# Optimal Uniform Secret Sharing

Maki Yoshida, Toru Fujiwara, *Member, IEEE*, and Marc P. C. Fossorier, *Fellow, IEEE*

***Abstract*— An important problem in secret sharing schemes is minimizing the share size. For ($k$, $n$)-threshold schemes and ($k$, $L$, $n$)-ramp schemes, constructions that minimize the share size are known. This paper presents optimal constructions for a more general class of access structures in which subsets with the same cardinality have the same amount of information about the secret. We refer to schemes with such uniform access structures as uniform secret sharing. We first derive a tight lower bound for share entropy and then present an optimal construction. Our lower bound exceeds that previously reported. The optimal construction encodes the secret value using one or more ramp schemes.**

***Index Terms*— Secret sharing, uniform access structures, entropy of shares, tight lower bound, optimal.**

## I. Introduction

A SECRET sharing scheme is a method of encoding a secret $s$ into $n$ shares $v_1, v_2, \ldots, v_n$ so that the secret can be recovered only from predefined subsets of shares called *authorized subsets*. A secret sharing scheme is *uniform* if every minimal authorized subset has the same cardinality [17]. Three special classes of uniform secret sharing have been studied in the literature: In the $(k, n)$-threshold schemes introduced in [4] and [16], the secret is recovered from any $k$ shares, and no information on the secret is obtained from $k-1$ or fewer shares. In the $(k, L, n)$-ramp schemes, or "$k$ out of $n$ to yield $L$" ramp schemes [5], [18], $k-1$ or fewer shares have partial information on the secret with a ratio of $\frac{l-k+L}{L}$ for $l$ shares with $k-L < l < k$. The third class is nonlinear function ramp schemes [19], which further extend the above-mentioned ramp schemes to those with nonlinear ratios.

We extend the notion of *uniform secret sharing* (USS) to secret sharing in which subsets of shares with the same cardinality have the same amount of information on the secret. The ratio of the amount of information is given by a monotonically increasing rational-valued function of the number of shares, which we call the *access function*. The access function for the $(k, n)$-threshold scheme takes zero or one value; that is, it is a step function. The $(k, L, n)$-ramp schemes are defined by truncated linear access functions that have rational numbers between zero and one. The nonlinear function schemes further extend the access functions to any rational-valued function.

In secret sharing, an important problem is to minimize the share size. This problem has been solved for the $(k, n)$-threshold and $(k, L, n)$-ramp schemes. Optimal constructions that minimize the size of shares have been presented in [16] and [18]. Let $\mathbf{H}(X)$ denote the entropy of random variable $X$. Let $S$ and $\xi_i$ denote the random variables induced by $s$ and $v_i$, respectively. Share size, which is measured by the entropy $\mathbf{H}(\xi_i)$, is given by the gradient of the slope of the truncated linear function. Specifically, the $(k, n)$-threshold and $(k, L, n)$-ramp schemes satisfy $\mathbf{H}(\xi_i) = \mathbf{H}(S)$ and $\mathbf{H}(\xi_i) = \frac{1}{L}\mathbf{H}(S) \leq \mathbf{H}(S)$, respectively. The results in [16] and [18] indicate that relaxing the requirement on information leakage improves efficiency in terms of share size. In [10], ramp schemes are used to construct efficient secure multiparty protocols.

For nonlinear functions, previous constructions are either insecure [19] or not tight, in the sense that the lower bound in [15], which was derived for a more general class including nonuniform cases. The results in [15] suggest that the derived lower bound may not be tight. Specifically, two examples of nonuniform secret sharing for which the entropy of some shares is larger than the lower bound in [15] are given. However, it is not clear whether the lower bound in [15] is tight for USS.

Our goal is to develop optimal USS for the most general class. We first derive a new lower bound on share entropy, and then present a construction that achieves that bound. The derived lower bound is generally larger than the lower bound in [15]. Whereas the lower bound in [15] is given by the maximum value of the gradient of the corresponding access function, this bound is given not only by the maximum value of the gradient, but also by the *local* maxima and minima of the gradient, depending on the number of these local extrema and their respective values. Thus, except for special access functions, this lower bound exceeds the bound in the previous papers. We identify the class of access functions for which the new bound equals the bound in [15].

