SECURITY AND COMMUNICATION NETWORKS
r . r 2010; :1 12
N DOI: 10.1002/ ec

RESEARCH ARTICLE

[illegible]

Z ba E a *1, Na a Pa a 2 a d Me dad N u a 3

[1] De a e C u e Sc e ce, S a d Be e U e , G.C., Te a , I a .
[2] I a a Re eac I u e I a Sc e ce a d Tec (IRANDOC), Te a , I a .
[3] De a e C u e & E ec ca E ee a d C u e Sc e ce, F da A a c U e , B ca Ra , USA.

[illegible]

The concept of *social secret sharing* was introduced in 2010 by Nojoumian et al. In Nojoumian et al.'s scheme (called SSS), the number of shares allocated to each party depends on the player's reputation and the way he interacts with other parties. In other words, weights of the players are periodically adjusted such that cooperativIn othe5niversityG.C.,ersitymosucther word-2

as applications of SSS in the context of cloud computing, rational cryptography and multiparty computation.

The initial social secret sharing construction is shown to be secure in both passive and active adversary models. For the later case, the authors use the verifiable proactive secret sharing scheme of [6] in their protocols. In SSS, reputation of each participant is re-evaluated periodically based on his availability and subsequently, the player's authority (i.e., player's weight or number of shares) will be adjusted. To make participants' old shares (from previous time period) invalid in the next time interval, each player's shares are proactively renewed at the beginning of each period while the secret remains unchanged. Finally, to provide various number of shares for different players, Nojoumian et al. use Shamir's weighted threshold secret sharing scheme [2]. As a result, the size of the share that each player receives is proportional to his assigned weight (which is determined based on his reputationo96-250(his)-0G0g1

Let $' = \{g_0; g_1; \ldots; g_{N-1}\}$ be a system of linearly independent, $N - 1$ times continuously differentiable real-valued, functions and $I'(E) = \{\alpha_i : i = 1; \cdots; N\}$ be a vector that is obtained by lexicographically ordering of entries of $I(E)$ (in $I'(E)$ the pair $(i; k)$ precedes $(i'; k')$ if and only if $i < i'$ or $i = i'$ and $k < k'$). Furthermore, let $\alpha_i(1)$ and $\alpha_i(2)$ denote the first and second elements of the pair $\alpha_i \in I'(E)$. Finally, let $C' = \{c_i' : i = 1; \cdots; N\}$ be another vector that is obtained by lexicographically ordering of entries of C (the ordering procedure is done based on indexes of elements in C).

Now, by using the elements $E; X$ and $'$, we are able to solve the Birkhoff interpolation problem as follows:

$$P(x) = \sum_{j=0}^{N-1} \frac{|A(E; X; '_j)|}{|A(E; X; ')|} g_j(x); \qquad (2)$$

where

$$A(E; X; ') = (a_{ij})_{N \times N}; \qquad (3)$$

$a_{ij} = g_{j-1}^{(\alpha_i(2))}(x_{\alpha_i(1)})$ for $i = 1; \cdots; N$ and $j = 1; \cdots; N$, $|\cdot|$ is the determinant operation and $A(E; X; '_j)$ can be computed by replacing $(j + 1)$-th column of matrix (3) with C'.

Equation (2) is widely used to construct hierarchical threshold secret sharing schemes using Birkhoff interpolation [18, 20, 21, 24]. However, relying upon this equation in which the entire column C' should be available, it might seem that we can not employ Birkhoff interpolation to construct dynamic or social secret sharing schemes (where each shareholder has access to only one entry of C'). In the following, we show how this equation can be modified to solve the problem.

By reformulating equation (2) (i.e., by expanding $|A(E; X; '_j)|$ down to its $(j + 1)$-th column), we have the following equation for the Birkhoff interpolating procedure (equation (1)):

$$P(x) = \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (-1)^{(i+j)} c_{i+1}' \frac{|A_i(E; X; '_j)|}{|A(E; X; ')|} g_j(x); \qquad (4)$$

which can be rewritten as

$$P(x) = \sum_{i=0}^{N-1} c_{i+1}' \sum_{j=0}^{N-1} (-1)^{(i+j)} \frac{|A_i(E; X; '_j)|}{|A(E; X; ')|} g_j(x) \quad ; \qquad (5)$$

where $A_i(E; X; '_j)$ can be computed from $A(E; X; '_j)$ by removing $(i + 1)$-th row and $(j + 1)$-th column.

