UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

PRIMITIVES ET PROTOCOLES CRYPTOGRAPHIQUES À SÉCURITÉ PROUVÉE

Par Monsieur Yannick SEURIN Discipline : Cryptographie Laboratoire : PRISM

Nous abordons deux aspects complémentaires de la sécurité prouvée en cryptographie.

soutenance de thèse

Dans une première partie, nous étudions la relation existant entre les deux modèles idéalisés les plus utilisés pour les preuves de sécurité : le modèle de l'oracle aléatoire et le modèle du chiffrement par blocs idéal. Nous montrons que ces deux modèles sont en fait équivalents : l'existence d'un cryptosystème sûr dans l'un des modèles implique l'existence d'un cryptosystème réalisant la même fonctionnalité et sûr dans l'autre modèle. En particulier, nous montrons dans le cadre de la théorie de l'indifférentiabilité que si un cryptosystème utilisant un chiffrement par blocs idéal est sûr, alors le cryptosystème reste sûr en remplaçant le chiffrement par blocs par la construction de Luby-Rackoff à 6 tours où les fonctions internes sont des oracles aléatoires publiquement accessibles.

Dans une seconde partie, nous étudions les protocoles cryptographiques fondés sur le problème LPN (*Learning Parity with Noise*). La proposition du schéma d'authentification HB+ par Juels et Weis à CRYPTO 2005 a suscité un très grand intérêt et de nombreuses variantes cherchant à renforcer la sécurité de ce protocole contre les attaques *man-in-the-middle* ont été proposées par la suite. Nous présentons des cryptanalyses de trois de ces variantes (HB++, HB*, et HB-MP), puis proposons les protocoles HB# et RANDOM-HB#. La sécurité de ce dernier contre une classe restreinte d'attaques *man-in-the-middle* peut être prouvée sous l'hypothèse de la difficulté du problème LPN. Nous proposons également un schéma de chiffrement probabiliste symétrique dont la sécurité contre les attaques à clairs choisis peut être réduite à la difficulté du problème LPN.

Abstract :

We address two complementary aspects of provable security in cryptography.

Firstly, we study the relation between two idealised models widely used in security proofs, the random oracle model and the ideal block cipher model. We prove that these two models are in fact equivalent: the existence of a cryptosystem secure in one of the models implies the existence of a cryptosystem realising the same functionality and secure in the other model. In particular, we prove in the indifferentiability framework that if a cryptosystem using an ideal block cipher is secure, then this cryptosystem remains secure when the block cipher is replaced by the Luby-Rackoff construction with 6 rounds where the inner functions are publicly accessible random oracles.

Then, we study cryptographic protocols based on the LPN problem (*Learning Parity with Noise*). The authentication protocol HB+ proposed by Juels and Weis at CRYPTO 2005 aroused much interest and several variants seeking to reinforce the security of this protocol against man-in-the-middle attacks were subsequently proposed. We present a cryptanalysis of three of these variants (HB++, HB*, and HB-MP), and then we propose the protocols HB# and RANDOM-HB#. The security of RANDOM-HB# against a limited class of man-in-the-middle attacks can be proven under the assumption of the difficulty of the LPN problem. We also propose a probabilistic symmetric encryption scheme whose security against chosen plaintext attacks can be reduced to the difficulty of the LPN problem.

Membres du jury :

David POINTCHEVAL, *Directeur de Recherche à l'Ecole Normale Supérieure, Paris - Rapporteur*
Serge VAUDENAY, *Professeur à l'Ecole Polytechnique Fédérale de Lausanne, Suisse - Rapporteur*
Jacques PATARIN, *Professeur à l'Université de Versailles Saint-Quentin-en-Yvelines - Directeur de Thèse*
Mihir BELLARE, *Professeur à l'Université de Californie San Diego, USA - Examinateur*
Anne CANTEAUT, *Directeur de Recherche à l'INRIA-Rocquencourt, Le Chesnay - Examinateur*
Pierre-Alain FOUQUE, *Maître de Conférences à l'Ecole Normale Supérieure, Paris - Examinateur*
Henri GILBERT, *Directeur de Recherche à Orange Labs Division R&D, Issy les Moulineaux - Examinateur*

Dernière mise à jour de cette page : 19 juin 2009