Efficient Secret Sharing Schemes Achieving Optimal Information Rate

Yongge Wang

KINDI Center for Computing Research, Qatar University, Qatar
and
Department of SIS, UNC Charlotte, USA
Email: yongge.wang@uncc.edu

Yvo Desmedt

Department of CS, UT Dallas
Email: Yvo.Desmedt@utdallas.edu

***Abstract*—One of the important problems in secret sharing schemes is to establish bounds on the size of the shares to be given to participants in secret sharing schemes. The other important problem in secret sharing schemes is to reduce the computational complexity in both secret distribution phase and secret reconstruction phase. In this paper, we design efficient threshold (n, k) secret sharing schemes to achieve both of the above goals. In particular, we show some sufficient conditions (e.g., the secret size $|s|$ is larger than n), for which efficient ideal secret sharing schemes exist. In the efficient ideal secret sharing schemes that we will construct, only XOR-operations on binary strings are required (which is the best we could achieve). These schemes will have many applications both in practice and in theory. For example, they could be used to design very efficient verifiable secret sharing schemes which will have broad applications in secure multi-party computation and could used to design efficient privacy preserving data storage in cloud systems.**

I. Introduction

Threshold secret sharing scheme is one of the most important cryptographic primitives that have been used in many areas of cryptographic applications. Since the concept of secret sharing scheme was introduced by Blakley [3] and Shamir [19], there have been considerable efforts on the study of the bounds of of share sizes, on the bounds of information rate, on the bounds of the number of participants for ideal threshold schemes, and on efficient secret sharing schemes. By an ideal threshold scheme, we mean a secret sharing scheme for which the size of the shares is the same as the size of the secret. Ideal threshold schemes have important applications in practice. For example, there has been interest in designing privacy-preserving data storage in cloud using efficient XOR-based ideal secret sharing schemes (see, e.g., Wang [21]).

In a simple secret sharing scheme, we have n participants, a secret s is encoded into n shares and each participant will receive one share. Any $k \leq n$ participants can come together and reconstruct the secret s though no $k-1$ participants could learn any information of the secret. These schemes are known as (n, k) threshold schemes.

One of the important problems in secret sharing schemes is to establish bounds on the size of the shares to be given to participants in secret sharing schemes, which is normally referred to as the information rate. Brickell and Stinson [6] gave several upper and lower bounds on the information rate of access structures based on graphs.

Ito, Saito, and Nishizeki [12] extended the threshold schemes to a general framework and proposed secret sharing schemes for any access structure. Benaloh and Leicher [2] observed that there are access structures in which any secret sharing scheme must give to some participant a share which is taken from a domain strictly larger than that of the secret. Capocelli et al. [7] further constructed a general access structure for secret sharing schemes for which any secret sharing scheme must give to a participant a share at least 50% greater than the secret size.

Desmedt and Frankel [11] proposed the black-box secret sharing scheme for which the distribution matrix and the reconstruction vectors are defined over the integer rings Z and are designed independently of the group G from which the secret and the shares are sampled. Desmedt and Frankel showed an example of (n, k) black-box threshold secret sharing scheme with information rate n. In other words, in order to share a single element in the black box group G among n participants, each participant will receive n elements from the black-box group G. By a result from Karchmer and Wigderson [13], it is easy to show that in order for n participants to share one element from the black box group G, each participant will receive at least $O(\log_2 n)$ elements from the black-box group. Cramer and Fehr [9] then improved these results by showing that the lower bound $O(\log_2 n)$ could be achieved in general Abelian groups. In particular, Cramer and Fehr developed a technique to design low degree integral extensions of the integer ring Z over which there exists a pair of sufficiently large Vandermonde matrices with co-prime determinants. The technique to use a pair of Vandermonde matrices with co-prime determinants could be used in other research areas to avoid the limit of Lenstra constant, where the Lenstra constant $l(S)$ of a ring S is defined as the largest integer l such that there exists an invertible $l \times l$ Vandermonde matrix with entries in S.

There has also been an extensive interest in designing efficient secret sharing schemes. For example, Kurihara et al.

