Ecole Doctorale STIC
Sciences & Technologies de l'Information et de la Communication

ED STIC - Proposition de Sujets de Thèse

pour la campagne d'Allocation de thèses 2011

Titre du sujet :	Preuve formelle de la prochaine fonction de hash SHA3
Mention de thèse :	Informatique
HDR Directeur de thèse inscrit à l'ED STIC :	Bertot Yves

Co-encadrant de thèse éventuel :

Nom :	Grégoire
Prénom :	Benjamin
Email :	Benjamin.Gregoire@inria.fr
Téléphone :	0492387559

Email de contact pour ce sujet :	Benjamin.Gregoire@inria.fr
Laboratoire d'accueil :	INRIA

Description du sujet :

La cryptographie joue un rôle essentiel dans le développement de solutions logicielles sûres. Néanmoins, il s'est avéré extrèmement difficile de concevoir des primitives cryptographiques correctes et d'imposer qu'elles soient utiliser correctement. L'histoire de la cryptographie abonde d'exemples de primitives et de protocoles cryptographiques très utilisés mais non-sûrs.

Pour des preuves à la main, les primitives cryptographiques sont devenues essentiellement invérifiables et les spécialistes en cryptologie militent pour le développements de techniques qui aident à maîtriser la complexité de leurs preuves. Les techniques basées sur les jeux sont une approche populaire: les preuves sont structurées en séquences de jeux, où les étapes de preuves établissent la validité de transitions entre deux jeux successifs. Les techniques basées sur les programmes forment une instance de cette approche. Les jeux sont présentés comme des programmes et la théorie des langages de programmation est utilisée pour justifier les étapes de

raisonnement. Même avec cette approche les preuves peuvent être longues et complexes, si bien que la vérification formelle est nécessaire pour atteindre un niveau de confidence élevé.

La bibliothèque CertyCrypt permet de vérifier formellement ce type de preuve en Coq. Elle a été utilisée pour prouver la sécurité sémantique de différentes primitives de cryptage et de signature (comme ElGama, Hashed-ElGamal, OAEP, FDH).

En 2007, l'institut américain des standards et technologies (NIST) a lancé une compétition pour développer un nouveau standard de fonction de hash. Cette compétition a été lancé en réponse aux faiblesses découvertes pour les fonctions de has connues sous le nom de md4 et md5. Cette compétition a reçu 64 soumissions (par comparaison AES avait reçu 14 soumissions en 1998). La nouvelle fonction de hash sera probablement annoncée avant le printemps 2012.

Le but de cette thèse est de fournir des preuves formelles vérifiées entièrement formellement pour l'algorithme en utilisant CertiCrypt. Dans un second temps, le but sera d'étendre les méthodologies développées pour CertiCrypt au langage C, de façon à fournir une preuve formelle complète de l'implémentation.

English version:

Cryptography plays an essential role in the development of secure
software solutions; yet it has proved extremely difficult to design
correct cryptographic primitives and to enforce their correct usage:
the history of cryptography is fraught with examples of widely used yet
unsecure primitives and protocols.

For pen-and-paper proofs, cryptographic primitives proofs have become
essentially unverifiable and cryptographers have argued in favor of
techniques that help tame the complexity of their proofs.
Game-based techniques provide a popular approach in which proofs are
structured as sequences of games,
and in which proof steps establish the validity of transitions between
successive games. Code-based techniques form an instance of this approach.
They take a code-centric view of games and rely on programming
language theory to justify proof steps. While code-based techniques
contribute to formalize the security statements precisely and to carry out
proofs systematically, typical proofs are so long and involved that formal
verification is necessary to achieve a high degree of confidence.

The CertiCrypt library allows to formally check this kind of proofs in Coq.
It has been used to prove the semantic security of different encryption and
signature primitives (like ElGamal, Hashed-ElGamal, OAEP, FDH).

In 2007, the National Institute of Standards and Technology (NIST)
launched a competition to develop the new standard for hash functions.

The competition was launched partially in response to major weaknesses in hash functions such as MD4 and MD5, and received very significant attention with 64 submissions (in contrast, there were 15 submissions for the Advanced Encryption Standard AES in 1998).
The new hash function will (tentatively) be announced by Spring 2012.

The goal of this thesis is to provide fully verified proofs for at least one submission (most likely Skein by Schneier et al.).
The verification will establish that the algorithm and its implementation verify relevant properties of hash functions: pre-image resistance, collision-resistance, second pre-image resistance, and pseudo-randomness.
The results will be used to actively promote the adoption of formal proofs by standardization bodies and by the cryptographic community.

In a first time, we will focus on providing fully verified proofs of the algorithm using CertiCrypt. In a second time, the goal will be to extend the methodologies developed in CertiCrypt to C, this will allows to provide fully verified proofs of the implementation.