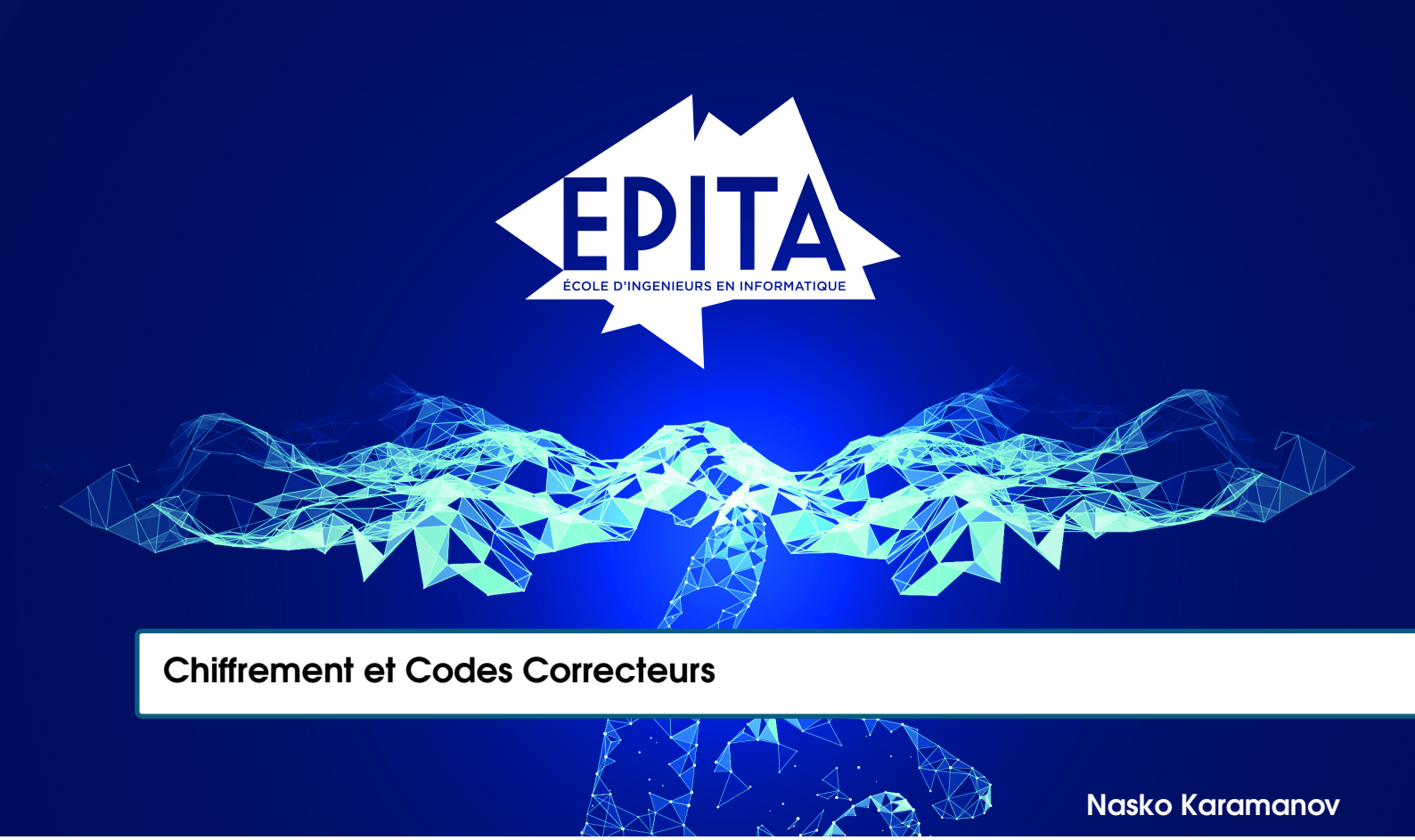

Chiffrement et Codes Correcteurs

Nasko Karamanov

1 Cryptographie et courbes elliptiques

Acquis d'apprentissage visés
— Utiliser les algorithmes d'un schema de chiffrement donné.
— Mettre en oeuvre un algorithme d'attaque pour déchiffrer un message donné.
— Expliquer quelques techniques standard de perturbation / sécurisation des cryptosystemes standards
— Identifier les algorithmes de chiffrement fragiles dans un contexte post-quantique.

