Evolving Secret Sharing in Almost Semi-honest Model

Jyotirmoy Pramanik[1] and Avishek Adhikari[2]

[1] Taki Government College, Taki, 743429, India
jyotirmoy@tgc.ac.in, jyotirmoy.pramanik2@gmail.com
https://sites.google.com/view/jyotirmoypramanik
[2] Presidency University, 86/1 College Street, Kolkata 700073, India
avishek.maths@presiuniv.ac.in, avishek.adh@gmail.com
https://www.isical.ac.in/~avishek_r/

Abstract. Evolving secret sharing is a special kind of secret sharing where the number of shareholders is not known beforehand, i.e., at time $t = 0$. In classical secret sharing such a restriction was assumed inherently i.e., the the number of shareholders was given to the dealer's algorithm as an input. Evolving secret sharing relaxes this condition. Pramanik and Adhikari left an open problem regarding malicious shareholders in the evolving setup, which we answer in this paper. We introduce a new cheating model, called the almost semi-honest model, where a shareholder who joins later can check the authenticity of share of previous ones. We use collision resistant hash function to construct such a secret sharing scheme with malicious node identification. Moreover, our scheme preserves the share size of Komargodski et al. (TCC 2016).

Keywords: Secret Sharing · Evolving · Malicious · Collision resistance.

1 Introduction

Secret sharing, initially introduced to safekeep cryptographic keys, has now evolved to have numerous applications in other protocols like multiparty computation, private information retrieval etc. The main motto of such a protocol is to *share* an information (usually encoded as a field element) among few *shareholders* so that some *qualified* combinations can recover it back whereas the other *forbidden* combinations may not. Few interesting articles and references on secret sharing are [1–4, 6, 7, 9, 12, 13, 17, 19, 21, 24, 37].

In simple words, evolving secret sharing [25] covers the special case of secret sharing where the number of shareholders is not known beforehand, i.e., at time $t = 0$. In classical secret sharing such a restriction was assumed inherently i.e., the total set of shareholders (or, at least the number of them) was given to the dealer's algorithm (the $\mathsf{ShareGen}$ algorithm) as an input. Evolving secret sharing relaxes this condition. This is a budding research direction that has attracted a good amount of researchers such as [10, 11, 16, 18, 20, 23, 26, 30].

In secret sharing, be it classical (bounded set of shareholders) or evolving, the context of *cheating* varies. For example, in *semi-honest* setup, shareholders follow the protocol but try to learn more information than their entitlement. On the other hand, *malicious* cheaters may deviate from the protocol according to their whim. In this manuscript, now onwards, we shall abuse the word 'cheater' to mean malicious cheaters only. In literature there exist many schemes which address cheaters such as [5, 8, 15, 14, 22, 27–29, 31–35].

Open problem: Despite some good amout of research in evolving secret sharing, to the best of our knowledge no work on malicious node detection or the so called *cheater identification* has been done yet. This question was asked by Pramanik and Adhikari in [30]. We answer this question in this paper using collision resistant hash functions and assumption of a public bulletin board. To the best of our knowledge, evolving schemes preserve qualified sets, i.e., once qualified, a set always remains so. We maintain this assumption in this work.

Organization: In section 1.1, we discuss threshold evolving secret sharing. In section 2, we breifly discuss hash functions. In section 3, we define a new model of cheating called the almost semi-honest model. We present our construction in section 4. In section 5, we leave two open problems.

Notations: In this work, we use the notations given in Appendix.

1.1 Threshold Evolving Secret Sharing

For completion, allow us to summarize how a threshold evolving secret sharing scheme, also known as (k, ∞) secret sharing scheme works. A shareholder, when he arrives, is assigned to a generation by the dealer. To be specific, $t \in \mathbb{N}$ is assigned to generation $g = \log_k t$. Naturally, the generations grow in size: For $g = 0, 1, 2, \ldots$ the g-th generation begins with the arrival of the k^g-th party. Hence, the size of the g-th generation is $size(g) = k^{g+1} - k^g = (k-1).k^g$. We state the evolving secret sharing on threshold access structure by [25] in figure 1.

Evolving Secret Sharing in the Threshold Setup

Let s be an l-bit secret. During the beginning of a generation g, the dealer stores k^g many l-bit strings s_A for all $A = (u_0, \ldots, u_{g-1}) \in \{0, \ldots, k\}^g$ (where if $g = 0$ it preserves only s). Each such s_A is an l-bit string that we share to the shareholders in generation g assuming that in generation $i \in \{0, \ldots, g-1\}$, u_i parties arrived.

