HyPoRes: An Hybrid Representation System for ECC

P. Martins[1] J. Marrez[2] J.-C. Bajard[2] L. Sousa[1]

[1]INESC-ID, Instituto Superior Técnico, Univ. Lisboa
[2]Sorbonnes Université, CNRS, LIP6, Paris, France

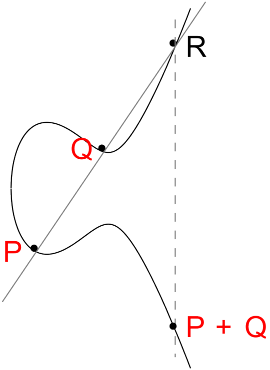
26th IEEE Symposium on Computer Arithmetic

Acknowledgement

This work was partially supported by Portuguese funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2019 and by the Ph.D. grant with reference SFRH/BD/103791/2014; by the ANR grant ARRAND 15-CE39-0002-01; through the Pessoa/Hubert Curien programme with reference 4335 (FCT)/40832XC (CAMPUSFRANCE); and by EU's Horizon 2020 research and innovation programme under grant agreement No. 779391 (FutureTPM).

Table of Contents

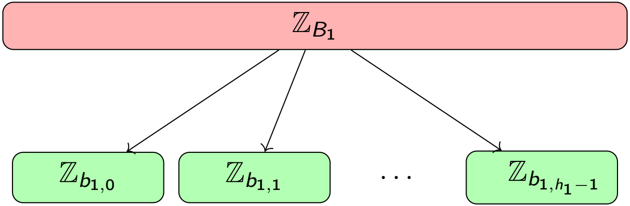
Elliptic Curve Cryptography



Point addition of two points over an EC defined in $\mathbb{R}$

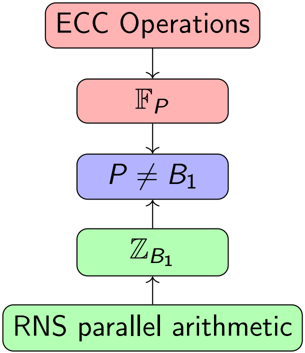
- Security based on the difficulty of computing n from $[n]P$ and P for curves defined over a finite field $\mathbb{F}_P$

Residue Number System



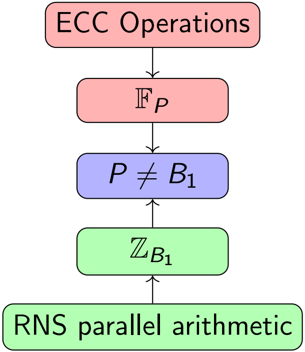
RNS breaks arithmetic modulo $B_1 = b_{1,0} \times \ldots \times b_{1,h_1-1}$ down to arithmetic modulo $b_{1,0}, \ldots, b_{1,h_1-1}$

Bridging the Gap



- **Montgomery Reduction**
  Maps operations in $\mathbb{F}_P$ to $\mathbb{Z}_{B_1}$ for any P with complexity of $\mathcal{O}(\log_2^2 P)$;
- **Hybrid-Positional Residue Number System (HPR)**
  Uses $P = B_1^n - \beta$ to reduce complexity to $\mathcal{O}(\log_2^{3/2} P)$.

Bridging the Gap



- **Montgomery Reduction**
  Maps operations in $\mathbb{F}_P$ to $\mathbb{Z}_{B_1}$ for any P with complexity of $\mathcal{O}(\log_2^2 P)$;
- **Hybrid-Positional Residue Number System (HPR)**
  Uses $P = B_1^n - \beta$ to reduce complexity to $\mathcal{O}(\log_2^{3/2} P)$.
  - Does not work for standardised primes

