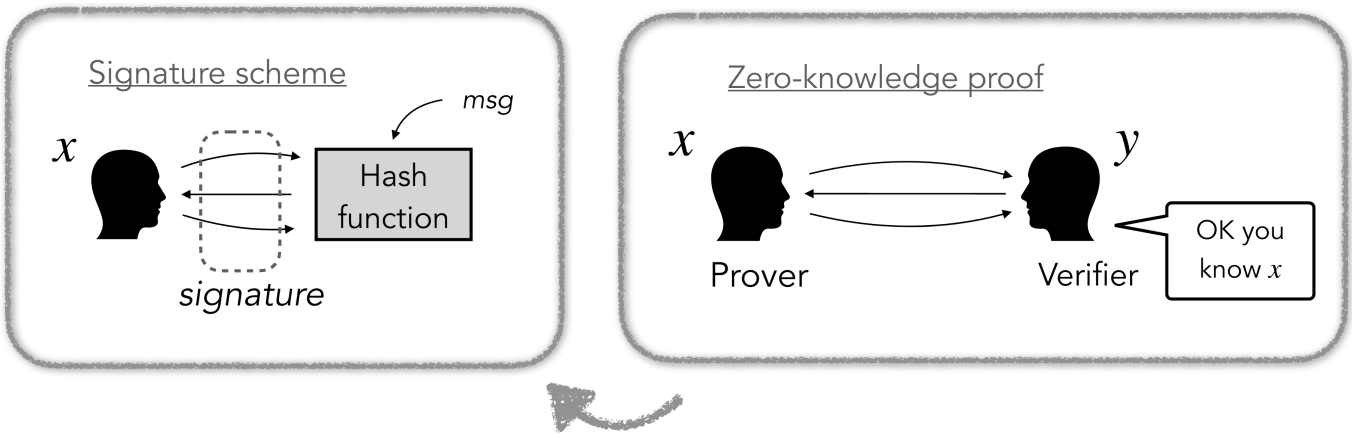
Zero-knowledge proofs of signatures, with applications to blockchains and confidential transactions



(Credit: Thibauld Feneuil)

Encadrant: Matthieu Rambaud (dept INFRES) & Joseph-André-Turk (Zama)
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 ? 3
Tags : zero-knowledge, confidential transactions, layers 2, sealed auctions, digital signatures

1 Contexte

Une "digital signature" est un algorithme permettant à Bob, en input un document M de son choix, de produire une chaîne de bits σ appelée *signature de Bob sur M*. Elle est reconnue valide par tous, et est *infalsifiable*, au sens où une Alice qui n'a jamais vu σ, serait incapable de la produire sans la *clé secrète* de Bob. Dans l'Union Européenne, la connaissance d'une clé secrète est synonyme d'identité [Com23]. La blockchain Ethereum utilise des signatures *agrégeables* ([Eth23a; JS21; Edg23] pour celles de type "BLS"). Il s'agit d'une technique permettant de compacter un grand nombre de signatures en une courte chaîne de bits, de surcroît plus rapide à vérifier [BDN18]. Des techniques cryptographiques plus sophistiquées appelés "zero-knowledge" (NIZK) permettent à l'agrégateur de masquer les signataires et leurs ordres de transactions, tout en prouvant que les ordres ont bien été traités. Ils sont utilisés en pratique dans les places de marché confidentielles (Zcash, "ZK-rollups") [Eth23b; BAZB20; Dai23; WWLC24]. Les NIZKs sont l'un des ingrédients des enchères confidentielles [Zam23], permettant de contrer les robots de front-running.

2 Attendus du projet: sujet A

Le sujet consiste à comprendre puis implémenter une NIZK rustique de beaucoup de signatures, publiée par votre 1er encadrant [ACR21, §5], à l'aide d'une librairie dédiée en Go [BPH+22]. L'extension suivante du projet peut donner à une publication: comparaison avec les performances d'une NIZK récente vendue comme plus rapide [DCX+23], puis intégration de leurs techniques dans un travail non encore publié [ACR21, §7].

En cas d'un deuxième groupe motivé, on pourra basculer sur des signatures agrégeables résistantes aux ordinateurs quantiques [FHSZ23].

3 Attendus du projet: sujet B

Ce sujet alternatif est plus "high level". La partie théorique consiste à étudier et à restituer au choix un article qui quantifie jusqu'où ces techniques procurent de la confidentialité sur les réserves, les positions etc. [CAE21; WWLC24]. Puis à utiliser une librairie au choix d'enchères confidentielles [Pen23; Azt23], voire contribuer à celle de votre 2e encadrant [JAT23].

References

[ACR21] T. Attema, R. Cramer, and M. Rambaud. "Compressed Sigma-Protocols for Bilinear Circuits and Applications to Logarithmic-Sized Transparent Threshold Signature Schemes". In: *ASIACRYPT*. 2021.

[Azt23] Aztec. *LWE Auction*. link. 2023.

[BAZB20] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh. "Zether: Towards Privacy in a Smart Contract World". In: *Financial Cryptography and Data Security - 24th International Conference*. 2020.

[BDN18] D. Boneh, M. Drijvers, and G. Neven. "Compact Multi-signatures for Smaller Blockchains". In: *ASIACRYPT*. 2018.

[BPH+22] G. Botrel, T. Piellard, Y. E. Housni, A. Tabaie, and I. Kubjas. *ConsenSys/gnark-crypto: v0.6.1*. 2022.

[CAE21] T. Chitra, G. Angeris, and A. Evans. *Differential Privacy in Constant Function Market Makers*. Cryptology ePrint Archive, Paper 2021/1101. 2021.

[Com23] E. Commission. *EIDAS*. link. 2023.

[Dai23] W. Dai. *Navigating Privacy on Public Blockchains*. link. 2023.

[DCX+23] S. Das, P. Camacho, Z. Xiang, J. Nieto, B. Bunz, and L. Ren. *Threshold Signatures from Inner Product Argument: Succinct, Weighted, and Multi-threshold*. ePrint 2023/598. 2023.

[Edg23] B. Edgington. *Upgrading Ethereum*. https://eth2book.info/latest/book.pdf. 2023.

[Eth23a] Ethereum. *Ethereum Altair upgrade*. https://github.com/ethereum/consensus-specs/blob/dev/specs/altair/bls.md. 2023.

[Eth23b] Ethereum.org. *Zero-Knowledge rollups*. https://ethereum.org/en/developers/docs/scaling/zk-rollups/. 2023.

[FHSZ23] N. Fleischhacker, G. Herold, M. Simkin, and Z. Zhang. "Chipmunk: Better Synchronized Multi-Signatures from Lattices". In: *CCS*. 2023.

[JAT23] JAT. *FHE CFMM*. link. 2023.

[JS21] Q. T. M. N. JP Aumasson (Taurus) and A. Sanso. *Security of BLS batch verification*. https://ethresear.ch/t/security-of-bls-batch-verification/10748. 2021.

[Pen23] Penumbra. *ZSwap*. link. 2023.

[WWLC24] F.-X. Wicht, Z. Wang, D. V. Le, and C. Cachin. "A Transaction-Level Model for Blockchain Privacy". In: *Financial Cryptography and Data Security - 28th International Conference*. 2024.

[Zam23] Zama. *What is Zama's fhEVM?* link. 2023.