[15] and Lv et al. [17] have tried to design efficient threshold secret sharing schemes for which only XOR operations on bit-strings are used in the distribution and reconstruction phases. However, the schemes in [17] are not accurate. For example, the authors in [17] designed a multi-secret sharing scheme with the following properties: *Let k, n be integers and $p > n + k$ be a prime number. For any Abelian group G, there is a (n, k) secret sharing scheme to share $(p-1)k$ elements in G, and each participant will receive a share of $p-1$ group elements.* Assume that each groud element in G could be represented by a l-bit string. For the scheme in [17], each participant receives $(p-1)l$-bits and the shared secret is $(p-1)kl$-bits. By the following theorem from Karnin, Greene, and Hellman [14, Theorem 1], this is impossible.

Theorem 1.1: (Karnin, Greene, and Hellman [14, Theorem 1]) For an (n, k) secret sharing scheme, we have

$$H(v_i) \geq H(s), \quad i = 0, \cdots, n-1$$

where s is the secret and $v_0, \cdots, v_{n-1}$ are the shares.

This paper will concentrate on the design of efficient threshold secret sharing scheme design. Though our main interest is to share binary strings of secrets (that is, strings of elements from $F = GF(2)$), our constructions will be given over general finite field $GF(q)$. Specifically, let s be a string of elements from a finite field $F = GF(q)$ and $k < n$ be two integers. we construct efficient (n, k) threshold secret sharing schemes to optimize the following two factors:

- efficient implementation: only XOR and cyclic shift operations are used in the secret distribution and reconstruction phases.
- optimal information rate: each participant should receive as short shares as possible.

Secret sharing schemes, for which the secret distribution and reconstruction phases are based on XOR and cyclic shift operations on binary strings, could be converted to secret sharing schemes on several Abelian groups on binary strings. Thus our results show that if we consider the secret element s from the black-box group G as binary strings, then we could achieve better information rate (better than the lower bound $O(\log_2 n)$ in [9]). Let $s = s_0 \cdots s_\tau \in G^\tau$ be the secret to be shared, then we have the following main results in this paper.

- If $\tau \geq \max\{\log_2 n, 2(n-k)\}$ or $\tau \geq n$, then there exists an efficient XOR-operation based ideal (n, k) secret sharing scheme such that each participant receives τ elements from $GF(q)$ as the share. In other words, we could design efficient ideal threshold secret sharing schemes with information rate 1.

Note that for $\tau < \max\{\log_2 n, 2(n-k)\}$, we can use the Reed-Solomon code to achieve the optimal information rate though the designed schemes are not necessarily ideal.

The structure of the paper is as follows. Section II briefly discuss the relationship between MDS codes and secret sharing schemes. Section III presents the XOR-based secret sharing schemes for the case $|s| \geq n$. Section IV presents the XOR-based secret sharing schemes for the case $|s| \geq \max\{\log_2 n, 2(n-k)\}$. Section V presents XOR based secret sharing schemes for $k = 2, 3, 4$. Finally, in Section VI, we briefly discuss how to design efficient XOR-based verifiable secret sharing schemes.

II. MDS codes and Secret Sharing Schemes

For an $[n, k, d]$ linear code, the Singleton bound claims that $d \leq n - k + 1$. An $[n, k, d]$ linear code is maximum distance separable (MDS) if $d = n-k+1$ (see, e.g., [18]). It is folklore (see, e.g., [4]) that each $[n, k, d]$ MDS code could be converted to an ideal and linear (n, k) threshold sharing scheme.

As an example, assume $GF(q^m)$ is a finite field and let

$$\begin{aligned} g(z) &= (z-1)(z-\alpha)\cdots(z-\alpha^{n-k-1}) \\ &= g_0 + g_1 z + \cdots + g_{n-k} z^{n-k} \end{aligned}$$

be the generator polynomial over $F = GF(q^m)$ for the Reed-Solomon code over a finite field $GF(q^m)$, where α is a primitive element of $GF(q^m)$. For information symbols $(f_0, f_1, \cdots, f_{k-1}) \in GF(q^m)^k$, let $f(z) = f_0 + f_1 z + \cdots + f_{k-1} z^{k-1}$. Then

$$g(z)f(z) = g_0 f_0 + (g_0 f_1 + g_1 f_0) z + (g_0 f_2 + g_1 f_1 + g_2 f_0) z^2 + \cdots$$

and the encoding symbols are $(c_0, \cdots, c_{n-1}) = (g_0 f_0, g_0 f_1 + g_1 f_0, \cdots)$. Alternatively, we could write the coding process as equation (1) in terms of generator matrix.