Question 1-1 Soit $E : y^2 = x^3 + 2x + 3$ sur $\mathbb{F}_7$ et $P = (2,1)$.

a) Le point $(3,4)$ est-il sur la courbe ?
b) Vérifier que P est sur la courbe.
c) Donner les coordonnées de $-P$?
d) Donner une formule pour l'inverse de $Q(x_Q, y_Q)$ en tant qu'élément de $E(\mathbb{F}_7)$.
e) Calculer $2P$.
f) Lister tous les points sur la courbe
g) Vérifier que le nombre de point corresponds à l'encadrement donné par le théorème de Hasse.
h) Faire le table d'addition.
i) Montrer que P est un générateur de $E(\mathbb{F}_7)$.
j) Si $Q = (3,1)$ que vaut $\log_P(Q)$?

Pour s'entraîner

k) Mêmes questions pour $E : y^2 = x^3 + x + 2$ sur $\mathbb{F}_5$ et $P = (1,2)$
l) Mêmes questions pour $E : y^2 = x^3 + 2x + 5$ sur $\mathbb{F}_{11}$ et $P = (0,4)$

Solution 1-1

a) $3^3+2\cdot 3+3\equiv 1 \mod 7$ et $4^2\equiv 2 \mod 7$ donc le point n'est pas sur la courbe.

b) $2^3+2\cdot 2+3\equiv 1=1^2 \mod 7$ donc P est sur la courbe

c) Par défintion sur $E(\mathbb{R})$ l'inverse de P est $-P=(2,-1)$ et $-1\equiv 6 \mod 7$ donc $-P=(2,6)$.

d) $-Q=(x_Q,-y_Q)=(x_Q,n-y_Q)$

e) On utilise les formules vues dans le cours : $m=(3x_P^2+a)(2\cdot y_P)^{-1}=(3\cdot 2^2+2)(2\cdot 1)^{-1}=0\cdot 2^{-1}=0 \mod 7$. Donc $x=m^2-x_P-x_P=0-2-2\equiv 3 \mod 7$ et $y=m(x_P-x)-y_P=-1=6 \mod 7$. Donc $2P=(3,6)$.

f) Le tableau suivant permet d'obtenir les points différents de l'élément neutre

x	x^3+2x+3	x^2
0	3	0
1	6	1
2	1	4
3	1	2
4	5	2
5	5	4
6	0	1

Pour la dernière colonne on peut utiliser le fait que $x^2=(-x)^2=(n-x)^2$ pour faire la moitié des calculs. On obtient donc $E(\mathbb{F}_7)=\{\mathcal{O},(2,1),(2,6),(3,1),(3,6),(6,0)\}$

g) Le théorème d'Hasse dit que $7+1-2\sqrt{7}\leq \text{Card}E(\mathbb{F}_7)\leq 7+1+2\sqrt{7}$ donc $3\leq \text{Card}E(\mathbb{F}_7)\leq 13$ donc 6 est bien dans cet intervalle.

h)

$+$	$\mathcal{O}$	$(2,1)$	$(2,6)$	$(3,1)$	$(3,6)$	$(6,0)$
$\mathcal{O}$	$\mathcal{O}$	$(2,1)$	$(2,6)$	$(3,1)$	$(3,6)$	$(6,0)$
$(2,1)$	$(2,1)$	$(3,6)$	$\mathcal{O}$	$(2,6)$	$(6,0)$	$(3,1)$
$(2,6)$	$(2,6)$	$\mathcal{O}$	$(3,1)$	$(6,0)$	$(2,1)$	$(3,6)$
$(3,1)$	$(3,1)$	$(2,6)$	$(6,0)$	$(3,6)$	$\mathcal{O}$	$(2,1)$
$(3,6)$	$(3,6)$	$(6,0)$	$(2,1)$	$\mathcal{O}$	$(3,1)$	$(2,6)$
$(6,0)$	$(6,0)$	$(3,1)$	$(3,6)$	$(2,1)$	$(2,6)$	$\mathcal{O}$

i) En utilisant le tableau on trouve : $2P=(3,6)$, $3P=(6,0)$, $4P=(3,1)$, $5P=(2,6)$ et $6P=\mathcal{O}$ donc P engendre $E(\mathbb{F}_7)$.

j) $4P=Q$ donc $\log_P(Q)=4$.

