# Finite field multiplication combining AMNS and DFT approach for Pairing Based Cryptography

Nadia El Mrabet[(1)] and Christophe Negre[(2)]

(1) Team Arith/LIRMM, Université Montpellier 2

(2) Team DALI/ELIAUS, Université de Perpignan

Queensland University of Technology, July 2009


# Outline

# Outline

# What is a pairing ?

## Properties

Let $G_1$, $G_2$ and $G_3$ be three groups with the same order $r$. A pairing is a map :

$$e : G_1 \times G_2 \longrightarrow G_3$$

which verifies the following properties :

- *Non degenerate ;*
- *Bilinearity ;*

# What is a pairing ?

## Properties

Let $G_1$, $G_2$ and $G_3$ be three groups with the same order $r$. A pairing is a map :

$$e : G_1 \times G_2 \longrightarrow G_3$$

which verifies the following properties :

- *Non degenerate ;*
- *Bilinearity ;*

### Consequences

$$\forall j \in \mathbb{N}, e([j]P, Q) = e(P, Q)^j = e(P, [j]Q)$$

# Elliptic Curve Cryptography and pairings

## Cryptanalysis

Pairings was used to transporte the discrete logarithme problem from an elliptic curve sub group to a finite field.

## Cryptography

Pairings allow the construction of novel protocols and simplification of existing protocols.

- The tri partite Diffie Hellman key exchange protocol (Joux 2001)
- The Identity Based Encryption (Boneh and Franklin 2001)
- Short signature scheme (Boneh, Lynn, Schackamm 2001)
- Group signatures schemes (Boneh, Schackamm, 2004)

# Pairings used

In cryptography, four pairings are principally used :

- the Weil pairing,
- the Tate pairing,
- the $\eta$ pairing,
- the Ate pairing.

All of them involved computation over a finite field $\mathbb{F}_p$ and over $\mathbb{F}_{p^k}$ an extension of this finite field.

# Pairings over elliptic curves : Implementation aspect

The Ate pairing is computed trought the Miller's algorithm.

- The complexity of one step during the Miller's algorithm is : $2kM_p + 6S_{p^k} + 7M_{p^k}$ for the Ate pairing.

- To improve the efficiency of the pairing we can
  - reduce the number of multiplication and addition in $\mathbb{F}_{p^k}$.
  - improve multiplication and addition in $\mathbb{F}_{p^k}$.

# Pairings over elliptic curves : Implementation aspect

The Ate pairing is computed trought the Miller's algorithm.

- The complexity of one step during the Miller's algorithm is : $2kM_p + 6S_{p^k} + 7M_{p^k}$ for the Ate pairing.

- To improve the efficiency of the pairing we can
  - reduce the number of multiplication and addition in $\mathbb{F}_{p^k}$.
  - improve multiplication and addition in $\mathbb{F}_{p^k}$.

# Outline

# Finite fields used in pairings evaluation

- The field $\mathbb{F}_p$
  - is the set of integer modulo a prime $p \geq 2^{160}$ .
  - The curve with fixed embedding degree $k$ are constructed with the Complex Multiplication method.
  - Consequence, the prime $p$ cannot be chosen freely and do not have peculiar property.
  - The multiplication modulo $p$ is done with generic algorithm (Montgomery, Barett).
- The field $\mathbb{F}_{p^k}$
  - It is the set of polynomials $\mathbb{F}_p[X]$ modulo an irreducible polynomial $P$ of degree $k$.
  - $k$ is in the interval $[6, 32]$ such that $p^k \geq 2^{1024}$.
  - $P = X^k - \mu$ where $\mu$ is small and as much as possible a power of 2.

# Multiplication in $\mathbb{F}_{p^k}$ with Karatsuba

We want to compute $U(X) \times V(X) \mod (X^k - \mu)$ where $k = 2^s$

# Multiplication in $\mathbb{F}_{p^k}$ with Karatsuba

We want to compute $U(X) \times V(X) \mod (X^k - \mu)$ where $k = 2^s$

Multiplication. We first compute $W = U \times V$.

1. We split $U$ and $V$ into two parts

$$U = U_0 + X^{k/2} U_1, \quad V = V_0 + X^{k/2} V_1$$

2. We compute recursivelly

$$\begin{aligned} W_0 &= U_0 V_0, \\ W_2 &= U_1 V_1, \\ W_1 &= (U_0 + U_1)(V_0 + V_1) - W_0 - W_2. \end{aligned}$$

3. We deduce $W = W_0 + X^{k/2} W_1 + X^k W_2$ which is equal to $U \times V$.

# Multiplication in $\mathbb{F}_{p^k}$ with Karatsuba

Reduction. The reduction modulo $X^k - \mu$ of $W$ is done as follows

$$\left(\sum_{i=0}^{k-1} w_i X^i\right) + \mu \left(\sum_{i=k}^{2k-2} w_i X^{i-k}\right).$$

- Toom-Cook-3 approach works like Karatsuba but with decomposition in 3 parts.

# Pairing-Friendly Fields

## Definition

- $\mathbb{F}_{q^k}$ is a pairing friendly field if $p \equiv 1\ mod(12)$ & $k = 2^i.3^j$.

## Theorem

- $\mathbb{F}_{p^k}$ a pairing friendly field, $\beta$ neither a square or a cube in $\mathbb{F}_p$.
  Then $X^k - \beta$ irreducible over $\mathbb{F}_p$.

## Consequences

- $\mathbb{F}_{p^k}$ can be constructed as a tower of quadratic and cubic extensions.
  $\Rightarrow$ a perceptible reduction of the cost of a multiplication in $\mathbb{F}_{p^k}$.
- The cost of one multiplication is equal to $3^i 5^j$ multiplications in $\mathbb{F}_p$.

