

Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidien
Théorème

Arithmétique modulaire pour la cryptographie

Thomas Plantard

Projet ARITH LIRMM — Université Montpellier II — UMR 5506 106 rue Ada 34592 Montpellier — Cedex 5

web: http://www.lirmm.fr/~plantard/ email: plantard@lirmm.fr

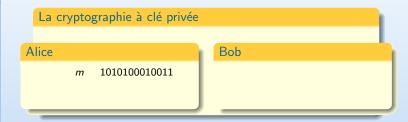
Le 15 décembre 2005



Le contexte cryptographique

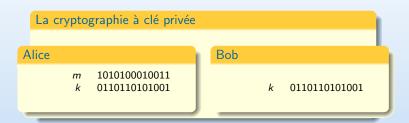
Arithmétique modulaire

Présentation





Présentation





Introduction Présentation

Contexte Multiplication Classes de modu

Pseudo Merse Généralisation Représentation

Modulaire Adapté

Nouvelle cla RED

Propriété
Construction

Cas général Réseaux Eu

Théorème

Conclusion

La cryptographie à clé privée

Alice

 $\begin{array}{ccc} m & 1010100010011 \\ k & 0110110101001 \\ c = m \otimes k & 1100010111010 \end{array}$

Bob

k 0110110101001

Thomas Plantard, LIRMM Le 15 décembre 2005 2/37



Présentation

La cryptographie à clé privée

Alice

 $c = m \otimes k$

1010100010011 m 0110110101001

1100010111010

Bob

1100010111010 0110110101001



Présentation

La cryptographie à clé privée

Alice

1010100010011 m 0110110101001 $c = m \otimes k$ 1100010111010

Bob

1100010111010 0110110101001 $m = c \otimes k$ 1010100010011

Introduction
Présentation
Contexte
Multiplication

Mersenne Pseudo Mers Généralisation Représentation

Représentation Modulaire Adapté

Nouvelle class RED Propriété

Construction
Cas général

Réseaux Euc Théorème La cryptographie à clé privée

Alice

 $\begin{array}{ccc} m & 1010100010011 \\ k & 0110110101001 \\ c = m \otimes k & 1100010111010 \end{array}$

Bob

c 1100010111010k 0110110101001 $m = c <math>\otimes$ k 1010100010011

La cryptographie à clé publique

Clé publique : g, p

Alice

Clé privée : a

- \bigcirc Alice calcule $g^a \mod p$
- Alice envoie à Bob g^a
- 3 Alice calcule $k = (g^b)^a \mod p$

Clé commune $k = g^{ab} \mod p$

Bob

Clé privée : b

- \bigcirc Bob calcule $g^b \mod p$
- ② Bob envoie à Alice g^b
- 3 Bob calcule $k = (g^a)^b \mod p$



Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire
Adapté
Vouvelle classe
RED
Propriété
Construction

Plan du mémoire

- Besoins arithmétiques en cryptographie
- état de l'art sur l'arithmétique modulaire
- Systèmes de représentation adaptés
- 4 Arithmétique modulaire pour de petits moduli

Arithmétique Modulaire pour la Cryptographie

Plan de l'exposé

Arithmétique modulaire

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté
Nouvelle class
RED
Propriété

Réseaux Euclidi Théorème

Introduction

- Présentation
- Contexte cryptographique
- La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
 - Conclusion



Arithmétique modulaire

Contexte

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits . . .



Arithmétique modulaire

Introduction

Contexte

Multiplication
Classes de moduli
Mersenne

Pseudo Mersenno Généralisation Représentation

Modulaire Adapté

RED Propriété
Construction

Cas général Réseaux Eucl Théorème

Théorème Conclusion

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, 2^{112} \Rightarrow 2048 bits . . .

RSA, Rivest, Shamir et Adleman (1978)

- Une exponentiation sur l'anneau $\mathbb{Z}/n\mathbb{Z}$
- Opération : Multiplication modulo n (composé)
- Sécurité : 2^{80} opérations $\Rightarrow 1024$ bits. $2^{112} \Rightarrow 2048$ bits . . .

Arithmétique modulaire

Contexte

L'échange de clé de Diffie Hellman (1970)

- Une exponentiation sur le corps $\mathbb{Z}/p\mathbb{Z}$
- Opération : Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits, $2^{112} \Rightarrow$ 2048 bits . . .

RSA, Rivest, Shamir et Adleman (1978)

- Une exponentiation sur l'anneau $\mathbb{Z}/n\mathbb{Z}$
- Opération : Multiplication modulo n (composé)
- Sécurité : 2^{80} opérations \Rightarrow 1024 bits. $2^{112} \Rightarrow$ 2048 bits ...

ECC, Koblitz et Miller (1985)

- Une exponentiation sur le groupe des points d'une courbe elliptique
- Opération : Inversion, Addition, Multiplication modulo p (premier)
- Sécurité : 2^{80} opérations \Rightarrow 160 bits, $2^{112} \Rightarrow 224$ bits ...

Multiplication

Multiplication Modulaire

- Entrée : a, b et p tel que $0 < a, b < p < 2^n$
- Sortie : r = ab + qp tel que $0 \le r, q < p$

Multiplications modulaires généralistes

- Taylor, 1981 : Mémorisation de la mise au carré modulaire.
- Blakley, 1983: "Double and Add" avec réduction à chaque étape.
- Montgomery, 1985 : Division par une puissance de la base.
- Barrett, 1986 : Approximation du quotient de la division.
- Takagi, 1992 : "Double and Add" en représentation redondante.

