ÉLÉMENT DE PORTFOLIO 01

Publication

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection.

URL de l'élément : `https://eprint.iacr.org/2022/223`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

En 2021, l'équipe ALMASTY a fortement remanié le cours *Cryptologie avancée et appliquée* en deuxième année du parcours **Sécurité, Fiabilité et Performances** (SFPN) du master informatique de Sorbonne Université en intégrant notamment la cryptographie fondée sur les réseaux euclidiens et la géométrie des nombres et les systèmes de preuves à divulgation nulle de connaissance.

Suite à des discussions au sein de l'équipe pédagogique, nous nous sommes intéressés au problème de la *somme (modulaire) de sous-ensembles* qui consiste à trouver, étant donné des entiers $w_1, \ldots, w_n$, t et q, un sous-ensemble des w_i dont la somme est égale à t modulo q, c'est-à-dire à trouver des bits $x_1, \ldots, x_n \in \{0, 1\}$ tels que

$$\sum_{i=1}^{n} x_i w_i = t \bmod q.$$

Ce problème $\mathcal{NP}$-complet (dans sa variante de décision naturelle) est considéré en cryptographie depuis les années 1980 comme une alternative intéressante aux hypothèses algorithmiques fondées sur la théorie des nombres. Il est en particulier censé fournir une sécurité dite *post-quantique*.

Nous nous sommes posés la question de l'existence d'un système à divulgation nulle de connaissance pour ce problème. Nous avons trouvé que plusieurs protocoles avaient été proposés (notamment dans [1, 2, 4, 6]) mais D. Vergnaud a eu une idée pour améliorer leur efficacité en utilisant une variante de la technique *MPC-in-the-head* qu'il venait justement d'étudier pour préparer l'un des cours. Il a présenté cette idée à une audience large lors de la réunion de lancement du projet ANR SANGRIA dont il est le coordinateur. Th. Feneuil (doctorant sous la direction de J.-C. Bajard, A. Joux et M. Rivain, au sein de la société CryptoExperts) était présent à cette réunion et a proposé des améliorations. Nous avons entamé une collaboration avec J. Maire (doctorant qui venait de commencer sa thèse au sein de l'équipe ALMASTY) et M. Rivain qui a abouti en la publication de ce travail à la conférence Asiacrypt 2022 [3].

La genèse de cet article illustre assez bien le fonctionnement de l'équipe ALMASTY avec une interaction importante entre l'enseignement et la recherche, des discussions ouvertes entre les membres (anciens et présents) de l'équipe et des interactions fortes avec le monde académique et le monde industriel.

3 PRÉSENTATION DE CET ÉLÉMENT

Dans ce travail, nous proposons des systèmes d'argument de connaissance à divulgation nulle de connaissance pour le problème de la somme modulaire de sous-ensembles. Les approches combinatoires précédentes, notamment celle due à Shamir, donnaient des arguments avec une complexité de communication cubique (dans le paramètre de sécurité). Des méthodes plus récentes, basées sur la technique *MPC-in-the-head*, produisent également des arguments avec une complexité de communication cubique (et seulement pour des modules q premiers).

Nous améliorons cette approche en utilisant un partage de secret sur de petits entiers (plutôt que modulo q) pour réduire la taille des arguments et supprimer la restriction du module premier. Comme ce partage peut révéler des informations sur le sous-ensemble secret, nous introduisons l'idée de rejet dans le paradigme *MPC-in-the-head*. Un soin particulier doit être apporté pour équilibrer les propriétés de complétude et de solidité et préserver la propriété de divulgation nulle de connaissance. Nous combinons cette idée avec deux techniques pour prouver

que le vecteur secret $(x_1, \ldots, x_n)$ (qui sélectionne le sous-ensemble) est bien constitué de coordonnées binaires. Nos nouvelles techniques ont l'avantage significatif d'aboutir à des arguments de taille indépendante du module q.

Nos nouveaux protocoles pour le problème de la somme modulaire de sous-ensembles réalisent une amélioration asymptotique en produisant des arguments de taille quadratique. Cette amélioration est également pratique : pour un module q de 256 bits la meilleure variante de nos protocoles produit des arguments de 13 Ko, alors que les propositions précédentes donnaient des arguments de 1180 Ko, pour le meilleur protocole général, et de 122 Ko, pour le meilleur protocole limité aux modules premiers. Nos techniques peuvent également être appliquées à des variantes vectorielles du problème de la somme modulaire de sous-ensembles et, en particulier, au problème des solutions entières courtes inhomogènes (*Inhomogeneous Small Integer Solution, ISIS*), pour lequel elles offrent une alternative efficace aux meilleurs protocoles connus lorsque l'anneau sous-jacent n'est pas petit et compatible avec les transformées en nombres entiers (*Number Theoretic Transform, NTT*). Nous montrons également comment adapter notre protocole pour construire des arguments efficaces de connaissance à divulgation nulle de connaissance d'un texte en clair ou de la clé dans le contexte du chiffrement complètement homomorphe. Lorsqu'ils sont appliqués au schéma TFHE, les arguments obtenus sont plus de 20 fois plus petits que ceux obtenus avec les protocoles précédents. Enfin, nous utilisons notre technique pour construire un schéma de signature numérique efficace basé sur une fonction pseudo-aléatoire due à Boneh-Halevi-Howgrave-Graham. La taille des signatures obtenues (environ 5 Ko pour un niveau de sécurité de 128 bits) est la plus courte parmi toutes les autres signatures basées sur le paradigme *MPC-in-the-Head*. Ce protocole a déjà donné lieu à des travaux ultérieurs (notamment un protocole de *mise en gage* disposant d'arguments à divulgation nulle de connaissance [5]).

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Carsten Baum and Ariel Nof. Concretely-efficient zero-knowledge arguments for arithmetic circuits and their application to lattice-based cryptography. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 495–526. Springer, 2020.

[2] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Efficient identification schemes using two prover interactive proofs. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 498–506. Springer, 1989.

[3] Thibauld Feneuil, Jules Maire, Matthieu Rivain, and Damien Vergnaud. Zero-knowledge protocols for the subset sum problem from MPC-in-the-head with rejection. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings*, volume 13792 of *Lecture Notes in Computer Science*, page 371–402. Springer, 2022.

[4] San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*, volume 7778 of *Lecture Notes in Computer Science*, pages 107–124. Springer, 2013.

[5] Jules Maire and Damien Vergnaud. Commitments with efficient zero-knowledge arguments from subset sum problems. In Mauro Conti and Gene Tsudik, editors, *Computer Security - ESORICS 2023 - 28th European Symposium on Research in Computer Security, The Hague, Netherlands, September 25-29, 2023, Proceedings*, volume to appear of *Lecture Notes in Computer Science*. Springer, 2023.

[6] Adi Shamir. A zero-knowledge proof for knapsacks. presented at a workshop on Probabilistic Algorithms, Marseille, March 1986.