Échange de clé authentifié par mot de passe post-quantique

La sécurité de nombreuses applications informatiques repose sur la cryptographie symétrique, mais la clé commune (dite « de session ») est échangée via la cryptographie asymétrique. Cette dernière est cependant vulnérable à l'attaque dite de l'« homme du milieu ». Pour l'éviter, il est nécessaire que les interlocuteurs s'authentifient mutuellement. Cela se fait généralement, par exemple sur le web, en utilisant des infrastructures à clés publiques, mais les ressources et la connectivité qu'elles requièrent en font des solutions inadaptées dans certains cas, notamment pour la lecture des données biométriques sur les cartes d'identité et passeports. Dans ce cas, une authentification par mot de passe, y compris de faible entropie (comme un code PIN), peut être utilisée, formant un protocole appelé PAKE (*Password Authenticated Key Exchange*) et sécurisé face aux attaques hors-ligne sur des communications interceptées.

Notre PSC a consisté à élaborer un PAKE post-quantique, c'est-à-dire résistant aux attaques qui seraient menées par un ordinateur quantique. Celui-ci est fondé sur le protocole CAKE publié par un groupe de chercheurs auquel appartient notre tutrice Mélissa Rossi.

Pour rendre ce protocole amont effectivement implémentable, nous avons résolu plusieurs problèmes théoriques. Pour empêcher les attaques *offline*, il était en particulier nécessaire d'encoder et de chiffrer du matériel cryptographique de manière à ce que le chiffré soit indiscernable d'une chaîne tirée aléatoirement. Nous avons aussi proposé un algorithme de chiffrement symétrique qui vérifie les propriétés de sécurité particulières de l'*ideal cipher*.

Une fois ces difficultés théoriques résolues, nous avons développé puis publié deux implémentations de CAKE en Python et en C, la première à des fins de démonstration algorithmique et la seconde pour estimer les performances plus précisément. Sur cette base, nous avons réalisé un démonstrateur physique fondé sur une *Raspberry Pi*. Celui-ci nous a permis de conclure notre PSC par des études de performance.

Nos travaux sont publiquement disponibles à l'adresse suivante : `https://github.com/pq-pake`.

Projet scientifique collectif INF08 — 2023-2024

Christopher Calvet, Guillaume Chirache, Timothée Fisher,
Thomas Sauvage et Emre Ucar

Encadrés par Mélissa Rossi