Moduli particuliers

- Trouver des moduli pour les tailles supérieures à 160 bits.
- Avec une réduction modulaire très efficace

État de l'art

Arithmétique modulaire

Présentation Contexte Multiplication

Classes de moduli

Mersenne
Pseudo Merser
Généralisation
Représentation
Modulaire
Adapté
Vouvelle classe
RED
Propriété

Construction
Cas général
Réseaux Euclid
Théorème
Conclusion

1 Introduction

- Présentation
- Contexte cryptographique
- La multiplication modulaire

2 Classes de moduli à réduction rapide

- Les nombres de Mersenne
- Les Pseudo nombres de Mersenne
- Les nombres de Mersenne Généralisés

3 Système de représentation

- Système de représentation modulaire
- Système de représentation adapté

4 Une nouvelle classe de moduli

- La réduction de coefficients
- Duamiitti
- Propriét
- Création de la classe de moduli

Cas général

- Les Réseaux Fuclidiens
- Théorème fondamental
- Conclusion

Les nombres de Mersenne

Mersenne, 1644

Arithmétique modulaire

Présentation
Contexte
Multiplication
Lasses de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire
Adapté
Jouvelle classe
RED
Propriété
Construction

Les nombres de Mersenne

• Nombre premier p de la forme $p = 2^n - 1$

Réduction

$$2^n \equiv 1 \pmod{p}$$

•
$$a = a_1 2^n + a_0$$

$$\bullet \ a \equiv a_1 + a_0 \pmod{p}$$

$$p = 31 = 2^5 - 1$$
, $a = 273$

$$^{\bullet} 2^5 \equiv 1 \pmod{31}$$

•
$$a = 8 \times 2^5 + 17$$

•
$$a \equiv 8 + 17 = 25 \pmod{31}$$

Coût = Deux Additions de n bits

Mersenne

Si $p = \beta^n - 1$ premier alors $\beta = 2$

•
$$\beta^n - 1 = (\beta - 1)(\beta^{n-1} + ... + 1)$$

• Si
$$\beta > 2$$
 alors $(\beta - 1) > 1$ divise p

n premier

- Si n pas premier alors n = uv avec u, v > 2
- $p = 2^n 1 = 2^{uv} 1 = (2^u)^v 1 = \beta^v 1$ alors p pas premier

Les nombres de Mersenne pour la cryptographie

- Impossible pour les tailles cryptographiques 160, 192, 224, ...
- n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607
- Le NIST et le SEC conseillent le nombre de Mersenne 2⁵²¹ 1

Les Pseudo nombres de Mersenne

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication

Contexte Multiplication Classes de modul

Pseudo Mersenne

Generalisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidien.
Théorème

Les Pseudo nombres de Mersenne

- Nombre premier p
- $p = 2^n c$ avec $c < 2^{\frac{n}{2}}$

Exemple

- n = 10
- o c = 3
- p = 1021

Réduction

- 2 $a \leftarrow a_1c + a_0$
- 3 $a = a_1 2^n + a_0$
- 4 $a \leftarrow a_1c + a_0$

Le coût

- 2 Multiplications de $\frac{n}{2}$ bits
- 4 Additions de $\frac{n}{2}$ bits

Les Pseudo nombres de Mersenne pour la cryptographie

Une bonne densité

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli

Pseudo Mersenne

Généralisation Représentation Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidier Théorème Conclusion

Les Pseudo nombres de Mersenne premiers

n	160	192	224	256	288	320
$ c _2$	6	8	6	8	8	8
	352	384	416	448	480	512
	10	9	9	8	6	10

Les Pseudo nombres de Mersenne pour ECC

①
$$\sec p_{160k1} = 2^{160} - (2^{32} + 2^{14} + 2^{12} + 2^9 + 2^8 + 2^7 + 2^3 + 2^2 + 1)$$

$$2 secp_{192k1} = 2^{192} - (2^{32} + 2^{12} + 2^8 + 2^7 + 2^6 + 2^3 + 1)$$

3
$$secp_{224k1} = 2^{224} - (2^{32} + 2^{12} + 2^{11} + 2^9 + 2^7 + 2^4 + 2 + 1)$$

Généralisation

Les nombres de Mersenne Généralisés

- Nombre p premier de la forme $p = P(2^k)$
- $P(X) = X^d C(X)$ avec $Deg(C) \le \frac{d}{2}$ et $C_i \in \{-1, 0, 1\}$

Un nombre de Mersenne Généralisé

•
$$P(X) = X^3 - X - 1$$

$$P(2^3) = 8^3 - 8 - 1 = 503$$

Coût

2d Additions de k bits

Généralisation

Les nombres de Mersenne Généralisés

- Nombre p premier de la forme $p = P(2^k)$
- $P(X) = X^d C(X)$ avec $Deg(C) \le \frac{d}{2}$ et $C_i \in \{-1, 0, 1\}$

Un nombre de Mersenne Généralisé

•
$$P(X) = X^3 - X - 1$$

$$P(2^3) = 8^3 - 8 - 1 = 503$$

Réduction

$$A = A_1 X^d + A_0$$

$$A \leftarrow A_1C + A_0$$

Coût

2d Additions de k bits

Les nombres de Mersenne Généralisés pour la cryptographie

Une densité quasi suffisante

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de modu
Mersenne

Pseudo Mersenne **Généralisation** Représentation Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidien Théorème Conclusion

Le nombre de nombres de Mersenne Généralisés avec k = 32

	n	160	192	224	256	288	320
#	MG	0	1	1	0	0	1
		352	384	416	448	480	512
		3	2	8	8	13	22

Les nombres de Mersenne Généralisés pour la cryptographie

Une densité quasi suffisante

Arithmétique modulaire

Généralisation

Le nombre de nombres de Mersenne Généralisés avec k = 32

n	160	192	224	256	288	320
#MG	0	1	1	0	0	1
	352	384	416	448	480	512
	3	2	8	8	13	22

Les nombres de Mersenne Généralisés pour ECC

①
$$sec_{192r1} P(X) = X^3 - (X+1)$$
 en 2^{64}

②
$$sec_{224r1} P(X) = X^7 - (X^3 + 1) \text{ en } 2^{32}$$

3
$$\sec_{256r1} P(X) = X^8 - (X^7 - X^6 - X^3 + 1)$$
 en 2^{32}

4
$$\sec_{384r1} P(X) = X^{12} - (X^4 + X^3 - X + 1)$$
 en 2^{32}



Système de représentation

Arithmétique modulaire

Représentation

- Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté

Laboratoire
d'informatique
de Robotique
et de Microffectronis
de Montpellier

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Représentation classique en base β

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

Exemple :
$$A = 1315 = [2, 4, 4, 3]_8$$
 $A = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Représentation classique en base β

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

Exemple : $A = 1315 = [2, 4, 4, 3]_8$ $A = 2 \times 8^3 + 4 \times 8^2 + 4 \times 8 + 3$

Représentation modulaire $\mathcal{B} = (p, n, \gamma, \rho)$

$$a = \sum_{i=0}^{n-1} a_i \gamma^i \mod p$$
 with $a_i \in \{0, \dots, \rho - 1\}$