# Outline

# Adapted Modular Number System

- Classical representation

$$a = \sum_{i=0}^{n-1} a_i \beta^i \text{ with } a_i \in \{0, \ldots, \beta - 1\}.$$

Example :for $\beta = 8$ we have $a = 1315 = [2, 4, 4, 3]_8$ ,i.e., $a = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$.

# Adapted Modular Number System

- Classical representation

$$a = \sum_{i=0}^{n-1} a_i \beta^i \text{ with } a_i \in \{0, \ldots, \beta - 1\}.$$

Example :for $\beta = 8$ we have $a = 1315 = [2, 4, 4, 3]_8$ ,i.e., $a = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$.

- Representation in AMNS : let $0 < \gamma < p$ and $n > 0$

$$a = \sum_{i=0}^{n-1} a_i \gamma^i \mod p \text{ with } a_i < p^{1/n}.$$

and $\gamma$ satisfies $\gamma^n = \lambda \mod p$ with $\lambda$ small.

- We will note $\mathfrak{a}(t) = \sum_{i=0}^{n-1} a_i t^i$ in polynomial form the AMNS representation of $a$.

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| | | | | | |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| | | | | | |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| | | | | |

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 1 | | | | |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| | | | | | |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| | | | | $-1$ |

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 1 | | | | |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| $-1+\gamma$ | $\gamma$ | $1+\gamma$ | | | |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| | | | | $-1$ |

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 1 | | | | |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| $-1+\gamma$ | $\gamma$ | $1+\gamma$ | | | |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| | | $-1+\gamma^2$ | $\gamma^2$ | $-1$ |

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 1 | $-\gamma^2$ | $1-\gamma^2$ | | |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| $-1+\gamma$ | $\gamma$ | $1+\gamma$ | $-\gamma-1$ | $-\gamma$ | $-\gamma+1$ |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| | | $-1+\gamma^2$ | $\gamma^2$ | $-1$ |

# AMNS example

Let $p = 17$ and $n = 3$ and $\gamma = 7$.

$$\gamma^0 = 1 \mod p, \gamma^1 = 7 \mod p, \gamma^2 = 15 \mod p.$$

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 0 | 1 | $-\gamma^2$ | $1-\gamma^2$ | $-1+\gamma+\gamma^2$ | $\gamma+\gamma^2$ |

| 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|
| $-1+\gamma$ | $\gamma$ | $1+\gamma$ | $-\gamma-1$ | $-\gamma$ | $-\gamma+1$ |

| 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|
| $-\gamma-\gamma^2$ | $1-\gamma-\gamma^2$ | $-1+\gamma^2$ | $\gamma^2$ | $-1$ |

# Lattice related to an AMNS

- The set

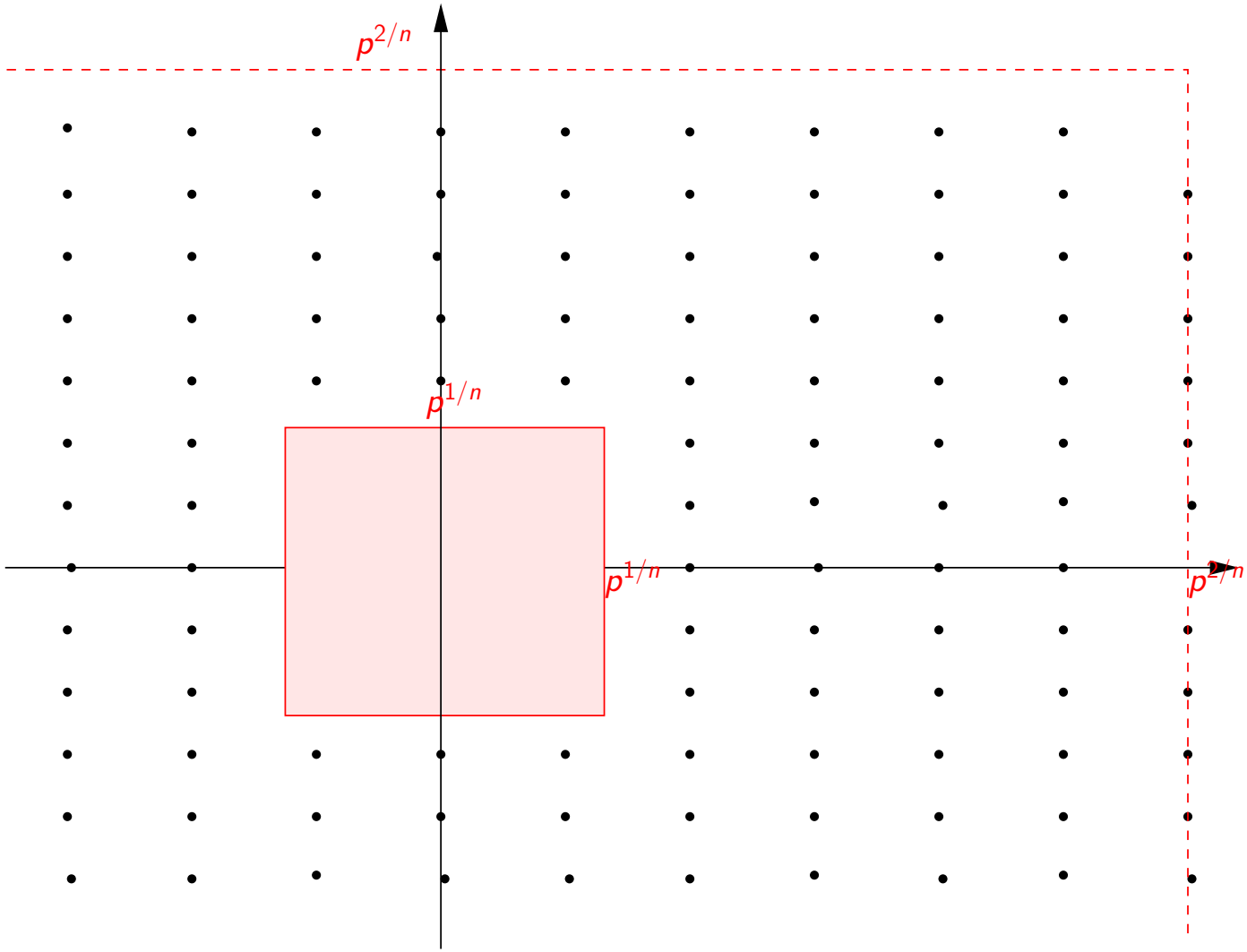
$$\mathcal{L} = \{\mathfrak{a}(t) \in \mathbb{Z}[t] \text{ t.q. } \deg \mathfrak{a}(t) < n \text{ et } \mathfrak{a}(\gamma) = 0 \mod p\}$$