The above Reed-Solomon code could be converted to a threshold secret sharing scheme by letting the secret be $s = g_0 f_0$ and distributing the shares $(c_1, c_2, \cdots, c_{n-1})$ to the $n-1$ participants respectively. It is straightforward to show that this is a perfectly secure threshold $(n-1, k)$ secret sharing scheme over $GF(q^m)$.

Indeed, applying the technique by Karnin, Greene, and Hellman [14], the above secret sharing scheme could be easily extended to an (n, k) threshold secret sharing scheme if we let $c_n = f_0 + \cdots + f_{k-1}$.

III. The Basic XOR-operation Based Secret Sharing Scheme

In this section, we present an efficient ideal secret sharing scheme using techniques from array codes design (see, e.g., Blaum and Roth [5] and Wang [20]). In the distribution and reconstruction phases of the scheme, only XOR and cyclic shift operations are needed. Though we are mainly interested in $GF(2)$, the scheme works in any finite field. Thus we will give a general construction with $F = GF(q)$.

Let $n > k$ be two integers and $s = s_0 \cdots s_{\tau-1} \in F^\tau$ be a string of elements from F with $\tau = |s| \geq n$. Let $p \geq \tau + 1$ be a prime number such that $\gcd(p, q) = 1$. In other words, p is not the characteristic of F. For an integer a, let $\langle a \rangle_p$ denote the integer $b \in \{0, \cdots, p-1\}$ such that $b \equiv a \pmod{p}$.

The secret sharing scheme $\mathcal{S}(p-1, n, k)$ over $F = GF(q)$ is defined as a collection of $(p-1) \times p$ matrices[1] $\Gamma = [c_{i,j}]$

[1]For our secret sharing scheme, it is sufficient to consider $(p-1) \times (n+1)$ matrices. For the convenience of discussion, we consider $(p-1) \times p$ matrices and use a shortened version of the matrices for distributing shares.

$$(c_0, \cdots, c_{n-1}) = (f_0, f_1, \cdots, f_{k-1}) \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{p-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & g_{n-2k+1} & g_{n-2k+2} & \vdots & g_{n-k} \end{pmatrix} \quad (1)$$

over $GF(q)$ as follows.

- For $0 \le i \le \tau - 1$, let $c_{i,0} = s_i$.
- For $\tau - 1 < i \le p - 1$, let $c_{i,0} = 0$.
- The matrix satisfies the following $p \cdot (n - k)$ linear constraints:

$$\sum_{j=0}^{n} c_{\langle m - jl \rangle_p, j} = 0 \qquad 0 \le m \le p-1, 0 \le l \le n-k-1. \quad (2)$$

In other words, $\mathcal{S}(p-1, n, k)$ consists of all $(p-1)\times p$ matrices such that the first column consists of the elements in s, and the entries along the p lines of slope l ($0 \le l \le n - k - 1$) sums to zero.

Each matrix $\Gamma \in \mathcal{S}(p-1, n, k)$ can be used as a distribution matrix for the secret sharing scheme by giving n participants the values from the columns $1, \cdots, n$ respectively. It remains to show that the secret sharing scheme is complete (any k participants could reconstruct the secret s) and private (any $k - 1$ participants learn zero information about the secret).

Let $M_p(x) = \sum_{i=0}^{p-1} x^i$ be a polynomial over $F = GF(q)$ and let $\mathcal{R}_p$ be the rings of polynomials of degree less than $p - 1$ with multiplication taken modulo $M_p(x)$. Let α be a root of $M_p(x)$ in $\mathcal{R}_p$ (note that $\alpha^p = 1$). For $r = p - k < p$, let H be the $r \times p$ matrix over $\mathcal{R}_p$ defined by

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{(p-1)} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(p-1)(r-1)} \end{bmatrix} \quad (3)$$

and let $\mathcal{C}$ be the linear code of length p over $\mathcal{R}_p$ with H as the parity matrix. Blaum and Roth [5] showed that the determinant of each $r \times r$ sub-matrix of H has a multiplicative inverse in $\mathcal{R}_p$. Hence H has rank r over $\mathcal{R}_p$. In other words, the code $\mathcal{C}$ is an MDS linear $[p, k, p-k+1]$ code which can be considered as the Reed-Solomon code over the ring $\mathcal{R}_p$. It should be noted that the code $\mathcal{C}$ is the same as the code discussed in Section II if we replace the finite field $GF(q^m)$ with $\mathcal{R}_p$.

