## Efficient and secure modular operations using the Adapted Modular Number System

Laurent-Stéphane Didier, Fangan-Yssouf Dosso, Pascal Véron

Université de Toulon<br>Laboratoire IMath

Journées codage \& cryptographie 2018
Aussois, le 08 octobre 2018

## Introduction

About the AMNS (Adapted Modular Number System):

- Goal: Perform efficiently and safely arithmetic operations with big integers for cryptographic algorithms.
- Main feature: Uses polynomial representation for its elements.

Our contribution:

- Generalisation of some works done by Nadia El-Mrabet, Christophe Negre, Thomas Plantard, and al.
- Implementation and comparison to classical methods like Montgomery modular multiplication.


## Plan

(1) Adapted modular number system

- Definition and example
- Arithmetic operations in the AMNS
(2) Generation of an AMNS
- Parameters set
- Computation of the internal reduction polynomial
(3) Implementation, results and comparison
- Implementation
- Results


## Definition: AMNS (Adapted Modular Number System)

Let $p$ be a prime integer.

## Definition

An AMNS for $p$ is defined by the tuple $\mathcal{B}=(p, n, \gamma, \rho)$ such that for every integer $0 \leqslant y<p$, there exists a polynomial $V(X)=v_{0}+v_{1} \cdot X+\cdots+v_{n-1} \cdot X^{n-1}$ which satisfies:

- $\left|v_{i}\right|<\rho$
- $y \equiv V(\gamma)(\bmod p)$
where $0<\gamma<p$ and $\rho \approx \sqrt[n]{p}$


## Example of AMNS

| 0 | 1 | 2 | 3 | 4 |
| :---: | :---: | :---: | :---: | :---: |
| 0 | 1 | $-X^{2}$ | $1-X^{2}$ | $-1+X+X^{2}$ |


| 5 | 6 | 7 | 8 | 9 | 10 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $X+X^{2}$ | $-1+X$ | $X$ | $1+X$ | $-X-1$ | $-X$ |


| 11 | 12 | 13 | 14 | 15 | 16 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $-X+1$ | $-X-X^{2}$ | $1-X-X^{2}$ | $-1+X^{2}$ | $X^{2}$ | -1 |

Table: The elements of $\mathbb{Z} / 17 \mathbb{Z}$ in $\mathcal{B}=(p, n, \gamma, \rho)=(17,3,7,2)$

## Arithmetic operations

Main operations:

- Addition: a simple polynomial addition.

But, the infinity norm of the result can be greater than $\rho$.

- Multiplication: a simple polynomial multiplication. But, the infinity norm of the result can be greater than $\rho$ (1) and the degree of the result can be greater than $n-1$. (2)
- In case 1 , an iternal reduction must be done.
- In case 2 , an external reduction must be done.


## Arithmetic operation: the external reduction

Let $\mathcal{B}=(p, n, \gamma, \rho)$ be an AMNS and $A, B \in \mathcal{B}$.
Let $\mathbf{C}=\mathbf{A} . \mathbf{B}$ be a polynomial, then $\operatorname{deg}(C) \leqslant 2 n-2$.

- Goal: Compute a polynomial $R$ such that: $R(\gamma) \equiv C(\gamma)$ $(\bmod p)$ and $\operatorname{deg}(R)<n$.
- Let $E(X)$ be a polynomial, such that: $E(X)=X^{n}-\lambda$ and $\mathbf{E}(\gamma) \equiv \mathbf{0}(\bmod \mathbf{p})$, (i.e: $\gamma$ is a nth-root modulo $p$ of $\lambda$ ).

Then, there exists $Q$ and $R$ such that: $C=Q . E+R$, where $\operatorname{deg}(R)<n$ and $R(\gamma) \equiv C(\gamma)(\bmod p)$.

- $E(X)=X^{n}-\lambda$, with $\lambda$ "small" (i.e: $\pm 1,2,3,4, \ldots$ )
- External reduction: $R=C(\bmod E)$


## Arithmetic operation: the internal reduction

Depends on the generation process of the AMNS.

