Multiplicative Linear Secret Sharing Without Interaction

Bo Mi, Darong Huang(✉), Jianqiu Cao, Ping Long, and Hongyang Pan

Institute of Information Science and Engineering, Chongqing Jiaotong University, Chongqing 400074, China
drhuang@cqjtu.edu.cn

Abstract. As an essential building block in cryptosystem, linear secret sharing is widely used to safeguard the confidentiality and reliability of outsourced data. Though addition and constant multiplication are extremely easy thanks to the linear operation over shared secrets, how to efficiently multiply multiple shares remains an open problem. In this paper, we devised a non-interactive multiplication scheme based on Shamir's secret sharing without parameter constrain. It is proved that our scheme is unconditionally secure if no more than k participants are compromised, meaning that both the security and access structure of Shamir's scheme are immensely retained.

Keywords: Secret sharing · Multiplication · Polynomial convolution · Unconditional security · Q2 access structure

1 Introduction

With the advent of big data era, massive information is collected, accessed and operated all the way. Nevertheless, large amounts of privacies relevant to these data are confronted with the peril of revelation since the communication channels are open and the storages are always consigned [1]. On the other hand, the reliability of stocked data is also prone to damages due to system failure, interference or tampering, which may severely jeopardize the availability of important data [2]. Though functionality and security seem like two contrary goals for information system, lots of cryptographic techs can be used to balance the requirements between them. Oriented to different applications such as secure multi-parity computation) [3], Byzantine agreement [4] and oblivious transfer [5], secret sharing schemes are extensively used as their building block to narrow the gaps of system performance and security [6].

Based on Lagrange polynomial and Chinese remainder theorem, Shamir [7] and Blakley [8] brought about the schemes of secret sharing for the first time. Following their work, a series of secret sharing schemes [9–14] are proposed focusing on specific access structures. Though Ito et al. [15] have devised an universal framework to realize secret sharing on general access structure, it is deemed as impractical since the share size is extraordinary large. However, once the access structure is equivalent to a small monotone span program, efficient secret sharing schemes can easily be achieved [16, 17].

X. Sun et al. (Eds.): ICAIS 2019, LNCS 11634, pp. 178–187, 2019.
https://doi.org/10.1007/978-3-030-24271-8_16

Another research attraction is related to the communication burden and rounds of secret sharing. As proved by Csirmaz [18], to share a ℓ-bits secret within a n-party network, the lower bound of share size is $\Omega(\ell n/log_2 n)$. Though the share sizes of best known schemes [19, 20] are far more larger than such benchmark, the size of shared data can practically approach $n^{\Omega(log_2 n)}$ by linear secret sharing. In order to conserve the confidentiality of shared secrets when compounded with each other, homomorphic computability is also considered as an important requirement for secret sharing [21]. Aiming at minimizing the traffic overhead, linear secret sharing schemes are always exploited in virtue of non-interactive addition and constant multiplication [22, 23]. However, when two shared secrets are multiplied, how to reduce or even eliminate unnecessary communications still remains an open problem [24]. The original homomorphic multiplication for linear secret sharing is presented by Gennaro et al. with $\ell(2k-1)^2$-bits1-round communication [25], which may incur a severe delay when arithmetic circuits are deep. In fact, as proved by Ishai et al. [26, 27], once more that third of the participants are honest, any circuit can be cryptically evaluated via a 2-round secret sharing protocol. That is to say, refraining the communication from homomorphic multiplication is possible. In [28], Barkol et al. presented a multiplication scheme which enables all participants to secretly convert d distinct secrets into an additive sharing of their product. And its verifiable version was then proposed by Yoshida et al. [29]. However, since the circuit depth is strictly limited by the number of participants and security level, their schemes are incapable of fulfilling the property of fully homomorphism. In order to address such defect, Watanabe et al. [30] devised a FHE (Fully Homomorphic Encryption) scheme at the expense of $2n$ extra shares for each secret. Based on the recursive construction, Blackburn et al. [31] presented an efficient multiplicative sharing scheme where the share size will slightly expand along with the increasing of network scales. Thereafter, Wang et al. [32] pointed out that the forementioned scheme is infeasible within MTA (Mutually Trusted Authority)-free environment [33] and disposed the problem of redundantly operating on the same secret. Moreover, numerous secret sharing schemes are successively proposed utilizing different algebraic structures such as discrete logarithm [34], lattice [35] and Abelian codes [36].

