Quelles courbes elliptiques?

Afin de résister aux diverses attaques connues, le système doit vérifier un certain nombre de conditions.

- Tout d'abord le nombre n doit être suffisamment grand, plus précisément on doit avoir au moins $n > 2^{160}$. En pratique on essaie de choisir N presque premier, c'est-à-dire de la forme $N = cn$ où n est un nombre premier (qu'on prendra alors pour ordre du groupe $\mathcal{G}$) et où $c \leq 4$.
- Dans tous les cas on prendra $n > 4\sqrt{q}$ de manière à assurer que $\mathcal{E}(\mathbb{F}_q)$ n'ait qu'un seul sous-groupe d'ordre n.
- Dans le cas où le corps utilisé est $\mathbb{F}_p$, on doit avoir $N \neq p$ pour éviter l'attaque de Semaev-Smart-Satoh-Araki.
- Pour éviter l'attaque du "pairing" de Weil-Tate on doit vérifier que $q^k \not\equiv 1 \quad (n)$ pour un petit nombre de valeurs de k, disons $1 \leq k \leq 20$.
- Dans le cas où on utilise un corps binaire $\mathbb{F}_{2^m}$, on doit prendre m impair afin de résister à l'attaque par descente de Weil.

Nous renvoyons à [**?**] pour les détails concernant ces restrictions.

Remarque : La forme de l'équation de la courbe dans le cas d'un corps binaire implique que celle-ci n'est pas super-singulière, ce qui évite l'attaque **MOV** de Menezes-Okamoto-Vanstone et de Frey-Rück.

Remarque : La mise en place effective d'un système ECDSA demande l'implémentation d'un certain nombre d'algorithmes, et en particulier le calcul effectif du nombre de points d'une courbe elliptique. Ce dernier problème a été largement étudié et a donné lieu à deux approches. La première approche consiste à partir d'une courbe elliptique et à calculer son nombre de points par l'algorithme de Schoof amélioré par Elkies et Atkin (algorithme SEA) puis par divers autres mathématiciens. La deuxième approche consiste à fixer un nombre de points et à chercher une courbe elliptique ayant ce nombre de points par la

méthode de multiplication complexe de Atkin-Morain (cas d'un corps premier $\mathbb{F}_p$) ou de Lay-Zimmer (cas d'un corps binaire).