Autour de l'échantillonnage par rejet

Julien Devevey

ENS de Lyon

L'échantillonnage par rejet est un élément central de nombreux protocoles d'authentification et de preuves interactives basés sur les réseaux Euclidiens, comme la signature de Lyubashevsky [Lyu12].

Son but est de transformer des échantillons i.i.d. de la forme $y_i + v_i$, où v_i dépend d'un secret mais pas y_i, en un échantillon z qui suit une distribution totalement indépendante du secret. Pour cela, un lancer de pièce biaisé et adaptatif décide si l'échantillon i doit être retenu ou si on doit examiner l'échantillon $i+1$, jusqu'à en retenir un. L'espérance du nombre d'échantillons rejetés correspond à la divergence de Rényi d'ordre infini entre la distribution de $y_i + v_i$ et celle de la cible z, mais outre cette dépendance, le choix de la distribution de z est libre. Il est alors souhaitable d'utiliser une distribution de faible norme en moyenne, afin d'améliorer la sécurité des protocoles.

Nous abordons les questions suivantes :

- Quel choix de distributions pour y_i et z permet de minimiser l'espérance de la norme de z ?
- Peut-on purement et simplement supprimer cette étape ?

Dans ce travail en cours, nous donnons une borne inférieure, qui est atteinte, sur la norme moyenne de z. Nous répondons aussi positivement à la dernière question, tout en détaillant les conséquences de ces modifications.

Ce travail est effectué avec Alain Passelègue et Damien Stehlé.

Références

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, 2012.