Question 1-2

a) Expliquer comment on peut adapter l'algorithme d'exponentiation rapide pour calculer nP.

b) Soit $E: y^2=x^3+3x+2$ sur $E(\mathbb{F}_{23})$ et $P=(0,5)$. Calculer $13P$.

Solution 1-2

a) Si $n=\sum 2^{n_i}$ est la décomposition binaire de n où $n_i\in\{0,1\}$ alors on calcule $2^{n_i}P$ et donc $nP=\sum(2^{n_i}P)$.

b) $13=1+2^2+2^3$. Avec les formules d'addition on obtient $2P=(4,3)$, $4P=(1,11)$, $8P=(11,3)$. Donc $13P=P+4P+8P=(12,15)+(11,3)=(6,11)$

..

Question 1-3 Le cryptosystème de Menezes-Vanstone est une variante de ElGamal pour les courbes elliptiques. Son schéma de chiffrement est donné dans le tableau suivant.

Alice	Bob
KeyGen	
Choisir p premier, E une courbe elliptique et un générateur $G \in E(\mathbb{F}_p)$	
	Choisir $b < \text{Card}E(\mathbb{F}_p)$, $K_b = bG$ Clé privée de Bob : sk $= b$
clé publique : pk $= (p, g, K_b)$	
Chiffrement	
Choisir $a < p$ Choisir un couple de messages $\boldsymbol{m} = (\boldsymbol{m}_1, \boldsymbol{m}_2) \in (\mathbb{Z}/p\mathbb{Z})^2$ $K_a = aG$, $K_1 = a(K_b) = (x_1, y_1)$ $\boldsymbol{c}_1 \equiv x_1 \boldsymbol{m}_1 \mod p$ $\boldsymbol{c}_2 \equiv y_1 \boldsymbol{m}_2 \mod p$ $\boldsymbol{c} = \text{Enc}(\boldsymbol{m}, \text{pk}) = (K_a, \boldsymbol{c}_1, \boldsymbol{c}_2)$	
Dechiffrement	
	$K_2 = bK_a = (x_2, y_2)$ $\boldsymbol{m}'_1 \equiv x_2^{-1} \boldsymbol{c}_1 \mod p$ $\boldsymbol{m}'_2 \equiv y_2^{-1} \boldsymbol{c}_2 \mod p$ $\text{Dec}(\boldsymbol{c}, \text{sk}) = (\boldsymbol{m}'_1, \boldsymbol{m}'_2)$

a) Décrire les ensembles de messages $\mathscr{M}$ et messages chiffrés $\mathscr{C}$.

b) Vérifier que $K_1 = K_2$

c) Vérifier la validité de ce cryptosystème.

d) Alice et Bob utilisent ce cryptosystème avec $E : y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{23}$ et $G = (2,6)$ d'ordre 30. La clé privé de Bob est sk $= 4$. Bob a reçu le message : $\boldsymbol{c} = ((18,21),16,6)$. Quel est le message que Alice a envoyé ?

e) Ce cryptosystème est il fragilisé par les ordinateur quantiques ?

Solution 1-3

a) $\mathscr{M} = (\mathbb{Z}/p\mathbb{Z})^2$ et $\mathscr{C} = E(\mathbb{F}_p) \times (\mathbb{Z}/p\mathbb{Z})^2$

b) $K_1 = aK_a = abG$ et $K_2 = bK_a = baG$ donc $K_1 = K_2$

c) Comme $(x_1, y_1) = (x_2, y_2)$ on a $m'_1 \equiv x_2^{-1} \boldsymbol{c}_1 \equiv x_1^{-1} x_1 \boldsymbol{m}_1 \equiv \boldsymbol{m}_1 \mod p$. Même raisonnement pour $\boldsymbol{m}'_2 \equiv \boldsymbol{m}_2 \mod p$.

