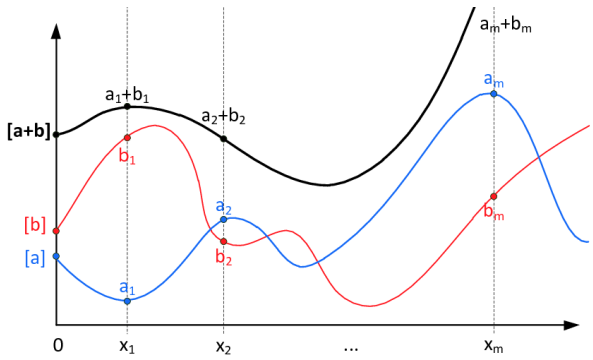
Broadcast Encryption or Secret sharing, and applications (with post-quantum security)



Encadrant: Matthieu Rambaud (dept INFRES)
Nombre d'étudiant·es minimum dans chaque instance de ce projet: 3
Nombre d'étudiant·es maximum dans chaque instance de ce projet: 6
Combien d'instances de ce projet proposez-vous ? 2
Tags : broadcast encryption, secret sharing, confidential voting, lattice-based cryptography

1 Contexte

L'algorithme dit de *secret sharing*, inventé par Shamir en 1979, permet à un dealer possédant un secret a de générer ce qu'on appelle des *shares* de a et de les distribuer à un nombre n de personnes en qui il ne fait pas totalement confiance. L'algorithme est paramétré par un *threshold number* $t < n$ tel que t shares parmi n ne révèlent rien sur a, alors que $t + 1$ shares permettent de reconstituer a. Concrètement, chaque share x_i est égale à l'évaluation en i d'un polynôme secret f choisi par le dealer et valant a en 0. En bonus, le fait que les évaluations de polynômes commutent avec leur addition, permet aux personnes de fabriquer un secret sharing d'une combinaison arbitraire de secrets dont ils possèdent les shares. Les applications sont infinies: élections confidentielles [Sch99], portefeuille digital délégué à plusieurs machines dont aucune n'est de confiance [Coi23] (utilisé par Coinbase sur 5M de wallets), calcul distribué sur des shared secrets, par exemple avec la librairie de ML Crypten de Facebook [Fac19], disclosure automatique d'un secret (par exemple un ordre de swap) conditionné à un événement public [SZ23].

L'étape vulnérable du secret sharing est la distribution des shares, une autre faiblesse est qu'un dealer corrompu pourrait mal former les shares, de sorte qu'elles ne garantiraient pas l'unicité du secret reconstruit à partir de $t+1$ shares. L'unicité a été traitée par un Artishow en 2022, qui a suivi [Sch99]. Cependant, c'est la distribution je préférerais mettre en avant cette année. La technique basique de cryptographie de [GHL22] permet de distribuer les shares en un seul envoi, par un canal public, et avec préservation de leur valeur secrète même si l'envoi est écouté par un ordinateur quantique.

2 Attendus du projet: (sujet A) Broadcast Encryption

Il s'avère qu'une simplification de la technique de [GHL22] permet de diffuser un message identique à beaucoup de personnes, en un seul envoi par un canal public. En outre, pour peu que les destinataires aient choisi leur clés publiques à partir d'une même chaîne aléatoire, la ratio de la taille de l'envoi par destinataire est 100 plus faible que si le message était envoyé séparément à chaque destinataire (c'est dû aux techniques de cryptographie basées sur les réseaux). Le sujet consiste à implémenter cette simplification: soit à partir du code en C++ des auteurs de [GHL22] (librairie `https://libntl.org/`), soit en utilisant des briques existantes dans une autre librairie, le choix est vaste. Une application naturelle est la diffusion d'un ordre militaire secret à beaucoup d'unités légères à la fois.

3 Attendus du projet: (sujet B) ZK de secret sharing

Cette fois, le sujet consiste à utiliser telle qu'elle l'implémentation de [GHL22], et de l'enrichir par des "preuves zero-knowledge" (NIZK) qui apportent la garantie publique que les secret shares ont bien été délivrées, sans montrer leur vraie valeur. L'implémentation actuelle utilise des NIZKs qui ne résistent pas aux ordinateurs quantiques, le but est de les remplacer par n'importe lesquelles ayant cette propriété de résistance (par exemple [CMS+23]).

References

[CMS+23] S. Chatel, C. Mouchet, A. U. Sahin, A. Pyrgelis, C. Troncoso, and J.-P. Hubaux. *PELTA – Shielding Multiparty-FHE against Malicious Adversaries*. CCS. 2023.

[Coi23] Coinbase. *Building user-focused web3 wallets at Coinbase*. link. 2023.

[Fac19] Facebook. *Crypten*. `https://crypten.ai/`. 2019.

[GHL22] C. Gentry, S. Halevi, and V. Lyubashevsky. "Practical Non-interactive Publicly Verifiable Secret Sharing with Thousands of Parties". In: *EUROCRYPT*. 2022.

[Sch99] B. Schoenmakers. "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting". In: *CRYPTO*. 1999.

[SZ23] S. Saereesitthipitak and D. Zindros. *Cassiopeia: Practical On-Chain Witness Encryption*. Financial cryptography workshop. 2023.