Ingénierie cryptographiques et protocoles — TD

Les attaques par courbes invalides

On présente dans ce TD une attaque bien connue contre certains protocoles à base de Diffie-Hellman "statique" sur courbes elliptiques.

Attaque contre les courbes sous forme de Weierstrass

Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique sous forme de Weierstrass réduite, définie sur un corps fini $\mathbb{F}_q$ (ou plus simplement $\mathbb{Z}/p\mathbb{Z}$) de caractéristique > 3, telle que le problème du logarithme discret sur E soit difficile.
Dans le cadre de cette attaque, on vous donne accès à un dispositif qui étant donné un point P, renvoie un point $[s]P$ où s est un entier secret.

1. Étant donnés deux points affines $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ de E, rappeler comment obtenir les coordonnées de $P_3 = P_1 + P_2$, en distinguant les cas où $P_1 = P_2$, $P_1 = -P_2$ et $P_1 \neq \pm P_2$. Comment les paramètres a et b de la courbe sont-ils reliés à ces coordonnées ?
2. Soient $P_0 = (x_0, y_0) \in (\mathbb{F}_q)^2$ et $b' = y_0^2 - x_0^3 - ax_0$. Montrer que P_0 appartient à la courbe elliptique $E' : y^2 = x^3 + ax + b'$.
3. On suppose que le dispositif ne vérifie pas que les valeurs en entrée sont des points de E. Quel sera le résultat d'une requête ayant pour entrée P_0 ?
4. Monter une attaque qui permet de retrouver le secret s avec un nombre polynomial d'appels au dispositif. Proposer une contre-mesure simple.
5. Application. La courbe $E : y^2 = x^3 - 3x + 73$ définie sur $\mathbb{Z}/199\mathbb{Z}$ admet 197 points rationnels. Sur l'entrée $P = (183, 117)$, le dispositif retourne $Q = (99, 36)$.
   (a) Montrer que le point P est sur la courbe $E' : y^2 = x^3 - 3x + 26$ (définie sur $\mathbb{Z}/199\mathbb{Z}$).
   (b) Quelques rapides calculs donnent $\#E' = 210$, $105\,Q = (101, 0)$, $70\,Q = 70\,P = (136, 149)$, $42\,Q = -84\,P = (173, 144)$, et $30\,Q = \mathcal{O} \neq 30\,P$.
   Retrouver la valeur de s.

Attaque contre l'échelle de Montgomery

On a vu en cours qu'il était possible de n'utiliser que les abscisses pour l'échange de clefs de Diffie-Hellman. En utilisant l'échelle de Montgomery, il est même possible de calculer l'abscisse de $k\,P$ avec un algorithme d'exponentiation rapide, sans calcul intermédiaire d'ordonnées.

Voici quelques formules. Soient P, Q deux points de la courbe E d'équation $y^2 = x^3 + ax + b$. Il est possible de donner une expression de $x(P + Q)$ connaissant seulement $x(P)$, $x(Q)$ et $x(P - Q)$:

$$x(P+Q) = f(x(P), x(Q), x(P-Q)) = \frac{-4b(x(P)+x(Q)) + (x(P)x(Q)-a)^2}{x(P-Q)(x(P)-x(Q))^2} \quad \text{si } P \neq \pm Q$$

$$x(2P) = g(x(P)) = \frac{(x(P)^2 - a)^2 - 8bx(P)}{4(x(P)^3 + ax(P) + b)} \quad \text{si } P \neq -P$$

On considère l'algorithme suivant :

Input : $x = x(P)$, $k = (k_l, \ldots, k_0)_2$
$x_0 \leftarrow x$; $x_1 = g(x)$
for $i = l - 1$ à 0 **do**
  if $k_i = 0$ **then**
    $x_1 \leftarrow f(x_1, x_0, x)$; $x_0 \leftarrow g(x_0)$
  else
    $x_0 \leftarrow f(x_1, x_0, x)$; $x_1 \leftarrow g(x_1)$
return x_0

---

1. Montrer que le résultat retourné par l'algorithme est l'abscisse de $k\,P$.
2. Expliquer pourquoi l'attaque précédente ne peut pas s'appliquer directement si cet algorithme est utilisé.

Soit $c \in \mathbb{F}_q$ un élément qui n'est pas un carré. On considère la courbe E_c d'équation $cy^2 = x^3 + ax + b$. On peut alors montrer que pour tout $x \in \mathbb{F}_q$,

— soit $x^3 + ax + b$ est un carré dans $\mathbb{F}_q$, et il existe alors $y \in \mathbb{F}_q$ tel que (x, y) appartienne à E
— soit $x^3 + ax + b$ n'est pas un carré dans $\mathbb{F}_q$, et alors $\frac{1}{c}(x^3 + ax + b)$ est un carré, et il existe donc $y \in \mathbb{F}_q$ tel que (x, y) appartienne à E_c

3. On suppose maintenant que notre dispositif utilise l'algorithme décrit ci-dessous et qu'il ne vérifie toujours pas les entrées. Que retourne-t-il lorsque l'entrée est un élément $x \in \mathbb{F}_q$ qui n'est pas l'abscisse d'un point de $E(\mathbb{F}_q)$?
4. On suppose dans cette question que E est "*twist-insecure*", i.e. que la cardinalité de la courbe E_c n'a que des petits facteurs premiers. Monter une attaque qui permet de retrouver de l'information sur s.
5. (Bonus) À l'aide de la propriété donnée ci-dessus, montrer que $\#E_c = 2q + 2 - \#E$.
   La courbe `brainpoolP256r1` est-elle "twist-secure" ? Et la courbe `secp256k1`, utilisé dans le protocole Bitcoin ?

Attaque contre les courbes sous forme d'Edwards

La courbe elliptique est maintenant donnée sous forme d'Edwards $Ed : ax^2 + y^2 = 1 + dx^2y^2$ avec a et d deux éléments distincts et non nuls de $\mathbb{F}_q$. On rappelle que la loi d'addition est donnée par

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

1. On suppose maintenant que le dispositif utilise la courbe Ed et la formule d'addition ci-dessus, mais ne vérifie toujours pas que les entrées sont des points de la courbe. Est-il possible d'adapter directement l'attaque de la question 4 ?
2. Soit $P_0 = (0, y_0) \in (\mathbb{F}_q)^2$. Montrer que le résultat retourné par le dispositif sur l'entrée P_0 est $(0, y_0^s)$. En déduire une attaque qui permet de retrouver s.

3. Application.
   La courbe Ed définie sur $\mathbb{F}_{47}$ admet 53 points rationnels. Sur l'entrée $(0, 40)$, le dispositif renvoie $(0, 38)$. Le but est d'appliquer l'attaque décrite précédemment pour retrouver s.
   (a) Sachant que $38^{23} = 40^{23} = -1$ [47], déduire la valeur de s modulo 2
   (b) Utiliser pas-de-bébé-pas-de-géant pour retrouver s modulo 23. On pourra utiliser les calculs suivants : $38^2 = 34$ [47], $40^2 = 2$ [47] et $2^{-5} = 25$ mod 47.
   (c) Conclure.