There are two main classes of AMNS:

- Optimal AMNS: internal reduction is done use vector-matrix multiplication. Matrix is chosen very sparse, but the generation process allows to choose only the size of the prime.
- General AMNS: internal reduction can be done in many ways. The generation process allows to choose the prime but the reduction is generally less efficient than that of the other class.


## The internal reduction: a Montgomery-like method

Let $\mathcal{B}=(p, n, \gamma, \rho, E)$, this method uses a polynomial $M$, such that: $M \in \mathcal{B}$ and $M(\gamma) \equiv 0(\bmod p)$.
Let $M^{\prime}=-M^{-1} \bmod (E, \phi)$, where $\phi \in \mathbb{N}^{*}$.

## Algorithm: RedCoeff

- 1: Input: a polynomial $V$, such that: $\operatorname{deg}(V) \leq n-1$
- 2: Ensure: $S(\gamma)=V(\gamma) \phi^{-1} \bmod p$
- 3: $Q \leftarrow V \times M^{\prime} \bmod (E, \phi)$
- 4: $R \leftarrow(V+Q \times M \bmod E)$
- 5: $S \leftarrow R / \phi$
- 6: return $S$


## Parameters set

The complete set of parameters for an AMNS is:

- $p$ : a prime integer.
- $n$ : the number of coefficients of elements in the AMNS.
- $\lambda$ : a "small" integer.
- $\gamma$ : a nth-root of $\lambda$ modulo $p$.
- $\rho$ : the upper-bound on the $\|.\|_{\infty}$ of the elements of $\mathcal{B}$.
- $E$ : the external reduction polynomial $\left(E(X)=X^{n}-\lambda\right)$.
- $\phi$ : the integer used in RedCoeff.
- $M$ : the internal reduction polynomial.
- $M^{\prime}$ : a polynomial such that $M^{\prime}=-M^{-1} \bmod (E, \phi)$.


## The internal reduction polynomial

The polynomial $M$ is such that:

- $M(\gamma) \equiv 0(\bmod p)$ and $\operatorname{deg}(M)<n$.
- $\rho \geqslant 2|\lambda| n\|M\|_{\infty}$ (i.e: $\|M\|_{\infty}$ is small)
- $M^{\prime}=-M^{-1} \bmod (E, \phi)$ exists.

Remarks:

- $M^{-1} \bmod (E, \phi)$ exists iff $\operatorname{gcd}(\operatorname{resultant}(\mathrm{E}, \mathrm{M}), \phi)=1$.
- We choose: $\phi=2^{k}$.

So, $M^{-1} \bmod (E, \phi)$ exists iff $\operatorname{resultant}(E, M)$ is odd.

## The internal reduction polynomial

If $E(X)=X^{n}-\lambda$ and $M(X)=m_{0}+\cdots+m_{n-1} X^{n-1}$, then resultant $(E, M)=\operatorname{det}\left(\mathcal{S}_{M, E}\right)$, where:

$$
\mathcal{S}_{M, E}=\left(\begin{array}{ccccccccc}
1 & 0 & \ldots & 0 & m_{n-1} & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & m_{n-2} & m_{n-1} & \ldots & 0 & 0 \\
\vdots & & \ddots & & \vdots & & & & \vdots \\
0 & 0 & \ldots & 1 & m_{1} & m_{2} & \ldots & m_{n-1} & 0 \\
0 & 0 & \ldots & 0 & m_{0} & m_{1} & \ldots & m_{n-2} & m_{n-1} \\
-\lambda & 0 & \ldots & 0 & 0 & m_{0} & \ldots & m_{n-3} & m_{n-2} \\
\vdots & & & & \vdots & & \ddots & & \vdots \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m_{0} & m_{1} \\
0 & 0 & \ldots & -\lambda & 0 & 0 & \ldots & 0 & m_{0}
\end{array}\right)
$$

Let $\mathcal{L}$ be a lattice such that:
$\mathcal{L}=\{v(X) \in \mathbb{Z}[X]$, such that: $\operatorname{deg}(v)<n$ and $v(\gamma) \equiv 0 \bmod (p)\}$.