Forme polynomiale

Le polynôme A[X] représente a dans $\mathcal{B} = (p, n, \gamma, \rho)$ si

$$\bullet \ A[\gamma] \equiv a \ (\bmod \ p)$$

•
$$Deg(A) \leq n$$

$$||A||_{\infty} < \rho$$

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème Conclusion

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $a = \sum_{i=0}^{2} a_i 7^i \mod 17$ with $a_i \in \{0, 1, 2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Modulaire

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $oldsymbol{o}$ $a=\sum_{i=0}^2 a_i 7^i mod 17$ with $a_i \in \{0,1,2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

ĺ	0	1	2	3	4	5
Ì	[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
ĺ	6	7	8	9	10	11
Î						
	12	13	14	15	16	
	•					

Présentation Contexte Multiplication Classes de moduli Mersenne Pseudo Mersenn

Modulaire

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $oldsymbol{o}$ $a=\sum_{i=0}^2 a_i 7^i mod 17$ with $a_i \in \{0,1,2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

0	1	2	2	1	E
U	1		3	4)
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
6	7	8	9	10	11
	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
12	13	14	15	16	

Présentation Contexte Multiplication Classes de moduli Mersenne Pseudo Mersenne

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- ullet $a=\sum_{i=0}^2 a_i 7^i \mod 17$ with $a_i \in \{0,1,2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

_						
	0	1	2	3	4	5
	[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			
Γ	6	7	8	9	10	11
		[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
Γ	12	13	14	15	16	
Г			[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- ullet $a = \sum_{i=0}^2 a_i 7^i \mod 17$ with $a_i \in \{0, 1, 2\}$
- $07^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

١.						
	0	1	2	3	4	5
	[0, 0, 0]	[0, 0, 1]	[0, 0, 2]			[1, 1, 0]
	6	7	8	9	10	11
	[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]		
	12	13	14	15	16	
	[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Représentat Modulaire

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $oldsymbol{o}$ $a=\sum_{i=0}^2 a_i 7^i mod 17$ with $a_i \in \{0,1,2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]	[2, 1, 1]	[2, 1, 2]	[1, 1, 0]
6	7	8	9	10	11
[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]	[2, 2, 0]	[2, 2, 1]
12	13	14	15	16	
[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne

Modulaire

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Exemple

- $(\gamma = 7, \rho = 3, n = 3, p = 17)$
- $oldsymbol{a} = \sum_{i=0}^2 a_i 7^i \mod 17$ with $a_i \in \{0,1,2\}$
- $7^0 = 1, 7^1 = 7, 7^2 \mod 17 = 15$

0	1	2	3	4	5
[0, 0, 0]	[0, 0, 1]	[0, 0, 2]	[2, 1, 1]	[2, 1, 2]	[1, 1, 0]
6	7	8	9	10	11
[1, 1, 1]	[0, 1, 0]	[0, 1, 1]	[0, 1, 2]	[2, 2, 0]	[2, 2, 1]
12	13	14	15	16	
[1, 2, 0]	[1, 2, 1]	[0, 2, 0]	[0, 2, 1]	[0, 2, 2]	

Question

- Si p, n et γ sont fixés, comment déterminer ρ_{min} ?
- Si p et n sont fixés, comment "bien" choisir γ ?

Présentation Contexte Multiplication Classes de moduli Mersenne Pseudo Mersenne

Modulaii Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème

Définition d'un système de représentation adapté

Un système de représentation modulaire $\mathcal{B}=(\gamma,\rho,\textit{n},\textit{p})$ sera dit adapté si

$$\gamma^n \mod p = c$$

avec c "petit".

Présentation Contexte Multiplication Classes de moduli Mersenne Pseudo Mersenne

Modulair Adapté

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Définition d'un système de représentation adapté

Un système de représentation modulaire $\mathcal{B}=(\gamma,\rho,\textit{n},\textit{p})$ sera dit adapté si

$$\gamma^n \mod p = c$$

avec c "petit".

Multiplication Modulaire dans ${\cal B}$

- **4** Multiplication polynomiale dans $\mathbb{Z}[X]$: U(X) ← A(X) B(X)
- ② Réduction polynomiale : $V(X) \leftarrow U(X) \mod (X^n c)$
- 3 Réduction des coefficients : $S \leftarrow CR(V)$, avec $S \equiv V(\gamma)$ (mod P)

ntroduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pequido Mersen

Modulai Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème

Un système de représentation adapté

•
$$p = 250043 \Rightarrow |p|_2 = 18$$

•
$$n = 3$$
, $\rho = 128$

$$\bullet$$
 $\gamma=127006$ tel que $c=2=\gamma^3 \bmod p$

Entrée

•
$$A = 7 + 30X + 100X^2 \Rightarrow A = 65842$$

•
$$B = 59 + 2X + 76X^2 \Rightarrow B = 8816$$

Exemple de système de représentation adapté

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de modu
Mersenne
Pseudo Mersen

Modulai Adapté

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Un système de représentation adapté

