Multi-precision PMNS with CIOS reduction

François Palma

Nicolas Méloni and Pascal Véron

Laboratoire IMATH
Université de Toulon

Modular Arithmetic

In Cryptography

- Diffie-Hellmann key exchange
  - Discrete Logarithm Problem
  - $\sim 1024, 2048, \ldots$ bits

Modular Arithmetic

In Cryptography

- Diffie-Hellmann key exchange
  - Discrete Logarithm Problem
  - $\sim 1024, 2048, \ldots$ bits
- RSA protocol
  - Integer Factorisation Problem
  - $\sim 2048, 4096, \ldots$ bits

Modular Arithmetic

In Cryptography

- Diffie-Hellmann key exchange
  - Discrete Logarithm Problem
  - $\sim 1024, 2048, \ldots$ bits
- RSA protocol
  - Integer Factorisation Problem
  - $\sim 2048, 4096, \ldots$ bits
- Elliptic Curve Cryptography (ECC)
  - Discrete Logarithm Problem (on elliptic curves)
  - $\sim 255, 521, \ldots$ bits

Modular Arithmetic

In Cryptography

- Diffie-Hellmann key exchange
  - Discrete Logarithm Problem
  - $\sim 1024, 2048, \ldots$ bits
- RSA protocol
  - Integer Factorisation Problem
  - $\sim 2048, 4096, \ldots$ bits
- Elliptic Curve Cryptography (ECC)
  - Discrete Logarithm Problem (on elliptic curves)
  - $\sim 255, 521, \ldots$ bits
- Module Lattice Key Encapsulation
  - (Ring) Learning With Error Problem
  - $\sim 10, 13, \ldots$ bits (23 bits for Dilithium)

Modular Arithmetic

In Cryptography

- Diffie-Hellmann key exchange
  - Discrete Logarithm Problem
  - $\sim 1024, 2048, \ldots$ bits
- RSA protocol
  - Integer Factorisation Problem
  - $\sim 2048, 4096, \ldots$ bits
- Elliptic Curve Cryptography (ECC)
  - Discrete Logarithm Problem (on elliptic curves)
  - $\sim 255, 521, \ldots$ bits
- Module Lattice Key Encapsulation
  - (Ring) Learning With Error Problem
  - $\sim 10, 13, \ldots$ bits (23 bits for Dilithium)
- Isogeny-based Cryptography
  - Explicit Isogeny Finding Problem
  - $\sim 512, 1024, \ldots$ bits

- Mersenne Primes
  - $p = 2^q - 1$ with prime q (Ex: $2^{521} - 1$)
  - Only 52 known currently

- Mersenne Primes
  - $p = 2^q - 1$ with prime q (Ex: $2^{521} - 1$)
  - Only 52 known currently
- Pseudo-Mersenne Primes
  - $p = 2^n - c$ with small c (Ex: $2^{255} - 19$)
  - Enough for most use cases

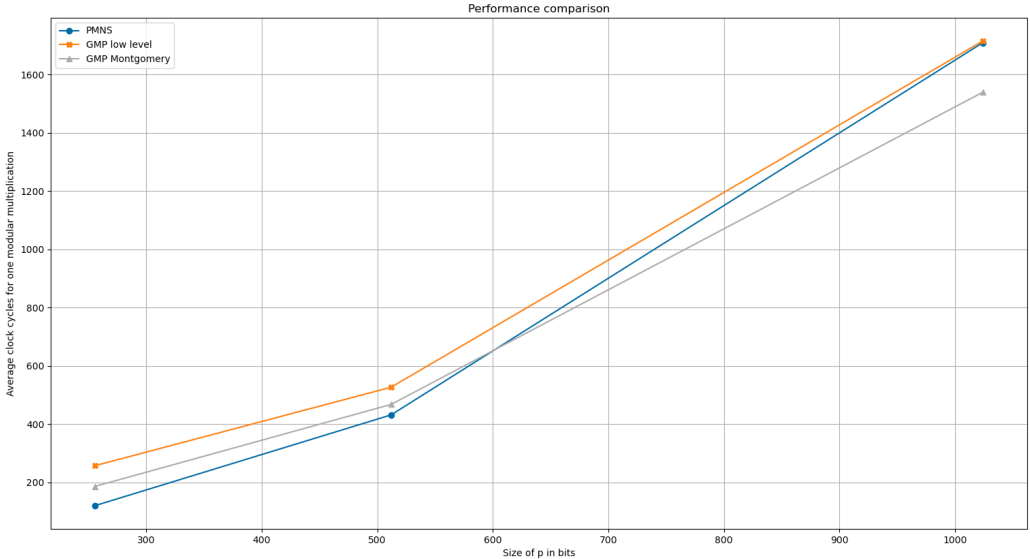
- Mersenne Primes
  - $p = 2^q - 1$ with prime q (Ex: $2^{521} - 1$)
  - Only 52 known currently
- Pseudo-Mersenne Primes
  - $p = 2^n - c$ with small c (Ex: $2^{255} - 19$)
  - Enough for most use cases
- General Methods
  - Montgomery reduction, Barret reduction, etc.
  - Representation systems (RNS, **PMNS**)