Due to the linear nature and Q2 access structure of Shamir's secret sharing, it is widely used as a building block for privacy-preserving implementation. Moreover, since Shamir's scheme is ideal [9], the size of a shared secret is only ℓn-bits uniformly distributed on n participants, which is commendably close to its lower bound. For the sake of homomorphic computation, the trait of its linearity refrained the operations of addition and constant multiplication from interactions. Nevertheless, even if the best multiplicative secret sharing scheme is exploited, non-negligible delay occurs due to a series of communications.

Considering that the multiplicative circuits are inevitable for most practical applications and the characteristics of low communication along with computation overheads must be conserved for real-time implementation, a non-interactive multiplication scheme is proposed for Shamir's secret sharing in this paper. The main idea is, once the identities of all participants are reasonably regulated, polynomial convolution can play

a part in reducing the overflowed orders incurred by trivial multiplication. The rest of this paper is organized as below.

In Sect. 2, a formal definition regarding Shamir's secret sharing is given, together with the defect analysis of some previous multiplicative secret sharing scheme. Then, a non-interactive multiplicative method and its correctness proof will be depicted in Sect. 3. Section 4 testified that our method is unconditionally secure and its performance is more preferable compared to related schemes. Finally, the paper will be concluded in Sect. 5.

2 Preliminary of Shamir's Secret Sharing

Based on Q2 access structure, Shamir's secret sharing is always recognized as a (k, n)-threshold scheme, where at least k shares amongst n pieces of a secret s should be gather to for information revealing. Since the essential idea of this threshold scheme is that any polynomial of degree $k-1$ can be exclusively determined by k points in virtue of Lagrange interpolation [7], a secret s can be divided into a series of shares $(x_i, f(x_i))$, $i = 1, 2, \cdots, n$, according to a stochastic polynomial

$$f_s(x) = s + a_1 x + a_2 x^2 + \cdots a_{k-1} x^{k-1}. \tag{1}$$

Without loss of generality, we assume that the coefficients a_j, $j = 1, 2, \cdots, k-1$, are independently and uniformly sampled from a finite field $\mathbb{F}_p$, where p is an odd prime. For any secret $s \in \mathbb{F}_p$, the scheme can be formally defined as follows.

Definition 1. The Shamir's secret sharing scheme is a triple function set $\prod = (\mathrm{DIT}, \mathrm{EVL}, \mathrm{REC})$ works on Q2 access structure, where

a. The secret holder computes $\{(x_i, f_s(x_i))\} \overset{\$}{\leftarrow} \mathrm{DIT}(s)$ in terms of formula (1) and distributes them to their correspondent receivers via authenticated and private channels. Denoting A as the set of all adversary structures, if $\mathrm{T} \backslash \mathrm{C} \notin \mathrm{A}$ for any $\mathrm{C} \in \mathrm{A}$ where $\mathrm{T} = \{1, 2, \cdots, n\}$, then

$$\Pr\left[\mathcal{A}\left([s]_{\mathrm{C}}\right) = s\right] = 1/p, \tag{2}$$

where $[s]_{\mathrm{C}}$ represents the set of shares corrupted by adversary $\mathcal{A}$.

b. For any constants c_1, c_2 and a pair of shares $[s_1]_{\mathrm{T}}, [s_2]_{\mathrm{T}}$, it is easy to non-interactively compute $[c_1 s_1 + c_2 s_2]_{\mathrm{T}} \leftarrow \mathrm{EVL}\left([s_1]_{\mathrm{T}}, [s_2]_{\mathrm{T}}, c_1, c_2\right)$ in terms of trivial addition and multiplication. In order to calculate $[s_1 s_2]_{\mathrm{T}} \leftarrow \mathrm{EVL}\left([s_1]_{\mathrm{T}}, [s_2]_{\mathrm{T}}\right)$, interactive fully homomorphic schemes do also exist [25]. When executing the function of $\mathrm{EVL}(\cdot)$, it is obvious that the requirements

$$\Pr\left[\mathcal{A}\left([\cdot]_{\mathrm{C}}, \mathrm{Com}_{\mathrm{T}}\right) = s, s \in \mathrm{S}\right] = 1/p \tag{3}$$

and

$$\Pr\left[\mathcal{A}\left([\cdot]_{\mathrm{C}}, \mathrm{Com}_{\mathrm{T}}\right) = \mathrm{REC}\left(\mathrm{EVL}\left([\mathrm{S}]_{\mathrm{T}}\right)\right)\right] = 1/p \tag{4}$$

must hold, where S stands for the set of original secrets and $[\cdot]_{\mathrm{C}}, \mathrm{Com}_{\mathrm{T}}$ are all corrupted shares along with intercepted communications.