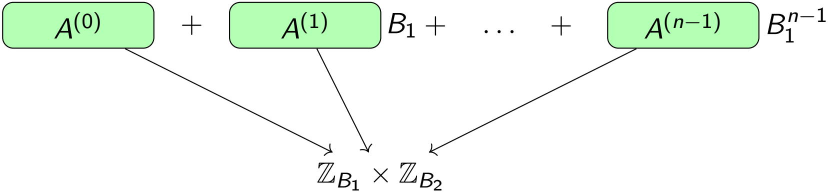
Table of Contents

Montgomery Reduction

$$\begin{tikzcd}
A \sim P^2 \arrow[d] & \\
\begin{array}{c} Q_1 \text{ s.t. } B_1 | A + Q_1 P \\ Q_1 = -AP^{-1} \bmod B_1 \end{array} \arrow[r, "\mathcal{O}(h_1 h_2)"] & Q_2 = Q_1 \bmod B_2 \arrow[d] \\
Z_1 = Z_2 \bmod B_1 & Z_2 = \frac{A + Q_1 P}{B_1} \text{ small} \arrow[l, "\mathcal{O}(h_1 h_2)"']
\end{tikzcd}$$

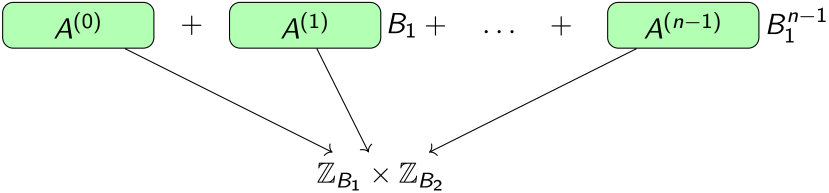
Complexity dominated by $\mathcal{O}(h_1 h_2)$ with $h_1 \sim h_2 \sim \log_2 P$

Hybrid-Positional Residue Number System



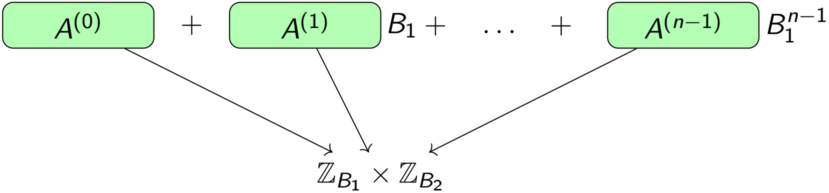
- $D = A \times C =$
  $D^{(0)} + D^{(1)} B_1 + \ldots + D^{(n-1)} B_1^{n-1} + D^{(n)} B_1^{n} + \ldots + D^{(2n-2)} B_1^{2n-2}$

Hybrid-Positional Residue Number System



- $D = A \times C =$
  $D^{(0)} + D^{(1)} B_1 + \ldots + D^{(n-1)} B_1^{n-1} + D^{(n)} B_1^{n} + \ldots + D^{(2n-2)} B_1^{2n-2}$
- For $P = B_1^n - \beta$:
  $D \equiv \left(D^{(0)} + \beta D^{(n)}\right) + \left(D^{(1)} + \beta D^{(n+1)}\right) B_1 + \ldots + D^{(n-1)} B_1^{n-1}$

Hybrid-Positional Residue Number System



- $D = A \times C = D^{(0)} + D^{(1)} B_1 + \dots + D^{(n-1)} B_1^{n-1} + D^{(n)} B_1^{n} + \dots + D^{(2n-2)} B_1^{2n-2}$
- For $P = B_1^n - \beta$: $D \equiv \left(D^{(0)} + \beta D^{(n)}\right) + \left(D^{(1)} + \beta D^{(n+1)}\right) B_1 + \dots + D^{(n-1)} B_1^{n-1}$
- Perform carry propagation to reduce the digits magnitude

