Threshold Value in Threshold Signature Schemes: Secure Bounds and Guidelines

1 Abstract

In this document, we discuss the secure bounds on the threshold value 't' in threshold signature schemes. The threshold value plays a crucial role in determining the security and efficiency of a threshold signature scheme. We provide guidelines for selecting the threshold value based on the security requirements and efficiency constraints of the protocol.

2 Definitions of Correctness Threshold and Reconstruction Threshold for Threshold Signature Schemes

Threshold signature schemes (TSS) require a minimum number of parties to cooperate to produce a valid signature. We distinguish two types of thresholds in TSS: Correctness threshold and Reconstruction threshold.

- Correctness threshold: This is the maximum number of malicious nodes that the TSS protocol can tolerate while ensuring that all honest nodes agree on the same secret-shared private key and the same public key corresponding to the private key.
- Reconstruction threshold: This is the minimum number of honest nodes that need to cooperate to produce a valid signature using their shares of the private key.

3 Low-threshold and High-threshold Schemes

Threshold signature schemes can be classified into two categories based on the reconstruction threshold.

- Low-threshold schemes: These are cryptographic protocols that set the reconstruction threshold to be identical to the correctness threshold. This means that any subset of t + 1 honest nodes can use the secret key for a threshold cryptosystem, but any subset of t or fewer nodes cannot learn anything about it. Low-threshold schemes provide security and availability, but not privacy against a powerful adversary that can acquire more than t shares of the secret key.
- High-threshold schemes: These are cryptographic protocols that set the reconstruction threshold to be higher than the correctness threshold. This means that more than t + 1 honest nodes are needed to use the secret key for a threshold cryptosystem, but any subset of t or fewer nodes cannot learn anything about it. High-threshold schemes provide security and privacy, but not availability against a powerful adversary that can prevent some honest nodes from participating in the protocol.

4 Lower and Upper Bounds for Threshold Value in Threshold Signature Schemes

The lower and upper bounds for the threshold value in threshold signature schemes depend on the security and efficiency requirements of the protocol.

For TSS schemes that provide both unforgeability and robustness, the threshold value should be lower than n/2, where n is the number of parties. If more than half of the parties are malicious, they can collude to either forge a signature or disrupt the signing protocol.

If only unforgeability is guaranteed, then a threshold value up to n-1 can be achieved. The upper bound for the threshold value is n-1 because at least one honest party is needed to participate in the signing protocol.

5 Muon Protocol Implementation

The Muon Protocol implementation is based on the Gennaro et al. 2007 paper, which achieves the optimal threshold upper bound for robust schemes. Thus, to guarantee both secrecy and correctness, the threshold value in the Muon Protocol implementation must be strictly less than n/2.

In light of this, the Muon Protocol implementation will enforce the selection of threshold values in a certain secure range to ensure that the security and efficiency requirements of the protocol are met. This threshold value must be over n/2 but higher values mean that we are using a high-threshold setting. Accordingly, since n-t malicious actors can prevent generation of new signatures this value must not be too high.

6 Discussion

Bounds and limitations on the value of threshold in cryptographic schemes depend on various factors, such as the security model, the network assumptions, the computational complexity, and the contrast ratio. Generally speaking, higher threshold values provide stronger privacy and resilience against malicious attacks, but lower threshold values provide better availability and performance. There are trade-offs between different parameters that need to be carefully considered when designing and implementing cryptographic schemes.

7 References

[1] Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme by Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin, Advances in Cryptology — EUROCRYPT 2002, Springer Berlin Heidelberg, 2002, pp. 629-647.

[2] Dan Boneh and Matt Franklin, Threshold signatures, Advances in Cryptology -- CRYPTO ’97, Lecture Notes in Computer Science, vol. 1294, Springer Berlin Heidelberg, 1997, pp