Definition

What is a PMNS?

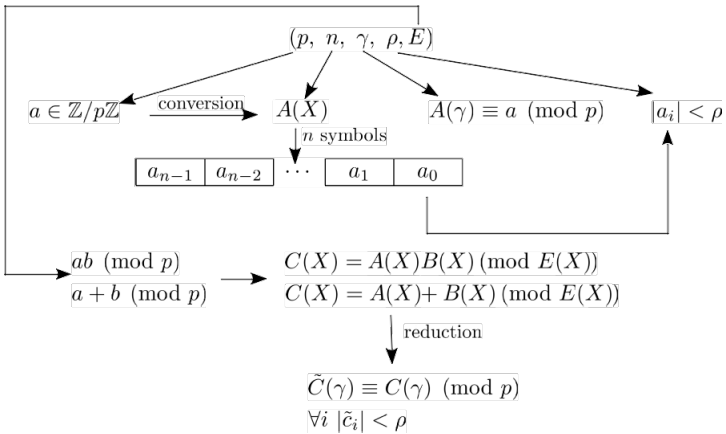
- Polynomial Modular Number System (PMNS) is a non-positional number system based on polynomial operations.
- Proposed as an extension of Mersenne numbers to generic primes by J.-C. Bajard, L. Imbert and T. Plantard in 2004.
- Fast modular operations
- Very adapted to parallel processing (SIMD and Multi-Threading).

Performances on small sizes



Definition

Polynomial Modular Number System



$E \in \mathbb{Z}[X]$ with $\deg(E) = n$ and $E(\gamma) \equiv 0 \pmod p$. Here we'll take $E(X) = X^n - \lambda$, $\lambda \in \mathbb{Z}^*$.

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$
- $C(X) = A(X)B(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$
- $C(X) = A(X)B(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $C'(X) = C(X) \pmod{E(X)} = -2X^2 + 3$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$
- $C(X) = A(X)B(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $C'(X) = C(X) \pmod{E(X)} = -2X^2 + 3$
- $T(X) = -2X^2 + X + 3$. $T(7) \equiv -88 \equiv 0 \pmod{11}$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$
- $C(X) = A(X)B(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $C'(X) = C(X) \pmod{E(X)} = -2X^2 + 3$
- $T(X) = -2X^2 + X + 3$. $T(7) \equiv -88 \equiv 0 \pmod{11}$
- $C''(X) = C'(X) - T(X) = -X$

Toy example

$\mathcal{B} = (p = 11, n = 3, \gamma = 7, \rho = 2, E = X^3 - 2)$

- $a = 8 \in \mathbb{Z}/11\mathbb{Z}, \quad a \underset{\mathcal{B}}{\equiv} A(X) = X^2 - X - 1$
- $deg(A) < 3$ and $A(7) \equiv 7^2 - 7 - 1 \equiv 41 \equiv 8 \pmod{11}$ but also $\forall i, |a_i| < 2$
- $b = 6 \in \mathbb{Z}/11\mathbb{Z}, \quad b \underset{\mathcal{B}}{\equiv} B(X) = X - 1$
- $C(X) = A(X)B(X) = (X^2 - X - 1)(X - 1) = X^3 - 2X^2 + 1$
- $C'(X) = C(X) \pmod{E(X)} = -2X^2 + 3$
- $T(X) = -2X^2 + X + 3$. $T(7) \equiv -88 \equiv 0 \pmod{11}$
- $C''(X) = C'(X) - T(X) = -X$
- $C''(\gamma) \equiv C''(7) \equiv -7 \equiv 4 \pmod{11}$
- $ab \equiv 8 \times 6 \equiv 48 \equiv 4 \pmod{11}$