Next, we show how to realize the lower bound. The key idea is to express the access function as a sum of truncated linear functions and encode the secret value by using optimal ramp schemes. Generally, many decompositions are possible. We show how to find the truncated linear access functions so that the decomposition achieves the derived lower bound.

*Related Work:* After our work in [21], the same results were independently achieved in [8] and [9]. There the problem is placed into a wider context: not only uniform secret sharing schemes with rational values, but also nonuniform

Manuscript received August 20, 2015; revised March 31, 2017 and August 29, 2017; accepted May 24, 2018. Date of publication November 9, 2018; date of current version December 19, 2018.

M. Yoshida is with the Cybersecurity Research Institute, National Institute of Information and Communications Technology, Koganei 184-8795, Japan (e-mail: maki-yos@nict.go.jp).

T. Fujiwara is with the Graduate School of Information Science and Technology, Osaka University, Suita 565-0871, Japan (e-mail: fujiwara@ist.osaka-u.ac.jp).

M. P. C. Fossorier is with ENSEA/UCP/CNRS UMR-8051, ETIS, 95014 Cergy-Pontoise, France (e-mail: mfossorier@ieee.org).

Communicated by A. Menezes, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2018.2852276

secret sharing with *real* values are considered. We note that in [8] and [9], optimality is constructed to the same class as in this work, including [21], i.e., the uniform rational-number class. For the uniform real-number class, [8] and [9] proved that the lower bound is achieved by taking the limit of a number of ramp schemes. That is, an infinite number of ramp schemes are required to achieve the lower bound. For the nonuniform class, optimal secret sharing is an open problem. In comparison with our lower bound, the lower bound in [8] and [9] is given by summing every positive change in the gradient.

In this paper and most of those in the literature, including [8], [9], and [21], the leakage is defined by the entropy. However, in many cryptographic applications of secret sharing, such as secure storage, the definition of leakage only via the entropy is not enough [11]. To solve this problem, *fractional secret sharing* was introduced in [11] where the uniformity of the conditional distribution of the secret given shares is required. While it has been proven that any *fractional access structure* that specifies the finite number of potential secrets for given shares is realized with the share size $n\,\mathbf{H}(S)$, an exact characterization of the best achievable share-size was left as an open problem. Our lower bound on the share entropy is common to fractional secret sharing, and the optimal construction satisfies this requirement. This means that this work answers the open problem for the uniform rational-numbered class.

The rest of this paper is organized as follows: In Section II, we define uniform secret sharing (USS) schemes that include the previous USS classes. In Section III, we derive a lower bound on the entropy of each share for any USS scheme. In Section IV, we present the optimal construction, which further satisfies the requirement of fractional secret sharing. Concluding remarks are given in Section V.

## II. Notation and Definitions

### A. Access Functions

Let $\mathcal{F}$ be the family of monotonically increasing rational-valued discrete functions $g : \{0, 1, \ldots, n\} \to \mathbb{Q}_{[0,1]}$ with $g(0) = 0$ and $0 \le g(n) \le 1$, where $\mathbb{Q}_{[0,1]}$ is the set of rational numbers between 0 and 1. We call $\mathcal{F}$ the family of *access functions* of uniform secret sharing. For every access function $g \in \mathcal{F}$, we define the *ramp end* and *ramp run* of $g$, denoted by $k$ and $L$ respectively, by

$$k = \min\{l \mid 0 \le l \le n, g(l) = g(n)\},$$
$$L = k - \max\{l \mid 0 \le l \le n, g(l) = 0\}.$$

We say that $g$ is *truncated linear* if

$$g(l) = \begin{cases} 0, & \text{for } 0 \le l < k - L, \\ \dfrac{g(n)}{L}(l - k + L), & \text{for } k - L \le l < k, \\ g(n), & \text{for } k \le l \le n. \end{cases} \quad (1)$$

Otherwise, $g$ is *nonlinear*.