## The internal reduction polynomial

(1) $M(\gamma) \equiv 0(\bmod p)$ and $\operatorname{deg}(M)<n$.
(2) $\|M\|_{\infty}$ is small.
(3) $M^{-1} \bmod (E, \phi)$ must exist.

- For (1) and (2), a small elements of $\mathcal{L}$ can be computed using a lattice reduction algorithm like LLL algorithm.
- For (3), Nadia EL MRABET and Nicolas GAMA show how construct a reduced base of $\mathcal{L}$ with at least one element $M$ for which $M^{-1}$ exists in the special case of $\lambda=-1$ (and $\phi=2^{k}$ ).


## The internal reduction polynomial

(1) $M(\gamma) \equiv 0(\bmod p)$ and $\operatorname{deg}(M)<n$.
(2) $\|M\|_{\infty}$ is small.
(3) $M^{-1} \bmod (E, \phi)$ must exist.

- For (1) and (2), a small elements of $\mathcal{L}$ can be computed using a lattice reduction algorithm like LLL algorithm.
- For (3), Nadia EL MRABET and Nicolas GAMA show how construct a reduced base of $\mathcal{L}$ with at least one element $M$ for which $M^{-1}$ exists in the special case of $\lambda=-1$ (and $\phi=2^{k}$ ).
- Our contribution here: For any nonzero integer $\lambda$,
- we proved that there exists at least one polynomial $M$ which satisfies points (1), (2) and (3).
- we described how to compute such $M$.


## The internal reduction polynomial: case $|\lambda|$ even

Let $\mathcal{L}=\{v(X) \in \mathbb{Z}[X]$, such that: $\operatorname{deg}(v)<n$ and $v(\gamma) \equiv 0 \bmod (p)\}$.

If $M(X)=m_{0}+\cdots+m_{n-1} X^{n-1}$ and $\phi=2^{k}$,
We proved that:

- $M^{-1} \bmod (E, \phi)$ exists iff $m_{0}$ is odd.
- Any reduced base of $\mathcal{L}$ contains at least one valid vector to be chosen as $M$.


## The internal reduction polynomial: case $|\lambda|$ odd

Let $\mathcal{L}=\{v(X) \in \mathbb{Z}[X]$, such that: $\operatorname{deg}(v)<n$ and $v(\gamma) \equiv 0 \bmod (p)\}$.

If $M(X)=m_{0}+\cdots+m_{n-1} X^{n-1}$ and $\phi=2^{k}$,

## We proved that:

$M^{-1} \bmod (E, \phi)$ exists iff $\operatorname{gcd}\left(\bar{M}, X^{n}-1\right)=1$
where $\bar{M}=\overline{m_{0}}+\cdots+\overline{m_{n-1}} X^{n-1}$ and $\overline{m_{i}}=m_{i}(\bmod 2)$.

## The internal reduction polynomial: case $|\lambda|$ odd

Let $\mathcal{M}_{2}$ be a base of the $\mathcal{L}$, such that:

$$
\mathcal{M}_{2}=\left(\begin{array}{cccccc}
p & 0 & 0 & \ldots & 0 & 0 \\
s_{1} & 1 & 0 & \ldots & 0 & 0 \\
s_{2} & 0 & 1 & \ldots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
s_{n-2} & 0 & 0 & \ldots & 1 & 0 \\
s_{n-1} & 0 & 0 & \ldots & 0 & 1
\end{array}\right)
$$

with: $s_{i}=t_{i}+k_{i} . p$, where $t_{i}=(-\gamma)^{i}(\bmod p), k_{i}=t_{i}(\bmod 2)$.

## We proved that:

For any reduced base $\mathcal{R}$ of $\mathcal{L}$ computed from $\mathcal{M}_{2}$, there exists at least one binary linear combination of the vectors of $\mathcal{R}$ which leads to a valid vector to be chosen as $M$.

## Implementation

- Computer spec: Intel Core i7-6700 (3.40GHz $\times 8$ ) , Ubuntu 16.04.4 LTS 64 bits, 32GB RAM.
- Implementation done using SageMath library.
- We wrote a C codes generator.
- We didn't use parallelization.


