Editorial
Volume 10:7, 2021

Journal of
Applied & Computational Mathematics

ISSN: 2168-9679 Open Access

Verifiable Secret Sharing Scheme Based on Certain Projective Transformation

Tom Wenston*

Department of computational mathematics, Pennsylvania State University, University Park, USA

Editorial

The main purpose of verifiable secret sharing scheme is to unravel the honesty problem of participants. During this paper, the concept of nonzero k-sub matrix and therefore the residual vector of system of hyper plane intersecting line equations are proposed. supported certain projective transformations in projective space, a verifiable (t, n)-threshold secret sharing scheme is meant by using the structure of solutions of linear equations and therefore the difficulty of solving discrete logarithm problems. The results show that this scheme can verify the correctness of the sub key provided by each participant before the reconstruction of the passkey, and may effectively identify the fraudster. The fraudster can only cheat by guessing and therefore the probability of success is merely 1/p. the planning of the scheme is exquisite and therefore the calculation complexity is little. Each participant only must hold a sub key, which is convenient for management and use. The analysis shows that the scheme during this paper meets the safety requirements and rules of secret sharing, and it's a computationally secure and effective scheme with good practical value.

Secret sharing may be a method proposed to unravel the matter of key management. It's mainly wont to prevent important information from being lost, destroyed, and altered or falling into the incorrect hands. It's a crucial subject in information security and cryptography. It's widely utilized in data management, financial network, e-commerce, e-government and lots of other fields. The essential idea of secret sharing is to share the passkey during a group of participants, which enables members of the authorized subset of participants to recover the passkey through the sub key they get, while members of any participant's unauthorized subset cannot recover the passkey through the sub key they get.

As early as 1979, the algorithm given by Shamir system is predicated on polynomial interpolation, while Blakley system is predicated on finite geometry. The (t,n) -threshold secret sharing scheme requires that any t or quite t members of n participants cooperate to derive the passkey , while no t−1 members cooperate to derive the passkey . After these two masters, more secret sharing schemes are proposed one after another, which are constructed by using mathematical knowledge and methods in several fields. For instance, the uses Reed-Solomon code to construct secret sharing scheme. Chinese Remainder Theorem to construct secret sharing scheme, the mathematical process on finite field to construct secret sharing scheme. The one-way function to construct secret sharing scheme, uses vector space to construct secret sharing scheme, etc. Especially in recent years, people have made some gratifying achievements within the design and research of more complex secret sharing schemes. It should be acknowledged that there could also be dishonest participants within the actual use of those schemes. In sight of the way to effectively prevent fraud, many authors have conducted in-depth research on them. Different schemes of secret sharing which will prevent fraud are proposed respectively.

However, none of the schemes mentioned above gives the probability of successful fraud accurately. Moreover, some schemes are complex in design, lack of intuition and conciseness, and fail to understand the planning principles of secret sharing schemes. The planning principle of secret sharing scheme isn't only to make sure its correctness, but also to concentrate to its security and effectiveness. Consistent with this principle, this paper designs a sort of secret sharing scheme supported certain projective transformation. This scheme uses the special projective transformation in projective space to create the connection between the passkey and therefore the sub key, in order that the dealer can find the sub key through the passkey to distribute the participants. Members of the authorized subset can gather their sub keys to seek out the connection between the components of the shadow sub key vector, and recover the shadow sub key alongside the residual vector of the intersecting line equations formed by the projection plane of the shadow sub key point within the space, so on synthesize the passkey. The key sharing scheme designed during this way accords with the thought of (t,n) -threshold secret sharing, which is straightforward, intuitive, practical and straightforward to implement.

***Address for Correspondence:** Tom Wenston, Department of Computational mathematics, Pennsylvania State University, University Park, USA, Email: tom.w@gmail.com*

Received 05 July 2021; **Accepted** 12 July 2021; **Published** 19 July 2021

How to cite this article: Tom Wenston. "Verifiable Secret Sharing Scheme Based on Certain Projective Transformation." J Appl Computat Math 9 (2021): e114.