Example 1 (Birkhoff Interpolation)
Let assume $X = \{1; 2; 3; 4\}$, $C = C' = \{c_1 = 10; c_2 = 28; c_3 = 24; c_4 = 6\}$ and matrix E be as follows:

$$E = \begin{matrix} 1 & 0 & 0 & \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \; :$$

As a result, we have $N = 4$ and $I(E) = I'(E) = \{\alpha_1 = (1; 1); \alpha_2 = (2; 1); \alpha_3 = (3; 3); \alpha_4 = (4; 4)\}$. It is easy to check that the Birkhoff interpolation problem that power such that $q > max\{2^{-t_1+2} \cdot (t_1 - 1)^{(t_1-1)}$

The sharing protocol

On input the secret $S \in GF(q)$, the dealer proceeds as follows:

1. With the assumption of equal authority for all the participants at the beginning of the sharing, gives all of them the same initial trust value $\xi_I = \xi_1 + (\xi_2 - \xi_1)$=2.
2. Let I_c be the subinterval that the initial trust value ξ_I belongs to and let $\mathcal{U}_c$ be the corresponding authority level. Places all the participants in $\mathcal{U}_c$, i.e., it is assumed that $\mathcal{U} = \mathcal{U}_c$ at the beginning of the sharing.
3. Generates a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t_1-2} x^{t_1-2} + S x^{t_1-1}$ over $GF(q)$, where $\{a_i\}_{i=0}^{t_1-2}$ are random values.
4. Computes the share corresponding to each participant $P_i \in \mathcal{U}$ as sh_P

The share renewal phase

Let $Autsub = \{P_{\alpha_0}; \cdots ; P_{\alpha_{t_k-1}}\}$ be an authorized subset of participants such that $ID_{P_{\ i}} < ID_{P_{\ i+1}}$ for $i = 0; \cdots ; t_k - 2$. Then, in order to renew the share of each participant $P_\beta \in \mathcal{U}$:

1. Each participant $P_{\alpha_i} \in Autsub$:

   (a) Constructs a polynomial $f_{1\alpha_i}(x) = a_{0\alpha_i} + \cdots + a_{(t_1-3)\alpha_i}x^{t_1-3} + a_{(t_1-2)\alpha_i}x^{t_1-2}$ over $GF(q)$, where $\{a_{j\alpha_i}\}_{j=0}^{t_1-2}$ are random values. Note that the degree of $f_{1\alpha_i}(\cdot)$ is $t_1 - 2$.

   (b) Uses his share from the previous time period and constructs a polynomial $f_{2\alpha_i}(x) = {}_{j=0}^{t_k-1}$ $[(-1)^{(i+j)} sh_{\alpha_i}(\frac{|A_i(E;X;'_j)|}{|A(E;X;')|})(\frac{(j)!}{(j+t_1-t_k)!})x^{j+t_1-t_k}]$ over $GF(q)$, where E is the interpolation matrix corresponding to the participants in $Autsub$ and their former authorities, i.e., $e_{i;t_k-t_j+1} = 1 \Leftrightarrow P_{\alpha_i} \in \mathcal{U}_j$, the other entries of E are all 0, $X = \{ID_{P_{\ 0}}; ID_{P_{\ 1}}; \cdots ; ID_{P_{\ t_k-1}}\}$, ID_{P_i} is the former identity of P_i and $' = \{1; x; x^2; \cdots ; x^{t_k-1}\}$.

   (c) Computes $f_{\alpha_i}(x) = f_{1\alpha_i}(x) + f_{2\alpha_i}(x)$.

   (d) For each $P_\beta \in \mathcal{U}$:

      i. Computes a subshare of P_β's new share from the secret S as $sh_{P_{\ i} \rightarrow}$

[illegible]

Next, our proposed construction is compared with Nojoumian et al.'s scheme in terms of the computational complexity. The comparison is based on the number of multiplication operations performed in each protocol.

