PUBLIC VERIFIABLE SECRET SHARING AND APPLICATIONS TO RANDOMNESS BEACONS

IGNACIO CASCUDO

Abstract. In this talk I will review some recent advances on the topic of publicly verifiable secret sharing and its applications to the construction of randomness beacons. The talk is based on a series of works in collaboration with Bernardo David, Lydia Garms, Anders Konring, Omer Shlomovits and Denis Varlakov.

Summary

Secret sharing schemes allow a dealer to distribute the knowledge of a secret among a number of parties according to certain access conditions (for example, that only a large enough subset of the parties can reconstruct the secret when they agree in doing so). Secret sharing schemes constitute one of the most well known cryptographic primitives.

In publicly verifiable secret sharing (PVSS), introduced in [1], the dealer publishes the shares in an encrypted form, and proves that these ciphertexts indeed hide a set of valid shares (i.e. a secret can be reconstructed from these shares) in such a way that any external verifier can be convinced of the validity of the sharing without obtaining information about the secret. In this way a PVSS scheme is a cryptographic commitment to a secret, that can be jointly opened by a large enough number of share receivers. PVSS has applications in electronic voting, multiparty computation and recently in the construction of distributed randomness beacons for its use in proof-of-stake blockchains. One notable work was [2] who introduced a simple construction for PVSS based on discrete logarithm hardness assumptions.

This talk will review a line of work ([3, 4, 5, 6]) starting in 2017 where we have subsequently reduced the complexity of PVSS and thereby improved its scalability for large number of parties, which is motivated especially by the aforementioned applications to distributed randomness beacons and other related uses. I will detail some of these efficiency improvements and briefly discuss how to utilize this tool to construct distributed randomness beacons.

References

[1] Markus Stadler. Publicly Verifiable Secret Sharing. In *EUROCRYPT 96*, volume 1070 of *LNCS*, pages 190–199. Springer, 1996. DOI 10.1007/3-540-68339-9_17.

The author has been partially supported by the Spanish Government under project SecuRing (ref. PID2019-110873RJ-I00/MCIN/AEI/10.13039/501100011033), by Madrid regional government as part of the program S2018/TCS-4339 (BLOQUES-CM) co-funded by EIE Funds of the European Union, and by a research grant from Nomadic Labs and the Tezos Foundation.

[2] Berry Schoenmakers. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. In *CRYPTO 99*, volume 1666 of *LNCS*, pages 148–164. Springer, 1999. DOI 10.1007/3-540-48405-1_10.

[3] Ignacio Cascudo and Bernardo David. SCRAPE: Scalable randomness attested by public entities. In *ACNS 17*, volume 10355 of *LNCS*, pages 537–556. Springer, Heidelberg, July 2017. DOI 10.1007/978-3-319-61204-1_27.

[4] Ignacio Cascudo and Bernardo David. ALBATROSS: Publicly AttestabLe BATched Randomness based On Secret Sharing. In *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 311–341. Springer, Heidelberg, December 2020. DOI 10.1007/978-3-030-64840-4_11.

[5] Ignacio Cascudo, Bernardo David, Omer Shlomovits and Denis Varlakov. Mt. Random: Multi-Tiered Randomness Beacons. In submission, preprint available at *IACR Cryptol. ePrint Arch.*, https://eprint.iacr.org/2021/1096, 2021.

[6] Ignacio Cascudo, Bernardo David, Lydia Garms, Anders Konring. YOLO YOSO: Fast and Simple Encryption and Secret Sharing in the YOSO Model. In submission, preprint available at *IACR Cryptol. ePrint Arch.*, https://eprint.iacr.org/2022/242, 2022.

Ignacio Cascudo; IMDEA Software Institute.
Email address: ignacio.cascudo@imdea.org