2 Hash Functions

Cryptographic hash functions or simply hash functions play an important role in efficiently 'hiding' an information. To be specific, a hash function $\mathcal{H}$ takes as input an arbitrary bit string x and outputs a fixed length output $\mathcal{H}(x)$. A hash function $\mathcal{H} : \mathcal{X} \to \mathcal{Y}$ is called *one way* or *pre-image resistant* if for given $y \in \mathcal{Y}$

(k, ∞) Secret Sharing

The owner of the secret sets the value of s_A where $A = (u_0, \ldots, u_g)$ as follows:
(Notation: let $s_{prev(A)} = s$ if $g = 0$ and $s_{prev(A)} = s_{(u_0,\ldots,u_{g-1})}$ otherwise.)

1. If $u_g = 0$, then set $s_A = s_{prev(A)}$ and HALT.
2. If $u_0 + \cdots + u_g < k$, then the owner of the secret:
   (a) samples $r_A \leftarrow \{0,1\}^l$ uniformly at random.
   (b) sets $s_A = s_{prev(A)} \oplus r_A$.
   (c) shares the l-bits r_A among the shareholders in the g-th generation using any ideal $(u_g, size(g))$-threshold secret sharing scheme (for example, Shamir's [37]).
3. If $u_0 + \cdots + u_g = k$, then the dealer shares the l-bit string $s_{prev(A)}$ among the parties in the g-th generation using using any ideal $(u_g, size(g))$-threshold secret sharing scheme.

Fig. 1. Construction of (k, ∞) Secret Sharing due to [25].

there is no efficient algorithm to find $x \in \mathcal{X}$ such that $\mathcal{H}(x) = y$. $\mathcal{H}$ is called *second pre-image resistant*, if for $x \in \mathcal{H}$, there is no efficient algorithm to find $x'(\neq x) \in \mathcal{X}$ such that $\mathcal{H}(x) = \mathcal{H}(x')$. In case of *collision resistant* hash function, there is no efficient algorithm to find distinct $x, x' \in \mathcal{X}$ such that $\mathcal{H}(x) = \mathcal{H}(x')$. It can be shown that collision resistance implies second pre-image resistance, which further implies onewayness. For further reading on the same one may refer [36, 38].

3 The 'Almost' Semi-Honest Model

We introduce a new cheating model in (evolving) secret sharing, called the almost semi-honest model. In this model, in short, a malicious shareholder may choose to submit incorrect (arbitrary) shares for reconstruction of the shared bit(s) but with a very high probability, will be detected by the *latter* shareholders, if so. Let us explain the same by the following game (figure 2).

Let $\mathcal{C}^{(r)}_{success}$ denote the probability that all the honest shareholders participating in $\mathsf{Reconst}$ accept share submitted by at least one $P_r \in \mathcal{L}_{\mathcal{C}}$. We call an evolving secret sharing scheme ϵ-secure if $\mathcal{C}^{(r)}_{success} < \epsilon$, $\forall P_r \in \mathcal{L}_{\mathcal{C}}$. We call this model *almost semi-honest*, because the latter shareholders' authenticity cannot be verified by prior shareholders, as, once distributed, refreshing of shares are not allowed.

Game between the scheme and a centralized cheater $\mathcal{C}$

1. A centralized cheater $\mathcal{C}$ chooses a *last* cheating shareholder.
2. $\mathcal{C}$ may corrupt at most c shareholders arrived before him. Let their collection be denoted by $\mathcal{L}_{\mathcal{C}}$.
3. Reconst round takes place, strictly consisting of at least one shareholder who has arrived after the last cheating shareholder.
4. In the reconstruction round Reconst, some of the shareholders in $\mathcal{L}_{\mathcal{C}}$ submit false shares.

Fig. 2. Cheating model

4 Our Construction

Let Π_k denote the (k, ∞) scheme described above, for some positive integer $k > 1$. Also, let $\mathcal{H}$ denote a collision resistant hash function. $\mathcal{H}$ is made public. Moreover, let c denote the maximum number of corruptions possible, where $k \geq 2c + 1$, i.e., we assume honest majority. We describe our construction in figure 3.

The scheme described above is an instance of (k, ∞) secret sharing with cheater identification property. To support our claim, we study the scheme case by case.