  is a lattice of rank $n$.
- The row of the following matrix form a basis of a lattice

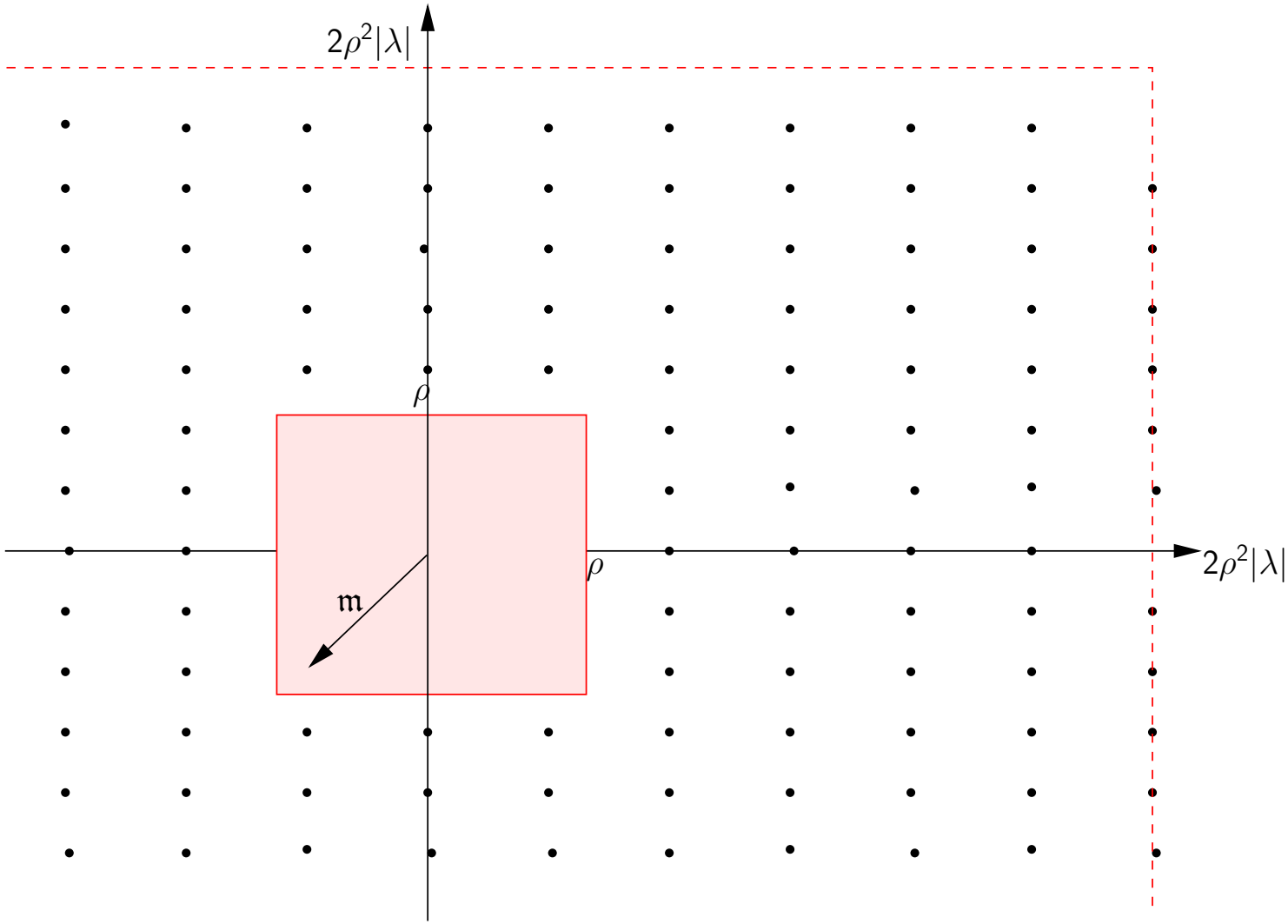
$$\mathcal{B} = \begin{pmatrix} p & 0 & 0 & 0 & \dots & 0 \\ -\gamma & 1 & 0 & 0 & \dots & 0 \\ -\gamma^2 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ -\gamma^{n-2} & 0 & 0 & \dots & 1 & 0 \\ -\gamma^{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow p \\ \leftarrow t - \gamma \\ \leftarrow t^2 - \gamma^2 \\ \vdots \\ \leftarrow t^{n-2} - \gamma^{n-2} \\ \leftarrow t^{n-1} - \gamma^{n-1} \end{matrix} .$$

- There exists a polynomial $\mathfrak{m}(t)$ such that $\mathfrak{m}(\gamma) = 0$ and $\|\mathfrak{m}\|_\infty \leq p^{1/n}$.