Furthermore, if we consider each matrix Γ in $\mathcal{S}(p-1, n, k)$ as a $(p-1) \times p$ array code, then Blaum and Roth's results [5] showed that $\mathcal{S}(p-1, n, k)$ is equivalent to $\mathcal{C}_s$ where

$$\mathcal{C}_s = \{(c_0, c_1, \cdots, c_{p-1}) \in \mathcal{C} : c_0 = \langle s_0, \cdots, s_{\tau-1}, 0, \cdots, 0 \rangle\}$$

Let $g(z) = g_0 + g_1 z + \cdots + g_r z^r$ be the generator polynomial for $\mathcal{C}$ over $\mathcal{R}_p$. Since α has a multiplicative inverse in $\mathcal{R}_p$, it is straightforward that g_0 has a multiplicative inverse in $\mathcal{R}_p$. Thus there exists $f_0^s \in \mathcal{R}_p$ such that

$$f_0^s g_0 = \langle s_0, \cdots, s_{\tau-1}, 0, \cdots, 0 \rangle \in \mathcal{R}_p \quad (4)$$

In other words, for any information symbol polynomial $f(z) = f_0^s + f_1 z + \cdots + f_{k-1} z^{k-1}$ with random $f_1, \cdots, f_{k-1} \in \mathcal{R}_p$, $f(z)g(z)$ generates a code in $\mathcal{C}_s$. Thus we have $\mathcal{C}_s \neq \emptyset$.

In a summary, if we consider the secret sharing scheme $\mathcal{S}(p-1, n, k)$ as a $(p-1) \times p$ array code, it is a non-empty MDS $[p, k, p-k+1]$ linear code over $\mathcal{R}_p$. By the comments in Section II, the secret sharing scheme $\mathcal{S}(p-1, n, k)$ is complete and private.

For the array code $\mathcal{C}$ with at most r erasure (and no errors), Blaum and Roth [5] described a decoding procedure with $O(r(p^2 + r))$ operations (additions and cyclic shift) over $GF(q)$. The decoding procedure by Blaum and Roth could be used as the secret reconstruction procedure for $\mathcal{C}_s$ (or equivalently, $\mathcal{S}(p-1, n, k)$). For the distribution phase, we can either use the generating polynomial $g(z)$ and information symbols $\langle f_0^s, f_1, \cdots, f_{k-1} \rangle$ (with random $f_1, \cdots, f_{k-1}$) to generate the shares or to solve the equations in (2) to generate the shares. For either case, the distribution could be done with addition and cyclic shift operations over $GF(q)$.

If we take the finite field as $F = GF(2)$, then both distribution and reconstruction phases for the secret sharing scheme $\mathcal{S}(p-1, n, k)$ requires only XOR operations.

IV. Efficient XOR based Secret Sharing Schemes with $|s| < n$

In Section III, we described efficient XOR operation based ideal secret sharing schemes for the case of $|s| \ge n$. In this section, we design efficient ideal secret sharing schemes for $|s| < n$.

Similarly, let $n > k$ be two integers and $s = s_0 \cdots s_{\tau-1} \in F^\tau$ be a string of elements from F with $\tau = |s| < n$. Let $p \ge n + 1$ be a prime number such that $\gcd(p, q) = 1$. The secret sharing scheme $\mathcal{S}'(p-1, n, k)$ over $F = GF(q)$ is defined as a collection of $(p-1) \times p$ matrices $\Gamma = [c_{i,j}]$ as in Section III with the following additional constraint.

- For $\tau \le i \le p - 1$ and $0 \le i \le p - 1$, $c_{i,j} = 0$.

In other words, $\Gamma \in \mathcal{S}'(p-1, n, k)$ if and only if $\Gamma \in \mathcal{S}(p-1, n, k)$ and the last $p - \tau - 1$ rows are zero vectors.

