Secret Sharing Based on the Social Behaviors of Players

Mehrdad Nojoumian and Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo, Waterloo, ON, N2L 3G1, Canada
{mnojoumi, dstinson}@uwaterloo.ca

Abstract. We introduce the notion of a Social Secret Sharing Scheme, in which shares are allocated based on a player’s reputation and the way he interacts with other participants. During the social tuning phase, weights of players are adjusted such that participants who cooperate will end up with more shares than those who defect.

1 Introduction

In cryptography, a threshold secret sharing scheme [4] is a construction where the secret is divided into $n$ shares to be distributed among players. Consequently, the secret is revealed if at least $t$ players cooperate with each other, while any subsets of $t - 1$ players cannot learn the secret.

In social networks, trust is the expectation that a player has about the future behavior of another player based on the history of their interactions, while reputation is the perception that a player creates by past behaviors about his intentions. If players $P_i$ for $1 \leq j \leq n$ and $j \neq i$ equally trust $P_i$, then the trust value is the same as the reputation value, i.e., our assumption in this paper.

Our motivation is that, in real world applications, components of a secure system may have different levels of importance (i.e., number of shares a player has) and reputation (i.e., cooperation with other players for the share renewal or secret recovery). For this reason, we believe a good construction should balance these two factors respectively. Therefore, as our main contribution, we propose a social secret sharing scheme where shares are allocated based on each player’s reputation. This scheme is called the social secret sharing scheme since it can be visualized in terms of players collaborating to recover the secret in a social network based on their reputations. This is similar to human social life where people share more secrets with whom they really trust and vice versa.

2 Social Secret Sharing Scheme

In social secret sharing, each participant initially receives a constant number of shares. As time passes, players are assigned weights based on their behaviors in the scheme. Consequently, each player receives a number of shares corresponding to his trust value. In fact, weights of participants are adjusted such that cooperative players receive more shares compared to non-cooperative ones. Alternatively, newcomers can join the scheme while corrupted players are disenrolled immediately.

The construction of a trust function is independent of our proposed scheme. Therefore, we use the trust management approach proposed in [2], where the authors first define six possible actions (i.e., encourage, give a chance, reward, penalize, take a chance, and discourage). Consequently, they apply monotonically increasing and decreasing functions in the case of cooperation and defection in order to compute players’ trust values. Now, we illustrate major definitions required for our scheme.

Definition 1. Cooperation $P_i(C)$: $P_i$ is available at the time of share renewal or secret recovery and sends correct information. Defection $P_i(D)$: $P_i$ is not available at the required time or probably responds with delay. Corruption $P_i(X)$: $P_i$ has been compromised by a passive adversary.

---

1 For the full version of this paper, see [3]
Definition 2. The Social Secret Sharing Scheme $\mathcal{S}^4$ is a three-tuple denoted as $\mathcal{S}^4(Sha, Tun, Rec)$ consisting of secret sharing, social tuning, and secret recovery. The only difference compared to the threshold scheme is $\text{Tun}$, where the weight of each $P_i$ is adjusted based on his trust value $T_i(p)$.

Definition 3. In $\mathcal{S}^4$, the total weight of uncorrupted players $\in \Delta$ must be equal or greater than the threshold. On the other hand, the total weight of colluders $\in \nabla$ must be less than the threshold. Finally, the weight of each player is bounded to a parameter much less than $t$, i.e., $w_i \leq m \ll t$.

3 Passive Adversary Model Construction

The proposed model consists of $n$ participants, $P_1, P_2, \ldots, P_n$, and a dealer who initiates the scheme. We assume the existence of private channels between each pair of players as well as a synchronized broadcast channel. All computations are performed in the finite field $\mathbb{Z}_q$. We consider the passive adversary model, where players follow protocols correctly but are curious to learn the secret. In addition, our passive adversary is mobile with unlimited computation power, that is, he may corrupt various players at different stages of the protocols’ executions in an unconditionally secure setting. $T_i(p)$ and $w_i(p)$ present the trust value and the weight of player $P_i$ at period $p$ accordingly. The initial trust value is zero for players. For the sake of simplicity, we sometimes replace $w_i$ with $w_i(p)$.

3.1 Secret Sharing (Sha)

Suppose, the dealer initiates a secret sharing scheme by generating a polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $t - 1$ in which its constant term is the secret $f(0) = \zeta [4]$. He sends shares of player $P_i$ for $1 \leq i \leq n$ according to his weight $w_i$, and then he leaves the scheme: $\varphi_{ij} = f(\vartheta_{ij})$ for $1 \leq j \leq w_i$, where $\vartheta_{ij} = im - m + j$ and $m$ is the maximum weight of any participant.

3.2 Social Tuning (Tun)

Our scheme provides a mechanism for assigning new weights to players based on their behaviors at the end of each time period, where by behavior we refer to a participant’s reputation.

Inactivating Non-cooperative Players’ Shares. Clearly, identifier $j$ for $1 \leq j \leq m$ should be inactivated for each player whose trust value has been decreased and activated for players whose trust values are risen or for newcomers. One particular approach is to inactivate a number of $\text{ids}$ for each player $P_i$ proportional to the amount that the player’s trust value $T_i(p)$ is decreased: $P_i(D) : \text{defection} \Rightarrow w_i(p) = \lfloor w_i(p - 1) \cdot (1 - \tau/2) \rfloor$, where $\tau = T_i(p - 1) - T_i(p) \geq 0$ is the coefficient of the weight reduction for the non-cooperative players. If $w_i(p)$ becomes zero, $P_i$ is removed from the scheme. Consequently, the total number of $\text{ids}$ to be activated in the entire scheme is given as follows: $\delta(p) = \sum_{i : \forall (D)} (w_i(p - 1) - w_i(p))$.

Activating Cooperative Players’ Shares. Given the number of $\text{ids}$ to be activated, we now define which players should receive extra shares and how many newcomers can enter into the scheme. For each participant $P_i$, consider the ratio of a player’s trust value $T_i(p)$ to the number of shares he is holding $w_i(p)$. This ratio $\rho = T_i(p)/w_i(p)$ increases with the participant’s trust value enhancement, and decreases as the participant gains more shares.

As a result, it is reasonable to activate $\text{ids}$ in participants for whom this ratio is highest, but this is not enough since we also need to consider newcomers whose trust values are zero. Therefore, to have a fair policy, we give the first priority to cooperative players for whom this ratio is both highest and positive, the second priority to newcomers, and the third priority to other cooperative players with negative trust values. However, the conditions of Definition 3 must be satisfied.
References