# Lattice related to an AMNS

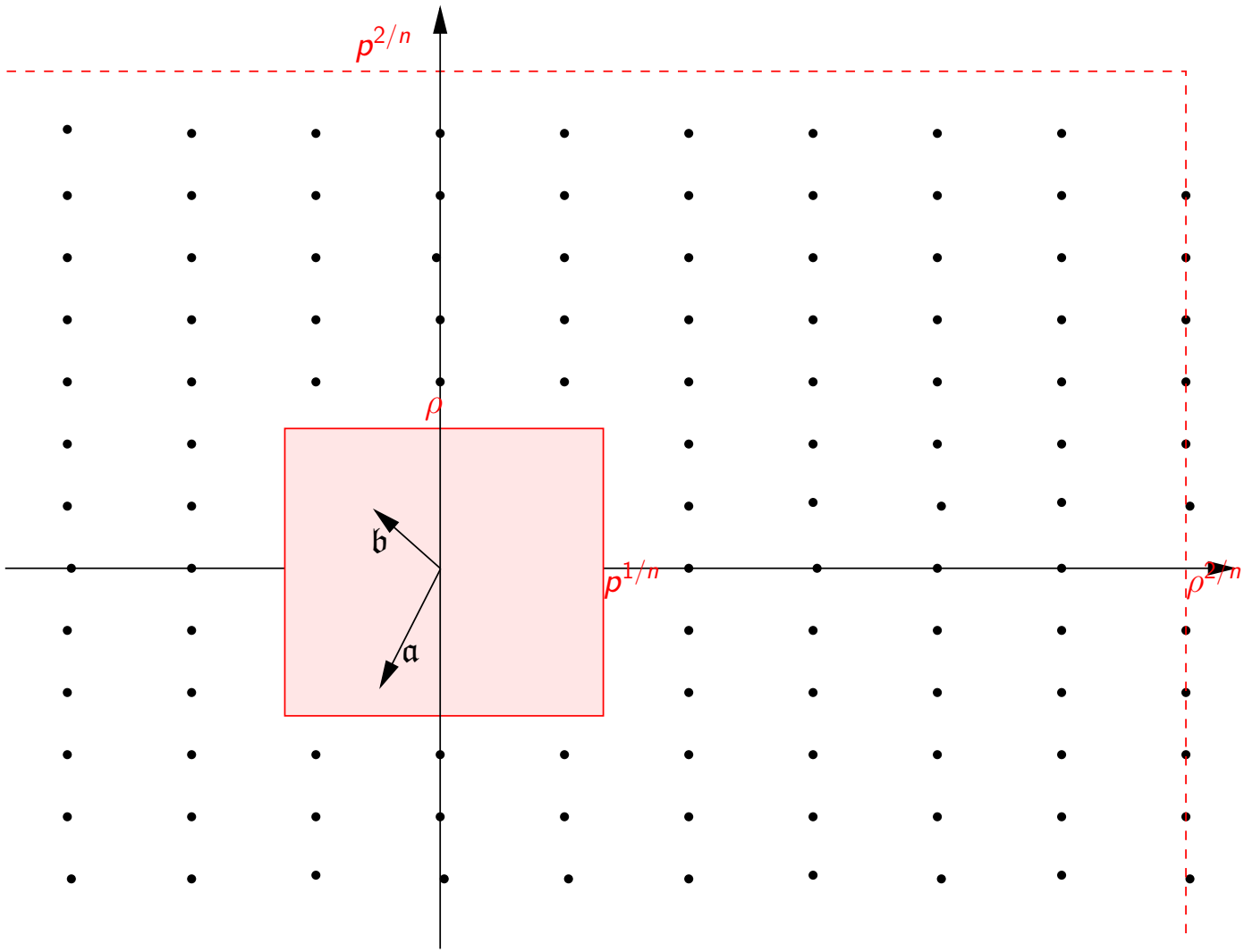


# Lattice related to an AMNS

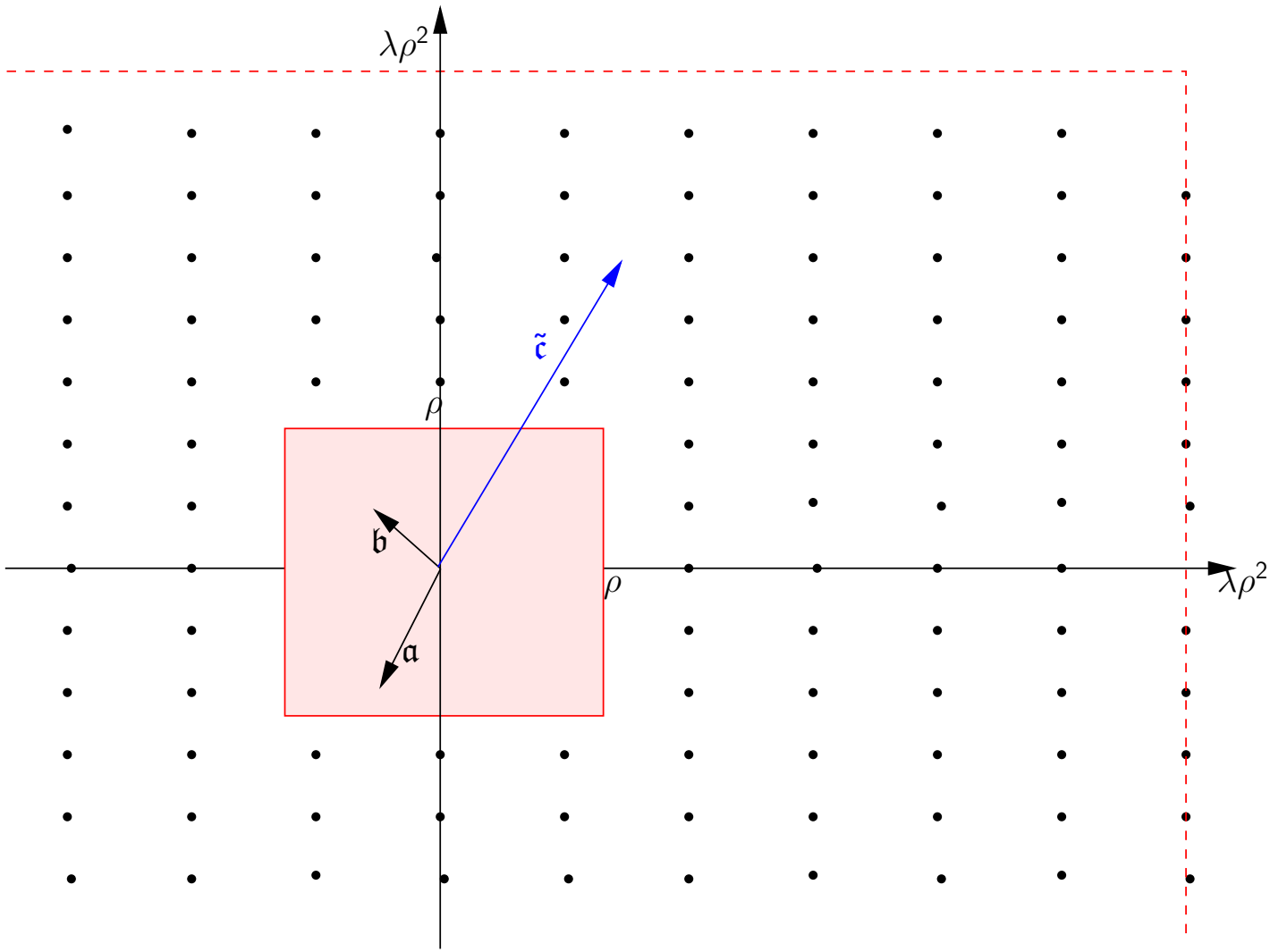



There exist $\mathfrak{m} \in \mathcal{L}$ such that $\|\mathfrak{m}\|_\infty \leq p^{1/n}$