For $g \in \mathcal{F}$ and $0 \le l < n$, define $\Delta_{g,l} \triangleq g(l + 1) - g(l)$, which indicates the leakage. We refer to $\Delta_{g,l}$ as the gradient of $g$ on $l$ or simply the *gradient*. Let $\Delta_g$ denote the maximum gradient, i.e., $\Delta_g = \max\{\Delta_{g,l} \mid 0 \le l < n\}$. In the following, we omit $g$ from the indices when it is clear from the context.

### B. Uniform Secret Sharing

Let $\mathbf{H}(\cdot)$, $\mathbf{H}(\cdot|\cdot)$, and $\mathbf{I}(\cdot;\cdot)$ denote the entropy, conditional entropy, and mutual information, respectively. For random variables $X, Y, Z$, and $W$, we have [22]

$$0 \le \mathbf{H}(X|ZW) \le \mathbf{H}(X|Z) \le \mathbf{H}(XY|Z), \quad (2)$$

and

$$\begin{aligned}\mathbf{H}(XY|Z) &= \mathbf{H}(X|Z) + \mathbf{H}(Y|XZ) \\ &= \mathbf{H}(Y|Z) + \mathbf{H}(X|YZ).\end{aligned} \quad (3)$$

For a random variable $X$, the support of the distribution is given by $\hat{X} = \{x \mid \Pr(X = x) > 0\}$. Throughout this paper, $P = \{1, \ldots, n\}$ denotes the set of $n$ players. We use subsets of $P$ as subindices for random variables. For a subset $A \subseteq P$ and a vector of random variables $(\xi_1, \ldots, \xi_n)$, $\xi_A$ denotes the subvector $(\xi_i)_{i \in A}$.

*Definition 1:* A *secret sharing* (SS) *scheme* is a random vector $(S, \xi_1, \ldots, \xi_n)$ in which the random variable $S$ and random vector $(\xi_1, \ldots, \xi_n)$ correspond, respectively, to the secret value and the shares that are distributed among the players in $P$. An SS scheme viewed as an abstract primitive is a triplet $(S, D)$, where $S$ is a distribution on a domain of secret values, and $D$ is a randomized distribution function that maps a secret value $s \in \hat{S}$ to shares $(v_1, \ldots, v_n)$ with $v_i \in \hat{\xi}_i$.

*Definition 2:* A *uniform secret sharing scheme* for an access function $g \in \mathcal{F}$ ($g$-USS scheme) is an SS scheme $(S, \xi_1, \ldots, \xi_n)$ or $(S, D)$ satisfying, for any $A \subseteq P$,

$$\mathbf{I}(S; \xi_A) = g(|A|)\mathbf{H}(S), \quad (4)$$

or, equivalently,

$$\mathbf{H}(S|\xi_A) = (1 - g(|A|))\mathbf{H}(S). \quad (5)$$

The classes of threshold and ramp schemes in [4], [5], [16], [18], and [19] are proper subclasses of USS schemes defined here. The nonlinear-function ramp schemes in [19] restrict $g$ to convex ($\Delta_{g,l} \le \Delta_{g,l+1}$ with $k - L \le l < k$) and concave ($\Delta_{g,l} \ge \Delta_{g,l+1}$ with $k - L \le l < k$) functions. The $(k, L, n)$-ramp schemes in [5] and [18] are the special case in which $g$ is truncated linear with $\Delta_g = 1/L$. The $(k, n)$-threshold schemes in [4] and [16] are a special case with $L = 1$.

In the following, without loss of generality, we assume that $g(n) = 1$ and $\mathbf{H}(S) > 0$. This assumption means that the secret value has some uncertainty, but can be identified from all shares.