c. Within the Q2 structure, the recovery function $\mathrm{REC}(\cdot)$ is capable of revealing the shared secret by

$$\Pr\left[\mathrm{REC}\left([s]_{\bar{\mathrm{c}}}\right) = s\right] = 1 \tag{5}$$

where $\bar{\mathrm{C}}$ is the complementary set of C.

It is worth noting that the multiplicative secret sharing presented in [25] is feasible only if $n \geq 2k-1$ with non-negligible communications. Though Barkol et al. [28] achieved a non-interactive scheme which can locally multiply d shared secrets, an auxiliary condition where $n > dk$ should also be satisfied. As for Watanabe's method [30], it is capable of performing multiplication even only k share holders are involved, the share size for each secret are 3 times than that of the primitive scheme and $4\ell k$-bits messages must be collected for each participant to achieve a share of multiplication result. To sum up, no existing multiplicative secret sharing scheme is in a position to avoid both interaction and parameter limitation, and that is why our research cut in.

3 Multiplicative Secret Sharing Without Interaction

The main reason that two shares should not be trivially multiplied can be attributed to the remarkable increment of polynomial order. For instance, when two shares $(x_i, f_a(x_i))$ and $(x_i, f_b(x_i))$ are directly multiplied by participant i, the result is $(x_i, f_a(x_i)f_b(x_i))$, where $f_a(x_i)f_b(x_i)$ can be written as

$$f_a(x_i)f_b(x_i) = ab + r_1 x_i + r_2 x_i^2 + \cdots r_{2k-2} x_i^{2k-2} \tag{6}$$

which turns the original scheme into a $(2k-1, n)$-threshold secret sharing. With the help of polynomial convolution, we caught a sight of how to reduce the multiplicative result back to a $k-1$ order polynomial and maintain its raw threshold without interaction.

Assuming that the polynomials $f_a(x_i)$ and $f_b(x_i)$ is represented as

$$f_a(x_i) = (a, a_1, a_2, \cdots, a_{k-1})\left(x_i^0, x_i^1, x_i^2, \cdots, x_i^{k-1}\right)^T \tag{7}$$

and

$$f_b(x_i) = (b, b_1, b_2, \cdots, b_{k-1})\left(x_i^0, x_i^1, x_i^2, \cdots, x_i^{k-1}\right)^T \tag{8}$$

respectively. Then $f_a(x_i)f_b(x_i)$ in formula (6) is equivalent to $\alpha+\beta$, where

$$\alpha=\left(\left(ab, ab_1+ba_1, \cdots, \sum_{\sigma+\tau=\mu} a_\sigma b_\tau, \cdots, \sum_{\sigma+\tau=k-1} a_\sigma b_\tau\right) \bmod p\right)\cdot \left(x_i^0, x_i^1, \cdots, x_i^\mu, \cdots, x_i^{k-1}\right)^T \tag{9}$$

and

$$\beta=\left(\left(\sum_{\sigma+\tau=k} a_\sigma b_\tau, \cdots, \sum_{\sigma+\tau=\omega} a_\sigma b_\tau, \cdots, a_{k-2}b_{k-1}+a_{k-1}b_{k-2}, a_{k-1}b_{k-1}\right) \bmod p\right)\cdot \left(x_i^{k-1}\left(x_i^1, \cdots, x_i^{\omega=k+1}, \cdots x_i^{k-2}, x_i^{k-1}\right)\right)^T, \tag{10}$$

where $a_0=a$ and $b_0=b$. Noting that the order of polynomial α is $k-1$ whose leading coefficient is exactly ab, so if we can figure out β then the share of ab for participant i can be trivially achieved by subtract β from $f_a(x_i)f_b(x_i)$. Based on forementioned observation, we construct a multiplicative secret sharing scheme as below.