•
$$p = 250043 \Rightarrow |p|_2 = 18$$

•
$$n = 3$$
, $\rho = 128$

$$\bullet$$
 $\gamma=127006$ tel que $c=2=\gamma^3 \bmod p$

Entrée

•
$$A = 7 + 30X + 100X^2 \Rightarrow A = 65842$$

•
$$B = 59 + 2X + 76X^2 \Rightarrow B = 8816$$

Multiplication Modulaire dans ${\cal B}$

$$U(X) = A(X) \times B(X)$$

$$U(X) = 413 + 1784X + 6492X^{2} + 2480X^{3} + 7600X^{4}$$

②
$$V(X) = U(X) \mod (X^3 - 2) \leftarrow 5373 + 16984X + 6492X^2$$

$$S(X) = ?$$

Adanté

Un système de représentation adapté

•
$$p = 250043 \Rightarrow |p|_2 = 18$$

•
$$n = 3$$
, $\rho = 128$

$$\bullet$$
 $\gamma=127006$ tel que $c=2=\gamma^3 \bmod p$

Entrée

•
$$A = 7 + 30X + 100X^2 \Rightarrow A = 65842$$

•
$$B = 59 + 2X + 76X^2 \Rightarrow B = 8816$$

Multiplication Modulaire dans \mathcal{B}

$$U(X) = A(X) \times B(X)$$

$$U(X) = 413 + 1784X + 6492X^{2} + 2480X^{3} + 7600X^{4}$$

②
$$V(X) = U(X) \mod (X^3 - 2) \leftarrow 5373 + 16984X + 6492X^2$$

$$S(X) = ?$$

ntroduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersenr

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidien
Théorème

Entrée

Un vecteur V

Réduction des coefficients

② WHILE
$$\rho \geq s_i$$
 DO

$$0 \quad t \leftarrow |S|_2$$

$$S = S_1 2^{t-k_1} + S_0$$

$$3 S_1 \leftarrow RED(S_1)$$

$$S \leftarrow S_1 2^{t-k_1} + S_0$$

• Un vecteur
$$S \equiv V$$

• Avec
$$s_i < \rho = 2^k$$

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidie
Théorème

Entrée

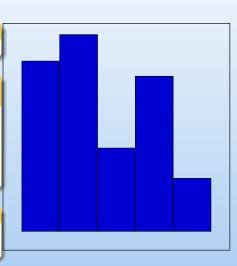
Un vecteur V

Réduction des coefficients

- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Modula Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidies
Théorème

Entrée

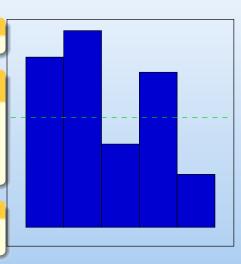
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidie
Théorème

Entrée

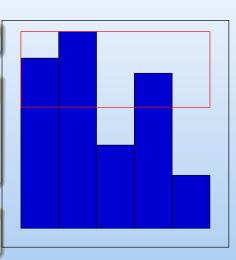
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidies
Théorème

Entrée

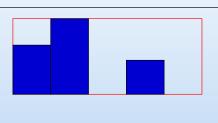
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidien
Théorème

Entrée

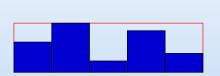
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Modula Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidier
Théorème

Entrée

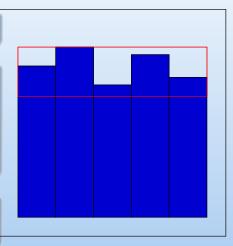
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- **2** WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $S_1 \leftarrow RED(S_1)$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidie Théorème

Entrée

Un vecteur V

Réduction des coefficients

② WHILE
$$\rho \geq s_i$$
 DO

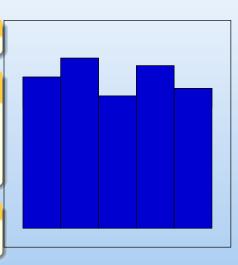
$$S = S_1 2^{t-k_1} + S_0$$

$$3 S_1 \leftarrow RED(S_1)$$

$$S \leftarrow S_1 2^{t-k_1} + S_0$$

• Un vecteur
$$S \equiv V$$

• Avec
$$s_i < \rho = 2^k$$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidien
Théorème

Entrée

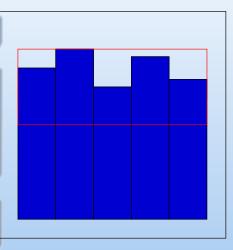
ullet Un vecteur V

Réduction des coefficients

- **2** WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$
 - $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersen

Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidie
Théorème

Entrée

Un vecteur V

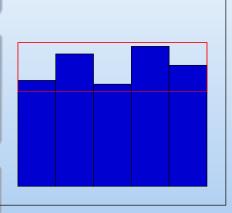
Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$

 - $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersenr

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidien
Théorème

Entrée

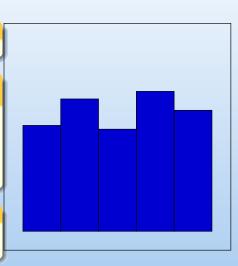
Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$
 - \bullet $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersen

Adapté

RED
Propriété
Construction
Cas général
Réseaux Euclidier
Théorème

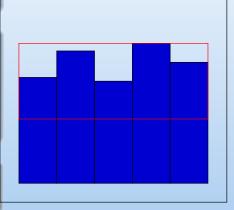
Entrée

Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO
 - $0 \quad t \leftarrow |S|_2$
 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$
 - $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne

Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidier
Théorème

Entrée

Un vecteur V

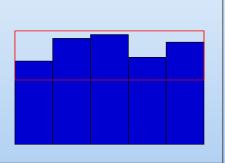
Réduction des coefficients

2 WHILE
$$\rho \geq s_i$$
 DO

$$S = S_1 2^{t-k_1} + S_0$$

• Un vecteur
$$S \equiv V$$

• Avec
$$s_i < \rho = 2^k$$



Introduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersen

Modula Adapté

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidies
Théorème

Entrée

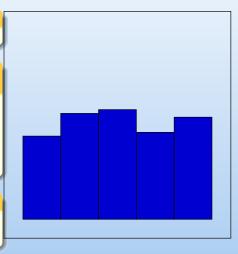
□ Un vecteur V

Réduction des coefficients

- ⑤ S ← V
- ② WHILE $\rho \geq s_i$ DO

 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$
 - $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$



Adapté

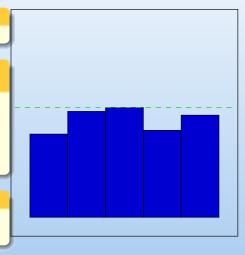
Entrée

Un vecteur V

Réduction des coefficients

- \bigcirc $S \leftarrow V$
- ② WHILE $\rho \geq s_i$ DO
 - $1 t \leftarrow |S|_2$
 - $S = S_1 2^{t-k_1} + S_0$
 - $3 S_1 \leftarrow RED(S_1)$
 - 4 $S \leftarrow S_1 2^{t-k_1} + S_0$

- Un vecteur $S \equiv V$
- Avec $s_i < \rho = 2^k$





Présentation Contexte Multiplication Classes de modul Mersenne Pseudo Merseni Généralisation

Adapté

Nouvelle classe RED Propriété Construction Cas général Réseaux Euclidiens Théorème

Problématique

- ullet Entrée : Un vecteur V avec $v_i < 2^{k_1}$
- Sortie : Un vecteur S avec $s_i < 2^{k_0}$ $(k_0 < k_1)$
- Avec $V \equiv S$ dans $\mathcal{B} : V(\gamma) \equiv S(\gamma) \pmod{p}$

Méthodes possibles

- Particulière : Classe de moduli avec une réduction efficace.
- Que Généraliste : Utilisation de table mémoire.