External view: An external shareholder with no shares can only view the hash function $\mathcal{H}$ and the digest of shares. Due to properties of hash function, it hides the shares. Similar arguments apply for a forbidden set.

Qualified set with no cheaters: In this case, whenever a qualified set of shareholders wish to recover the secret, they use the reconstruction algorithm of Π_k and recover the secret bit(s). Moreover, they cannot guess the shares of the other shareholders from their digest.

Cheaters' view: The c colluding cheaters can, before the secret reconstruction phase takes place, see c of their shares and the public digests of other shares, the latter of which doesn't aid them. Moreover, c shares in a k threshold scheme, is not enough to learn the secret bit(s).

Semi-honest shareholders' view: The honest shareholders may easily check the authenticity of modified shares by verifying using the public digest. Suppose the security parameter of the hash $\mathcal{H}$ is δ, then the probability that at least one of the cheaters modifies share but does not get caught is bounded above by $c \cdot 2^{-\delta}$. In other words, our construction is $c \cdot 2^{-\delta}$-secure.

A construction for (k, ∞) secret sharing with cheater identification

Dealer's Algorithm: The dealer shares a bit secret as follows.

1. When the t^{th} shareholder arrives, the dealer calls the share generation protocol of Π_k and outputs a share v_t.
2. Moreover, the dealer calculates the hash $\mathcal{H}(v_t)$, and publishes it on a public bulletin board.
3. The t^{th} shareholder is handed over his share v_t.

Reconstructing Shareholders' Algorithm: Suppose at some point of time t, a set of shareholders $\mathcal{R}_t \subset \mathcal{A}_t$, the latest access structure, wish to recover the secret bit(s).

1. If the reconstructing shareholders do not form a qualified set, ABORT.
2. If they form a qualified set:
   (a) (Round-1): Every shareholder announces his share.
   (b) (Local computation): Every shareholder P_i checks if v_s where $s \in \{j : P_j \in \mathcal{R}_t\} \setminus \{i\}$ matches its hash from the public bulletin. If it doesn't match for some shareholder, he marks him as a cheater.
   (c) If a shareholder gets marked as a cheater by at least $c + 1$ shareholders, he is put in a list $\mathcal{L}$ of cheaters. If $\mathcal{R} \setminus \mathcal{L}$ remains a qualified set, they reconstruct using the reconstruction algorithm of Π_k and output the secret bit(s) and $\mathcal{L}$, else they output a symbol $\perp$ and $\mathcal{L}$.

Fig. 3. The Construction

Note that our construction preserves the share size of the underlying (k,∞) scheme, namely that of [25]. Based on the case by case discussion above, we may restate the following result from [25], modified to suit our context.

Theorem 1. *For every $k, l \in \mathbb{N}$ our construction gives a secret sharing scheme for the evolving (k,∞) access structure with cheater identification and an l-bit secret in which for every $t \in \mathbb{N}$ the share size of the t^{th} party is bounded by $kt \cdot \max\{l, \log kt\}$. The construction is $c \cdot 2^{-\delta}$ secure.*

The share size may be further modified to $(k-1)\log t + 6k^4 l \log\log t \cdot \log\log\log t + 7k^4 l \log k$.

5 Concluding Remarks

In this paper, we answer the open problem from [30] regarding cheating shareholders in the evolving setup. For the same, we introduce a new cheating model, called the almost semi-honest model, where a shareholder who joins later can check the authenticity of share of previous ones. We use collision resistant hash function to construct such a secret sharing scheme with malicious node identification. Moreover, our scheme preserves the share size of [25].

The kind of model that we introduce here probably does the best that can be done in the evolving setup, since refreshing shares is not allowed. However, the authors are hopeful that the use of public bulleting board may not be mandatory and leave that as an open problem. In this regard, use of some decentralized mechanism like blockchain might be of interesting, and demands more research in this direction. Moreover, since, evolving secret sharing schemes are, as it is, expensive, use of hash function, yielding computational security instead of information theoretic security, is probably a better option . Constructing information theoretically secure cheater identifiable evolving secret sharing scheme is left as another open problem.

Acknowledgment

The research of the second author is partially supported by DST-SERB Project MATRICS vide Sanction Order: MTR/2019/001573 and DST-FIST project. In the end, the authors would like to thank the anonymous reviewers who have suggested constructive modifications, rectifications and amplifications, resulting in the current form of manuscript.

