

Diverse modules and zero-knowledge

Fabrice Ben Hamouda--Guichoux

Le manuscrit de thèse et ce résumé se concentrent sur un des axes principaux de mon travail de thèse : les *diverse modules*, leurs liens avec les *smooth* (ou *universal*) *projective hash functions* (SPHF), et leurs applications aux arguments à divulgation nulle de connaissance (*zero-knowledge*).

Les arguments ou preuves à divulgation nulle de connaissance sont des primitives cryptographiques fondamentales introduites par Goldwasser, Micali et Rackoff en 1985. 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. Par exemple, de tels arguments sont utilisés par le système de vote électronique *Helios* 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* (SPHF) ont été introduites par Cramer et Shoup en 2002. Depuis, elles ont trouvé de nombreuses autres applications : les schémas d'authentification par mot de passe qui sont maintenant utilisés dans le protocole *Thread* de *Nest* pour l'Internet des objets ; les schémas d'*oblivious transfer* qui sont une brique de base de nombreux protocoles de calcul sécurisé ; et les signatures en blanc, utiles pour la monnaie électronique notamment. Les SPHF 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 SPHF, mais aussi montré comment adjoindre des propriétés additionnelles aux SPHF et comment utiliser ces propriétés additionnelles pour renforcer la sécurité des applications sus-citées. 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 SPHF actuelles sont construites de cette manière ou pourraient l'être sans perte d'efficacité.

La notion de *diverse modules* présente de nombreux avantages. Tout d'abord, les *diverse modules* facilitent grandement la construction de SPHF pour des langages complexes. Ensuite, ils peuvent aisément être combinés et étendus, de façon à ce que les SPHF résultantes correspondent à la conjonction ou la disjonction des langages des SPHF originales, ou de façon à ce qu'elles satisfassent des propriétés additionnelles utiles pour des applications plus complexes ou plus sûres. 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.

Si le manuscrit de thèse se concentre sur les SPHF et leurs applications aux preuves à divulgation nulle de connaissance, nos contributions ne se limitent pas 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 (PRF) et d'extensions de ces PRF. Nous nous sommes également intéressés à la quantité d'aléa nécessaire dans certaines implémentations sécurisées de primitives cryptographiques.