Une nouvelle classe de moduli

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation

Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidier

- 1 Introduction
 - Présentation
 - Contexte cryptographique
 - La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriété
 - Création de la classe de moduli
- Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
 - Conclusion

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adapté

RED Propriété Construction Cas général Réseaux Euclidien Théorème

Entrée

• Un vecteur V avec $v_i < 2^{k_1}$ et $k_1 = k + t$

Algorithme *RED*

$$S \leftarrow \overline{V}M + V$$
, où $M \equiv 2^k Id$ dans B

- Un vecteur $S \equiv V$ dans \mathcal{B}
- Avec $s_i < 2^{k_0}$ et $k_0 = k + 1$

Introduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersenr

Modulaire Adapté

Nouvelle clas

Propriété

Construction
Cas général
Réseaux Euclidiens
Théorème

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans $\mathcal B$ avec ξ_i "petit".
- $2^k \equiv \xi_{n-1} \gamma^{n-1} + \xi_{n-2} \gamma^{n-2} \cdots + \xi_1 \gamma + \xi_0 \pmod{p}$
- $^{\bullet} \gamma^n \equiv c \pmod{p}$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Generation

Adapté
Nouvelle cla

RED Propriét

Propriété

Cas général Réseaux Euclidien: Théorème

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1} \gamma^{n-1} + \xi_{n-2} \gamma^{n-2} \cdots + \xi_1 \gamma + \xi_0 \pmod{p}$
- $\bullet \gamma^n \equiv c \pmod{p}$

$$\begin{pmatrix} 2^{k} & 0 & \cdots & 0 & 0 \\ 0 & 2^{k} & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 2^{k} & 0 \\ 0 & 0 & \cdots & 0 & 2^{k} \end{pmatrix} \equiv \begin{pmatrix} & & & & \\ & & & & \\ & & & & \\ \end{pmatrix}$$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation

Nouvelle c

Propriété

Construction
Cas général
Réseaux Euclidien:
Théorème

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans $\mathcal B$ avec ξ_i "petit".
- $2^k \equiv \xi_{n-1} \gamma^{n-1} + \xi_{n-2} \gamma^{n-2} \cdots + \xi_1 \gamma + \xi_0 \pmod{p}$
- $\bullet \gamma^n \equiv c \pmod{p}$

$$\begin{pmatrix} & & & & & \\ & & & & & \\ 0 & 0 & \cdots & 0 & 2^k \end{pmatrix} \equiv \begin{pmatrix} & & & & & \\ & & & & & \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_1 & \xi_0 \end{pmatrix}$$
(1)

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation

RED Propriété

Construction
Cas général
Réseaux Euclidien

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans $\mathcal B$ avec ξ_i "petit".
- $2^k \equiv \xi_{n-1} \gamma^{n-1} + \xi_{n-2} \gamma^{n-2} \cdots + \xi_1 \gamma + \xi_0 \pmod{p}$
- $\bullet \gamma^n \equiv c \pmod{p}$

$$\begin{pmatrix} & & & & & & \\ & & & & & & \\ 0 & 0 & \cdots & 2^{k} & 0 \\ 0 & 0 & \cdots & 0 & 2^{k} \end{pmatrix} \equiv \begin{pmatrix} & & & & & \\ & & & & & \\ \xi_{n-2} & \xi_{n-3} & \cdots & \xi_{0} & \mathbf{c}\xi_{n-1} \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_{1} & \xi_{0} \end{pmatrix}$$
(1)

Propriété

Écriture de 2^k dans $\mathcal{B} = (p, n, \gamma, \rho)$

- Un vecteur ξ représentant 2^k dans \mathcal{B} avec ξ_i "petit".
- $2^k \equiv \xi_{n-1} \gamma^{n-1} + \xi_{n-2} \gamma^{n-2} \cdots + \xi_1 \gamma + \xi_0 \pmod{p}$
- $\bullet \gamma^n \equiv c \pmod{p}$

$$\begin{pmatrix} 2^{k} & 0 & \cdots & 0 & 0 \\ 0 & 2^{k} & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 2^{k} & 0 \\ 0 & 0 & \cdots & 0 & 2^{k} \end{pmatrix} \equiv \begin{pmatrix} \xi_{0} & \mathbf{c}\xi_{n-1} & \cdots & \mathbf{c}\xi_{2} & \mathbf{c}\xi_{1} \\ \xi_{1} & \xi_{0} & \cdots & \mathbf{c}\xi_{3} & \mathbf{c}\xi_{2} \\ \vdots & & & & \vdots \\ \xi_{n-2} & \xi_{n-3} & \cdots & \xi_{0} & \mathbf{c}\xi_{n-1} \\ \xi_{n-1} & \xi_{n-2} & \cdots & \xi_{1} & \xi_{0} \end{pmatrix}$$

$$(1)$$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Modulaire Adapté

RED

Propriété

Cas général Réseaux Euclidien Théorème

Entrée

•
$$\mathcal{B} = (p = 250043, n = 3, \gamma = 127006, \rho = 128)$$
 avec $\gamma^n \equiv 2$

$$\circ$$
 $\gamma^3 = 2 \mod p$ et $2^6 = 1 + \gamma^2 \mod p$

$$\begin{pmatrix} 2^6 & 0 & 0 \\ 0 & 2^6 & 0 \\ 0 & 0 & 2^6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \tag{2}$$

• Un vecteur V = [22, 444, 120] avec $V_i < 2^9$

RED

$$V = [0, 6, 1]2^6 + [22, 60, 56]$$

②
$$S \leftarrow [0,6,1]M + [22,60,56] = [12,8,1] + [22,60,56]$$

$$S = [57, 68, 34]$$
 avec $S_i < 2^{k+1} = 2^7 = 128$

Un exemple de Réduction de Coefficients

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersenr
Généralisation
Représentation
Modulaire