## III. A Lower Bound

We derive a lower bound on the entropy of each share by focusing on the gradient of the access function $g$. In general, the gradient $\Delta_l$ repeatedly increases and decreases with $l$. The last gradient of successive increases (resp. decreases) is referred to as a *local maximum* (resp. *local minimum*). To precisely define them, we define $\Delta_{-1}$ and $\Delta_n$ with $\Delta_{-1} = \Delta_n = 0$, implying that the gradient of $g$ first increases from zero, and finally decreases to zero. The gradient $\Delta_l$ with $0 \le l < n$ is a *local maximum* if for some $l'$ with $-1 \le l' < l$, $\Delta_{l'} < \Delta_{l'+1} = \cdots = \Delta_l$ and that $\Delta_l > \Delta_{l+1}$. Note that the maximum gradient $\Delta$ is also a local maximum.

We call $\Delta_l$ with $0 \le l < n$ a *local minimum* if, for some $l'$ with $-1 \le l' < l$, $\Delta_{l'} > \Delta_{l'+1} = \cdots = \Delta_l$ and that $\Delta_l < \Delta_{l+1}$. Looking at local maxima and minima, the gradient of $g$ first becomes a local maximum, then alternates between local minima and maxima, and finally decreases from the final local maximum to zero, but does not end in a local minimum because $\Delta_{n-1} \ge \Delta_n = 0$ (i.e., the latter condition of a local minimum) is not satisfied. Thus, the number of local maximum gradients of $g$ is at least one, and is one more than that of the local minimum gradients. The same holds on any interval bounded by zero gradients, because the zero gradients play the role of dummy leftmost and rightmost gradients.

The lower bound on the entropy of shares is given by the relative values of the local maxima and minima of the gradient of the access function as expressed in the theorem below.

*Theorem 1:* For an access function $g \in \mathcal{F}$, let $M$ denote the number of local maximum gradients of $g$. Let $\hat{l}_j$ with $1 \le j \le M$ (respectively, $\check{l}_j$ with $1 \le j < M$) denote the point at which the gradient is the $j$-th local maximum (respectively, the $j$-th local minimum). For a number $x$, let $(x)^+$ denote its positive part, i.e., $(x)^+ = \max\{0, x\}$. For any $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ with $g \in \mathcal{F}$ and any player $i \in P$,

$$\mathbf{H}(\xi_i) \ge \left(\sum_{j=1}^{M} \Delta_{\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{\check{l}_j}\right)\mathbf{H}(S) \tag{6}$$

$$\ge \Delta\mathbf{H}(S), \tag{7}$$

and

$$\left(\sum_{j=1}^{M} \Delta_{\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{\check{l}_j}\right)\mathbf{H}(S)$$

$$= \sum_{l=0}^{n-1}(\Delta_l - \Delta_{l-1})^+\mathbf{H}(S) \tag{8}$$

$$= \sum_{l=1}^{n}(\Delta_{l-1} - \Delta_l)^+\mathbf{H}(S). \tag{9}$$

The equality in (7) holds if and only if $M = 1$.

Eq. (6) first appeared in the preliminary version of this paper [21]. This lower bound is larger than the previous lower bound $\Delta\mathbf{H}(S)$ in [15] if $M > 1$. Note that by Eq. (8) our lower bound is equivalent to $\sum_{l=0}^{n-1}(\Delta_l - \Delta_{l-1})^+\mathbf{H}(S)$, which is presented in [8] and [9]. Eq. (9) is a new formula given in this paper.

Eq. (8) can be interpreted as meaning that each share must have information on the secret for every *increase* in the leakage rate, but not for any decrease. Thus, the total amount of necessary information on the secret is at least the sum of the first successive *increasing* values given by $\Delta_{\hat{l}_1}$ and the $j$-th ones given by $\Delta_{\hat{l}_j} - \Delta_{\check{l}_{j-1}}$ with $1 < j \le M$. Interestingly, Eq. (9) gives another interpretation such that each share must have information on the secret for every *decrease* in the leakage rate, but not for any increase. That is, the total amount of necessary information on the secret is at least the sum of the $j$-th successive *decreasing* values given by $\Delta_{\hat{l}_j} - \Delta_{\check{l}_j}$ with $1 \le j < M$ and the last ones given by $\Delta_{\hat{l}_M}$. If the leakage rate increases only once (i.e., $M = 1$), then the share size only needs to exceed the first increasing value $\Delta$, and we get the previous lower bound in [15]. Otherwise, the share needs additional information on the secret to recover the loss caused by the increase and decrease in the leakage rate. Thus, the new lower bound is generally larger than the previous one, except for the case $M = 1$.