Carry Propagation

$$
\begin{tikzcd}
D_1^{(i)} \bmod B_1 \arrow[r, "\mathcal{O}(h_1 h_2)"] & D_1^{(i)} \bmod B_2 \arrow[d] \arrow[dd, bend left] \\
C_1^{(i)} = C_2^{(i)} \bmod B_1 \arrow[dd] & C_2^{(i)} = \frac{D_2^{(i)} - D_1^{(i)}}{B_1} \arrow[l, "\mathcal{O}(h_1 h_2)"'] \arrow[dd, bend left] \\
 & D_2^{(i)} = D_1^{(i)} \\
D_1^{(i+1)} = D_1^{(i+1)} + C_1^{(i)} & D_2^{(i+1)} = D_2^{(i+1)} + C_2^{(i)}
\end{tikzcd}
$$

Complexity dominated by $\mathcal{O}(n^2(h_1 + h_2) + nh_1h_2)$ with $nh_1 \sim nh_2 \sim \log_2 P$

Table of Contents

Hybrid Polynomial-Residue Number System

$$
\begin{tikzcd}
 & & \mathbb{Z}_{B_1} \times \mathbb{Z}_{B_2} & & \\
\boxed{A^{(0)}} \arrow[urr] \arrow[drr] & + & \boxed{A^{(1)}}\, X \arrow[u] \arrow[d] & + \quad \ldots \quad + & \boxed{A^{(n-1)}}\, X^{n-1} \arrow[ull] \arrow[dll] \\
 & & a = \sum_{i=0} A^{(i)} \gamma^i \bmod P & &
\end{tikzcd}
$$

Hybrid Polynomial-Residue Number System

$$\mathbb{Z}_{B_1} \times \mathbb{Z}_{B_2}$$

$$\boxed{A^{(0)}} + \boxed{A^{(1)}} X + \ \dots \ + \boxed{A^{(n-1)}} X^{n-1}$$

$$a = \sum_{i=0} A^{(i)} \gamma^i \bmod P$$

$\boxed{\gamma \text{ is the n-}th\text{ root of a small value } \beta \text{ over } \mathbb{F}_P}$ $\Rightarrow X^n - \beta \cong 0$

Hybrid Polynomial-Residue Number System

$\boxed{\gamma \text{ is the n-}\textit{th}\text{ root of a small value } \beta \text{ over } \mathbb{F}_P} \Rightarrow X^n - \beta \cong 0$

- $D = A \times C = D^{(0)} + D^{(1)}X + \ldots + D^{(n-1)}X^{n-1} + D^{(n)}X^n + \ldots + D^{(2n-2)}X^{2n-2}$

Hybrid Polynomial-Residue Number System

$\boxed{\gamma \text{ is the n-}th\text{ root of a small value } \beta \text{ over } \mathbb{F}_P}$ $\Rightarrow X^n - \beta \cong 0$

- $D = A \times C = D^{(0)} + D^{(1)}X + \ldots + D^{(n-1)}X^{n-1} + D^{(n)}X^n + \ldots + D^{(2n-2)}X^{2n-2}$
- $D \equiv D - (D^{(n)} + \ldots + D^{(2n-2)}X^{n-2}) \times (X^n - \beta) \equiv \left(D^{(0)} + \beta D^{(n)}\right) + \left(D^{(1)} + \beta D^{(n+1)}\right) B_1 + \ldots + D^{(n-1)}B_1^{n-1}$

Hybrid Polynomial-Residue Number System

γ is the n-*th* root of a small value β over $\mathbb{F}_P$ $\Rightarrow X^n - \beta \cong 0$

- $D = A \times C = D^{(0)} + D^{(1)}X + \ldots + D^{(n-1)}X^{n-1} + D^{(n)}X^n + \ldots + D^{(2n-2)}X^{2n-2}$
- $D \equiv D - (D^{(n)} + \ldots + D^{(2n-2)}X^{n-2}) \times (X^n - \beta) \equiv \left(D^{(0)} + \beta D^{(n)}\right) + \left(D^{(1)} + \beta D^{(n+1)}\right) B_1 + \ldots + D^{(n-1)} B_1^{n-1}$
- Perform Montgomery reduction to reduce the digits magnitude

