Abstract

Two secret sharing schemes that use Asmuth-Bloom sequence and are based on Chinese Reminder Theorem (CRT) are proposed in this paper. The first scheme is designed for the case of a single secret and the second one is an extension of the first scheme to the case of multi-secrets. Novelty of the proposed schemes is that the shares of the participants are reusable i.e. same shares are applicable even with a new secret. Also only one share needs
to be kept by each participant even for the multi-secret sharing scheme. Further, the schemes are capable of verifying the honesty of the participants including the dealer. Correctness of the schemes is also discussed.

References

- M. Stadler, Publicly verifiable secret sharing. Advances in Cryptology,
Reusuable Multi-Stage Multi-Secret Sharing Scheme based on Asmuth-Bloom Sequence


Index Terms

Computer Science  Security

Keywords
Multi-secret  Mignotte's Sequence  Asmuth-bloom Sequence  Crt  Secret Sharing Scheme.