

Mise en accord de clé au sein d'un groupe avec authentification par mot de passe

- Thématique : cryptologie
- Lieu du stage : Laboratoire d'Informatique de l'École normale supérieure
- Ville : Paris
- Équipe de Cryptographie – <http://www.di.ens.fr/CryptoGroup.html>
- Directeur de stage : David Pointcheval
<http://www.di.ens.fr/users/pointche> – David.Pointcheval@ens.fr

- Présentation générale du domaine :

Ce stage sera effectué dans l'équipe de cryptographie du Laboratoire d'Informatique de l'ENS qui est l'une des principales équipes de recherche en cryptographie en Europe.

La mise en accord de clé est une primitive cryptographique permettant à des individus d'établir un canal sécurisé. Afin de garantir l'identité des personnes impliquées, elles doivent s'authentifier. Une méthode classique consiste à reposer sur une infrastructure de clés publiques, en signant les échanges. Nous voulons nous affranchir d'une telle infrastructure difficile à mettre en œuvre : les individus vont s'authentifier à l'aide d'un simple mot de passe.

De tels protocoles de mise en accord de clés entre deux individus authentifiés par un mot de passe existent et sont efficaces [1, 2, 3, 5, 6, 7]. En revanche, lorsqu'il s'agit d'établir une telle clé au sein d'un groupe, peu de schémas existent, et l'efficacité n'est pas au rendez-vous [4].

- Objectifs du stage :

Notre équipe est en cours d'étude d'un nouveau protocole de mise en accord de clé de session au sein d'un groupe, avec authentification par mot de passe, qui est efficace (seulement 2 ou 3 échanges sont nécessaires, contrairement aux propositions précédentes). Le but de ce stage serait tout d'abord de se familiariser avec les outils cryptographiques utilisés, puis d'implémenter ce protocole via des applets java.

- Connaissances préalables : un peu de théorie des nombres, programmation en java.

Références¹

- [1] M. Abdalla, O. Chevassut, and D. Pointcheval. One-time Verifier-based Encrypted Key Exchange. In *PKC '05*, LNCS 3386, Springer-Verlag, 2005.
- [2] M. Abdalla and D. Pointcheval. Simple Password-Based Encrypted Key Exchange Protocols. In *CT-RSA '05*, LNCS, Springer-Verlag, 2005.
- [3] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated Key Exchange Secure Against Dictionary Attacks. In *EUROCRYPT '00*, LNCS 1807, Springer-Verlag, 2000.
- [4] E. Bresson, O. Chevassut, and D. Pointcheval. Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks. In *ASIACRYPT '02*, LNCS 2501, Springer-Verlag, 2002.
- [5] E. Bresson, O. Chevassut, and D. Pointcheval. Security Proofs for Efficient Password-Based Key Exchange. In *ACM CCCS '03*, ACM Press, 2003.
- [6] E. Bresson, O. Chevassut, and D. Pointcheval. New Security Results on Encrypted Key Exchange. In *PKC '04*, LNCS 2947, Springer-Verlag, 2004.
- [7] D. Catalano, D. Pointcheval, and T. Pornin. IPAKE : Isomorphisms for Password-based Authenticated Key Exchange. In *CRYPTO '04*, LNCS 3152, Springer-Verlag, 2004.

¹toutes disponibles sur <http://www.di.ens.fr/users/pointche>.