Problems with the Internal Reduction

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E(X) = X^5 - 2$)

- $A(X) = -16418323151436339X^4 + 276252764540687X^3 + 7437842018938432X^2 + 15470279641088753X - 2872875599240331$
- $B(X) = 8415344909652960X^4 + 11618420586034114X^3 + 4878049157314445X^2 - 12466769851259518X + 13065840613549045$

Problems with the Internal Reduction

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E(X) = X^5 - 2$)

- $A(X) = -16418323151436339X^4 + 276252764540687X^3 + 7437842018938432X^2 + 15470279641088753X - 2872875599240331$
- $B(X) = 8415344909652960X^4 + 11618420586034114X^3 + 4878049157314445X^2 - 12466769851259518X + 13065840613549045$
- $C(X) = A(X)B(X) \pmod{E} = -261170376783951124298044453147 99X^4 - 323361586801243385440149246043390X^3 - 486557228677722166863040666055161X^2 + 209372165676495862076393950487709X + 807732958307539765529003803418995$

Problems with the Internal Reduction

($p = 726589512580075827165577815940205655126075658084463158895150129844038996753 09$, $n = 5$, $\gamma = 472336245400502276405725161213198813429259421923382283164897368044854918329 57$, $\rho = 18014398509481984$, $E(X) = X^5 - 2$)

- $A(X) = -16418323151436339X^4 + 276252764540687X^3 + 7437842018938432X^2 + 15470279641088753X - 2872875599240331$
- $B(X) = 8415344909652960X^4 + 11618420586034114X^3 + 4878049157314445X^2 - 12466769851259518X + 13065840613549045$
- $C(X) = A(X)B(X) \pmod{E} = -261170376783951124298044453147 99X^4 - 323361586801243385440149246043390X^3 - 486557228677722166863040666055161X^2 + 209372165676495862076393950487709X + 807732958307539765529003803418995$
- $T(X) = -261170376783951137028752688855 27X^4 - 323361586801243386353102368891163X^3 - 486557228677722166596847906695602X^2 + 209372165676495862217556218662421X + 807732958307539764312874335104100$

Montgomery Modular Multiplication

Algorithm 1 Montgomery Modular Multiplication

Require: m the modulus, $a \in \mathbb{Z}/m\mathbb{Z}$, $b \in \mathbb{Z}/m\mathbb{Z}$, $\phi = 2^h$ with $h \in \mathbb{N}^*$ such that $2^{h-1} < m < 2^h$.

Ensure: $c \equiv ab\phi^{-1} \bmod m$, with $c \in \mathbb{Z}/m\mathbb{Z}$

1: $c \leftarrow a \times b$
2: $q \leftarrow c \times m^{-1} \bmod \phi$
3: $c \leftarrow (c - q \times m)/\phi$ # Exact division
4: **return** c

$(c \times m^{-1} \bmod \phi) \times m \equiv c \pmod{\phi}$ so $c - q \times m \equiv 0 \pmod{\phi}$.

Montgomery Lattice Reduction

Adaptation by C. Negre and T. Plantard in 2008.