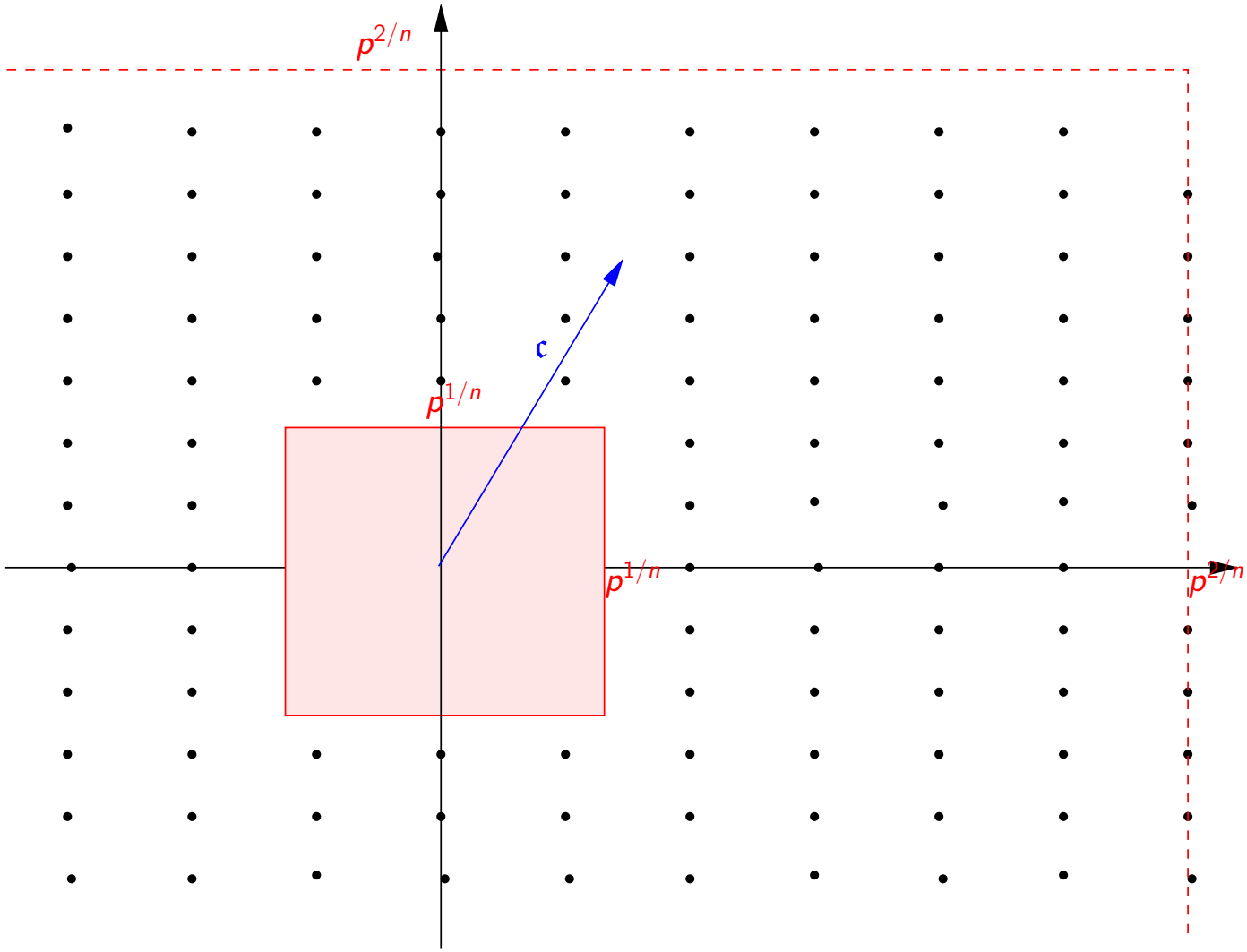
# Lattice related to an AMNS



# Lattice related to an AMNS

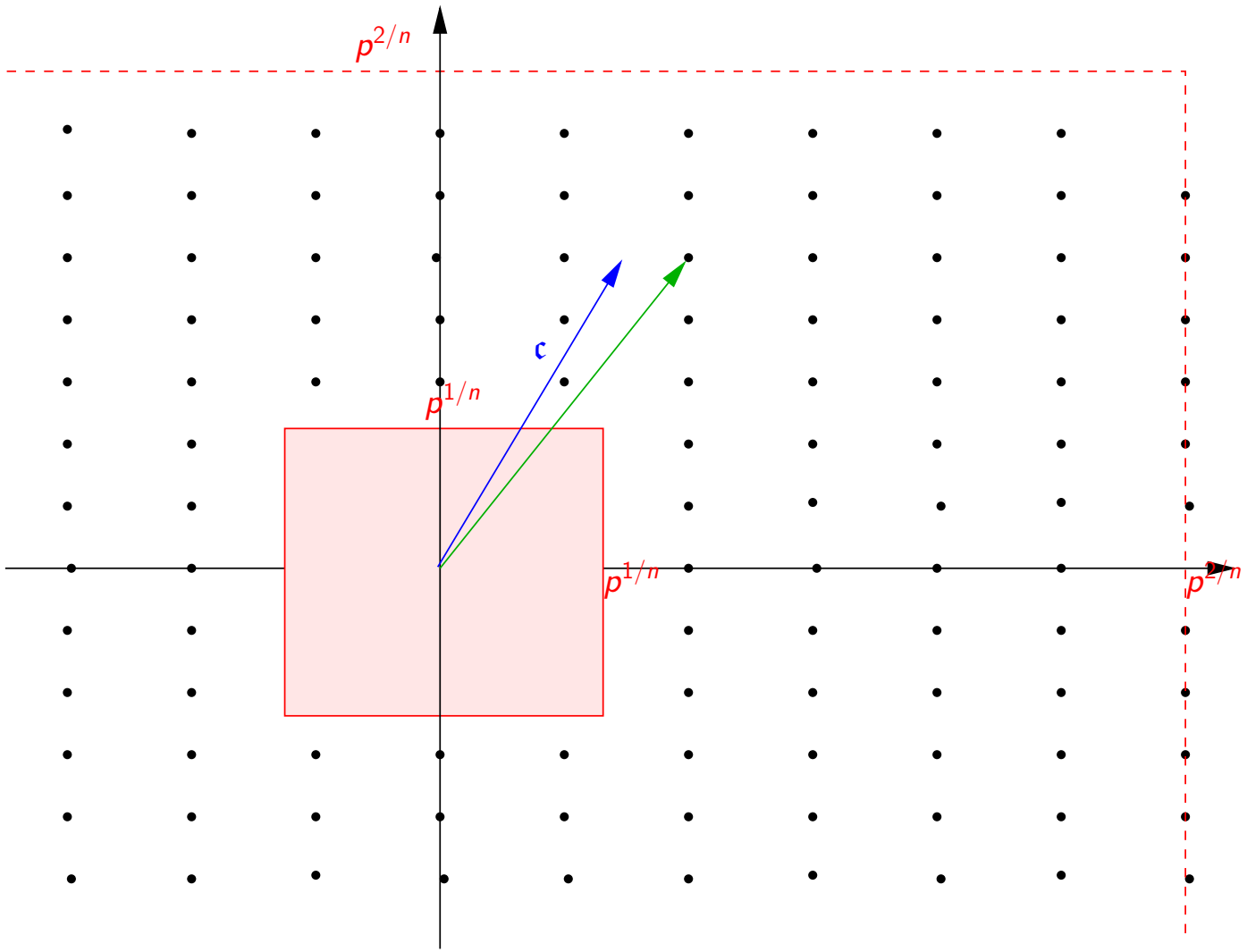


# Lattice related to an AMNS

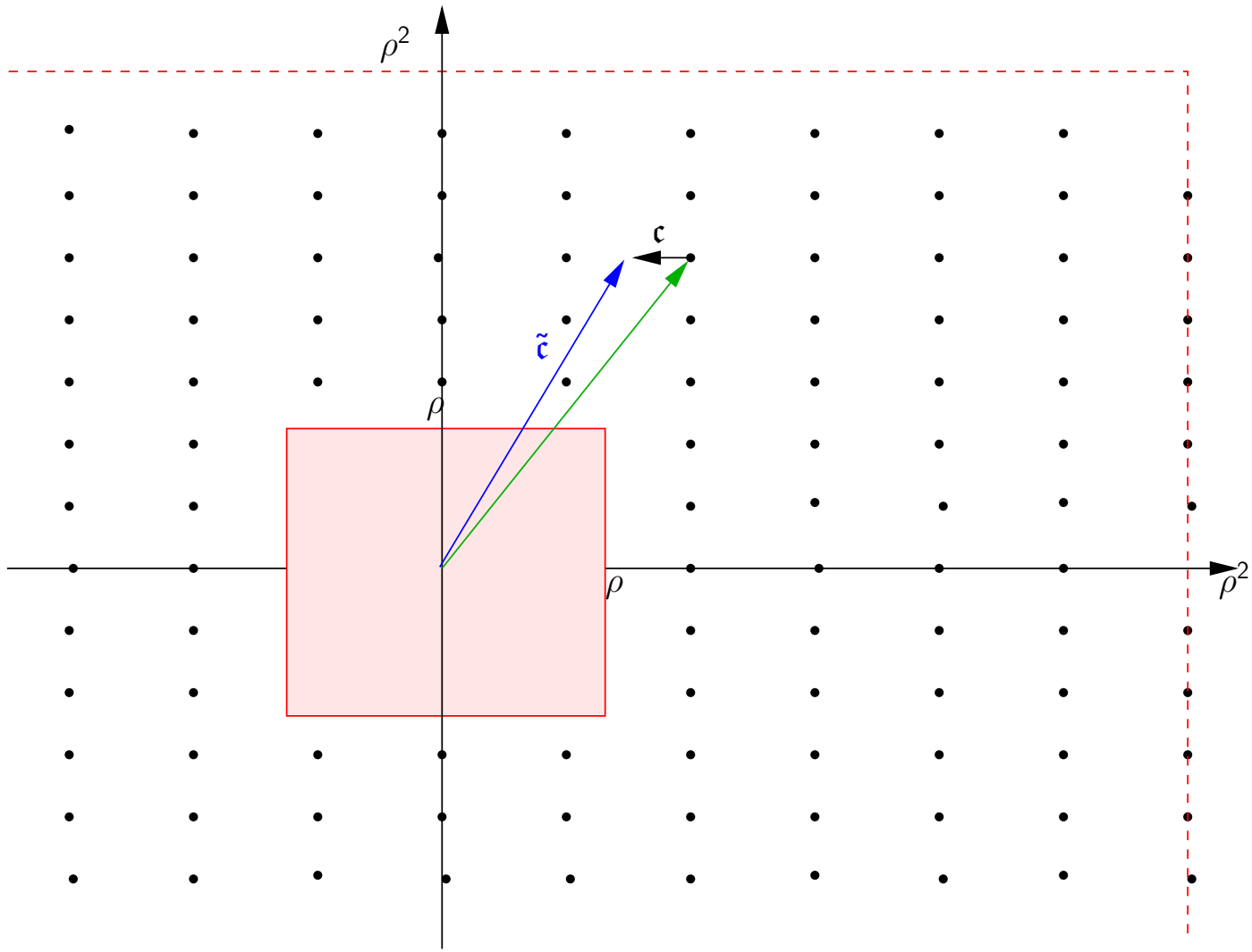



$\mathfrak{c} = \mathfrak{a} \times \mathfrak{b} \mod t^n - \lambda$ satisfies $\|\mathfrak{c}\|_\infty \leq np^{2/n}$

# Lattice related to an AMNS



# Lattice related to an AMNS




$\mathfrak{r}$ satisfait $\|\mathfrak{r}\|_\infty \leq np^{1/n}$ and represents $r = a \times b \mod p$

# Coefficients reduction with a Montgomery approach (Plantard-Negre 07)

- Idea : using a short polynomial $\mathfrak{m}(t)$ of the lattice to kill the lower part of the coefficients.
- Let $\ell$ such that $2^\ell \cong p^{1/n}$

1. $\mathfrak{q} \leftarrow a \times b \times \mathfrak{m}^{-1} \mod (t^n - \lambda, 2^\ell)$
2. $\mathfrak{r} \leftarrow ((a \times b - \mathfrak{q} \times \mathfrak{m} \mod t^n - \lambda)/2^\ell$

# Coefficients reduction with a Montgomery approach (Plantard-Negre 07)

- Idea : using a short polynomial $\mathfrak{m}(t)$ of the lattice to kill the lower part of the coefficients.
- Let $\ell$ such that $2^\ell \cong p^{1/n}$