## About performance and memory consumption

- The smaller $n$ is, the better performances and memory consumption are.
- Let $k$ be the computer word size and $p$ a prime number. Then, the optimal value for $n$ is: $\left\lfloor\frac{\log _{2} p}{k}\right\rfloor+1$


## Number of AMNS and performances ratio

| $p$ size | 192 |  |  | 224 |  |  | 256 |  |  |
| :--- | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathbf{n}$ | $\mathbf{4}$ | $\mathbf{5}$ | $\mathbf{6}$ | $\mathbf{4}$ | $\mathbf{5}$ | $\mathbf{6}$ | $\mathbf{5}$ | $\mathbf{6}$ | $\mathbf{7}$ |
| ratio 1 | $\mathbf{0 . 8 6}$ | 1.41 | 2.04 | $\mathbf{0 . 5 7}$ | $\mathbf{0 . 9 8}$ | 1.41 | $\mathbf{0 . 9 8}$ | 1.42 | 1.84 |
| ratio 2 | 0.10 | 0.17 | 0.24 | 0.08 | 0.14 | 0.19 | 0.14 | 0.20 | 0.26 |
| ratio 3 | 0.21 | 0.34 | 0.49 | 0.16 | 0.27 | 0.39 | 0.30 | 0.43 | 0.55 |


| $p$ size | 384 |  |  | 521 |  |  |
| :--- | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathbf{n}$ | $\mathbf{7}$ | $\mathbf{8}$ | $\mathbf{9}$ | $\mathbf{1 0}$ | $\mathbf{1 1}$ | $\mathbf{1 2}$ |
| ratio 1 | $\mathbf{0 . 9 8}$ | 1.34 | 1.67 | $\mathbf{0 . 9 5}$ | 1.18 | 1.36 |
| ratio 2 | 0.19 | 0.25 | 0.31 | 0.25 | 0.29 | 0.34 |
| ratio 3 | 0.43 | 0.58 | 0.73 | 0.56 | 0.69 | 0.80 |

- ratio 1: AMNS / OpenSSL Montgomery modular mult. method
- ratio 2 : AMNS / OpenSSL default modular multiplication method
- ratio 3 : AMNS / GNU MP multiplication + modular reduction


## Conclusion

We have shown that:

- For any prime integer, it is possible to generate many AMNS.
- AMNS can be an interesting alternative to classical methods like Montgomery modular multiplication, for arithmetic operations.
- It is always possible to find an internal reduction polynomial for any nonzero $\lambda$. We explained how to compute it.

Some perspectives:

- Implement AMNS using its high parallelization capability.
- Make experiments with AMNS for protection against side channel attacks.


# Thank you for your attention. 

## Questions?

## The internal reduction polynomial

- $M^{-1} \bmod (E, \phi)$ exists iff $\operatorname{gcd}(\operatorname{resultant}(E, M), \phi)=1$.
- We choose: $\phi=2^{k}$.

So, $\operatorname{gcd}($ resultant $(E, M), \phi)=1$ iff resultant $(E, M)$ is odd.

- resultant $(E, M)=\operatorname{det}\left(\mathcal{S}_{M, E}\right)$, where:

$$
\mathcal{S}_{M, E}=\left(\begin{array}{ccccccccc}
1 & 0 & \cdots & 0 & m_{n-1} & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & m_{n-2} & m_{n-1} & \cdots & 0 & 0 \\
\vdots & & \ddots & & \vdots & & & & \vdots \\
0 & 0 & \cdots & 1 & m_{1} & m_{2} & \cdots & m_{n-1} & 0 \\
0 & 0 & \cdots & 0 & m_{0} & m_{1} & \cdots & m_{n-2} & m_{n-1} \\
-\lambda & 0 & \cdots & 0 & 0 & m_{0} & \cdots & m_{n-3} & m_{n-2} \\
\vdots & & & & \vdots & & \ddots & & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & m_{0} & m_{1} \\
0 & 0 & \cdots & -\lambda & 0 & 0 & \cdots & 0 & m_{0}
\end{array}\right)
$$

with: $E(X)=X^{n}-\lambda$ and $M(X)=m_{0}+\cdots+m_{n-1} X^{n-1}$.