Algorithm 2 Montgomery-like Polynomial Multiplication

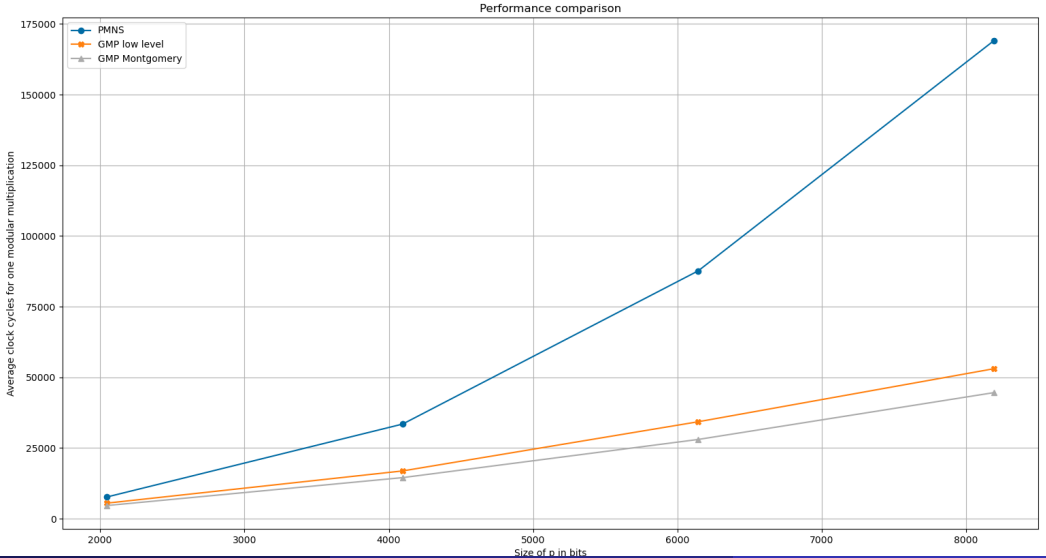
Require: $\mathcal{B} = (p,\ n,\ \gamma,\ \rho, E)$ a PMNS, $A, B \in \mathcal{B} \times \mathcal{B}$, $M \in \mathbb{Z}[X]$ such that $M(\gamma) \equiv 0 \pmod{p}$, $\phi = 2^h$ with $h \in \mathbb{N}^*$.

Ensure: $C(\gamma) \equiv A(\gamma)B(\gamma)\phi^{-1} \bmod p$, with $C' \in \mathcal{B}$

1: $C \leftarrow A(X) \times B(X) \pmod{E(X)}$
2: $Q \leftarrow C(X) \times M^{-1}(X) \pmod{E(X), \phi}$
3: $T \leftarrow Q(X) \times M(X) \pmod{E(X)}$
4: $C \leftarrow (C(X) - T(X))/\phi$ # Exact division
5: return C

For performance reasons ϕ is taken as $\phi = 2^{64}$.

