Application du système cryptographique Shamir's Secret Sharing en finance : l'authentification bancaire

Hamza BA-MOHAMMED

Concours National Commun 2021

Sommaire :

0.1 Positionnement thématique

MATHÉMATIQUES (Algèbre), MATHÉMATIQUES (Arithmétiques modulaire), INFORMATIQUE (Cryptographie)

0.2 Professeur encadrant du candidat

Mr Mustapha LAAMOUM

0.3 Motivation

Etant passionné par la cryptographie depuis que j'ai appris à coder un programme qui décrypte le chiffrement de César au lycée, je choisis de soutenir mon TIPE sur un système cryptographique plus avancé afin d'avoir une excellente opportunité de développer mes connaissances dans ce domaine fascinant.

0.4 Ancrage

La sécurité des données numériques s'avère un des plus grands enjeux sociétaux du 21e siècle. Le développement de systèmes cryptographiques forts et optimaux est donc une nécessité pour répondre à ce besoin, d'où l'utilité de cette recherche.

0.5 Mots-clés

en français :	en anglais :
Le partage de clé secrète de Shamir	*Shamir's Secret Sharing*
Cryptographie	*Cryptography*
Interpolation de Lagrange	*Lagrange's interpolation*
Méthode formelle	*Formal method*
Authentification	*Authentication*

0.6 Bibliographie commentée

La cryptographie est une discipline qui permet de chiffrer des données dans le but de les protéger et limiter leur accès en assurant 3 critères primaires : la confidentialité, l'authenticité et l'intégrité des informations cryptées. De nos jours, la cryptographie figure un acteur principal dans plusieurs activités humaines, notamment la protection de la vie privée et les différents échanges virtuels. [3]

Prouver la sécurité d'un système cryptographique est une étape primordiale avant de l'adopter, surtout quand il vise des missions de haute sensibilité, en particulier dans les domaines militaire, financier et aérospatial. On utilise dans ce cas des preuves mathématiques rigoureuses, qu'on nomme la méthode formelle, et qui permet de recouvrer tous les cas d'attaque possibles en théorie. Cette méthode s'avère beaucoup plus rapide et sûre que la méthode calculatoire qui, par contre, évolue le fonctionnement du système expérimentalement dans le maximum de situations possibles limitées par les performances techniques du simulateur, laissant toujours une marge d'incertitude plus large associée aux situations les plus exotiques. [5]

Le besoin d'une méthode efficace pour partager un secret entre plusieurs personnes est devenu rapidement une question fréquente dans la communauté informatique, toutefois sans réponse, jusqu'à ce que le cryptologue Adi Shamir, eut l'idée du système cryptographique ainsi connu sous son nom pour répondre à ce besoin, et qu'il publia dans une feuille scientifique depuis l'Institut de Technologies de Massachusetts (MIT) en novembre 1979. [4]

Le système cryptographique Shamir's Secret Sharing (SSS) permet de partager un secret S numérique (ou converti au format numérique) entre un groupe de N personnes tel qu'il faut un minimum de K personnes quelconques parmi les N personnes pour pouvoir reconstruire le secret S. L'idée consiste à génerer un polynôme P de degré $K-1$ sur un corps fini Z/pZ (p premier), tel que son coefficient constant est le message S. Avec ce polynôme, on peut créer des couples $(X_i, P(X_i) \mod p)$ qui sont les clés privées. Pratiquement, leur nombre est limité par les bits de codage du matériel informatique, qui peut aller pourtant jusqu'à 128 bits ou plus. Ainsi, en utilisant l'interpolation de Lagrange et avec K clés ou plus, on peut retrouver le secret $S = P(0)$,

et l'obtention de n'importe quel nombre M de clés inférieur strictement à K ne permet aucune information supplémentaire sur le secret crypté. Le nombre p doit être stictement supérieur à tous les coefficients du polynôme, y compris le secret S [4]. La génération de grands nombres premiers peut être suffisamment optimisée grâce à l'algorithme des cribles d'Eratosthène[2]. Entre autres, ceci implique l'appel d'autres méthodes de calcul en arithmétique des corps finis, notamment l'inverse p-modulaire en interpolation de Lagrange, qui peut être calculé facilement avec le petit théorème de Fermat, étant donné la primalité du nombre p[2] . Par ailleurs, cet algorithme a été prouvé indécidable, et donc incassable même avec une recherche par force brute : quoiqu'on peut générer tous les polynômes possibles, on ne peut pas savoir lequel était celui utilisé lors du cryptage en absence d'informations supplémentaires.[6]