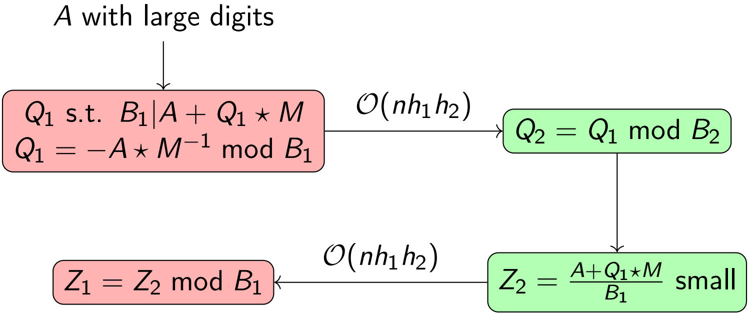
Hybrid Polynomial-Residue Number System

- Lattice $\mathcal{L}(\Gamma)$ of the representations of zero

$$\Gamma = \begin{bmatrix} P & 0 & \dots & 0 \\ -\gamma & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\gamma^n & 0 & \dots & 1 \end{bmatrix}$$

- Each line in Γ corresponds to either $P = 0 \bmod P$ or $-\gamma^i + X^i$, which when evaluated at $X = \gamma$ produces a value congruent with 0
- Minskowski's theorem guarantees that $\mathcal{L}(\Gamma)$ contains a nonzero vector M of norm at most $(\det\mathcal{L}(\Gamma))^{1/n} = P^{1/n}$

Hybrid Polynomial-Residue Number System

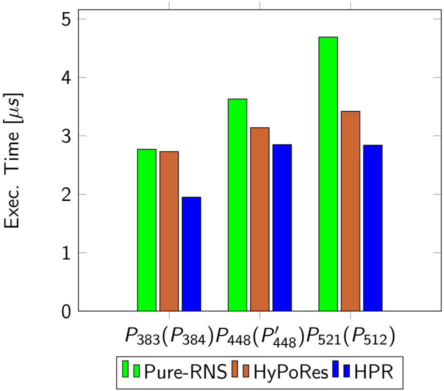


$\star$ denotes multiplication in $\mathbb{Z}[X]/(X^n - \beta)$

Complexity dominated by $\mathcal{O}(n^2(h_1 + h_2) + nh_1 h_2)$ with $nh_1 \sim nh_2 \sim \log_2 P$

Table of Contents

Experimental Results



Average execution time of a pure-RNS and the proposed approaches for standardised primes, as well as of HPR with specially crafted primes on a i7-3770K

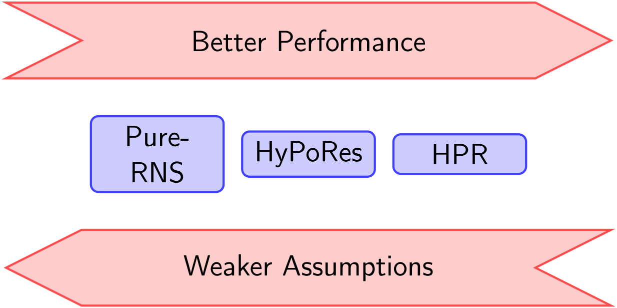
Table of Contents

Protection against SCAs

- Choose γ as the root of $E(X) = E^{(0)} + \ldots + E^{(n-1)}X^{n-1} + X^n$
- Operate over $\mathbb{Z}[X]/(E(X))$ instead of $\mathbb{Z}[X]/(X^n - \beta)$
- Choose a E at random at the beginning of point multiplication
- Change representations throughout the execution of the algorithm by precomputing representations of γ^i in the target system

Table of Contents

Conclusion



- HyPoRes multiplication has subquadratic time complexity
- Montgomery reduction is slower than carry propagation so HyPoRes is slower than HPR, but works for any prime
- Redundant representations are possible, improving resistance against SCAs

Thank you!

Any questions?