Let n denote the maximum number of parties who can join the scheme and let t be the threshold of the scheme; note that $n > t$. Also, let w (for the sake of simplicity $w = t$) be the maximum weight of each player in Nojoumian et al.'s scheme. In our construction, the number of players in authorized subsets are not fixed (i.e., there can be authorized subsets with the size of $t_1, t_2, \cdots,$ or t_m). As a result, the computational complexity of the social tuning and reconstruction protocols of our scheme depends on the number of parties who execute these protocols. Therefore, we consider the worst case scenario where the size of the subset of players is equal to t_1. Furthermore, it would be realistic to assume that, in our scheme, the authority of each player belonging to the lowest level is equal to the authority of a player who possesses only one share in Nojoumian et al.'s scheme, that is, $t_1 = t$.

In the sharing protocol of our scheme, the dealer computes the derivatives of a polynomial of degree $t - 1$, which can be done in $O(t^2)$. Furthermore, he performs, at most, n polynomial evaluations. The computational complexity of a polynomial evaluation (for a polynomial of degree t) is $O(t)$. As a result, the sharing protocol of our scheme has a complexity of $O(t^2 + tn) \in O(tn)$. In Nojoumian et al.'s scheme, the dealer performs, at most, wn polynomial evaluations where degrees of polynomials are t. Therefore, the sharing protocol of Nojoumian et al.'s scheme has a complexity of $O(wtn) \in O(t^2 n)$.

In both constructions, the share renewal phase is the time consuming part of the social tuning protocol. In our scheme, each player requires to compute a polynomial using his old share and parts of the Birkhoff interpolation method (Item 1.b of Figure 4). Furthermore, he computes different derivatives of a polynomial of degree $t - 1$ at n points (Item 1.d of Figure 4). The former procedure has a complexity of $O(t^4)$ using the naive approach, i.e., computing $t + 1$ determinants of size $t \times t$ according to equation (2). However, it is known that the determinant of an $t \times t$ matrix can be computed in $O(M(t))$ time, where $M(t)$ is the minimum time required to multiply any two $t \times t$ matrices [27]. The best known solution for matrix multiplication requires $O(t^{2:373})$ operations [28], therefore, the generation of $f_{1\alpha_i}(\cdot)$ in step 1.b of Figure 4 and the Birkhoff interpolation method have complexities of $O(t^{3:373})$. The latter procedure has a complexity of $O(tn)$. Therefore, the social tuning phase of our scheme requires $O(t^{3:373} + tn)$ operations. However, in the social tuning phase of Nojoumian et al.'s scheme, each player evaluates a polynomial of degree $t - 1$ at wn points, i.e., proactive share update. Assuming $w = t$, this takes $O(t^2 n)$ operations.

Finally, in the reconstruction protocol of our scheme, a trusted party who has access to the shares of an authorized subset of players can recover the secret by solving the corresponding Birkhoff interpolation problem. As we stated earlier, this takes $O(t^{3:373})$ operations. However, the reconstruction protocol of Nojoumian et al.'s scheme uses the Lagrange interpolation method that takes $O(t \log t)$ operations via the Vandermonde matrix.

[illegible] S

We proposed an ideal social secret sharing scheme using a hierarchical TSS scheme. We illustrated that our construction is more efficient in terms of the share size, communication complexity and computational complexity of the "sharing" protocol compared to the standard social secret sharing scheme. We also showed that the "social tuning" and "reconstruction" protocols of standard social secret sharing are computationally more efficient than those of our proposed scheme. This seems a reasonable compromise because the number of execution of social tuning protocol can be predetermined ahead of time. Furthermore, the reconstruction protocol is executed only once throughout the secret's lifetime. Finally, protecting a single share is less costly and easier than protecting a set of shares.

The proposed scheme is only secure in the passive adversarial model. Using a similar method to the one used in [24], it is straightforward to obtain a computationally secure version of the proposed scheme in the active adversarial model. However, modifying the proposed scheme in such a way that the result would

Symposium on Foundations of Computer Science FOCS, 1985; 383–395.