On s'intéresse finalement à l'application de ce système cryptographique, dans la gestion d'accès aux comptes bancaires des sociétés multinationales. Par définition, ce type de comptes bancaires nécessite le consentement et l'agréement de la majorité du bureau administartif de la société en question avant toute opération bancaire, soit 51%. Ce besoin peut être réalisé en posant $k = [n/2]+1$. Parmi les avantages de ce système, sa haute sécurité et sa flexibilté : on peut générer de nombreuses clés, détruire certaines clés existantes, choisir n'importe quelle combinaison de k clés pour accéder au secret, et enfin gérer le compte bancaire sans dévoiler sa clé secrète qui représente dans ce cas le secret S, et qui n'est manipulée qu'en arrière-plan du système. [1]

0.7 Problématique retenue

Il s'agit d'étudier le système cryptographique Shamir's Secret Sharing pour l'exploiter dans la finance, précisemment dans l'authentification des comptes bancaires à propriétaires multiples, ceci dit en simulant à l'aide des outils de Pyhton 3 un système d'authentification bancaire à la base de ce système cryptographique.

0.8 Objectifs du TIPE du candidat

Je me propose de :
- Découvrir la cryptographie et la preuve de sécurité,
- Etudier l'histoire et l'aspect mathématique du système cryptographique SSS,
- Explorer les méthodes de preuve de validité d'un système cryptographique,
- Simuler le cryptage, le décryptage et l'attque par force brute sur un chiffrement par SSS,
- Concevoir et simuler un système bancaire d'authentification par chiffrement SSS.

0.9 DOT

1/ Août 2020 - Octobre 2020: brain-storming (recherche d'idées et de ressources pour le TIPE à travers tous les moyens disponibles)

2/ Novembre 2020 : étude de la démarche détaillée du TIPE et de ses différents éléments et documents.

3/ Décembre 2020 : choix du sujet et de la problématique du TIPE. Choix de travailler individuellement.

4/ Janvier 2021 : contact d'un ingénieur en cyber-sécurité (Mr Souhail Mssassi) via appel téléphonique pour prise d'éclairages concernant le sujet du TIPE.

5/ Février 2021 : rédaction des premiers éléments du TIPE (titre, ancrage, motivation, début du MCOT et du DOT)

6/ Mars 2021 : implémentation du code informatique des différents programmes de simulation nécessaires aux simulations de cryptage/décryptage/attaque et synthèse des résultats des simulations.

7/ Avril 2021 : saisie de la bibliographie commentée et des références bibliographiques. Changement de la problématique de "amélioration du système SSS" à la problématique actuelle.

8/ Mai 2021 : conception et réalisation du système d'authentification bancaire à l'aide su chiffrement SSS. Consultation d'un étudiant à l'ENSIAS (Mr Alaa Zniber) pour orientation dans la cybersécurité en finance. Réalisation du support numérique du TIPE.

Références bibliographiques

[1] K. D. Gupta et al. “Shamir’s Secret Sharing for Authentication without Reconstructing Password”. In: (2020).

[2] Antti Laaksonen. “Guide to Competitive Programming”. In: Springer, Cham, 2017. Chap. 11. DOI: 10.1007/978-3-319-72547-5.

[3] David Lubicz and Florence Schadle. “Quelques problèmes de sécurité en rapport avec les méthodes formelles”. In: (2010).

[4] Adi Shamir. “How to share a secret”. In: (1979).

[5] Pierre-Yves Strub. *La logique pour vérifier les algorithmes de sécurité de manière autonome et sûre*. vu le 17/04/2021. URL: https://www.youtube.com/watch?v=jVBlUAOoNBA&ab_channel=Ecolepolytechnique.

[6] Alan Turing. “On Computable Numbers, with an Application to the Entscheidungsproblem”. In: (1937).