Proof of Possession in Schnorr-based Threshold Signature Schemes

1 ABSTRACT

Designing and implementing threshold signature schemes that ensure each party has a valid share of the secret key and does not deviate from the prescribed steps is a challenge. A malicious party could generate invalid shares or signatures, breaking the security or functionality of the scheme. To prevent these attacks, it is necessary to have a mechanism that allows each party to prove that they possess their share of the secret key without revealing it to anyone else. This is called proof of possession.

In this report, we discuss why proof of possession is important in the Muon scheme and how it can be added to the Muon implementation. The previous version of the Muon scheme used hash-commitments as a means to prevent rogue key attacks. However, it is recognized that proof of possession is a more commonly accepted solution in the field of threshold signatures and can further enhance the security and efficiency of the scheme.

2 PROOF OF POSSESSION IN VARIOUS THRESHOLD SIGNATURE SCHEMES

Proof of possession has been used in different threshold signature schemes to ensure the validity of the shares. For instance, in RSA-based threshold signature schemes, Paillier encryption and zero-knowledge proofs are used, while Pedersen commitments and zero-knowledge proofs are used in some ECDSA-based threshold signature schemes. In Schnorr-based threshold signature schemes, proof of possession is achieved by using Schnorr signatures as proofs of knowledge, as seen in MuSig2 and FROST2 schemes.

3 PROOF-OF-POSSESSION IN SCHNORR-BASED THRESHOLD SIGNATURE SCHEMES

To formally define proof of possession for Schnorr-based threshold signatures, we can use the following notation:

- Let G be a cyclic group of prime order q with generator g.

- Let H be a hash function modeled as a random oracle that maps arbitrary inputs to elements of G.

- Let (x, P) be a public/private key pair for Schnorr signatures, where $x \in Z_q$ is the secret key and $P = g^x \in G$ is the public key.

- Let (x_i, P_i) be a share of (x, P) for party $i \in [n]$, where $x_i \in Z_q$ is the secret share and $P_i = g^{x_i} \in G$ is the public share.

Proof of possession for Schnorr-based threshold signatures means that each party i can prove that they know their secret share x_i without revealing it to anyone else. This can be done by using Schnorr signatures as proofs of knowledge, as follows:

- Party i chooses a random nonce $r_i \in \ Z_q$ and computes $R_i \ = \ g^{r_i} \ \in \ G.$

- Party i computes $c_i = H(R_i, P_i, m)$, where m is an arbitrary message (e.g., an identifier for the proof).

- Party i computes $s_i = r_i - c_i * x_i \ mod \ q$ and sends (R_i, s_i) to other parties as their proof of possession.

- Other parties verify that $s_i \ \in \ Z_q$ and $g^{s_i} \ = \ R_i P_i^{H(R_i, P_i, m)}$ holds.

If party i knows their secret share x_i, they can easily compute s_i such that verification succeeds. If party i does not know their secret share x_i, they cannot compute s_i without knowing r_i or breaking the discrete logarithm problem. Therefore, this proves that party i possesses their secret share without leaking any information about it.

4 CONCLUSION

In conclusion, proof of possession based on Schnorr proofs is a more commonly accepted solution for guarding against rogue key attacks compared to hash commitments used in the previous version of the Muon scheme. Currently, the use of proof-of-possession enhances the security and efficiency of the scheme by verifying that all parties have valid shares before generating signatures.

5 REFERENCES

[1] Crites, Elizabeth, Chelsea Komlo, and Mary Maller. "How to prove Schnorr assuming Schnorr: security of multi-and threshold signatures." Cryptology ePrint Archive (2021).

[2] Shoup, Victor. "Practical threshold signatures." In Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19, pp. 207-220. Springer Berlin Heidelberg, 2000.

[3] Komlo, Chelsea, and Ian Goldberg. "FROST: flexible round-optimized Schnorr threshold signatures." In Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27, pp. 34-65. Springer International Publishing, 2021.

[4] Ruffing, Tim, Viktoria Ronge, Elliott Jin, Jonas Schneider-Bensch, and Dominique Schröder. "ROAST: Robust Asynchronous Schnorr Threshold Signatures." IACR Cryptol. ePrint Arch. 2022 (2022): 550.