1. $\mathfrak{q} \leftarrow a \times b \times \mathfrak{m}^{-1} \mod (t^n - \lambda, 2^\ell)$
2. $\mathfrak{r} \leftarrow ((a \times b - \mathfrak{q} \times \mathfrak{m} \mod t^n - \lambda)/2^\ell$

We have an algorithm similar to classical Montgomery algorithm, and with similar efficiency.
The arithmetic over $\mathbb{F}_p$ using an AMNS representation is efficient.

# Multiplication dans $\mathbb{F}_{p^k}$

Let $U(X), V(X) \in \mathbb{F}_p[X]$ with degree $k-1$, on compute the product of $U$ and $V$ as follows

1. Polynomial multiplication $W(X) = U(X) \times V(X)$, using multi-evaluation/interpolation approach.
2. The reduction modulo $X^n - \mu$ is easily done.

# Polynomial multiplication with multi-evaluation

We fix $n \geq 2k - 1$ distinct elements $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_p$.

# Polynomial multiplication with multi-evaluation

We fix $n \geq 2k-1$ distinct elements $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_p$.

1. *Multi-evaluations.* Let $U(X)$ and $V(X)$ with degree $k-1$. We compute

$$\begin{aligned} \hat{U} &= (U(\alpha_0), \ldots, U(\alpha_{n-1})) \\ \hat{V} &= (V(\alpha_0), \ldots, V(\alpha_{n-1})) \end{aligned}$$

which is done through a matrix-vector product

$$\hat{U} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{k-1} \\ \vdots & & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{k-1} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix}.$$

# Polynomial multiplication with multi-evaluation

We fix $n \geq 2k-1$ distinct elements $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_p$.

1. *Multi-evaluations.* Let $U(X)$ and $V(X)$ with degree $k-1$. We compute

$$\begin{aligned} \hat{U} &= (U(\alpha_0), \ldots, U(\alpha_{n-1})) \\ \hat{V} &= (V(\alpha_0), \ldots, V(\alpha_{n-1})) \end{aligned}$$

which is done through a matrix-vector product

$$\hat{U} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{k-1} \\ \vdots & & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{k-1} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix}.$$

2. *Term by term Multiplications.*

$$\hat{W} = (\hat{u}_0 \times \hat{v}_0, \hat{u}_1 \times \hat{v}_1, \ldots, \hat{u}_{n-1} \times \hat{v}_{n-1}).$$

# Polynomial multiplication with multi-evaluation

We fix $n \geq 2k-1$ distinct elements $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_p$.