## Existence of the internal red. poly.: case $|\lambda|$ even

If $|\lambda|$ is even, then resultant $(E, M)$ and the determinant of $\mathcal{H}$ have the same parity; with:

$$
\mathcal{H}=\left(\begin{array}{ccccccccc}
1 & 0 & \ldots & 0 & m_{n-1} & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & m_{n-2} & m_{n-1} & \ldots & 0 & 0 \\
\vdots & & \ddots & & \vdots & & & & \vdots \\
0 & 0 & \ldots & 1 & m_{1} & m_{2} & \ldots & m_{n-1} & 0 \\
0 & 0 & \ldots & 0 & m_{0} & m_{1} & \ldots & m_{n-2} & m_{n-1} \\
0 & 0 & \ldots & 0 & 0 & m_{0} & \ldots & m_{n-3} & m_{n-2} \\
\vdots & & & & \vdots & & \ddots & & \vdots \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m_{0} & m_{1} \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m_{0}
\end{array}\right)
$$

So, $M^{-1} \bmod (E, \phi)$ exists iff $m_{0}$ is odd.

## Computation of the internal red. poly.: case $|\lambda|$ even

Let $\mathcal{M}_{1}$ be a base of the $\mathcal{L}$, such that:

$$
\mathcal{M}_{1}=\left(\begin{array}{cccccc}
p & 0 & 0 & \ldots & 0 & 0 \\
t_{1} & 1 & 0 & \ldots & 0 & 0 \\
t_{2} & 0 & 1 & \ldots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
t_{n-2} & 0 & 0 & \ldots & 1 & 0 \\
t_{n-1} & 0 & 0 & \ldots & 0 & 1
\end{array}\right)
$$

with $t_{i}=(-\gamma)^{i}(\bmod p)$.
Any reduced base of $\mathcal{M}_{1}$ contains at least one valid vector to be chosen as $M$.

## The internal reduction polynomial: case $|\lambda|$ odd

If $|\lambda|$ is odd, then resultant $(\mathrm{E}, \mathrm{M})$ and the determinants of $\mathcal{H}_{1}$ and $\mathcal{H}_{2}$ have the same parity; with:
$\mathcal{H}_{1}=\left(\begin{array}{ccccccccc}1 & 0 & \cdots & 0 & \overline{m_{n-1}} & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & \overline{m_{n-2}} & \overline{m_{n-1}} & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & \overline{\overline{m_{1}}} & \overline{\overline{m_{2}}} & \cdots & \overline{m_{n-1}} & 0 \\ 0 & 0 & \cdots & 0 & \overline{m_{0}} & \frac{\overline{m_{1}}}{\overline{m_{0}}} & \cdots & \overline{m_{n-2}} & \overline{m_{n-1}} \\ -1 & 0 & \cdots & 0 & 0 & \overline{m_{n-3}} & \overline{m_{n-2}} \\ \vdots & & & & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \overline{m_{0}} & \overline{m_{1}} \\ 0 & 0 & \cdots & -1 & 0 & 0 & \cdots & 0 & \overline{m_{0}}\end{array}\right)$
$\mathcal{H}_{2}=\left(\begin{array}{ccccc}\overline{m_{0}} & \overline{m_{1}} & \ldots & \overline{m_{n-2}} & \overline{m_{n-1}} \\ \overline{m_{n-1}} & \overline{m_{0}} & \ldots & \overline{m_{n-3}} & \overline{m_{n-2}} \\ \vdots & & \ddots & & \vdots \\ \overline{m_{2}} & \overline{m_{3}} & \ldots & \overline{m_{0}} & \overline{m_{1}} \\ \overline{m_{1}} & \overline{m_{2}} & \ldots & \overline{m_{n-1}} & \overline{m_{0}}\end{array}\right)$ with: $\overline{m_{i}}=m_{i}(\bmod 2)$.
So, $M^{-1} \bmod (E, \phi)$ exists iff $\operatorname{gcd}\left(\bar{M}, X^{n}-1\right)=1$.