*Proof:* Let $1 \le j < M$. From the definition of local maximum and local minimum, it follows that

$$(\Delta_{\check{l}_j+1} - \Delta_{\check{l}_j})^+ + \cdots + (\Delta_{\hat{l}_{j+1}} - \Delta_{\hat{l}_{j+1}-1})^+ = \Delta_{\hat{l}_{j+1}} - \Delta_{\check{l}_j},$$
$$(\Delta_{\hat{l}_j+1} - \Delta_{\hat{l}_j})^+ + \cdots + (\Delta_{\check{l}_j+1} - \Delta_{\check{l}_j})^+ = 0.$$

We also have

$$(\Delta_0 - \Delta_{-1})^+ + \cdots + (\Delta_{\hat{l}_1} - \Delta_{\hat{l}_1-1})^+ = \Delta_{\hat{l}_1}.$$

Summing up these, we get Eq. (8). Similarly, we have

$$(\Delta_{\hat{l}_j} - \Delta_{\hat{l}_j+1})^+ + \cdots + (\Delta_{\check{l}_j-1} - \Delta_{\check{l}_j})^+ = \Delta_{\hat{l}_j} - \Delta_{\check{l}_j},$$
$$(\Delta_{\check{l}_j} - \Delta_{\check{l}_j+1})^+ + \cdots + (\Delta_{\hat{l}_{j+1}-1} - \Delta_{\hat{l}_{j+1}})^+ = 0,$$
$$(\Delta_{\hat{l}_M} - \Delta_{\hat{l}_M+1})^+ + \cdots + (\Delta_{n-1} - \Delta_n)^+ = \Delta_{\hat{l}_M},$$

and then Eq. (9) holds.

To prove Eq. (6), choose any sequence of strictly increasing subsets of participants

$$\emptyset = A_0 \subset A_1 \subset \cdots \subset A_{n-1} = P \setminus \{i\},$$

and let $A_n = P$, $0 \le l < n$. It holds that

$$\mathbf{H}(\xi_i|\xi_{A_l}) = \mathbf{H}(\xi_i|\xi_{A_l}S) + \Delta_l\mathbf{H}(S). \tag{10}$$

as shown at the bottom of this page. Thus,

$$\begin{aligned}\mathbf{H}(\xi_i|\xi_{A_l}) &- \mathbf{H}(\xi_i|\xi_{A_{l+1}})\\ &= \mathbf{H}(\xi_i|\xi_{A_l}S) - \mathbf{H}(\xi_i|\xi_{A_{l+1}}S)\\ &\quad + (\Delta_l - \Delta_{l+1})\mathbf{H}(S) \quad \text{(from (10))}\\ &\ge (\Delta_l - \Delta_{l+1})\mathbf{H}(S). \quad \text{(from (2))}\end{aligned}$$

Similarly, $\mathbf{H}(\xi_i|\xi_{A_l}) - \mathbf{H}(\xi_i|\xi_{A_{l+1}}) \ge 0$, and thus,

$$\mathbf{H}(\xi_i|\xi_{A_l}) \ge \mathbf{H}(\xi_i|\xi_{A_{l+1}}) + (\Delta_l - \Delta_{l+1})^+\mathbf{H}(S).$$