Performance on large sizes



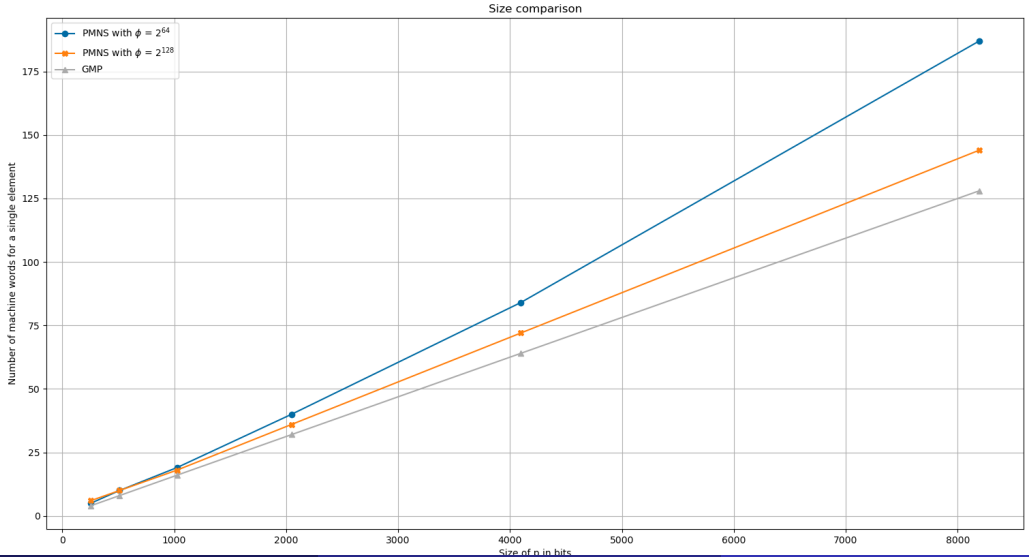
Internal Reduction Matrix

We can view multiplication by M mod $E(X) = X^n - \lambda$ as multiplication by

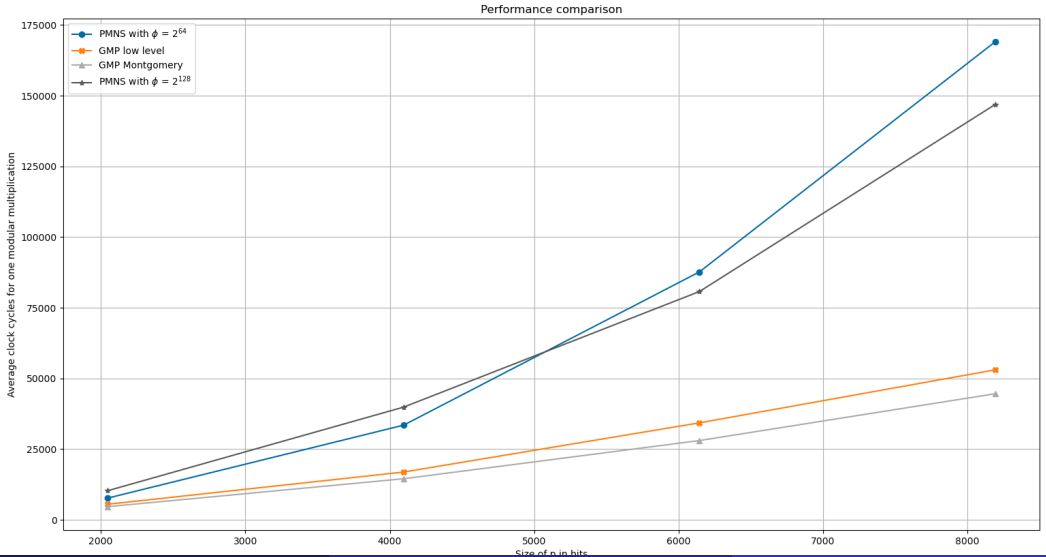
$$\mathcal{M} = \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ \lambda m_{n-1} & m_0 & \dots & m_{n-2} \\ \vdots & \ddots & \ddots & \vdots \\ \lambda m_1 & \lambda m_2 & \dots & m_0 \end{pmatrix} \begin{matrix} \leftarrow M \\ \leftarrow X.M \bmod E \\ \\ \leftarrow X^{n-1}.M \bmod E \end{matrix}$$

From Minkowski we can expect $\|\mathcal{M}\|_1 \approx (n!p)^{\frac{1}{n}}$.
We need $\phi > \|\mathcal{M}\|_1$ for parameter consistency so n will grow too much for large p.
In 2023, Meloni et al. suggest we take $\phi = 2^{128}$ instead of $\phi = 2^{64}$.

Size Comparison



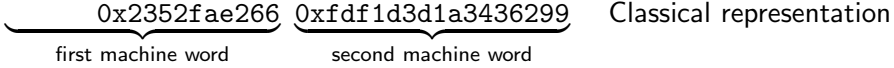
Results on large sizes



How to fix this?

Reduced coefficients in computer arithmetic

If we need to store `0x2352fae266fdf1d3d1a3436299` in memory:

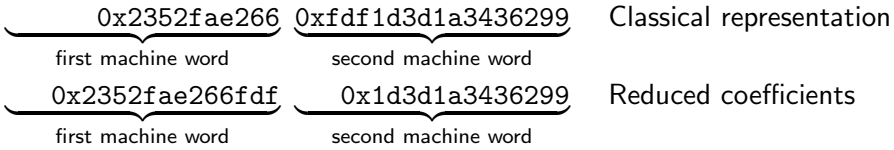


Classical representation

How to fix this?

Reduced coefficients in computer arithmetic

If we need to store `0x2352fae266fdf1d3d1a3436299` in memory:



This lets us postpone carry propagation to the very end.