Distribution $\{(x_i, f_s(x_i))\} \overset{\$}{\leftarrow} \mathrm{DIT}(s)$:

Define $p<x_i<q$ as the identity of participate i, where $q>p+n$ is a positive integer and $\gcd(x_i,p)=\gcd\left(\left(x_i^{-k}-1\right)^{-1}, p\right)=1$. Then calculate $f_s(x_i)$ according to formula (1) modulo $\left(x_i^k-1\right)$, which will be distributed to i as her share of secret s.

Multiplication $[ab]_\mathrm{T} \leftarrow \mathrm{EVL}\left([a]_\mathrm{T}, [b]_\mathrm{T}\right)$:

Participant i locally computes

$$f_{ab}(x_i)=f_a(x_i)f_b(x_i)-\left(x_i^{-k}-1\right)^{-1}\left(\left(f_a(x_i)f_b(x_i) \bmod \left(x_i^k-1\right)\right)-f_a(x_i)f_b(x_i)\right) \tag{11}$$

modulo $\left(x_i^k-1\right)$ as her share of ab.

Since participant i is provided with all information about $f_a(x_i), f_b(x_i)$ and x_i, no interaction is necessary for her to calculate formula (11). In order to testify the correctness of our protocol, a Lemma is given in advance.

Lemma 1. For $\forall\, \theta \in \{0, 1, \cdots, k-1\}$, if $\left\|\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right\|_\infty < x_i-1$ then

$$\alpha+x_i^{-k}\beta<x_i^k-1. \tag{12}$$

Proof. Since $\alpha+x_i^{-k}\beta$ is a $k-1$ order polynomial, which can be written as $\sum_{\theta=0}^{k-1}\left(\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right)x_i^\theta$, we have

$$0 \le \alpha+x_i^{-k}\beta \le \left\|\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right\|_\infty \left(x_i^0+x_i^1+\cdots+x_i^\theta+\cdots+x_i^{k-1}\right). \tag{13}$$

Once $\left\|\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right\|_\infty < x_i-1$, then

$$\alpha + x_i^{-k}\beta < (x_i - 1)\left(x_i^0 + x_i^1 + \cdots + x_i^\theta + \cdots + x_i^{k-1}\right) \tag{14}$$

and the formula (12) holds.

Now, we are ready to claim the validity of our multiplicative secret sharing scheme in the following theorem.

Theorem 1. If $x_i > p$, any participant i is able to non-interactively multiply the shares of two secrets retaining the property of (k, n)-threshold.

Proof. According to polynomial convolution, the formula $f_a(x_i)f_b(x_i) \bmod \left(x_i^k - 1\right)$ can be represented as $\alpha + x_i^{-k}\beta + t\left(x_i^k - 1\right)$ for some non-positive integer t. Once the condition $\left\|\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right\|_\infty < x_i - 1$ stands, then

$$f_a(x_i)f_b(x_i) \bmod \left(x_i^k - 1\right) = \alpha + x_i^{-k}\beta \tag{15}$$

in terms of Lemma 1. Denoting $\varphi(x_i)$ as

$$\begin{aligned} \varphi(x_i) &= f_a(x_i)f_b(x_i) mod \left(x_i^k - 1\right) - f_a(x_i)f_b(x_i) \\ &= \left(r_0', r_1', \cdots, r_{k-2}', 0, -r_0', -r_1', \cdots, -r_{k-2}'\right) \cdot \\ &\quad \left(x_i^0, x_i^1, \cdots, x_i^{k-2}, x_i^{k-1}, x_i^k, x_i^{k+1}, \cdots, x_i^{2k-2}\right)^T, \end{aligned} \tag{16}$$

where $r_\delta' = \sum_{\sigma=\delta+1}^{k-1} a_\sigma b_{\tau=k-\sigma+\delta}$ for $\delta = \{0, 1, \cdots, k-2\}$, it can be easily seem that

$$\beta = \left(x_i^{-k} - 1\right)^{-1} \varphi(x_i) \tag{17}$$

which is exactly the second term of $\alpha + \beta$. Noting that $\left\|\sum_{\sigma+\tau=\theta \bmod k} a_\sigma b_\tau\right\|_\infty \equiv p - 1 \bmod p$, thus our protocol is correct if $x_i > p$.

4 Security and Performance Analysis

Since the coefficients of polynomial $f_s(x)$ is independently and uniformly sampled from a finite field $\mathbb{F}_p$, the secret s is unconditionally secure if less than k shares are compromised [7]. For clarity, we interpret this property as a formal description.