4. Feldman P. A Practical Scheme for Non-interactive Verifiable Secret Sharing. *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, SFCS ’87, 1987; 427–438.
5. Pedersen TP. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO ’91, 1992; 129–140.
6. Stinson DR, Wei R. Unconditionally secure proactive secret sharing scheme with combinatorial structures. *Selected Areas in Cryptography*, *Lecture Notes in Computer Science*, vol. 1758. Springer, 2000; 200–214.
7. Herzberg A, Jarecki S, Krawczyk H, Yung M. Proactive secret sharing or: How to cope with perpetual leakage. *Advances in Cryptology CRYPT0 95*, *Lecture Notes in Computer Science*, vol. 963, Springer, 1995; 339–352.
8. Nojoumian M, Stinson DR. On dealer-free dynamic threshold schemes. *Advances in Mathematics of Communications (AMC)* 2013; **7**(1):39–56.
9. Benaloh JC, Leichter J. Generalized secret sharing and monotone functions. *8th Annual International Cryptology Conference CRYPTO*, *LNCS*, vol. 403, Springer, 1988; 27–35.
10. Nojoumian M, Stinson DR. Brief announcement: Secret sharing based on the social behaviors of players. *29th ACM Symposium on Principles of Distributed Computing (PODC)*, 2010; 239–240.
11. Nojoumian M, Stinson DR, Grainger M. Unconditionally secure social secret sharing scheme. *IET Information Security (IFS), Special Issue on Multi-Agent and Distributed Information Security* 2010; **4**(4):202–211.
12. Nojoumian M, Stinson DR. Social secret sharing in coud computing using a new trust function. *10th IEEE Annual International Conference on Privacy, Security and Trust (PST)*, 2012; 161–167.
13. Nojoumian M, Stinson DR. Socio-rational secret sharing as a new direction in rational cryptography. *3rd International Conference on Decision and Game Theory for Security (GameSec)*, *LNCS*, vol. 7638, Springer, 2012; 18–37.
14. Wang Y, Liu Z, Wang H, Xu Q. Social rational secure multi-party computation. *Concurrency and Computation: Practice and Experience* 2014; **26**(5):1067–1083.
15. Brickell EF. Some ideal secret sharing schemes. *Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT ’89, 1990; 468–475.
16. Lin C, Harn L, Ye D. Ideal perfect multilevel threshold secret sharing scheme. *Information Assurance*

and Security, 2009. IAS ’09. Fifth International Conference on, vol. 2, 2009; 118–121.

17. Simmons GJ. How to (really) share a secret. *Proceedings on Advances in cryptology*, CRYPTO ’88, 1990; 390–448.
18. Tassa T. Hierarchical Threshold Secret Sharing. *Journal of Cryptology* 2007; **20**(2):237–264.
19. Tassa T, Dyn N. Multipartite Secret Sharing by Bivariate Interpolation. *Journal of Cryptology* 2009; **22**(2):227–258.
20. Guo C, Chang CC, Qin C. A hierarchical threshold secret image sharing. *Pattern Recognition Letters* 2012; **33**(1):83–91.
21. Pakniat N, Noroozi M, Eslami Z. Secret image sharing scheme with hierarchical threshold access structure. *Journal of Visual Communication and Image Representation* 2014; **25**(5):1093 – 1101.
22. Basu A, Sengupta I, Sing JK. Secured hierarchical secret sharing using ecc based signcryption. *Security and Communication Networks* 2012; **5**(7):752–763.
23. Padró C, Sáez G. Secret sharing schemes with bipartite access structure. *Information Theory, IEEE Transactions on* 2006; **46**(7):2596–2604.
24. Pakniat N, Noroozi M, Eslami Z. Distributed key generation protocol with hierarchical threshold access structure. *IET Information Security* 2015; **9**:248–255.
25. Eslami Z, Pakniat N, Noroozi M. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata. *Computer Architecture and Digital Systems (CADS), 2015 18th CSI International Symposium on*, 2015; 1–6.
26. Nojoumian M, Lethbridge TC. A new approach for the trust calculation in social networks. *E-business and Telecommunication Networks: 3rd International Conf on E-Business, CCIS*, vol. 9, Springer, 2008; 64–77.
27. Ibarra OH, Moran S, Hui R. A generalization of the fast lup matrix decomposition algorithm and applications. *Journal of Algorithms* 1982; **3**(1):45–56.
28. Williams VV. Multiplying matrices faster than coppersmith-winograd. *44th Symposium on Theory of Computing Conference STOC*, ACM, 2012; 887–898.

DOI: 10.1002/ ec