Montgomery CIOS

Algorithm 3 Montgomery CIOS Modular Multiplication

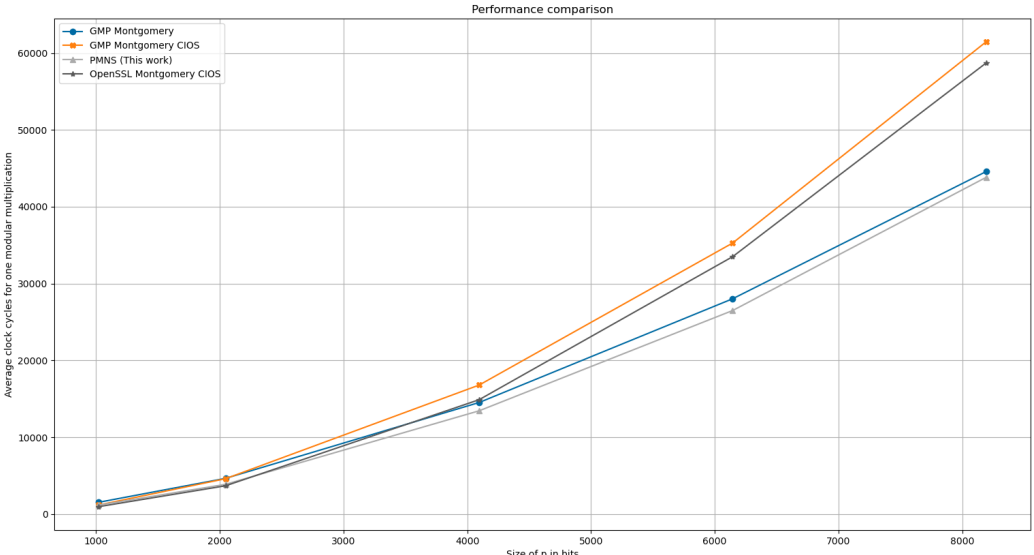
Require: m the modulus, $a \in \mathbb{Z}/m\mathbb{Z}$, $b \in \mathbb{Z}/m\mathbb{Z}$, $\phi = (2^{64})^h$ with $h \in \mathbb{N}^*$ such that $(2^{64})^{h-1} < m < (2^{64})^h$.

Ensure: $c \equiv ab\phi^{-1} \bmod m$, with $c \in \mathbb{Z}/m\mathbb{Z}$

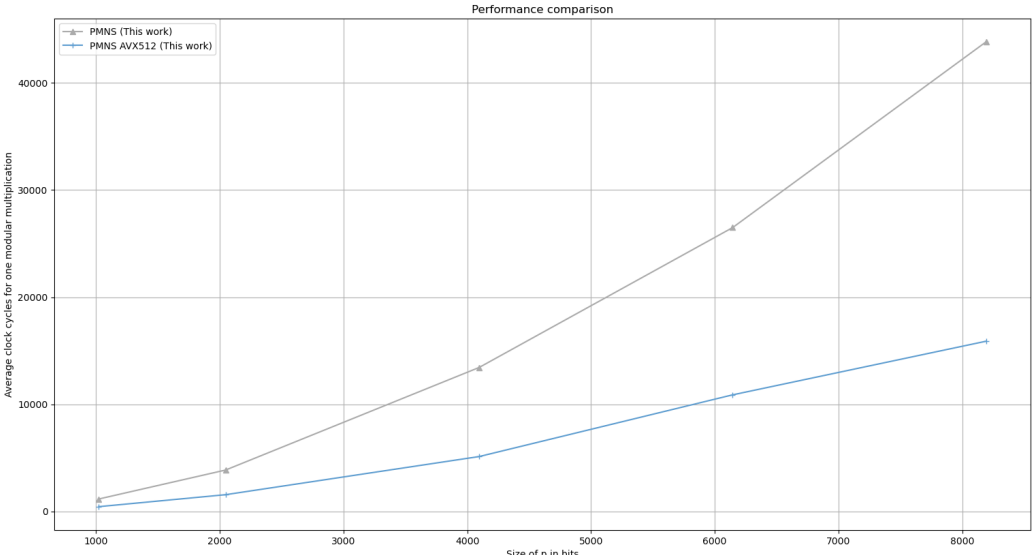
1: $c \leftarrow 0$
2: **for** $i = 0..h-1$ **do**
3: $\quad c \leftarrow c + a \times (\left\lfloor \frac{b}{(2^{64})^i} \right\rfloor \bmod 2^{64})$
4: $\quad q \leftarrow c \times m' \bmod 2^{64}$
5: $\quad c \leftarrow (c - q \times m)/\phi$ # Exact division
6: **end for**
7: **return** c

We only need the lower 64 bits of m^{-1}.

