AUTOUR DU SIDH : LES PROTOCOLES MD-SIDH ET M-SIDH

Daniel TIEUDJO
Dpartement de Mathmatiques et Informatique
Université de Ngaoundéré
tieudjo@yahoo.com

30 Mai 2024

Résumé :

Le protocole d'échange de clés de type Diffie-Hellman basé sur les isogénies des courbes elliptiques supersingulières appelé Supersingular Isogeny Diffie-Hellman Key Exchange Protocol, en abrgé (SIDH KEP) a été d'une grande actualité ces dernières années. En effet, espoir de la cryptographie post quantique depuis les années 2000, il est passé de candidat favori ou très sérieux du NIST au maillon faible de la cryptographie post quantique bas´e sur les courbes elliptiques depuis août 2022. Le SIDH a subi des attaques successives et ceci a conduit a des améliorations. Des nouvelles versions du SIDH ont été proposées. La série des 3 exposés proposés fait une revue de ce parcours du SIDH. Une présentation détaillée du SIDH a été faite (exposé de Mai 2023), les attaques sur le SIDH ont été parcourues (exposé du 30 Novembre 2023). Ces attaques ont conduit á des nouvelles variantes du SIDH, notamment le "masked torsion points" SIDH (M-SIDH) de T.B. Fouotsa et le "masked degree" SIDH (MD-SIDH) de T. Moriya. Ce dernier protocole sera illustré et implémenté sur SAGEMATH. Quelques problmes de recherche seront posés.

Le présent exposé portera donc essentiellement sur les nouvelles versions du SIDH : MD-SIDH et M-SIDH

Mots Clés :

Protocole d'échange de clés, Isogénies supersingulières, SIDH, Degré de l'isogénie, Points de torsion.

Bibliographie utile :

1. T. B. Fouotsa, *SIDH with masked torsion point images*, Cryptology ePrint Archive, (2022) https ://eprint.iacr.org/2022/1054.pdf
2. T. Moriya, *Masked-degree SIDH*, Cryptology ePrint Archive, Paper 2022/1019, (2022). https ://eprint.iacr.org/2022/1019
3. C. Petit, T.B. Fouotsa, T. Moriya *M-SIDH and MD-SIDH : countering SIDH attacks by masking information*, Eurocrypt 2023, 2023