# Secret Sharing Based on the Social Behaviors of Players

Mehrdad Nojoumian and Douglas R. Stinson

David R. Cheriton School of Computer Science

**Definition 2.** *The Social Secret Sharing Scheme $S^4$ is a three-tuple denoted as $S^4(Sha; Tun; Rec)$ consisting of secret sharing, social tuning, and secret recovery. The only difference compared to the threshold scheme is $Tun$, where the weight of each $P_i$*

**Share Renewal.** In the rst phase, initial shares for newcomers or newly activated *ids* of existing players are generated. For the sake of simplicity, assume each participant has one identi er in the following enrollment protocol. As a result, $t$ players are enough to generate the initial share for a newcomer. We also assume this protocol is executed in a single time slot. In the second phase, players proactively update their shares [1], while disenrolled *ids* do not receive any more shares.

`Phase-1: enrollment protocol`

1. First, $t$ players $P_i$ are selected (e.g., 1 $i$ $t$), and then each of these players computes his corresponding Lagrange constant: $_i$ = Q$_{1\ j\ t;i\neq j}$($k$ $j$)=($i$ $j$), where $i; j; k$ are players' *ids*.
2. After that, each participant $P_i$ multiplies his share $'_i$ by his Lagrange interpolation constant, and randomly splits the result into $t$ portions, i.e., $'_i$ $_i$ = $@_{1i}$ + $@_{2i}$ + + $@_{ti}$ for 1 $i$ $t$.
3. Players exchange $@_{ji}$'s accordingly through pairwise channels. Therefore, each $P_j$ holds $t$ values. $P_j$ adds them together and sends the result to $P_k$, that is, $_j$ = P$^{t}_{i=1}$ $@_{ji}$.
4. Finally, player $P_k$ adds these values $_j$ for 1 $j$ $t$ together to compute his share $'_k$ = P$^{t}_{j=1}$ $_j$.

`Phase-2: renewal protocol`

1. To update shares, each player $P_u$ generates a random polynomial $g^u(x)$ 2 $\mathbb{Z}_q[x]$ of degree $t$ 1 with a zero constant term.
2. Player $P_u$ then sends $w_i$ shares to $P_i$ for 1 $i$ $n$. That is, $^{u}_{ij}$ = $g^u(\#_{ij})$ for 1 $j$ $w_i$, where $\#_{ij}$ = $im$ $m$ + $j$ and $m$ is the maximum weight of any participant.
3. Finally, each player $P_i$ updates his share by adding up the auxiliary shares $^{u}_{ij}$ to his share $'_{ij}$ as follows: $'_{ij}$ = $'_{ij}$ + P$^{n}_{u=1}$ $^{u}_{ij}$ for 1 $j$ $w_i$.

### 3.3 Secret Recovery ($\mathcal{R}ec$)

Authorized players 2 are able to recover the secret if P$_{P_i 2}$ $w_i$ $t$. In this case, players $P_i$ 2 send their shares $'_{ij}$ for 1 $j$ $w_i$ to a selected participant to reconstruct $f(x)$ by Lagrange interpolation, consequently, the secret $f(0)$ = is recovered.

**Theorem 4.** *Our social secret sharing scheme $S^4(Sha; Tun; Rec)$ is unconditionally secure under the passive mobile adversary model.*

*Proof.* The security of $Sha$ and $Rec$ are the same as the security of the Shamir's secret sharing scheme [4]. The security of $Tun$ depends on the share renewal step which is proven in [3].

## 4 Conclusion

The proposed scheme has a variety of desirable properties: it is *unconditionally secure*, meaning that it does not rely on any computational assumptions; *proactive*, refreshing shares at each cycle without changing the secret; *dynamic*, allowing changes to the access structure after the initialization; *weighted*, allowing the cooperative players to gain more authority in the scheme.

## References

[1] Herzberg, A., Jarecki, S., Krawczyk, H., and Yung, M. Proactive secret sharing or: How to cope with perpetual leakage. In *CRYPTO* (1995), D. Coppersmith, Ed., vol. 963 of *LNCS*, Springer, pp. 339{352.

[2] Nojoumian, M., and Lethbridge, T. A New Approach for the Trust Calculation in Social Networks. In *E-business and Telecommunication Networks: 3rd ICE-B, Selected Papers* (2008), vol. 9, Springer, pp. 64{77.

[3] Nojoumian, M., Stinson, D. R., and Grainger, M. Unconditionally secure social secret sharing scheme. *To appear in IET Information Security, Special Issue on Multi-Agent and Distributed Information Security* (2010).

[4] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (1979), 612{613.