## Generation of the internal red. poly.: case $|\lambda|$ odd

## Proposition

Let $R_{n}=\mathbb{F}_{2}[X] /\left(X^{n}-1\right)$ be the algebra of all polynomials modulo $\left(X^{n}-1\right)$ over $\mathbb{F}_{2}$. Let $C_{n}$ be the ring of $n \times n$ binary circulant matrices.
Let $\Omega$ be the application defined as follows:

$$
\begin{aligned}
& \Omega \\
& \left.\begin{array}{cc}
R_{n} & \rightarrow \\
a_{0}+\cdots+a_{n-1} X^{n-1} & \mapsto
\end{array} \begin{array}{ccccc}
a_{0} & a_{1} & \ldots & a_{n-2} & a_{n-1} \\
a_{n-1} & a_{0} & \ldots & a_{n-3} & a_{n-2} \\
\vdots & & \ddots & & \vdots \\
a_{2} & a_{3} & \ldots & a_{0} & a_{1} \\
a_{1} & a_{2} & \ldots & a_{n-1} & a_{0}
\end{array}\right)
\end{aligned}
$$

Then, $R_{n}$ is isomorphic to $C_{n}$ and $\Omega\left(R_{n}\right)=C_{n}$.

## Computation of the internal red. poly.: case $|\lambda|$ odd

Let $\mathcal{M}_{2}$ be a base of the $\mathcal{L}$, such that:

$$
\mathcal{M}_{2}=\left(\begin{array}{cccccc}
p & 0 & 0 & \ldots & 0 & 0 \\
s_{1} & 1 & 0 & \ldots & 0 & 0 \\
s_{2} & 0 & 1 & \ldots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
s_{n-2} & 0 & 0 & \ldots & 1 & 0 \\
s_{n-1} & 0 & 0 & \ldots & 0 & 1
\end{array}\right)
$$

with: $s_{i}=t_{i}+k_{i} . p$, where $t_{i}=(-\gamma)^{i}(\bmod p)$ and $k_{i}=t_{i}$ $(\bmod 2)$.

For any reduced base $\mathcal{R}$ of $\mathcal{M}_{2}$, there exists at least one binary linear combination of the vectors of $\mathcal{R}$ which leads to a valid vector to be chosen as $M$.

The internal reduction: a Montgomery-like method

Let $\mathcal{B}=(p, n, \gamma, \rho, E)$.
Let $A, B \in \mathcal{B}$, and $C=\operatorname{Red} \operatorname{Coeff}(A \cdot B(\bmod E))$.
Then, $C \in \mathcal{B}$ if:

- $\rho \geqslant 2|\lambda| n\|M\|_{\infty}$
- $\phi \geqslant 2|\lambda| n \rho$


## Conversion from binary to AMNS : an algorithm

Let $\mathcal{B}=(p, n, \gamma, \rho, E, M, \phi)$ be an AMNS.
First precompute representatives $P_{i}(X)$ of $\rho$ powers in $\mathcal{B}$, i.e $P_{i} \equiv\left(\rho^{i}\right)_{\mathcal{B}}$, for $i=1, \ldots, n-1$.

The algorithm:
(1) Input: $a \in \mathbb{Z} / p \mathbb{Z}$
(2) Ensure: $A \equiv(a . \phi)_{\mathcal{B}}$
(3) $b=\left(a \cdot \phi^{2}\right) \bmod p$
(9) $b=\left(b_{n-1}, \ldots, b_{0}\right)_{\rho}$
(6) $U \leftarrow \sum_{i=0}^{n-1} b_{i} . P_{i}(X)$
(6) $A \leftarrow \operatorname{RedCoeff}(U)$
(C) return $A$

## Existence of AMNS

## Proposition

Let $E(X)=X^{n}-\lambda$, for $\lambda \in \mathbb{Z} \backslash\{0\}$. Let $g$ be a generator of $(\mathbb{Z} / p \mathbb{Z})^{\times}$and $y$ such that $g^{y} \equiv \lambda \bmod p$. If $\operatorname{gcd}(n, p-1) \mid y$, then there exists $\operatorname{gcd}(n, p-1)$ roots $\gamma$ of $E(X)$ in $\mathbb{Z} / p \mathbb{Z}$.

