Étude d'un schéma de signature multivarié post-quantique : OV$\widehat{+}$

Encadrants. Pierre Pébereau

Mots clés. Cryptographie, cryptanalyse, systèmes polynomiaux, algèbre linéaire

Contexte et Résumé. En 1994, Shor propose un algorithme quantique polynomial pour résoudre des problèmes de théorie des nombres (log discret, factorisation) sur lesquels repose la cryptographie à clé publique alors utilisée (RSA, DSA, ECDSA, ...). Dès lors, les cryptologues et états ont cherché à obtenir des algorithmes de cryptographie à clé publique dits "post-quantiques".

En particulier, en 2017, le NIST (National Institue for Standards and Technologies, une agence américaine) a lancé une compétition visant à standardiser des algorithmes post-quantiques, à laquelle de nombreuses équipes internationales ont soumis des candidats. En 2022, 3 algorithmes de signatures ont été standardisés (Dilithium, Falcon, SPHINCS+) ainsi qu'un algorithme de chiffrement (Kyber). Malgré tout, le NIST a lancé un nouvel appel à soumissions pour des signatures reposant sur des hypothèses de sécurité différentes, et avec une emphase sur les performances (taille des signatures, vitesse, ...). Dans ce contexte, de nombreux algorithmes multivariés ont été proposés, leur principal atout étant leur vitesse et la faible taille des signatures.

Parmi ces candidats multivariés, une famille d'algorithmes basés sur le schéma "Unbalanced Oil and Vinegar" (UOV dans la suite) se distingue par ses performances et le nombre de soumission. Dans ce projet, on s'intéressera à une alternative d'un candidat du premier round proposée dans le document original mais non soumise à la compétition.

Un schéma de signature multivarié est caractérisé par une clé publique qui est un système d'équations polynomiales quadratiques, et une signature est une solution d'un translaté du système publique (la translation dépendant du message). Le schéma UOV permet de signer des messages en se donnant comme fonction à trappe un espace linéaire de solutions du système. Lorsque cet espace est trop grand, on retrouve un ancien schéma appelé "Oil and Vinegar" qui est vulnérable à une attaque polynomiale classique.

Le schéma étudié durant le projet sera une modification de "Oil and Vinegar" consistant à remplacer un petit nombre d'équations de la clé publique par des équations aléatoires.

Description détaillée du travail attendu. Les étudiants se familiariseront avec les algorithmes de génération de clé, de signature et de vérification d'UOV/OV [3], puis implémenteront et étudieront les performances de l'attaque originale de Kipnis et Shamir [4]. Une fois ce travail effectué, ils étudieront la proposition UOV$\widehat{+}$ [2, 1] et en particulier OV$\widehat{+}$. Ils implémenteront les algorithmes de génération de lé, de signature et de vérification pour ce schémas, puis ils entameront la cryptanalyse (l'étude de la sécurité) du schéma OV$\widehat{+}$. Pour l'implémentation, je recommande l'utilisation de Sagemath [5].

1. Lire [4].
2. Implémenter les algorithmes de génération de clé, de signature et de vérification pour le schéma OV décrit dans [4], ainsi qu'une batterie de tests.
3. Implémenter l'attaque décrite dans [4, Sections 3, 4.2, 4.3].

4. Calculer la complexité théorique de cette attaque, comparer à la complexité annoncée dans l'article, et comparer avec la complexité pratique. La complexité théorique est-elle pessimiste, optimiste, ou exacte ?
5. Lire [2] et [1].
6. Implémenter les algorithmes de génération de clé, de signature et de vérification pour le schéma OV$\widehat{+}$.
7. Se familiariser avec la méthodologie d'évaluation de la sécurité d'un algorithme cryptographique.
8. Évaluer la sécurité d'OV$\widehat{+}$ avec $q^{2t} \geqslant 2^{\lambda}$. Faut-il plus de 2^{λ} opérations binaires pour "casser" le schéma ?

Références

[1] Cogliati, B., Faugère, J.C., Fouque, P.A., Goubin, L., Larrieu, R., Macario-Rat, G., Minaud, B., Patarin, J. : Vox-sign (2023), `http://vox-sign.com/files/vox_nist.pdf`, consulted 05/10/2023

[2] Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L. : A new perturbation for multivariate public key schemes such as HFE andUOV. Cryptology ePrint Archive, Paper 2022/203 (2022), `https://eprint.iacr.org/2022/203`

[3] Kipnis, A., Patarin, J., Goubin, L. : Unbalanced oil and vinegar signature schemes. In : Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 206–222. Springer (1999). https ://doi.org/10.1007/3-540-48910-X_15, `https://doi.org/10.1007/3-540-48910-X_15`

[4] Kipnis, A., Shamir, A. : Cryptanalysis of the oil & vinegar signature scheme. In : Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 257–266. Springer (1998). https ://doi.org/10.1007/BFb0055733, `https://doi.org/10.1007/BFb0055733`

[5] The Sage Developers : SageMath, the Sage Mathematics Software System (2022), `https://www.sagemath.org`, dOI 10.5281/zenodo.6259615