d) On a $4(18,21) = (21,9)$. En utilisant Bézout : $23 \times (-10) + 21 \times 11 = 1$ on obtient $21^{-1} \equiv 11 \mod 23$ et $23 \times (-3) + 14 \times 5 = 1$ donc $14^{-1} = 5$. $\boldsymbol{m}_1 = 11 \cdot 16 \equiv 15 \mod 23$ et $\boldsymbol{m}_2 = 5 \cdot 6 \equiv 7 \mod 23$. Donc $\boldsymbol{m} = (15,7)$.

e) Oui, car basé sur le problème du log discret

Question 1-4 La **Signature numérique ECDSA (Elliptic curve digital signature algorithm)** a le schéma suivant (en général on l'applique à $h(\boldsymbol{m})$ ou h est une fonction d'hachage).

Alice	Bob
KeyGen	
Choisir p premier, E une courbe elliptique et un générateur $G \in E(\mathbb{F}_p)$ d'ordre n Choisir $a < n$, $K_a = aG$ Clé privée de Alice : sk $= a$ clé publique : pk $= (p, n, G, E, K_a)$	
Sign	
Choisir $k < n$ Choisir un message $\boldsymbol{m} = \in (\mathbb{Z}/n\mathbb{Z})$ $M = kG = (x_M, y_M)$ et $r = x_M \mod n$ $\boldsymbol{c} = (\boldsymbol{m} + ar)k^{-1} \mod n$ Si $r = 0$ ou $\boldsymbol{c} = 0$ recommencer $\sigma = (r, \boldsymbol{c})$	
Vérification	
	$B = \boldsymbol{c}^{-1}(\boldsymbol{m}G + rK_a) = (x_B, y_B)$ Si $r \equiv x_B \mod n$ retourner 1

Validité : $\boldsymbol{c}^{-1}(\boldsymbol{m}G + rK_a) = k(\boldsymbol{m}+ar)^{-1}(\boldsymbol{m}G + raG) = k(\boldsymbol{m}+ar)^{-1}(\boldsymbol{m}+ar)G = kG$
et c'est bien la première coordonnée de ses points qu'on vérifie.

a) Alice utilise cette signature avec $E : y^2 = x^3 + 2x + 2$, $G = (5,1)$, $p = 17$ et $n = 19$. Elle décide d'utiliser $a = 7$, calcule $K_a = aG = (0,6)$ et publie sa clé publique. Le message que Bob a reçu est 26, signé avec $\sigma = (7,17)$. Peut-il être sûr que le message provient d'Alice ?

b) Ce schéma de chiffrement est il fragilisé par les ordinateur quantiques ?

Solution 1-4

a) Bob calcule $c^{-1} = 17^{-1} = 9 \mod 19$.
$B = (mG + rK_a) = 9(26(5,1) + 7(0,6))9 \cdot 26(5,1) + 9 \cdot 7(0,6)$
Comme on s'intèresse aux coordonnées modulo 19 : $9 \cdot 26 = 6 \mod 19$ et $9 \cdot 7 \equiv 6 \mod 19$
$B = 6(5,1) + 6(0,6) = (7,11)$ et $x_B \equiv r \mod 19$ donc le message provient d'Alice.

b) Le schéma est basé sur le logarithme discret, donc fragilisé par les ordinateurs quantiques.

Question 1-5 Soit $E : y^2 = x^3 + 2x + 6$ sur $\mathbb{F}_7$, $P = (1,3)$ un générateur de $E(\mathbb{F}_7)$ et $Q = (4,6)$.

a) Encadrer $\log_P Q$.

b) Calculer $\log_P Q$

Pour s'entrâiner

c) Même questions avec $E : y^2 = x^3 + 2x + 2$ sur F_{13}, $P = (3,3)$ et $Q = (6,3)$.

Solution 1-5

a) Avec le théorème de Hasse on obtient $3 \leq E(\mathbb{F}_7) \leq 13$.

b) Baby-step liste : $\mathcal{O}, (1,3), (2,2), (5,1)$, Giant-step : $(4,6), (5,1)$. La collision arrive pour $3P = Q - 3P$, donc $Q = 6P$.

c) $L_1 = \mathcal{O}, (3,3), (4,3), (6,10), (12,8)$, $L_2 = (6,3), (11,4), (4,3)$ donc $2P = Q - 6P$ et $Q = 9P$