1. *Multi-evaluations.* Let $U(X)$ and $V(X)$ with degree $k-1$. We compute
$$\begin{aligned} \hat{U} &= (U(\alpha_0), \ldots, U(\alpha_{n-1})) \\ \hat{V} &= (V(\alpha_0), \ldots, V(\alpha_{n-1})) \end{aligned}$$
which is done through a matrix-vector product
$$\hat{U} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{k-1} \\ \vdots & & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{k-1} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix}.$$

2. *Term by term Multiplications.*
$$\hat{W} = (\hat{u}_0 \times \hat{v}_0, \hat{u}_1 \times \hat{v}_1, \ldots, \hat{u}_{n-1} \times \hat{v}_{n-1}).$$

3. *Interpolation.* We get back to the polynomial form of $W$ with interpolation in $\alpha_i$.

# Using DFT

- We choose $\alpha$ a primitive $n$-th root of unity and $\alpha_i = \alpha^i$.

# Using DFT

- We choose $\alpha$ a primitive $n$-th root of unity and $\alpha_i = \alpha^i$.
- The multi-evaluation uses the matrix

$$\Omega = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(n-1)2} \\ \vdots & & & & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{bmatrix} \quad (1)$$

# Using DFT

- We choose $\alpha$ a primitive $n$-th root of unity and $\alpha_i = \alpha^i$.
- The multi-evaluation uses the matrix

$$\Omega = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(n-1)2} \\ \vdots & & & & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{bmatrix} \tag{1}$$

- The interpolation if $\alpha' = \alpha^{n-1}$, uses the matrix

$$\Omega^{-1} = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha' & \alpha'^2 & \cdots & \alpha'^{n-1} \\ 1 & \alpha'^2 & \alpha'^4 & \cdots & \alpha'^{(n-1)2} \\ \vdots & & & & \vdots \\ 1 & \alpha'^{n-1} & \alpha'^{2(n-1)} & \cdots & \alpha'^{(n-1)(n-1)} \end{bmatrix} \tag{2}$$

# Using DFT

- We choose $\alpha$ a primitive $n$-th root of unity and $\alpha_i = \alpha^i$.
- The multi-evaluation uses the matrix

$$\Omega = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(n-1)2} \\ \vdots & & & & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{bmatrix} \tag{1}$$

- The interpolation if $\alpha' = \alpha^{n-1}$, uses the matrix

$$\Omega^{-1} = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha' & \alpha'^2 & \cdots & \alpha'^{n-1} \\ 1 & \alpha'^2 & \alpha'^4 & \cdots & \alpha'^{(n-1)2} \\ \vdots & & & & \vdots \\ 1 & \alpha'^{n-1} & \alpha'^{2(n-1)} & \cdots & \alpha'^{(n-1)(n-1)} \end{bmatrix} \tag{2}$$

In other words, there are only multiplications by $\alpha^i$.

# Combination of AMNS and DFT

For the AMNS we choose

- $n = k$,
- $\gamma$ such that $\gamma^n = -1$,
- $\alpha = \gamma$ a primitive $2k$-th root of unity in $\mathbb{F}_p$.

Consequences

- The multiplication by $\gamma^i$ is a simple cyclic shift

$$\begin{aligned} a\gamma^j &= (\sum_{i=0}^{n-1} a_i t^i) t^j \mod t^n + 1 \\ &= (\sum_{i=0}^{j-1} -a_{n-j+i} t^i) + (\sum_{i=j}^{n-1} a_{i-j} t^i). \end{aligned}$$

- The multiplication by $\Omega$ and $\Omega^{-1}$ requires only additions in $\mathbb{F}_p$.

# Outline

# Complexity

- Cost of the approach of Karatsuba-Toom-Cook : for $k = 2^i 3^j$ this requires $3^i 5^j$ multiplications.
- Cost of the approach AMNS-DFT : it requires $2k$ multiplications.

TABLE: Complexity comparison for practical extension degree $k$

| Method | $k$ | Cost of $Mult_{F_{p^k}}$ | |
|---|---|---|---|
| | | # Add. in $\mathbb{F}_p$ | # Mult. in $\mathbb{F}_p$ |
| Karatsuba/Toom-Cook (Friendly Field) | 6 | 60 | 15 |
| Karatsuba/Toom-Cook (Friendly Field) | 8 | 72 | 27 |
| Our approach with FFT and $E = t^8 + 1$ | 8 | 192 | 16 |
| Karatsuba/Toom-Cook (Friendly Field) | 9 | 160 | 25 |
| Our approach with FFT and $E = t^8 + 1$ | 9 | 208 | 18 |
| Our approach with FFT and $E = t^8 + 1$ | 10 | 240 | 23 |
| Our approach with $E = \sum_{i=0}^{10}(-t)^i$ | 11 | 902 | 22 |
| Karatsuba/Toom-Cook (Friendly Field) | 12 | 180 | 45 |
| Our approach with $E = \sum_{i=0}^{10}(-t)^i$ | 12 | 1408 | 24 |
| Our approach with $E = \sum_{i=0}^{10}(-t)^i$ | 13 | 1430 | 28 |
| Karatsuba/Toom-Cook (Friendly Field) | 16 | 248 | 81 |
| Our approach with FFT and $E = t^{16} + 1$ | 16 | 480 | 32 |
| Our approach with FFT and $E = t^{16} + 1$ | 17 | 512 | 34 |
| Our approach with FFT and $E = t^{16} + 1$ | 18 | 576 | 39 |
| Karatsuba/Toom-Cook (Friendly Field) | 18 | 480 | 75 |

# Conclusion

- We have presented a method combining AMNS and DFT for multiplication in $\mathbb{F}_{p^k}$.
- The theoretical results show that our approach seems interisting.
- Implementation (work in progress), will take in account the small overcost due to AMNS and additions, it will show if it is interesting in practice.

Thank you for your attention.
Any question ?