RED Propriété

Construc

Cas général Réseaux Euclidier Théorème

Entrée

•
$$\mathcal{B} = (\gamma = 127006, \rho = 128, n = 3, P = 250043)$$
 avec $\gamma^n \equiv 2$

$$V = [6492, 16984, 5373]$$

Étape

$$S = [2524, 984, 1853]$$

$$S = [532, 544, 357]$$

$$S = [32, 56, 121]$$

$$S = [32, 56, 121]$$
 avec $s_i < 128$

ntroduction Présentation Contexte Multiplication Classes de moduli Mersenne

Mersenne
Pseudo Mersen
Généralisation
Représentation
Modulire

Nouvelle class RED Propriété Construction

Construction
Cas général
Réseaux Euclidien
Théorème

Un système de représentation adapté : $\mathcal{B} = (p, n, \gamma, \rho)$

- Le modulo p
- 2 Le nombre de chiffres n
- \bigcirc La base γ
- ullet Le majorant des chiffres ho

Création d'un modulo p et du système $\mathcal B$ correspondant

- En fonction de la taille des chiffres (32, 64...), nous déduisons n.
- Nous voulons c = -2, -1, 2.
- Nous voulons $\|\xi\|_{\infty} = 1, 2$.
- Construire M avec ξ et c.
- Nous savons que $p|det(2^kId M)$
- Nous en déduisons p tel que p premier et $p \sim 2^{kn}$
- Calculer γ racine $gcd(X^n c, 2^k \xi(X)) \mod p$

Un exemple de système de représentation

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli

Mersenne
Pseudo Mersenne
Généralisation
Représentation

Adapté Nouvelle class RED Propriété

Construction
Cas général
Réseaux Euclidiens
Théorème

Exemple

- Taille des chiffres, 32 bits et taille du modulo, 256 bits $\Rightarrow n = 8$
- c = 2
- $\xi = [0, 0, 1, 0, 0, 0, 0, 1] (\xi(X) = X^5 + 1)$
- p = 115792089021636622262124715160334756877804245386980633020041035952359812890593 p est premier et $p \sim 2^{256}$
- γ racine $\gcd(X^8-2,2^{32}-X^5-1)\pmod{p}$ $\gamma=144740111277045777827655893952245323141792170589214$ 88395049827733759590399996

Un exemple de système de représentation

Arithmétique modulaire

Construction

Exemple

- Taille des chiffres. 32 bits et taille du modulo. 256 bits $\Rightarrow n = 8$
- \circ c=2
- $\xi = [0, 0, 1, 0, 0, 0, 0, 1] (\xi(X) = X^5 + 1)$
- p = 115792089021636622262124715160334756877804245386980633020041035952359812890593 p est premier et p $\sim 2^{256}$
- γ racine $gcd(X^8 2, 2^{32} X^5 1) \pmod{p}$ $\gamma = 144740111277045777827655893952245323141792170589214$ 88395049827733759590399996

Propriété de la classe

- Généralisation : elle contient les classes de la "famille des nombres de Mersenne"
- Bonne densité : elle contient de nouveau moduli.
- Grande efficacité : coût inférieur et parallélisation.

Construction

Proposition pour la cryptographie

Moduli				Coût en additions k bits			
\mathcal{B}	p	n	k	RedExt	RedInt	Total	Gain
\mathcal{B}_{128}	128	4	32	6	8	14	-26%
\mathcal{B}_{160}	160	5	32	8	10	18	-10%
\mathcal{B}_{192_a}	192	6	32	10	12+6	28	+17%
\mathcal{B}_{192_b}	192	6	32	10	12	22	-8%
\mathcal{B}_{224}	224	7	32	12	14	26	-11,5%
\mathcal{B}_{256}	256	8	32	14	16	30	-50%
\mathcal{B}_{288_a}	288	9	32	36	14	50	
\mathcal{B}_{288_b}	288	9	32	16	18	34	
\mathcal{B}_{320_a}	320	10	32	36	11	47	
\mathcal{B}_{320_b}	320	10	32	18	20	38	
\mathcal{B}_{352}	352	11	32	20	22	42	
\mathcal{B}_{384_a}	384	12	32	54	19	73	-13%
\mathcal{B}_{384_b}	384	12	32	22	24	46	_45%
\mathcal{B}_{384_c}	384	12	32	22	24	46	-45%
\mathcal{B}_{416}	416	13	32	24	26	50	
\mathcal{B}_{448_a}	448	14	32	26	28	54	
\mathcal{B}_{448_b}	448	14	32	26	28	54	
\mathcal{B}_{480_a}	480	15	32	28	30	58	
\mathcal{B}_{480_b}	480	15	32	56	16	78	
\mathcal{B}_{512}	512	16	32	30	32	62	

Cas général

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de modu
Mersenne
Pseudo Mersen
Généralisation

Nouvelle cla RED Propriété

Cas général Réseaux Euclidie

Théorème
Conclusion

1 Introduction

- Présentation
- Contexte cryptographique
- La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriét
 - Création de la classe de modul
- Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
 - Conclusion

Les Réseaux Euclidiens

Minkowski, 1896

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire
Adapté
Vouvelle classe

Propriété
Construction
Cas général
Réseaux Euclidiens
Théorème
Conclusion

Définition d'un réseau euclidien

• Un réseau $\mathcal L$ est l'ensemble des combinaisons linéaires entières de d vecteurs $\mathbf b_i$ indépendants de $\mathbb R^n$ avec $d \le n$:

$$\mathcal{L} = \mathbb{Z} \, \mathbf{b}_1 + \dots + \mathbb{Z} \, \mathbf{b}_d = \{ \lambda_1 \mathbf{b}_1 + \dots + \lambda_d \mathbf{b}_d : \lambda_i \in \mathbb{Z} \}$$

- d est la dimension.
- \bullet **B** = ($\mathbf{b}_1, \dots, \mathbf{b}_d$) est une *base*.

