The Challenge Value in Schnorr Signature Schemes

1 Abstract

In this report, we discuss the importance of including the public key in the calculation of the hash challenge in Schnorr signatures. The Muon protocol utilizes Schnorr signatures in threshold setting, and the inclusion of the public key in the challenge hash is crucial to ensure the security of the protocol. As a result of our survey, we concluded that the addition of the public key (Y) in the hashed challenge (c) is necessary to prevent various attacks and enhance security.

To address this issue, we revised the Muon protocol to include the public key Y in the challenge hash. The new challenge hash for the Muon protocol is calculated similar to the following formula

$$c = H(K||Y||m)$$

With this modification, the Muon protocol now has enhanced security against some attacks.

2 Challenge Value in Schnorr Signatures

The challenge value c in Schnorr signature schemes is usually the result of hashing a random nonce point K, the message m, and the public key Y of the signer. The inclusion of the public key Y in the challenge hash is necessary for security reasons, as it prevents some possible attacks such as:

- Related Key Attack: An attacker who knows a relation between two private keys x_1 and x_2 can use a signature from one signer to forge a signature from another signer on the same message by modifying the response value.
- Key Substitution Attack: An attacker who can modify or replace public keys can use a signature from one signer to forge a signature from another signer on any message by modifying both the challenge and response values.

Therefore, it is recommended to include the public key Y in the challenge hash to bind the signature to a specific public key and prevent these attacks. Moreover, the inclusion of the public key in the challenge hash can also improve the efficiency of the verification process, as it allows for precomputation of certain values. Some variants of Schnorr signatures also include other values in the challenge hash, such as proofs of possession or auxiliary commitments, to enhance security or efficiency.

3 Conclusion

The inclusion of the public key in the hashed challenge of Schnorr signatures can potentially enhance the security of protocols that use Schnorr signature. The revised Muon protocol, which now includes the

public key in the challenge hash, is now more secure and able to use Schnorr signatures safely against possible attack scenarios.

4 REFERENCES

[1] Wuille, Pieter, Nick, Jonas, and Tim Ruffing. "Bip 340: Schnorr Signatures for secp256k1." Avail-able: https://github. com/bitcoin/bips/blob/master/bip-3040.mediawiki (2020).

[2] Schnorr, Claus-Peter. "Efficient signature generation by smart cards." Journal of cryptology 4 (1991): 161-174.

[3] Gennaro, Rosario, Steven Goldfeder, and Arvind Narayanan. "Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security." In Applied Cryptography and Network Security: 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings 14, pp. 156-174. Springer International Publishing, 2016.