Différences entre couplage symétrique et asymétrique : étude de protocoles et implémentation

Aurore Guillevic, Thales et ENS
Travaux en partie en collaboration avec Renaud Dubois et Marine Sengelin Le Breton

Soumission la conférence C2 à Dinard

La cryptographie bilinéaire connaît un bel essor depuis bientôt une douzaine d'années. Après la période de doutes due aux attaques MOV et FR sur les courbes supersingulières, les découvertes constructives publiées en 2001 ont lancé une nouvelle mode en cryptographie, tant pour les programmeurs que pour les concepteurs de protocole. Les deux articles fondateurs sont dus à A. Joux à ANTS IV, montrant la voie à de nouveaux protocoles, et à D. Boneh, B. Lynn et H. Shacham à ASIACRYPT 2001, proposant un schéma de signature courte. Les seules courbes elliptiques alors connues et acceptables pour le calcul d'un couplage (de Weil ou Tate) étaient supersingulières. Pour ces raisons historiques, la communauté des concepteurs de protocole a retenu qu'un couplage est une application bilinéaire symétrique, de type $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, le choix entre couplage symétrique ou asymétrique ($e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$) étant laissé à la discrétion du programmeur. L'essence de la preuve de sécurité ne change presque pas, il faut éventuellement rajouter des entrées au problème sous-jacent si un isomorphisme explicite entre $\mathbb{G}_1$ et $\mathbb{G}_2$ n'est pas disponible. En pratique, les gains en temps de calcul et taille des paramètres sont considérables lorsque l'on retranscrit un protocole en version asymétrique. L'illustration sera faite avec le protocole de diffusion chiffrée de D. Boneh, C. Gentry et B. Waters de 2005.

Cette même année, D. Boneh, E.-J. Goh et K. Nissim proposent un système de chiffrement homomorphe utilisant la propriété d'ElGamal pour additionner dans les exposants, et un couplage pour multiplier une fois dans les exposants. La sécurité de ce schéma repose sur le problème de décision de sous-groupe. Mais en pratique, on se rend compte que les paramètres sont de taille quasiment dissuasive (plus de 6000 bits pour un élément de $\mathbb{G}_T$) et le temps pour une opération s'exprime en secondes. Des schémas proposant les mêmes fonctionnalités mais reposant sur d'autres hypothèses de sécurité (travaux de D. Freeman puis A. Lewko) permettent une implémentation avec des courbes ordinaires, donc un couplage asymétrique, où les tailles de paramètre et temps d'exécution restent raisonnables et comparables à ce qui est attendu en cryptographie bilinéaire. Une implémentation pratique de chaque protocole utilisant la LIBCRYPTOLCH du Laboratoire Chiffre sera présentée afin de comparer concrètement chaque version, à un niveau de sécurité de 128 bits.

Enfin, de nouvelles hypothèses de sécurité n'ont de sens qu'avec un couplage asymétrique, comme l'hypothèse Diffie-Hellman externe (XDH). Elle repose sur la difficulté de calculer un isomorphisme entre $\mathbb{G}_1$ et $\mathbb{G}_2$, supposée aussi forte que celle d'un calcul de logarithme discret. Les derniers travaux sur ce sujet de S. Ramanna, S. Chatterjee et P. Sarkar présentés à PKC 2012 en montrent notamment l'intérêt, une implémentation sera aussi présentée.