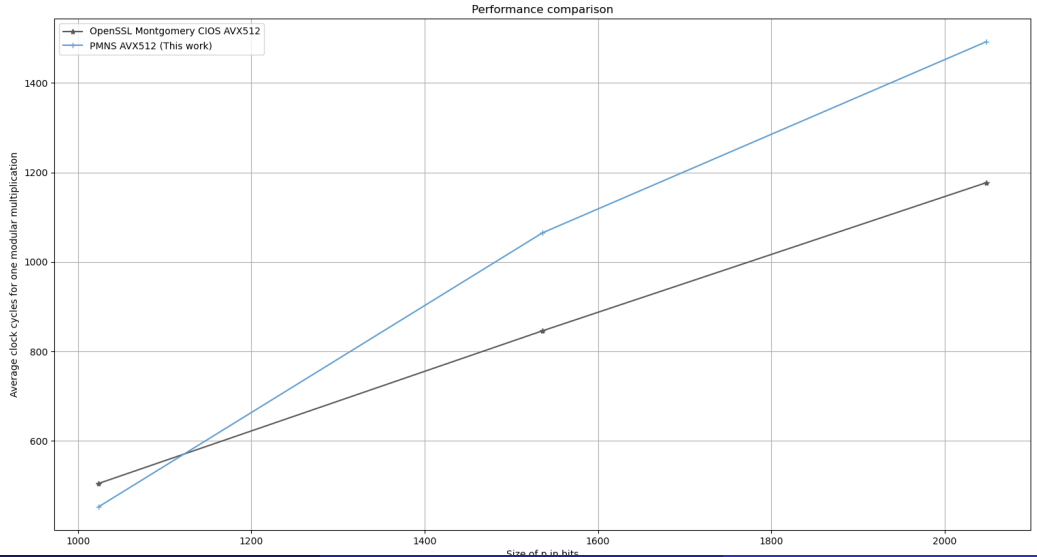
Results


Performance comparison
GMP Montgomery
GMP Montgomery CIOS
PMNS (This work)
OpenSSL Montgomery CIOS
Average clock cycles for one modular multiplication
Size of n in bits
0
10000
20000
30000
40000
50000
60000
1000
2000
3000
4000
5000
6000
7000
8000

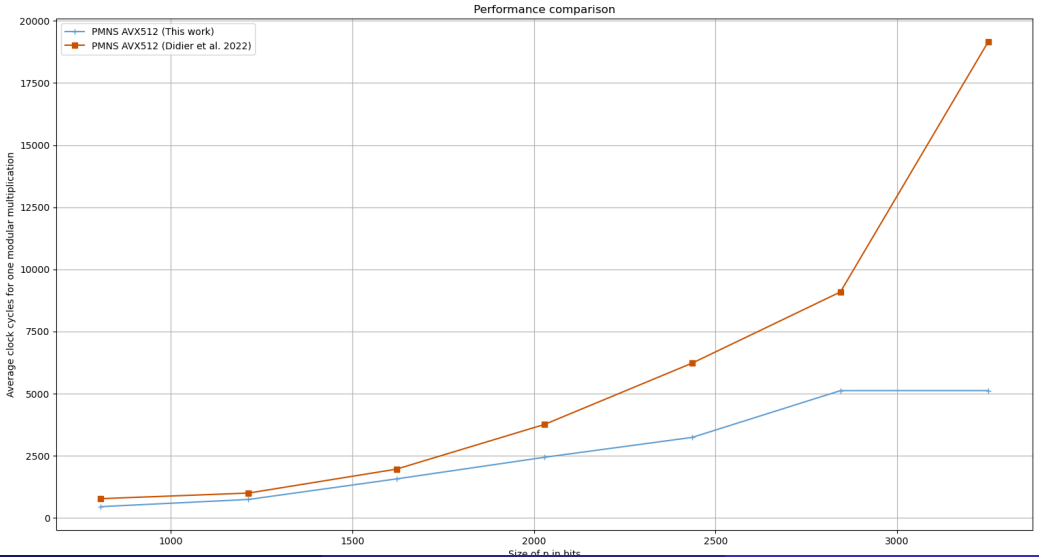
AVX512 vs Sequential



AVX512 vs OpenSSL



AVX512 vs Previous work



Thank you

Thank you for your attention.