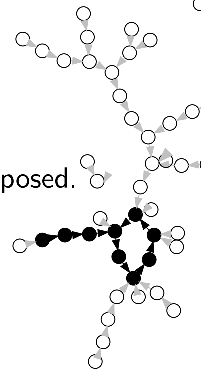
Eliminating fruitless cycles



Issue of fruitless cycles is known and several fixes are proposed.

Summary: most of them got it wrong.

Eliminating fruitless cycles

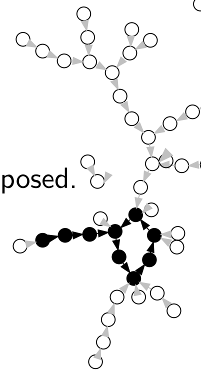


Issue of fruitless cycles is known and several fixes are proposed.
Summary: most of them got it wrong.

So what to do?
Choose a big r, e.g. $r = 2048$.
$1/(2r) = 1/4096$ not too frequent cycles.

Check for cycles occasionally and escape cycle deterministically:
Let $\bar{W}$ be the smallest point in the cycle;
escape by computing $2\bar{W}$.

Eliminating fruitless cycles



Issue of fruitless cycles is known and several fixes are proposed.
Summary: most of them got it wrong.

So what to do?
Choose a big r, e.g. $r = 2048$.
$1/(2r) = 1/4096$ not too frequent cycles.

Check for cycles occasionally and escape cycle deterministically:
Let $\bar{W}$ be the smallest point in the cycle;
escape by computing $2\bar{W}$.

Consequence: preserve most of negation speedup.
3 slides of work for $\sqrt{2}$?!

See ePrint 2011/003 for more details and historical comments.