"SVP": Le problème du plus court vecteur

- NP-Dur
- Approximation de SVP par LLL (Lenstra, Lenstra, Lovasz), 1982

"CVP": Le problème du plus proche vecteur

- NP-Dur
- Approximation de CVP par Babai, 1986

Laboratoire d'informatique de Robotique et de Microfloctron de Montpellier

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire

RED Propriété Construction Cas général

Réseaux Euclidiens Théorème Un réseau ${\cal L}$

Exemple

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire

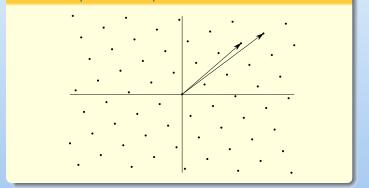
Représentation Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général

Cas général Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 29 & 31\\ 21 & 26 \end{pmatrix} \tag{3}$$

"SVP": Le problème du plus court vecteur



LIRMM

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation

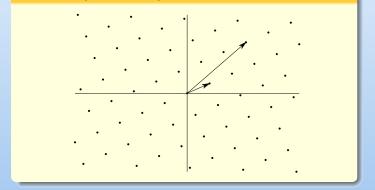
Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général

Cas général Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5\\ 21 & 26 \end{pmatrix} \tag{4}$$

"SVP": Le problème du plus court vecteur



Exemple

Arithmétique modulaire

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation

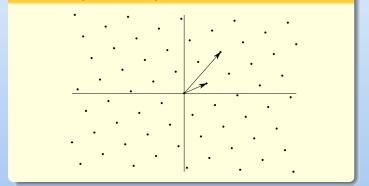
Modulaire
Adapté
Nouvelle classe
RED
Propriété
Construction

Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5\\ 13 & 21 \end{pmatrix} \tag{5}$$

"SVP": Le problème du plus court vecteur



Exemple

Arithmétique modulaire

LIRMM

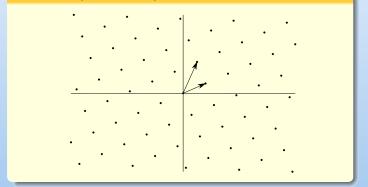
ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn Généralisation

Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général

Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{6}$$



ntroduction Présentation Contexte Multiplication Classes de modul Mersenne Pseudo Merseni

Modulaire Adapté Nouvelle class RED Propriété

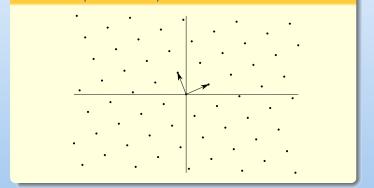
Propriété
Construction
Cas général
Réseaux Euclidie

Réseaux Euclidiens Théorème Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

"SVP": Le problème du plus court vecteur



ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Mersenne
Pseudo Mersenderalisation
Représentation
Modulaire
Adapté
Nouvelle class
RED
Propriété
Construction

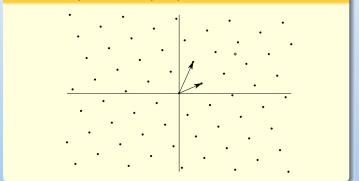
Cas général
Réseaux Euclidiens
Théorème

Un réseau $\mathcal L$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

Le plus proche vecteur : $(20,20) \equiv (20,20) \pmod{\mathcal{L}}$



ntroduction Présentation Contexte Multiplication Classes de modul Mersenne Pseudo Mersenr

Mersenne
Pseudo Mers
Généralisatio
Représentation
Modulaire
Adapté
Nouvelle class
RED
Propriété
Construction

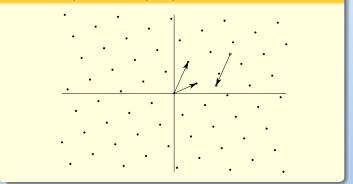
Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

Le plus proche vecteur : $(20,20) \equiv (15,4) \pmod{\mathcal{L}}$



ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Représentation
Modulaire
Adapté
Nouvelle class
RED
Propriété
Construction

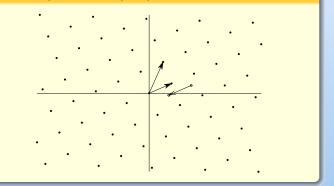
Cas général Réseaux Euclidiens Théorème

Un réseau $\mathcal L$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

Le plus proche vecteur : $(20,20) \equiv (7,-1) \pmod{\mathcal{L}}$



ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Généralisation Représentation Modulaire Adapté Nouvelle class RED Propriété Construction

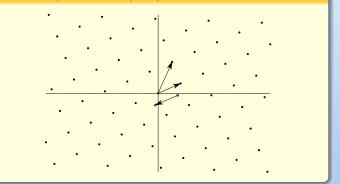
Cas général Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

Le plus proche vecteur : $(20,20) \equiv (-1,6) \pmod{\mathcal{L}}$



ntroduction
Présentation
Contexte
Multiplication
Classes de modul
Mersenne
Pseudo Mersen Généralisation

Modulaire Adapté Nouvelle cla

RED Propriété
Construction

Construction
Cas général
Réseaux Fucl

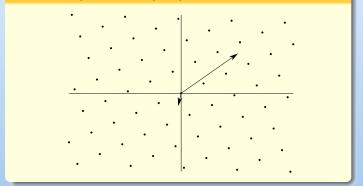
Réseaux Euclidiens Théorème

Un réseau ${\cal L}$

$$\mathcal{B} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \tag{7}$$

Le plus court vecteur : (8,5).

Le plus proche vecteur : $(20,20) \equiv (-1,6) \pmod{\mathcal{L}}$



Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Modulaire
Adapté
Nouvelle classe

Nouvelle class RED Propriété Construction

Réseaux Eucli

Redéfinition de la réduction des coefficients

- ullet Entrée : Un vecteur V de \mathbb{Z}^n
- Sortie : Un vecteur S de \mathbb{Z}^n plus "court" pour la norme $\|.\|_{\infty}$
- Avec $V \equiv S \mod \mathcal{L}$ où \mathcal{L} est l'ensemble des vecteurs représentant 0 (Si $V(\gamma) \equiv 0 \mod p$ alors $V \in \mathcal{L}$)
- Approximation CVP_{∞} sur des réseaux totaux.

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED

Théorème

Redéfinition de la réduction des coefficients

- ullet Entrée : Un vecteur V de \mathbb{Z}^n
- ullet Sortie : Un vecteur S de \mathbb{Z}^n plus "court" pour la norme $\|.\|_{\infty}$
- Avec $V \equiv S \mod \mathcal{L}$ où \mathcal{L} est l'ensemble des vecteurs représentant 0 (Si $V(\gamma) \equiv 0 \mod p$ alors $V \in \mathcal{L}$)
- Approximation CVP_{∞} sur des réseaux totaux.

Théorème

• Si $X^n - c$ irréductible dans \mathbb{Z} alors

$$\rho_{min} \leq |c| p^{\frac{1}{n}}$$

• $\mathcal{B} = (p, n, c^{1/n}, |c|p^{\frac{1}{n}})$ est un système de représentation modulaire.

