Efficient on–line secret sharing

M. Valls[1], J.L. Villar[2], and E. Márquez[2]

[1] Dept. Matemàtica. Universitat de Lleida. Spain.
magda@eup.udl.es
[2] Dept. de Matemàtica Aplicada i Telemàtica
Universitat Politècnica de Catalunya. Spain.
jvillar@mat.upc.es

Extended abstract

A secret sharing scheme is a method of dividing a secret among a set of participants, in such a way that only some authorized subsets will be able to obtain the secret. The collection of subsets of participants qualified to reconstruct the secret is usually referred to as the access structure of the secret sharing scheme. These schemes are useful in any important protocol that requires the concurrence of several designated people. We refer the reader to the excellent survey paper [6] for a detailed discussion of secret sharing schemes.

Krawczyck [3] proved in 1994 that the size of the shares could be smaller than the size of the secret, if the security of the scheme was based on computational assumptions, that is to say, it is assumed that the adversaries' computational resources are bounded. Such schemes are called computationally secure secret sharing schemes. In 1995, Cachin [2] suggested an on-line computational secure secret sharing scheme for a general access structure, which had the following good capabilities:

- The shares that had to be distributed (and that had to be stored by every participant) were as short as the secret.
- Multiple secrets could be reconstructed, just by changing some public information. Only one share per participant was needed to be distributed.
- Participants could be dynamically added or deleted without having to redistribute new shares to the existing participants.

Moreover, Pinch [5] had already improved Cachin's scheme in two senses, firstly by allowing the re–usage of the initial distributed shares (without the usage of a distributed computation sub-protocol) and then by allowing that the reconstruction could be done in a public channel. All these capabilities relied on the fact that some information had to be stored in a publicly accessible central location. But, in both cases, the amount of public information was of the order of the number of authorized subsets allowed in the access structure, that is $O(|\Gamma|)$, what makes these protocols impractical. For instance, in a (t, n)–threshold access structure, such a number is $|\Gamma| = \binom{n}{t}$ which is of the order of n^t, so it increases rapidly with n.

We present a computationally secure [3] secret sharing scheme for a vector space structure [1] . This scheme also maintains the previous capabilities and, what is more important, overcomes the problems of Cachin's and Pinch's schemes, because the amount of information that must be publicly accessible is just of the order of the number of participants, $\mathrm{O}(n)$. Moreover, as well as in Pinch's proposal, the initial distributed shares can be reused in order to reconstruct several secrets (this is due to the fact that in the reconstruction process, no participant needs to reveal his share). In this protocol, not only the reconstruction can take place by means of insecure channels, but also the distribution of the initial shares is done by means of a Diffie-Hellman key exchange [4] between the dealer and every participant. Then, the dealer determines a suitable vector space construction for the access structure Γ, for which the private-shares are exactly the keys agreed with each participant. Finally, the dealer publishes some information that will allow each authorized subset to get the secret. Moreover, even when the access structure is changed, the initial key agreed with the dealer is maintained as the private–share of each participant.

References

1. E.F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 6:105–113, 1989.
2. C. Cachin. On–line secret sharing. *Lecture Notes in Computer Science. Proc. Cryptography and Coding 5th IMA Conference*, 1025:190–198, 1995.
3. H. Krawczyck. Secret sharing made short. *Lecture Notes in Computer Science. CRYPTO'93*, 773:136–146, 1994.
4. A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of applied cryptography.* CRC Press, 1997.
5. R.G.E. Pinch. On-line multiple secret sharing. *Electronic Letters*, 32:1087–1088, 1996.
6. D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992.