Lemma 2. The Shamir's secret sharing scheme is unconditionally secure, where the secret recovery advantage of any adversary $\mathcal{A}$ is

$$\begin{aligned} \mathbf{Adv}_{f_s}^{sr}(\mathcal{A}) &= \Pr\left[\mathcal{A}\left([s]_C\right) = s, s \in \mathbb{F}_p\right] \\ &= 1/p, \end{aligned} \tag{18}$$

if $T \backslash C \notin A$ for any $C \in A$ where $T = \{1, 2, \cdots, n\}$.

It is obvious that because no information is exchanged when multiplying two shares $f_a(x_i)$ and $f_b(x_i)$ in our scheme, the secrets a and b are still unconditionally secure according to Lemma 2.

In order to prove the information-theory security of $[ab]_{\mathrm{C}}$, we consider an experiment where the adversary runs $\mathcal{A}$ as a subroutine to recover ab.

$$
\begin{aligned}
&\text{Experiment } \mathbf{Exp}^{sr}_{f_{ab}}(\mathcal{B})\\
&[a]_{\mathrm{T}} \xleftarrow{\$} \mathrm{DIT}(a), [b]_{\mathrm{T}} \xleftarrow{\$} \mathrm{DIT}(b)\\
&[ab]_{\mathrm{T}} \leftarrow \mathrm{EVL}\big([a]_{\mathrm{T}}, [b]_{\mathrm{T}}\big)\\
&b \leftarrow \mathrm{REC}\big([b]_{\bar{c}}\big)\\
&a' \leftarrow \mathcal{A}\big([a]_{\mathrm{C}}\big)\\
&s = a'b\\
&\text{If } s = ab \text{ return } 1, \text{ else return } 0
\end{aligned}
$$

By contrary, our scheme is also unconditionally secure as below.

Theorem 2. The proposed multiplicative scheme is information-theoretically secure, where the advantage of any adversary $\mathcal{B}$ who expect to reveal ab is

$$
\begin{aligned}
\mathbf{Adv}^{sr}_{f_{ab}}(\mathcal{B}) &= \Pr\big[\mathcal{B}\big([ab]_{\mathrm{C}}\big) = ab, ab \in \mathbb{F}_p\big]\\
&= 1/p,
\end{aligned}
\tag{19}
$$

if $\mathrm{T}\backslash\mathrm{C} \notin \mathrm{A}$ for any $\mathrm{C} \in \mathrm{A}$ where $\mathrm{T} = \{1, 2, \cdots, n\}$.

Proof. The proof is straight-forward that if $\mathbf{Adv}^{sr}_{f_{ab}}(\mathcal{B}) > 1/p$, the probability that $\mathcal{B}$ recovers s where $s = ab$ is greater than $1/p$. Since b is plain for him, it implies that $\mathcal{A}$ can reveal a with an advantage $\mathbf{Adv}^{sr}_{f_s}(\mathcal{A}) > 1/p$ as well, which is a contradiction against Lemma 2.

The multiplicative secret sharing scheme in Sect. 3 also suggests that it achieves preferable performance with regard to parameter constrain, share size and communication burden. Three linear secret sharing protocols [25, 28, 30] are investigated for comparison as illustrated in Table 1.

Table 1. Comparison amongst multiplicative secret sharing of [25, 28, 30] and the proposed

Benchmarks	Multiplicative schemes			
	In [25]	In [28]	In [30]	The proposed
Share size (bits)	$n\lceil log_2 p \rceil$	$2n\lceil log_2 p \rceil$	$3n\lceil log_2 p \rceil$	$kn\lceil log_2 q \rceil$
Parameter constrain	$n > 2k - 2$	$n > dk$	\	\
Multiplication traffic load (bits)	$(2k-1)^2\lceil log_2 p \rceil$	0	$4k^2\lceil log_2 p \rceil$	0
Multiplication round	1	0	1	0

As we can see from the above table, each piece of share is $k\lceil log_2 q \rceil$-bits in our scheme to retain all information within α. Fortunately, the threshold parameters k and n are relatively inappreciable compared with p and q is only bounded with $q > p + n$, meaning that the share size of our scheme, which is sub-linearly proportional to that of [25, 28, 30], is reasonable for practical application. Concerning the number of

participants who are engaged in secret multiplication, at least $2k-1$ and dk members are necessary for the schemes of [25] and [28] to multiply d shares correctly. Though the scheme of [30] is capable of multiplying shared secrets only if k participants are involved, massive communications are inevitable since every participant has to collect $4k\lceil log_2 p\rceil$ pieces of information for correct operation. As for our scheme, although the condition of $n \geq k$ must be fulfilled to actualize Q2 access structure, no interaction will be necessary due to the locality of multiplication and the constrain on threshold parameters can be eliminate because each secret is only attached to one piece of shares for each participant.