References

1. A. Adhikari. Linear Algebraic Techniques to Construct Monochrome Visual Cryptographic Schemes for General Access Structure and Its Applications to Color Images. *Designs, Codes and Cryptography*, 73(3):865–895, Dec 2014.

2. A. Adhikari and M. Bose. A New Visual Cryptographic Scheme using Latin Squares. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, pages 1198–1202, 05 2004.
3. A. Adhikari, M. Bose, D. Kumar, and B. K. Roy. Applications of Partially Balanced Incomplete Block Designs in Developing $(2, n)$ Visual Cryptographic Schemes. *IEICE Transactions*, 90-A(5):949–951, 2007.
4. A. Adhikari, T. K. Dutta, and B. K. Roy. A New Black and White Visual Cryptographic Scheme for General Access Structures. In *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, pages 399–413, 2004.
5. A. Adhikari, K. Morozov, S. Obana, P. S. Roy, K. Sakurai, and R. Xu. Efficient threshold secret sharing schemes secure against rushing cheaters. In *Information Theoretic Security - 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers*, pages 3–23, 2016.
6. A. Adhikari and S. Sikdar. A New $(2, n)$-Visual Threshold Scheme for Color Images. In *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, pages 148–161, 2003.
7. M. R. Adhikari and A. Adhikari. *Basic Modern Algebra with Applications*. Springer, 2014.
8. T. Araki. Efficient (k, n) threshold secret sharing schemes secure against cheating from n-1 cheaters. In *Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Townsville, Australia, July 2-4, 2007, Proceedings*, pages 133–142, 2007.
9. A. Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, pages 11–46, 2011.
10. A. Beimel and H. Othman. Evolving ramp secret-sharing schemes. In *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, pages 313–332, 2018.
11. A. Beimel and H. Othman. Evolving ramp secret sharing with a small gap. In *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, pages 529–555, 2020.
12. G. R. Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on(AFIPS)*, volume 00, pages 313–317, 12 1979.
13. E. F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, pages 468–475, 1989.
14. S. Cabello, C. Padró, and G. Sáez. Secret sharing schemes with detection of cheaters for a general access structure. *Des. Codes Cryptography*, 25(2):175–188, 2002.
15. M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Des. Codes Cryptography*, 5(3):183–187, 1995.
16. S. S. Chaudhury, S. Dutta, and K. Sakurai. AC^0 constructions for evolving secret sharing schemes and redistribution of secret shares. *IACR Cryptol. ePrint Arch.*, 2019:1428, 2019.
17. R. Cramer, I. B. Damgård, N. Döttling, S. Fehr, and G. Spini. Linear secret sharing schemes from error correcting codes and universal hash functions. In *Advances in*

Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II, pages 313–336, 2015.
18. P. D'Arco, R. D. Prisco, A. D. Santis, A. L. P. del Pozo, and U. Vaccaro. Probabilistic secret sharing. In *43rd International Symposium on Mathematical Foundations of Computer Science, MFCS 2018, August 27-31, 2018, Liverpool, UK*, pages 64:1–64:16, 2018.
19. A. Das and A. Adhikari. An efficient multi-use multi-secret sharing scheme based on hash function. *Appl. Math. Lett.*, 23(9):993–996, 2010.
20. Y. Desmedt, S. Dutta, and K. Morozov. Evolving perfect hash families: A combinatorial viewpoint of evolving secret sharing. In *Cryptology and Network Security - 18th International Conference, CANS 2019, Fuzhou, China, October 25-27, 2019, Proceedings*, pages 291–307, 2019.
21. S. Dutta, T. Bhore, M. K. Sardar, A. Adhikari, and K. Sakurai. Visual secret sharing scheme with distributed levels of importance of shadows. In *Proceedings of the Fifth International Conference on Mathematics and Computing - ICMC 2019, Bhubaneswar, India, February 6-9, 2019*, pages 19–32, 2019.
22. S. Dutta, P. S. Roy, A. Adhikari, and K. Sakurai. On the robustness of visual cryptographic schemes. In *Digital Forensics and Watermarking - 15th International Workshop, IWDW 2016, Beijing, China, September 17-19, 2016, Revised Selected Papers*, pages 251–262, 2016.
23. S. Dutta, P. S. Roy, K. Fukushima, S. Kiyomoto, and K. Sakurai. Secret sharing on evolving multi-level access structure. In *Information Security Applications - 20th International Conference, WISA 2019, Jeju Island, South Korea, August 21-24, 2019, Revised Selected Papers*, pages 180–191, 2019.
24. S. Dutta, M. K. Sardar, A. Adhikari, S. Ruj, and K. Sakurai. Color visual cryptography schemes using linear algebraic techniques over rings. In *Information Systems Security - 16th International Conference, ICISS 2020, Jammu, India, December 16-20, 2020, Proceedings*, pages 198–217, 2020.
25. I. Komargodski, M. Naor, and E. Yogev. How to share a secret, infinitely. In *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, pages 485–514, 2016.
26. I. Komargodski and A. Paskin-Cherniavsky. Evolving secret sharing: Dynamic thresholds and robustness. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, pages 379–393, 2017.
27. K. Kurosawa, S. Obana, and W. Ogata. t-cheater identifiable (k, n) threshold secret sharing schemes. In *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings*, pages 410–423, 1995.
28. W. Ogata and H. Eguchi. Cheating detectable threshold scheme against most powerful cheaters for long secrets. *Des. Codes Cryptography*, 71(3):527–539, 2014.
29. J. Pramanik and A. Adhikari. Ramp secret sharing with cheater identification in presence of rushing cheaters. *Groups Complexity Cryptology*, 11(2):103–113, 2019.
30. J. Pramanik and A. Adhikari. Evolving secret sharing with essential participants. In *Proceedings of International Conference on Frontiers in Computing and Systems*, pages 691–699. Springer Singapore, 2021.
31. J. Pramanik, S. Dutta, P. S. Roy, and A. Adhikari. Cheating detectable ramp secret sharing with optimal cheating resiliency. In *Information Systems Security - 16th International Conference, ICISS 2020, Jammu, India, December 16-20, 2020, Proceedings*, pages 169–184, 2020.

32. J. Pramanik, P. S. Roy, S. Dutta, A. Adhikari, and K. Sakurai. Secret sharing schemes on compartmental access structure in presence of cheaters. In *Information Systems Security - 14th International Conference, ICISS 2018, Bangalore, India, December 17-19, 2018, Proceedings*, pages 171–188, 2018.
33. P. S. Roy, A. Adhikari, R. Xu, K. Morozov, and K. Sakurai. An efficient robust secret sharing scheme with optimal cheater resiliency. In *Security, Privacy, and Applied Cryptography Engineering - 4th International Conference, SPACE 2014, Pune, India, October 18-22, 2014. Proceedings*, pages 47–58, 2014.
34. P. S. Roy, A. Adhikari, R. Xu, K. Morozov, and K. Sakurai. An efficient t-cheater identifiable secret sharing scheme with optimal cheater resiliency. *IACR Cryptology ePrint Archive*, 2014:628, 2014.
35. P. S. Roy, S. Dutta, K. Morozov, A. Adhikari, K. Fukushima, S. Kiyomoto, and K. Sakurai. Hierarchical secret sharing schemes secure against rushing adversary: Cheater identification and robustness. In *Information Security Practice and Experience - 14th International Conference, ISPEC 2018, Tokyo, Japan, September 25-27, 2018, Proceedings*, pages 578–594, 2018.
36. S. K. Sanadhya and P. Sarkar. New collision attacks against up to 24-step SHA-2. In *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings*, pages 91–103, 2008.
37. A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
38. L. Song, G. Liao, and J. Guo. Non-full sbox linearization: Applications to collision attacks on round-reduced keccak. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, pages 428–451, 2017.

Appendix

Here we collect all the symbols used in this work.

Symbol	**Meaning**
t	time
l	bit length of secret value
$\mathsf{ShareGen}$	share distribution protocol
$\mathsf{Reconst}$	secret recovery protocol
k	secret recovery threshold
g	generation number
$a \leftarrow X$	sampling an element a from the set X
$\oplus$	addition modulo 2
$size(g)$	size of the g^{th} generation
$\mathcal{C}$	centralized malicious cheater
$\mathcal{L}_{\mathcal{C}}$	shareholders under control of $\mathcal{C}$
Π_k	the (k, ∞) secret sharing due to [25]
$\mathcal{H}$	collision resistant hash
$\mathcal{A}_t$	restriction of access structure at time t
$\mathcal{R}_t$	reconstructing shareholders from $\mathcal{A}_t$
P_t	t^{th} shareholder