Université Gaston Berger de Saint-Louis

(U. G. B.)

UFR Sciences Appliquées et Technologiques

(S. A. T.)

ÉCOLE DOCTORALE DES SCIENCES ET DES TECHNOLOGIES

Projet de thèse

M. Mamadou Makhtar LO

Email : lo.mamadou-makhtar@ugb.edu.sn

Année académique 2020-2021

Table des matières

1. Chiffrement Unidirectionnel et Chiffrement Bidirectionnel

1.1. **Contexte.** Un des objectifs de base de la cryptographie en général et du chiffrement en particulier est d'assurer la confidentialité de données. Il paraît même nécessaire qu'un système de chiffrement ne peut permettre l'accès au message(texte clair) qu'au destinataire du texte chiffré. Ainsi, transférer le texte clair à un autre destinataire nécessiterait un accès au texte clair et à la clé de chiffrement de l'autre destinataire.
Cependant avec le développement des outils technologiques tels que le stockage sur réseau (Drive, iCloud, Mega etc..), le Cloud Computing ou le transfert de fichiers entre objets connectés (IoT), il devient nécessaire de permettre le partage de données et le contrôle d'accès des utilisateurs du réseau tout en assurant la sécurité des données. En 1998, Matt Blaze et al. [2] introduisait la notion de *atomic proxy functions* qui permettrait de transformer un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé sans pour autant avoir accès au texte clair ou aux clés de déchiffrement. On parle de serveur de re-chiffrement ou *Proxy Re-Encryption*(PRE).

Les PRE qui étaient à l'origine conçus pour être des systèmes de suivi de courriers chiffrés sont aujourd'hui utilisés pour le contrôle d'accès et les partages de données notamment en *Cloud Computing*. [4] [1] [9].
Dans leurs travaux, Blaze and al. [2] proposèrent un schéma de PRE basé sur El Gamal [5]. Toutefois, il aura fallu attendre Ateniese et Al. [1] pour avoir une première définition formelle des PRE et de leurs modèles de sécurité. On a ainsi pu observer une évolution des PRE ces vingt dernières années avec la construction de nouveaux modèles, des preuves de sécurité et une utilisation plus large.

1.2. **Définitions.** Un schéma de serveur de re-chiffrement peut être défini par la donnée de cinq algorithmes {*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*} tels que :

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.

— *Re-Chiffrer* transforme (re-chiffre) à l'aide de la *clé proxy* un texte chiffré pour le délégant en un texte chiffré pour le délégué.
— *Dechiffrer* déchiffre le texte chiffré à l'aide de la clé de déchiffrement.

Ainsi, suivant la confiance entre le délégant(*Alice*) et le délégué (*Bob*), on peut distinguer deux catégories de PRE : celle basée sur le ***chiffrement bidirectionnel*** et celle sur le ***chiffrement unidirectionnel***.

1.2.1. *Chiffrement Bidirectionnel.* Pour un schéma de serveur de re-chiffrement bidirectionnel, la *clé proxy* utilisée pour transformer un chiffré pour *Alice* en un chiffré pour *Bob* peut aussi être utilisée pour transformer un texte chiffré pour *Bob* en un texte pour *Alice*.
Le schéma proposé par Blazer en 1998 peut être considéré comme bidirectionnel.

1.2.2. *Chiffrement Unidirectionnel.* Contrairement au bidirectionnel, un serveur de re-chiffrement unidirectionnel ne permet la délégation que dans un sens. Ivan et Al. [6] seront les premiers en 2003 à construire une méthode générique pour construire un schéma pouvant être considéré comme unidirectionnel.

2. Problématique et Objectifs

2.1. **Problématique.** Le modèle proposé par Blaze et Al.[**?**] en 1998 ne résistait pas aux attaques par collusion, le proxy et le délégué pouvait aussi toujours collaborer pour retrouver la clé du délégant. En 2003, Ivan et Al.[6] proposeront une méthode générique pour construire un serveur de re-chiffrement unidirectionnel, toutefois ces schémas ne résistaient toujours pas à l'attaque par collusion et n'optimiser pas l'utilisation des clés.
Cependant, en 2005, Ateniese et Al. [1] formalisent la notion de PRE et ses modèles de sécurité et construisent un schéma PRE résistant aux attaques par collusion et achevant une sécurité CPA. Ils posèrent le problème de la construction de modèle achevant la sécurité CCA. Plusieurs modèles ont pu ainsi être construits : Canetti et Al. avec un PRE bidirectionnel et CCA-sûr (2007)[3], Libert et Al. avec un PRE unidirectionnel RCCA-sûr (2008) [8], Shao et Al. avec le premier modèle CCA-sûr sans forme bilinéaire(2009)[10], Kirshanova et Al avec leur modèle basé sur LWE et CCA-sûr(2014)[7]...

2.2. **Objectifs Scientifiques.** De manière concrète, nous nous intéresserons dans ce travail aux aspects théoriques et pratiques des serveurs de re-chiffrement unidirectionnel et de re-chiffrement bidirectionnel. Nous travaillerons, en particulier, sur les modèles de sécurité et la construction de schémas efficaces et leurs applications.

2.3. **Méthodologie de recherche.** La recherche couvrira tous les aspects théoriques et pratiques de la question, notamment :
— les aspects définitionnels, par l'analyse des modèles existants et la proposition éventuelle de nouveaux modèles ;
— les aspects cryptographiques théoriques par l'analyse des modèles de sécurité et le design de ;

— les aspects cryptographiques pratiques par l'implantation et le déploiement de schémas à sécurité prouvée dans les modèles proposées.

Visa des encadreurs

Pr. Mohamed Ben MAAOUIA

Dr. Demba SOW

Références

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1) :1–30, 2006.

[2] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, *Advances in Cryptology — EUROCRYPT'98*, pages 127–144, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[3] Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 185–194, 2007.

[4] Julien Devigne. *Protocoles de re-chiffrement pour le stockage de données*. Theses, Université de Caen, December 2013.

[5] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4) :469–472, 1985.

[6] Anca-Andreea Ivan and Yevgeniy Dodis. Proxy cryptography revisited. In *NDSS*, 2003.

[7] Elena Kirshanova. Proxy re-encryption from lattices. In *International Workshop on Public Key Cryptography*, pages 77–94. Springer, 2014.

[8] Benoît Libert and Damien Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. In *International Workshop on Public Key Cryptography*, pages 360–379. Springer, 2008.

[9] Yepeng Liu, Yongjun Ren, Qirun Wang, and Jinyue Xia. The development of proxy re-encryption. *Journal of Cybersecurity*, 2(1) :1, 2020.

[10] Jun Shao and Zhenfu Cao. Cca-secure proxy re-encryption without pairings. In *International Workshop on Public Key Cryptography*, pages 357–376. Springer, 2009.