The computational performance of our scheme is also commendable since the operation of formula (11) is trivial. Noting that, because every participant is provided with her unique identity x_i, she can initially compute $\left(x_i^k - 1\right)$ and $\left(x_i^{-k} - 1\right)^{-1}$ once for all. That is to say, when securely multiplying two pieces of shares, only two integer multiplications and subtractions along with one modular operation need to be executed.

5 Conclusion

In order to privately multiply shared secrets without interaction, a novel multiplicative scheme is presented based on (k, n)-threshold Shamir's secret sharing. The main idea behind the proposed scheme is that we can subtly eliminate the overflowed terms of two plainly multiplied polynomials with the help of convolution. It is proved that our method is capable of correctly retaining the product of secrets as the first coefficient of a $k-1$ order polynomial with unconditional security. Compared with relevant schemes, our method is preferable since no communication and system parameter constrain are necessary.

Acknowledgments. This work is supported by the National Science Foundation of China P. R. (NSFC) under Grants 61703063, 61573076, 61663008; Chongqing Research Program of Basic Research and Frontier Technology under Grant CSTC2017jcyjAX0411; the Scientific Research Foundation for the Returned Overseas Chinese Scholars under Grant 2015-49; the Program for Excellent Talents of Chongqing Higher School under Grant 2014-18; Science and Technology Research Project of Chongqing Municipal Education Commission of China P. R. under Grants KJ1705139, KJ1600518, KJ1705121 and KJ1605002; Chongqing Municipal Social Livelihood Science and Technology Innovation Project under Grant CSTC2016shmszx30026; Urumqi Science and Technology Plan Project under Grant Y161320008.

References

1. El-Sayed, H., Sankar, S., Prasad, M., et al.: Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access **6**(99), 1706–1717 (2018)
2. SabatÉ, M., Costa, M.A., Kozuma, K., et al.: Survey on various data integrity attacks in cloud environment and the solutions. In: International Conference on Circuits, Power and Computing Technologies, pp. 1076–1081. IEEE (2013)

3. Patel, K: Secure multiparty computation using secret sharing. In: International Conference on Signal Processing, Communication, Power and Embedded System, pp. 863–866. IEEE (2017)
4. Liu, J., Li, W., Karame, G.O., et al.: Scalable byzantine consensus via hardware-assisted secret sharing. IEEE Trans. Comput. 1 (2016)
5. Xie, M.M., Liao, X.F., Zhou, Q.: Generalized oblivious transfer protocol in distributed setting based on secret sharing. Comput. Eng. **40**(3), 184–187 (2014)
6. Attasena, V., Darmont, J., Harbi, N.: Secret sharing for cloud data security: a survey. VLDB J. **2017**(2), 1–25 (2017)
7. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
8. Blakley, G.R.: Safeguarding cryptographic keys, p. 313. IEEE Computer Society (1979)
9. Brickell, E.F.: Some ideal secret sharing schemes. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 468–475. Springer, Heidelberg (1990). https://doi.org/10.1007/3-540-46885-4_45
10. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 67–79. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-57220-1_53
11. Van Dijk, M., Kevenaar, T., Schrijen, G.J., et al.: Improved constructions of secret sharing schemes by applying (λ, w)-decompositions. In: Proceedings of the IEEE International Symposium on Information Theory, p. 282. IEEE (2003)
12. Beimel, A., Weinreb, E.: Monotone circuits for monotone weighted threshold functions. Elsevier North-Holland, Inc. (2006)
13. Li, H., Liu, H.: Multi-access structure secret sharing schemes without dealer. Nat. Sci. J. Harbin Normal Univ. (2013)
14. Basit, A., Kumar, N.C., Venkaiah, V.C., et al.: Multi-stage multi-secret sharing scheme for hierarchical access structure. In: International Conference on Computing, Communication and Automation. IEEE (2017)
15. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electron. Commun. Jpn. **72**(9), 56–64 (2010)
16. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_3
17. Karchmer, M., Wigderson, A.: On span programs. In: IEEE Conference on Structure in Complexity Theory, pp. 102–111. IEEE Computer Society (1993)
18. Csirmaz, L.: The size of a share must be large. J. Cryptol. **10**(4), 223–231 (1997)
19. Jhanwar, M.P., Safavi-Naini, R.: Unconditionally-secure robust secret sharing with minimum share size. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 96–110. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_9
20. Tran, T., Rahman, M., Bhuiyan, M.Z.A., et al.: Optimizing share size in efficient and robust secret sharing scheme for big data. IEEE Trans. Big Data **PP**(99), 1 (2017)
21. Boyle, E., Couteau, G., Gilboa, N., et al.: Homomorphic secret sharing: optimizations and applications. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 2105–2122. ACM (2017)
22. Damgård, I., Fitzi, M., Kiltz, E., Nielsen, J.B., Toft, T.: Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 285–304. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_15
23. Nishide, T., Ohta, K.: Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 343–360. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_23

