Speeding up Elliptic Curve Scalar Multiplication without Either Precomputation or Adaptive Coordinates

Mike Hamburg
Rambus Cryptography Research

Original paper

- Kim, Choe, Kim, Kim, Hong, submitted to CHES 2017
  - https://eprint.iacr.org/2017/669.pdf

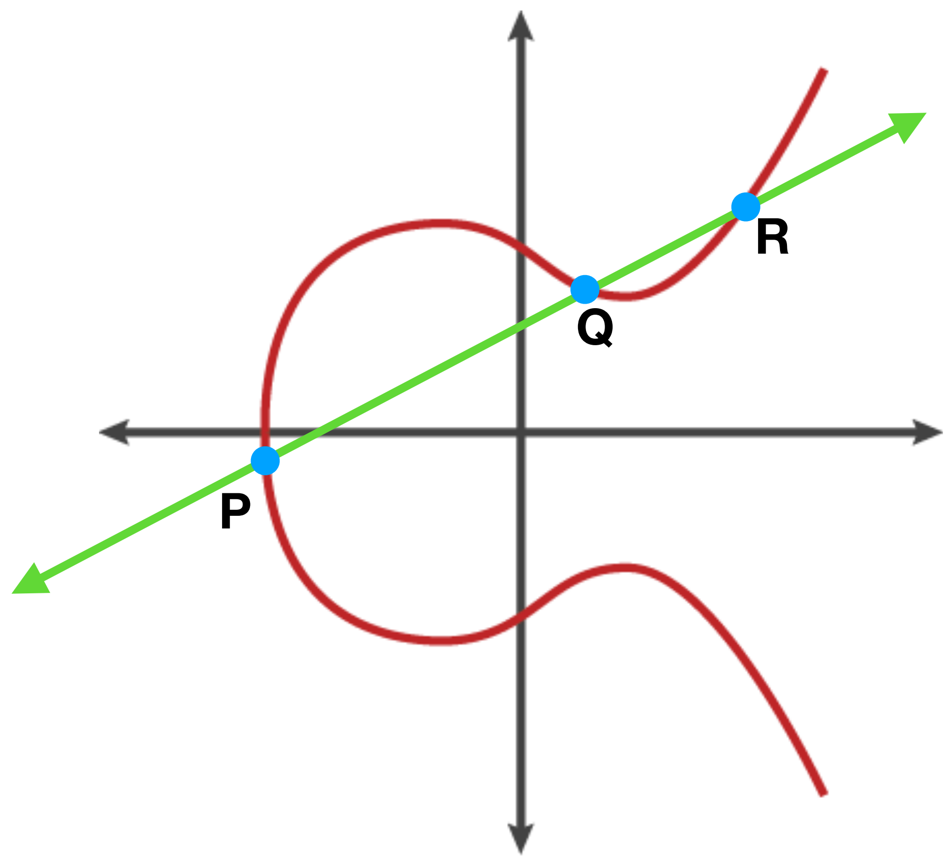
- Speed up Montgomery ladder on short Weierstrass curves
  - Uses complicated “on-the-fly adaptive coordinates”
  - ~ 12M+12.5A/bit, 8-10 registers
    - vs ~14M/bit for previous work

Gist of the idea

- State of Montgomery ladder: (P,Q,R) where P+Q+R = 0
  - P,Q,R are on a line y=mx+b
- Jacobian co-Z representation:

$$z^2 \cdot x_P,\ z^2 \cdot x_Q,\ z^2 \cdot x_R,$$

$$z^3 \cdot y_P,\ z \cdot m$$



Refinement

12M + 8.5A/bit, 6 registers

Coordinates

$$\begin{aligned} X_0 &:= 3Z^2 \cdot x_0 \\ X_1 &:= Z^2 \cdot (x_1 - x_0) \\ X_2 &:= Z^2 \cdot (x_2 - x_0) \\ Y_0 &:= 2Z^3 \cdot y_0 \\ M &:= 2Z \cdot \frac{y_1 - y_0}{x_1 - x_0} \end{aligned}$$

Jacobi co-Z setup trick: odd degree on Y,M -> can do x-only!

Ladder step

$$\begin{aligned} Y_1 &\leftarrow Y_0 + M \cdot X_1 \\ k &\leftarrow Y_1^2 \\ z &\leftarrow Y_1 \cdot (X_2 - X_1) \\ X_0' &\leftarrow X_0 \cdot z^2 \\ Y_0' &\leftarrow Y_0 \cdot z^3 \\ l &\leftarrow k + M \cdot z \\ M' &\leftarrow 2 \cdot X_1 \cdot (X_2 - X_1)^2 - k - l \\ X_2' &\leftarrow k \cdot l \\ X_1' &\leftarrow (M'/2)^2 - X_0' - X_2' \end{aligned}$$

Future work

- Submit Curve256224192961 to TLS 1.3
- Simplify DPA countermeasures
- Defuse nuclear crisis