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Genéralisation
Représentation
Modulaire
Adanté

Adapté
Nouvelle classe
RED
Propriété
Construction

Le réseau
$$\mathcal{L}$$

$$\mathbf{B} = \left(\begin{array}{c} \\ \\ \end{array} \right) \tag{8}$$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Genéralisation
Représentation
Modulaire
Adanté

Adapté
Nouvelle classe
RED
Propriété
Construction

Le réseau
$$\mathcal{L}$$

$$\mathbf{B} = \left(\begin{array}{c} \\ \\ \end{array} \right) \tag{8}$$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Adanté

Nouvelle class
RED
Propriété
Construction

Le réseau
$$\mathcal{L}$$

$$B = \begin{pmatrix} & & & \\ & & & \\ 0 & 0 & \cdots & 0 & p \end{pmatrix}$$
 (8)

ntroduction Présentation Contexte Multiplication Classes de moduli Mersenne Pseudo Mersenne Généralisation Représentation Modulaire

Nouvelle classe RED Propriété Construction

Le réseau
$$\mathcal{L}$$

$$\mathbf{B} = \begin{pmatrix} & & & & \\ & & & & \\ 0 & 0 & \cdots & 1 & -\gamma \\ 0 & 0 & \cdots & 0 & p \end{pmatrix}$$
 (8)

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation

Représentat Modulaire Adapté

Nouvelle class RED Propriété Construction

Réseaux Euc

Théorème

Le réseau
$$\mathcal{L}$$

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -\gamma^{n-1} \\ 0 & 1 & \cdots & 0 & -\gamma^{n-2} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & -\gamma \\ 0 & 0 & \cdots & 0 & p \end{pmatrix}$$
(8)

Théorème

Le réseau \mathcal{L}

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -\gamma^{n-1} \\ 0 & 1 & \cdots & 0 & -\gamma^{n-2} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & -\gamma \\ 0 & 0 & \cdots & 0 & p \end{pmatrix}$$
(8)

Analyse du réseau \mathcal{L}

- Le déterminant $Det(\mathcal{L}) = p$ et la dimension d = n
- Théorème de Minkowski $\Rightarrow \exists \mathbf{m} \in \mathcal{L}$ tel que $\|\mathbf{m}\|_{\infty} \leq p^{1/n}$
- $||(m_{n-1}, m_{n-2}, \ldots, m_1, m_0)||_{\infty} \le p^{1/n}$

Théorème

Le réseau
$$\mathcal{L}'$$

$$\mathbf{B}' = \left(\begin{array}{c} \\ \\ \end{array} \right) \tag{9}$$

Théorème

Le réseau
$$\mathcal{L}'$$

$$B' = \begin{pmatrix} & & & & \\ & & & & \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix} \tag{9}$$

ntroduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Généralisation
Représentation
Modulaire
Admité

Modulaire Adapté Nouvelle classe RED Propriété Construction Cas général

Le réseau
$$\mathcal{L}'$$

$$B' = \begin{pmatrix} & & & & & & & & & & & & & & & & & \\ & & & & & & & & & & & & & & \\ & & & & & & & & & & & & & \\ & & & & & & & & & & & & & \\ m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} & & & & & & \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 & cm_{n-1} & & & & & \\ & & & & & & & & & & & & \\ \end{array}$$
(9)

Théorème

Le réseau
$$\mathcal{L}'$$

$$B' = \begin{pmatrix} m_0 & cm_{n-1} & \cdots & cm_2 & cm_1 \\ m_1 & m_0 & \cdots & cm_3 & cm_2 \\ \vdots & & & \vdots \\ m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix}$$
(9)

Théorème

Le réseau \mathcal{L}'

$$\mathbf{B'} = \begin{pmatrix} m_0 & cm_{n-1} & \cdots & cm_2 & cm_1 \\ m_1 & m_0 & \cdots & cm_3 & cm_2 \\ \vdots & & & \vdots \\ m_{n-2} & m_{n-3} & \cdots & m_0 & cm_{n-1} \\ m_{n-1} & m_{n-2} & \cdots & m_1 & m_0 \end{pmatrix}$$
(9)

Analyse du réseau \mathcal{L}'

- ${}_{\bullet} \ \mathcal{L}' \subseteq \mathcal{L}$
- $\|\mathbf{B'}_i\|_{\infty} \leq |c|p^{\frac{1}{n}}$
- Si B' est une base alors $\forall v, \exists u, v \equiv u \pmod{\mathcal{L}}$

Conclusion

Arithmétique modulaire

Introduction
Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire

Adapté
Nouvelle classe
RED
Propriété
Construction
Cas général
Réseaux Euclidie

Conclusion

1 Introduction

- Présentation
- Contexte cryptographique
- La multiplication modulaire
- 2 Classes de moduli à réduction rapide
 - Les nombres de Mersenne
 - Les Pseudo nombres de Mersenne
 - Les nombres de Mersenne Généralisés
- 3 Système de représentation
 - Système de représentation modulaire
 - Système de représentation adapté
- 4 Une nouvelle classe de moduli
 - La réduction de coefficients
 - Propriét
 - Création de la classe de modul
- Cas général
 - Les Réseaux Euclidiens
 - Théorème fondamental
- 6 Conclusion

ntroduction
Présentation
Contexte
Multiplication
Mersenne
Pseudo Mersenn
Généralisation
Représentation
Modulaire
Adapté
Nouvelle classe
RED
Propriété

Conclusion

Système de représentation modulaire

- Une nouvelle représentation adaptée au modulaire
- Une nouvelle classe de moduli efficace pour ECC
- Des algorithmes généralistes pour RSA

Autre ...

- Multiplications modulaire à précalculs calibrables
- Optimisation du changement de base en RNS
- Algorithmique modulaire à forte mémorisation

Présentation
Contexte
Multiplication
Classes de moduli
Mersenne
Pseudo Mersenne
Pseudo Mersenne
Représentation
Modulaire
Adapté
Vouvelle classe
RED
Propriété
Construction

Conclusion

Implantation Étyple des per

Étude des possibilités de parallélisation

Système de représentation modulaire

Interpolation

Autre ...

- Implantation
- Étude des réseaux en norme $\|.\|_{\infty}$