24. Boyle, E., Gilboa, N., Ishai, Y., et al.: Foundations of homomorphic secret sharing. In: 9th Innovations in Theoretical Computer Science Conference, vol. 21, pp. 1–20 (2018)
25. Gennaro, R., Rabin, M.O., Rabin, T.: Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proceedings of the ACM Symposium on Principles of Distributed Computing, pp. 101–111. ACM Press (1998)
26. Ishai, Y., Kushilevitz, E.: Randomizing polynomials: a new representation with applications to round-efficient secure computation. In: Proceedings of the Symposium on Foundations of Computer Science, pp. 294–304. IEEE (2000)
27. Ishai, Y., Kushilevitz, E., Meldgaard, S., Orlandi, C., Paskin-Cherniavsky, A.: On the power of correlated randomness in secure computation. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 600–620. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36594-2_34
28. Barkol, O., Ishai, Y., Weinreb, E.: On d-multiplicative secret sharing. J. Cryptol. **23**(4), 580–593 (2010)
29. Yoshida, M., Obana, S.: Verifiably multiplicative secret sharing. In: International Conference on Information Theoretic Security, pp. 73–82 (2017)
30. Watanabe, T., Iwamura, K., Kaneda, K.: Secrecy multiplication based on a (k, n)-threshold secret-sharing scheme using only k servers. In: Park, J., Stojmenovic, I., Jeong, H., Yi, G. (eds.) Computer Science and its Applications. LNEE, vol. 330, pp. 107–112. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-45402-2_16
31. Blackburn, S.R., Burmester, M., Desmedt, Y., Wild, P.R.: Efficient multiplicative sharing schemes. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 107–118. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_10
32. Wang, H., Lam, K.Y., Xiao, G.-Z., Zhao, H.: On multiplicative secret sharing schemes. In: Dawson, E.P., Clark, A., Boyd, C. (eds.) ACISP 2000. LNCS, vol. 1841, pp. 342–351. Springer, Heidelberg (2000). https://doi.org/10.1007/10718964_28
33. Jackson, W.A., Martin, K.M., O'Keefe, C.M.: Mutually trusted authority-free secret sharing schemes. J. Cryptol. **10**(4), 261–289 (1997)
34. Boyle, E., Gilboa, N., Ishai, Y.: Group-based secure computation: optimizing rounds, communication, and computation. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 163–193. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_6
35. Pilaram, H., Eghlidos, T.: An efficient lattice based multi-stage secret sharing scheme. IEEE Trans. Dependable Secure Comput. **14**(1), 2–8 (2017)
36. Shi, M., Guan, Y., Solé, P.: Two new families of two-weight codes. IEEE Trans. Inf. Theory **PP**(99), 1 (2017)
37. Gopinath, V., Bhuvaneswaran, R.S.: Design of ECC based secured cloud storage mechanism for transaction rich applications. CMC: Comput. Mater. Continua **57**(2), 341–352 (2018)
38. Zhong, J., Liu, Z., Xu, J.: Analysis and improvement of an efficient controlled quantum secure direct communication and authentication protocol. CMC: Comput. Mater. Continua **57**(3), 621–633 (2018)