SECRET KEY DISTRIBUTION TECHNIQUE USING THEORY OF NUMBERS

S. Srinivasan
P. Muralikrishna

School of Advanced Sciences
VIT University
Vellore – 632014
India
e-mails: smrail@gmail.com
pmkrishna@rocketmail.com

N. Chandramowliswaran

Visiting Faculty
Indian Institute of Management Indore
Indore – 453 331
India
e-mail: ncmowli@hotmail.com

Abstract. A group key distribution protocol can enable members of a group to share a secret group key and use it for secret communications. In this article we review the number of share holders require to reconstruct the secret grouped among them. The confidentiality of our proposed protocol is unconditionally secure.

Key words: Key distribution, Secret Sharing.

AMS Classification: 94A60, 94A62.

1. Introduction

Secret sharing is a technique for protecting sensitive data, such as cryptographic keys. It is used to distribute a secret value to a number of parts or shares that have to be combined together to access the original value. These shares can then be given to separate parties that protect them using standard means, e.g., memorize, store in a computer or in a safe. Secret sharing is used in modern cryptography to lower the risks associated with compromised data.

A threshold scheme enables a secret to be shared among a group of ℓ members providing each member with a share. The scheme has a threshold $t + 1$ if any subset with cardinality $t+1$ out of the ℓ shares enables the secret to be recovered. We will use the notation $(t+1, \ell)$ to refer to such a scheme. Ideally, in a $(t+1)$ threshold scheme, t shares should not give any information on the secret. We will discuss later how to express this information. Sharing a secret spreads the risk of compromising the value across several parties. Standard security assumptions of secret sharing schemes state that if an adversary gains access to any number of shares lower than some defined threshold, it gains no information of the secret value. The first secret sharing schemes were proposed by Shamir [1] and Blakley [5].

Cryptography is the collection of methods and approaches for concealing information in communications from the access by uninvited or unauthorized parties. A logical art for dealing with this problem is known from early antiquity and it developed along the centuries, mostly in the frame in which two parties, say nobleman and general, or concealed lovers, communicated in written by sending each other messages which could only be understood when knowing some additional data, secret keys and the details for the procedure of encrypting and decrypting the messages algorithm. Algorithms were often assembled from a collection of useful basic ideas, known by tradition.

The group communication has been developed extensively in many applications currently. Ensuring the security of a group communication has become one of the most important issues in the development. Generally speaking, the security properties of a group communication include two basic aspects, that is, (i) the messages transmitted within the group can only be shared by authorized group members, but not by any unauthorized users and (ii) the transmitted messages must be able to be authenticated by members. The security properties mentioned previously imply that a group session key must be used by authorized group members to encrypt and authenticate the messages.

Suppose we have a large number of people, processes, or systems that want to communicate with one another in a secure fashion. Let's further add this group of people or processes or systems is not static, meaning that the individual entities may join or leave the group at any time. In such case, if the owner of the secret can fix the number of share holders, then it will be useful to distribute the shares.

This paper is organized as follows. In Section 2, we provide a technique to fix the number of share holders to reconstruct the distributed secret among the share holders and Conclusion is given in Section 3.

2. Main result

In this section, we consider a secret S and attain a protocol to identify the number of share holders, those who are having the distributed shares among them.

Theorem 2.1. *For any positive integer $k \geq 2$, there exists $k + \dfrac{k(k-1)}{2}$ share holders, sharing the common secret S.*

Proof. Select the secret positive integers α, β, α_i and β_i with $1 \leq i \leq k$. Define

$$M = \beta\left(\sum_{j=1}^{k} \beta_j^2 + \sum_{i<j} \beta_i\beta_j\right) - 1,$$

where $i, j \in \{1, 2, ..., k\}$, $a = \alpha M + \beta$, $a_j = \alpha_j M + \beta_j$ for $j \in \{1, 2, ..., k\}$ and

$$N = \frac{a\left(\sum\limits_{j=1}^{k} a_j^2 + \sum\limits_{i<j} a_i a_j\right) - 1}{M}.$$

Select a secret S such that $(S, N) = 1$.
Define $Y_i \equiv Saa_i^2 \ (mod\ N)$ for $i \in \{1, 2, ..., k\}$.

$$X_{i,j} \equiv Saa_ia_j \ (mod\ N) \text{ for } i < j \text{ and } i, j \in \{1, 2, ..., k\}.$$

Now, it is easy to observe

$$\sum_{i=1}^{k} Y_i + \sum_{i<j} X_{i,j} \equiv S \ (mod\ N).$$

This completes the proof. ■

3. Conclusion

Cryptography was born in early ages as a skill of mental combinations put at the service of privacy and military protection. It developed along time into a highly mathematized discipline, which unites the science of concealing with the analysis of attacks into one single unit, cryptorology. There have been numerous interesting attempts to use the large list of NP complete problems. This paper hardly deals the expected number of share holder in order to share a secret with positive integer $k \geq 2$.

References

[1] Adi Shamir, *How to share a secret*, Communications of the ACM, 22 (11) (1979), 612-613.

[2] Barnard, S., Child, J.M., *Higher Algebra*, Macmillan and Co., 1952.

[3] Beimel, A., *Secret-sharing schemes: a survey*, Proceedings of the Third international conference on Coding and cryptology, Berlin, Heidelberg, 2011, Springer-Verlag, IWCC'11, 11-46.

[4] Berlekamp, E.R., *Algebraic Coding Theory*, NY, McGraw-Hill, 1968.

[5] Blakley, G.R., *Safeguarding cryptographic keys*, Proceedings of the National Computer Conference 48 (1979), 313-317.

[6] Herstein, I.N., *Topics in Algebra*, 2nd Edition, John Wiley, 1975.

[7] Mignotte, M., *How to share a secret*, Advances in Cryptology - Eurocrypt82, LNCS, Springer-Verlag, 149 (1983), 371-375.

[8] Muralikrishna, P., Srinivasan, S., Chandramowliswaran, N., *Secure Schemes for Secret Sharing and Key Distribution using Pell's equation*, International Journal of Pure and Applied Mathematics, 85 (5) (2013), 933-937.

[9] Srinivasan, S., Muralikrishna, P., Chandramowliswaran, N., *Authenticated Multiple Key Distribution using Simple Continued Fraction*, International Journal of Pure and Applied Mathematics, 87 (2) (2013), 349-354.

[10] Srinivasan, S., Muralikrishna, P., Chandramowliswaran, N., *Authenticated Key Distribution using given set of Primes for Secret Sharing*, Submitted.

[11] Niven, I., Zuckerman, H.S., Montgomery, H.L., *An Introduction to the Theory of Numbers*, John Wiley.

[12] Apostol, T.M., *Introduction to Analytic Number Theory*, Springer.

Accepted: 19.12.2013