Diverse modules et preuves à divulgation nulle de connaissance

Fabrice Benhamouda [1]

Prix de thèse Gilles Kahn 2016

Fabrice Benhamouda a soutenu sa thèse [2] en juillet 2016 à l'École normale supérieure de Paris (membre de l'université de recherche Paris Sciences et Lettres), sous la direction de Michel Abdalla et David Pointcheval. Il effectue actuellement un stage postdoctoral au sein de l'équipe de cryptographie d'IBM Research à New York aux États-Unis.

Les arguments ou preuves à divulgation nulle de connaissance sont des primitives cryptographiques fondamentales introduites par Goldwasser, Micali et Rackoff en 1985 [13] et considérées comme l'une des contributions les plus importantes de Goldwasser et Micali dans le communiqué leur décernant le prix Turing en 2012 [3]. Ils permettent à un utilisateur, appelé prouveur, de démontrer à un autre utilisateur, appelé vérifieur, qu'un certain fait est vrai, sans révéler aucune information, si ce n'est la véracité de ce fait. Les faits considérés sont l'appartenance d'un mot à un langage NP. Les applications des arguments à divulgation nulle de connaissance sont innombrables en cryptographie, où ils sont en général incontournables dans les constructions de protocoles sécurisés.

1. https://www.normalesup.org/~fbenhamo
2. https://hal.inria.fr/tel-01399476
3. http://www.acm.org/press-room/awards/turing-award-12

Par exemple, de tels arguments sont utilisés par le système de vote électronique *Helios*[4] pour s'assurer que les utilisateurs forment correctement leur bulletin de vote. Du fait de l'importance des arguments à divulgation nulle de connaissance, de nombreuses variantes ont été considérées pour satisfaire différentes applications. Les outils développés dans cette thèse permettent la construction d'un certain nombre de ces variantes.

Les *smooth* (ou *universal*) *projective hash functions* (SPHFs) ont été introduites par Cramer et Shoup en 2002 [11]. Depuis, elles ont trouvé de nombreuses autres applications : les schémas d'authentification par mot de passe [14, 12, 7, 1] qui sont maintenant utilisés dans le protocole *Thread*[5] de *Nest* pour l'Internet des objets ; les schémas d'*oblivious transfer* [1] qui sont une brique de base de nombreux protocoles de calcul sécurisé ; et les signatures en blanc [10, 7], utiles pour la monnaie électronique notamment. Les SPHFs peuvent être vues comme des preuves implicites d'appartenance à certains langages.

Au cours de cette thèse, nous avons non seulement étendu la classe des langages supportés par les SPHFs, mais aussi montré comment adjoindre des propriétés additionnelles aux SPHFs et comment utiliser ces propriétés additionnelles pour renforcer la sécurité des applications susmentionnées. Pour cela, nous avons proposé la notion de *diverse modules*, qui généralise la notion de *diverse vector spaces* déjà présente dans l'article original de Cramer et Shoup mais que nous avons exploitée et développée dans nos papiers.

Un *diverse module* est essentiellement une représentation d'un langage, comme un sous-module d'un module plus grand, un module étant un espace vectoriel sur un anneau. À n'importe quel *diverse module* est associée une SPHF pour le même langage. Par ailleurs, presque toutes les SPHFs actuelles sont construites de cette manière ou pourraient l'être sans perte d'efficacité.

La notion de *diverses modules* présente de nombreux avantages. Tout d'abord, les *diverse modules* facilitent grandement la construction de SPHFs pour des langages complexes. Ensuite, ils peuvent aisément être combinés et étendus, de façon à ce que les SPHFs résultantes correspondent à la conjonction ou la disjonction des langages des SPHFs originales, ou de façon à ce qu'elles satisfassent des propriétés additionnelles utiles pour des applications plus complexes ou plus sûres [9]. Enfin, les *diverse modules* ont permis la construction des premiers arguments non-interactifs à divulgation nulle de connaissance et *one-time simulation-sound* (une propriété très forte) pour les langages linéaires sur les groupes cycliques, où la preuve est constituée d'un seul élément de groupe, même si le témoin du langage est arbitrairement grand [5].

Si le manuscrit de thèse se concentre sur les SPHFs et leurs applications aux preuves à divulgation nulle de connaissance, nos contributions ne se limitent pas

4. `https://heliosvoting.org`
5. `https://www.threadgroup.org`

à ce thème. En particulier, nous avons aussi proposé un cadre général algébrique pour la construction et la preuve de sécurité des fonctions pseudo-aléatoires (PRFs) et d'extensions de ces PRFs [4, 2, 3]. Nous nous sommes également intéressé à la quantité d'aléa nécessaire dans certaines implémentations sécurisées de primitives cryptographiques [6]. Nous avons aussi étudié les preuves à divulgation nulle de connaissance sur les réseaux euclidiens [8] qui peuvent potentiellement offrir des solutions cryptographiques sûres contre les ordinateurs quantiques.

Références

[1] M. Abdalla, F. Benhamouda, O. Blazy, C. Chevalier, and D. Pointcheval. SPHF-friendly non-interactive commitments. In *ASIACRYPT 2013*.

[2] M. Abdalla, F. Benhamouda, and A. Passelègue. An algebraic framework for pseudorandom functions and applications to related-key security. In *CRYPTO 2015*.

[3] M. Abdalla, F. Benhamouda, and A. Passelègue. Multilinear and aggregate pseudorandom functions : New constructions and improved security. In *ASIACRYPT 2015*.

[4] M. Abdalla, F. Benhamouda, A. Passelègue, and K. G. Paterson. Related-key security for pseudorandom functions beyond the linear barrier. In *CRYPTO 2014*.

[5] M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems : New constructions and applications. In *EUROCRYPT 2015*.

[6] S. Belaïd, F. Benhamouda, A. Passelègue, E. Prouff, A. Thillard, and D. Vergnaud. Randomness complexity of private circuits for multiplication. In *EUROCRYPT 2016*.

[7] F. Benhamouda, O. Blazy, C. Chevalier, D. Pointcheval, and D. Vergnaud. New techniques for SPHFs and efficient one-round PAKE protocols. In *CRYPTO 2013*.

[8] F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, and G. Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *ASIACRYPT 2014*.

[9] F. Benhamouda, G. Couteau, D. Pointcheval, and H. Wee. Implicit zero-knowledge arguments and applications to the malicious setting. In *CRYPTO 2015*.

[10] O. Blazy, D. Pointcheval, and D. Vergnaud. Round-optimal privacy-preserving protocols with smooth projective hash functions. In *TCC 2012*.

[11] R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT 2002*.

[12] R. Gennaro and Y. Lindell. A framework for password-based authenticated key exchange. In *EUROCRYPT 2003*.

[13] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *ACM STOC 1985*.

[14] J. Katz, R. Ostrovsky, and M. Yung. Efficient password-authenticated key exchange using human-memorable passwords. In *EUROCRYPT 2001*.