# Une mise en revue des couplages

Razvan Barbulescu

Les applications bilinéaires non-dégénérées sont des outils importants pour les protocoles cryptographiques récents comme l'échange de clé tripartite. Avec les applications bilinéaires associées aux réseaux euclidiens, les couplages de Weil sont les seules constructions qui peuvent être calculées en rapidement et dont l'inversion est difficile.

Pour une courbe elliptique $E$ définie sur un corps fini $\mathbb{F}_q$, un entier $r$ et un point rationnel $P \in E$ d'ordre $r$ on définie le couplage de Weil (restreint au sous-groupe engendré par $P$) par

$$\begin{array}{rccc} e_{E,r,P,\mu}: & \frac{\mathbb{Z}}{r\mathbb{Z}}P \times \frac{\mathbb{Z}}{r\mathbb{Z}}P & \to & \mu^{\mathbb{Z}/r\mathbb{Z}} \\ & ([a]P, [b]P) & \mapsto & \mu^{ab}, \end{array}$$

où $\mu$ est une racine $r$ème de l'unité dans la clôture algébrique de $\mathbb{F}_q$. Les couplage de Weil restreint à $\mathbb{Z}$P est aussi une forme bilinéaire symétrique non-dégénérée, donc offre une définition alternative pour le même objet, modulo un changement éventuel de $\mu$. Le couplage de Weil se calcule en temps polynomial alors que les meilleurs attaques consiste à résoudre calculer $a$ soit à partir de $[a]P$ (problème du logarithme discret(DLP) sur les courbes elliptiques) soit à partir de $\mu^a$ (problème des logarithmes discrets dans les corps finis).

On appelle degré de plongement d'un couplage associé à $E/\mathbb{F}_q$ et $r$ le plus petit $k$ tel que $\Phi_r$ a une racine dans $\mathbb{F}_{q^k}$. La proportion des paires $E/\mathbb{F}_q$ et $r$ avec un petit degré de plongement étant très faible, elles ne peuvent pas être construite en choisissant des courbes au hasard et en calculant leur $k$. Mise à part une famille peu utilisée, les familles de couplages sont des solutions du système d'équations CM, et demande d'utiliser la méthode CM. On obtient ainsi cinq types : supersingulières, Cocks-Pinch, Dupond-Enge-Morain, creuse (ex. MNT) et complètes(ex. BN). Le seul type qui permet de produire un nombre considérable de couplages à la volée est le dernier.

La sécurité des couplages a été estimée sous une hypothèse : le logarithme discret dans les corps finis est aussi dur que la factorisation d'un module RSA. En effet, le meilleur algorithme pour calculer de tels logarithmes discrets est le crible algébrique (NFS), une version de l'algorithme utilisé également pour factoriser des modules RSA. Cet algorithme a une version plus rapide, appelée SNFS, pour factoriser des nombres de forme spéciale : $P(u)$ avec $u$ entier et $P \in \mathbb{Z}[x]$ de degré donné et $\|P\|_\infty$ inférieur à une constante absolue.

SNFS n'a pas été adapté au cas du logarithme discret dans des corps $\mathbb{F}_{q^k}$ avec $k \neq 1$ avant 2013, quand Joux et Pierrot ont proposé un algorithme de même complexité asymptotique que la version SNFS pour la factorisation. Néanmoins cet algorithme a été considéré comme non-pratique et les recommandations des tailles n'ont pas été changées.

En collaboration avec Pierrick Gaudry et Thorsten Kleinjung [BGK15] nous avons réhabilité un algorithme d'Oliver Schirokauer, appelé le crible algébrique

des tours d'extensions. Cette version a été également considérée comme non-pratique. Par une deuxième collaboration avec Taechan Kim [KB16] nous avons combiné cette version avec celle de Joux-Pierrot et nous obtenons une méthode pratique, qui demande de changer les tailles des clés.

# Références


[Bar16] Razvan Barbulescu. A brief history of pairings. In *International Workshop on the Arithmetic of Finite Fields WAIFI 2016*, volume 10064 of *Lecture Notes in Comput. Sci.*, Gand, Belgium, 2016. Université de Gand, Springer.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The Towed Number Field Sieve. In *Advances in Cryptology – ASIACRYPT 2015*, volume 9453 of *Lecture Notes in Comput. Sci.*, pages 31–55, 2015.

[KB16] T. Kim and R. Barbulescu. Extended tower number field sieve : A new complexity for medium prime case. In *Advances in Cryptology – CRYPTO 2016 (part 1)*, volume 9815 of *Lecture Notes in Comput. Sci.*, pages 543–571, 2016.