## Corollary 1

If $\operatorname{gcd}(n, p-1)=1$ then there exists a unique nth-root $\gamma$ of $\lambda$ in $\mathbb{Z} / p \mathbb{Z}$, for any $\lambda \in \mathbb{Z} \backslash\{1\}$.

Corollary 2
If $\operatorname{gcd}(n, p-1)>1$ then there exists at least one non-trivial nth-root $\gamma$ of 1 . So, one can take $\lambda=1$.

## Existence of $M$ proof

## Proposition

Let $\mathcal{G}=\left\{\mathcal{G}_{1}, \ldots, \mathcal{G}_{n}\right\}$ be a reduced basis of the lattice $\mathcal{L}$ obtained from the basis $\mathcal{M}_{2}$. Then, there exists a linear combination $\left(\beta_{1}, \ldots, \beta_{n}\right)$ with $\beta_{i} \in\{0,1\}$ such that $M=\sum_{i=1}^{n} \beta_{i} \mathcal{G}_{i}$ satisfies $\operatorname{gcd}\left(\bar{M}, X^{n}-1\right)=1$.

## Existence of $M$ proof

## Proof.

First, we have that:

$$
\overline{\mathcal{M}_{2}}=\left(\begin{array}{cccccc}
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & 1 & \ldots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
0 & 0 & 0 & \ldots & 1 & 0 \\
0 & 0 & 0 & \ldots & 0 & 1
\end{array}\right)
$$

where $\overline{\mathcal{M}}_{2 i j}=\mathcal{M}_{2 i j}(\bmod 2)$.
Each line $i$ of $\overline{\mathcal{M}_{2}}$ corresponds to the polynomial $X^{i} \in R_{n}$, for $0 \leqslant i<n$. This means that $\overline{\mathcal{M}_{2}}$ is a basis of $R_{n}$.

## Existence of $M$ proof

## Proof.

Let $U \in R_{n}$ be a polynomial such that $\operatorname{gcd}\left(U, X^{n}-1\right)=1$.
As $\overline{\mathcal{M}_{2}}$ is a basis of $R_{n}$, it exists $T=\left(t_{1}, \ldots, t_{n}\right) \in \mathbb{F}_{2}^{n}$ such that $U=T \cdot \overline{\mathcal{M}_{2}}$. As $T \cdot \overline{\mathcal{M}_{2}}=\overline{T . \mathcal{M}_{2}}$, we obtain that $U=\bar{T} \cdot \mathcal{M}_{2}$.
We have $T . \mathcal{M}_{2} \in \mathcal{L}$, so there exists $V=\left(v_{1}, \ldots, v_{n}\right) \in \mathbb{Z}^{n}$ such that $V . \mathcal{G}=T . \mathcal{M}_{2}$, as $\mathcal{G}$ is a basis of $\mathcal{L}$. Thus, $U=\overline{V \cdot \mathcal{G}}$.
Let $\beta=\left(\beta_{1}, \ldots, \beta_{n}\right) \in \mathbb{F}_{2}^{n}$ such that $\beta_{i}=v_{i}(\bmod 2)$, then we have $U=\overline{\beta . \mathcal{G}}$.
Let $M \in \mathcal{L}$ be a polynomial such that $M=\sum_{i=1}^{n} \beta_{i} \mathcal{G}_{i}$, then $\bar{M}=U$, hence $\operatorname{gcd}\left(\bar{M}, X^{n}-1\right)=1$.

## References

(1) Mrabet, N.E., Gama, N.: Efficient multiplication over extension fields. In: WAIFI. Lecture Notes in Computer Science, vol. 7369, pp. 136-151. Springer (2012)
(2) Nègre, C., Plantard, T.: Efficient modular arithmetic in adapted modular number system using lagrange representation. In: Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia. pp. 463-477 (2008)
(3) Plantard, T.: Arithmétique modulaire pour la cryptographie. Ph.D. thesis, Montpellier 2 University, France (2005)