Let $\mathcal{C}$ and $\mathcal{C}_s$ be the linear codes defined in Section III. Define

$$\mathcal{C}'_s = \{(c_0, c_1, \cdots, c_{p-1}) \in \mathcal{C}_s : c_i = \langle c_{i,0}, \cdots, c_{i,\tau-1}, 0, \cdots, 0 \rangle\}.$$

If we consider each matrix in $\mathcal{S}'(p-1, n, k)$ as a $(p-1) \times p$ array code, then it is straightforward to check that $\mathcal{S}'(p-1, n, k)$ is equivalent to the linear code $\mathcal{C}'_s$. Thus in case that

$\mathcal{C}'_s$ is not empty, $\mathcal{S}'(p-1,n,k)$ is an efficient ideal secret sharing scheme for the case of $\tau = |s| < n$. In the following, we show a sufficient condition for $\mathcal{C}'_s \neq \emptyset$.

With the above constraint, the equation (2) has $(p-1)\tau$ unknowns and $p(p-k)$ equations. It is straightforward that (2) has a solution (i.e., the matrix Γ exists) if and only if $(p-1)\tau \geq p(n-k)$. In order to achieve the MDS property, we also need the property $\tau \geq \log_q p$ (otherwise, there are not enough elements in $\mathcal{R}_p$ for $h_1, \cdots, h_{p-1}$ with only non-zero entries in the first τ positions).

Without loss of generality, we may assume that for each n, there exists a prime number p with $n+1 \leq p \leq 2n$. Then we have $\frac{p(n-k)}{p-1} \leq \frac{p(n-k)}{n} \leq 2(n-k)$. Thus for $\tau \geq \max\{\log_q p, 2(n-k)\}$, there exist solutions for the equation (2). Hence $\mathcal{C}'_s \neq \emptyset$. In a summary, for $\tau \geq \max\{\log_q p, 2(n-k)\}$, we can design an efficient ideal secret sharing scheme based on XOR operations.

For a secret s with $\tau = |s| < n$ and $\tau < \max\{\log_q p, 2(n-k)\}$, where p is a prime larger than n, we could use Reed-Solomon code over finite field $GF(q^{\log_q n})$ to design secret sharing schemes so that each participant receives $\log_q n \geq \tau$ bits for the secret s. But the scheme based on the Reed-Solomon code over finite field is not efficient (not XOR-operation based). Alternatively, we could pad s to a string of length n and then use our efficient XOR based ideal secret sharing scheme that we have discussed in this section and the previous section. In any cases, the resulting secret sharing scheme is not ideal.

V. Efficient XOR based secret sharing scheme for $k = 2, 3, 4$

The authors of [16] showed that if 2 is primitive in F_p, then one can construct $(p-1)/\sigma \times (p-1)$ MDS array codes such that the information symbols could be recovered from any 3 (respectively, 4) columns of the encoding symbols using XOR operations. These codes could be easily converted to ideal secret sharing schemes for $\tau = |s| \geq n/3$ (respectively $\tau = |s| \geq n/4$). We will not give the details here.

VI. Efficient XOR based VSS

In this section, we briefly show that it is straightforward to convert our (n,k) ideal secret sharing scheme in Section III to a verifiable secret sharing schemes using the techniques discussed in [1], [10], [8].

In the following, we will use notations from Section III. Specifically, let $\mathcal{R}_p$ be the rings of polynomials of degree less than $p-1$. Let f_0^s be the secret value defined in the equation (4) and let $G = [\mathbf{v}_0, \cdots, \mathbf{v}_{n-2}]$ be the generator matrix obtained by removing the first column $(g_0, 0, \cdots, 0)^T$ from the Reed-Solomon code generator matrix in the right hand side of the equation (1). Then the efficient verifiable $(n-1,k)$ secret sharing is as follows:

- The dealer chooses a symmetric $k \times k$ matrix R at random over $\mathcal{R}_p$, except that the upper left corner element in R is f_0^s.
- The dealer computes the $k \times (n-1)$ matrix $R \times G$ and securely sends the i-th column $\mathbf{u}_i$ of $R \times G$ to the participant P_i for all $i \leq n-2$.
- Participant P_i sends to each participant P_j the value $\mathbf{v}_j^T \cdot \mathbf{u}_i$, who compares this to $\mathbf{v}_i^T \cdot \mathbf{u}_j$ and broadcast a message "complaint(i,j)" if the values are different.
- In response to "complaint(i,j)", the dealer must broadcast the $s_{i,j}$ in the matrix $G^T \times R \times G$.
- If any participant P_i finds that the information broadcasted by the dealer does not match the information sent in Step 2, P_i broadcasts an "accusation".
- In response to accusation to P_i, the dealer must broadcast all information sent to P_i in step 2.
- The information broadcast by the dealer in the previous step may lead to further accusation. The process continues until the information broadcast by the dealer self-contradicts itself, or he has been accused by at least k participants, or no new accusation occurs. In the first two cases, the dealer is corrupt. For the last case, the commit protocol is accepted by the honest players and accusing players accept the share broadcast for them by the dealer.

In the above VSS protocol, the major computation complexity comes from the computation of $R \times G$ and $G^T \times R \times G$ over $\mathcal{R}_p$. By using the algorithms developed by Blaum and Roth [5]), these computations are reduced to addition and cyclic shift operations over the finite field $GF(q)$. If we use $GF(2)$ as the underlying finite field, then only XOR operations are needed. Thus the above VSS protocol is very efficient. It should be noted that the above VSS protocol could be further simplified to lower the round complexity using the techniques developed in [8].

References

[1] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. STOC '88*, pages 1–10, New York, NY, USA, 1988. ACM.

[2] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Proc. CRYPTO '88*, pages 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[3] G. R. Blakley. Safeguarding cryptographic keys. *Managing Requirements Knowledge, International Workshop on*, 0:313, 1979.

[4] G. R. Blakley and G. A. Kabatianski. Ideal perfect threshold schemes and MDS codes. In *IEEE Conf. Proc., Int. Symp. Information Theory, ISIT' 95*, pages 488–488, 1995.

[5] M. Blaum and R. M. Roth. New array codes for multiple phased burst correction. *IEEE Trans. on Information Theory*, 39(1):66–77, 1993.

[6] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. In *Proc. CRYPTO*, pages 242–252. Springer-Verlag, 1990.

[7] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, 6:157–168, 1993.

[8] Ashish Choudhury, Kaoru Kurosawa, and Arpita Patra. The round complexity of perfectly secure general vss. In *Proc. 5th int. con. Information theoretic security*, ICITS'11, pages 143–162, Berlin, Heidelberg, 2011. Springer-Verlag.

[9] R. Cramer and S. Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In *CRYPTO*, pages 272–287, 2002.

[10] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT'00*, pages 316–334, Berlin, Heidelberg, 2000. Springer-Verlag.

[11] Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM Journal on Discrete Mathematics*, 7(4):667–679, 1994.

[12] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electron. Comm. Jpn. Pt. III*, 72:56–64, 1989.

[13] M. Karchmer and A. Wigderson. On span programs. In *In Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111. IEEE Computer Society Press, 1993.

[14] E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Trans. Information Theory*, 29(1):35 – 41, jan 1983.

[15] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka. A new (k, n)-threshold secret sharing scheme and its extension. In *Proc. 11th Int. Conf. Information Security*, ISC '08, pages 455–470, Berlin, Heidelberg, 2008. Springer-Verlag.

[16] E. Louidor and R. M. Roth. Lowest density MDS codes over extension alphabets. *IEEE Trans. Inf. Theor.*, 52(7):3186–3197, 2006.

[17] C. Lv, X. Jia, J. Lin, J. Jing, L. Tian, and M. Sun. Efficient secret sharing schemes. In *Communications in Computer and Information Science*, volume 186, pages 114–121. Springer Berlin Heidelberg, 2011.

[18] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. NH Pub. Company, 1978.

[19] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[20] Yongge Wang. Array BP-XOR codes for reliable cloud storage systems. In *Proc IEEE ISIT 2013*, pages 326–330. IEEE Press, 2013.

[21] Yongge Wang. Privacy-preserving data storage in cloud using array BP-XOR codes. *IEEE Trandactions on Cloud Computing*, 2015.