Secrect Sharing Progress

Joan Ngure

Report

In perfect secrecy, for any message x given any cipher text y;

$$p(x|y) = p(x)$$

In a secret sharing scheme perfect secrecy is satisfied since for any message x given any number of shares s less than the threshold t:

$$p(x|s_1, \cdots, s_{t-1}) = p(x)$$

In case a player decides to give a forged share in shamir's secret sharing scheme, other players will reconstruct a fake secret but the cheater alone can get the correct secret. Constructing a hash function of the secret, is one of the simplest ways to detect cheating. If secret S = H(s) then the players can check whether the reconstructed secret S′ = S. However with access to the secret's hash function, it is possible to reconstruct the secret by trying different ways of constructing hash functions and matching it with the secret's hash function. The security of such a scheme relies on the hardness of the problem.
Several schemes for cheater and cheating detection have been proposed. (still working on this, below are the references I am planning to use.)

References

[1] Marco Carpentieri, Alfredo De Santis, and Ugo Vaccaro. "Size of shares and probability of cheating in threshold schemes". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1993, pp. 118–125.

[2] Hugo Krawczyk. "Secret sharing made short". In: *Annual International Cryptology Conference*. Springer. 1993, pp. 136–146.

[3] Yanxiao Liu. "Linear (k, n) secret sharing scheme with cheating detection". In: *Security and Communication Networks* 9.13 (2016), pp. 2115–2121.

[4] Robert J. McEliece and Dilip V. Sarwate. "On sharing secrets and Reed-Solomon codes". In: *Communications of the ACM* 24.9 (1981), pp. 583–584.

[5] Daniel Pasailă, Vlad Alexa, and Sorin Iftene. “Cheating detection and cheater identification in crt-based secret sharing schemes”. In: *International Journal of Computing* 9.2 (2010), pp. 107–117.

ref.bib