Knowing that $\mathbf{H}(\xi_i) = \mathbf{H}(\xi_i|\xi_{A_0})$, and $\mathbf{H}(\xi_i|\xi_{A_n}) = 0$, we get

$$\mathbf{H}(\xi_i) \ge \sum_{l=1}^{n}(\Delta_{l-1} - \Delta_l)^+\mathbf{H}(S) \tag{11}$$

by summing. From Eqs. (8), (9), and (11), Eq. (6) follows. ∎

$$\begin{aligned}\mathbf{H}(\xi_i|\xi_{A_l}) &= \mathbf{H}(S|\xi_{A_l}) - \mathbf{H}(S|\xi_i\xi_{A_l}) + \mathbf{H}(\xi_i|\xi_{A_l}S) \quad \text{(from (3))}\\ &= (1 - g(|A_l|))\mathbf{H}(S) - (1 - g(|A_l \cup \{i\}|))\mathbf{H}(S) + \mathbf{H}(\xi_i|\xi_{A_l}S) \quad \text{(from (5))}\\ &= \mathbf{H}(\xi_i|\xi_{A_l}S) + \Delta_l\mathbf{H}(S).\end{aligned}$$

Our lower bound in Eq. (6) uncovers a useful fact: only the extrema affect share size. Using this fact, we can identify the class of access functions for which this lower bound is as small as the one in [15]. Let $\mathcal{F}_{\rm sim} \subset \mathcal{F}$ be the class of access functions whose gradient has only one local maximum, called the *simple class*.

*Corollary 1:* For any $g \in \mathcal{F}$,

$$\sum_{j=1}^{M} \Delta_{\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{\check{l}_j} = \sum_{l=0}^{n-1} (\Delta_l - \Delta_{l-1})^+ = \Delta,$$

if and only if $g \in \mathcal{F}_{\rm sim}$.

We further determine the class of access functions for which the lower bound on $\mathbf{H}(\xi_i)$ equals $\mathbf{H}(S)$, meaning that we cannot shorten the share size to be smaller than that of the secret. Let $\mathcal{F}_{\rm com}$ be the class of access functions that increase to one in a staircase pattern, called the *complicated class*. Specifically, $\mathcal{F}_{\rm com}$ consists of the access functions $g \in \mathcal{F}$ satisfying, for any $\Delta_l > 0$ with $0 \le l < n$: $\Delta_{g,l-1} = \Delta_{g,l+1} = 0$.

*Corollary 2:* For any $g \in \mathcal{F}$,

$$\sum_{j=1}^{M} \Delta_{\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{\check{l}_j} = \sum_{l=0}^{n-1} (\Delta_l - \Delta_{l-1})^+ = 1,$$

if and only if $g \in \mathcal{F}_{\rm com}$.

*Proof:* If $g \in \mathcal{F}_{\rm com}$, all nonzero gradients $\Delta_l$ are local maxima because $\Delta_{l-1} = \Delta_{l+1} = 0$ (i.e., $\Delta_{l-1} < \Delta_l$ and $\Delta_l > \Delta_{l+1}$). Thus, every local minimum gradient has a value of zero. Therefore,

$$\left(\sum_{j=1}^{M} \Delta_{\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{\check{l}_j}\right) = g(n) - 0 = 1.$$

On the other hand, if $g \notin \mathcal{F}_{\rm com}$, then there exist successive positive gradients, at least one of which (denoted by $\Delta_l$) is a local maximum and an adjacent positive gradient (i.e., $\Delta_{l-1}$ or $\Delta_{l+1}$) is not a local maximum. Thus, the summation of the local maximum gradients is smaller than the total increasing amount of $g$, i.e., is smaller than $g(n) = 1$. From Eq. (8), the above equalities hold. ■

We note that the "simple" access functions are either convex, concave, or convex-then-concave. A complicated access function consists of alternating one-run and zero-gradient slopes and increases to one overall.

As shown in the next section, our lower bound is tight. Thus, for any $g \in \mathcal{F}_{\rm sim}$, $\mathbf{H}(\xi_i) = \Delta\mathbf{H}(S)$ in the optimal $g$-USS schemes, whereas for any $g \in \mathcal{F}_{\rm com}$, there is no $g$-USS scheme with $\mathbf{H}(\xi_i) < \mathbf{H}(S)$ and the optimal $g$-USS schemes achieve $\mathbf{H}(\xi_i) = \mathbf{H}(S)$.

## IV. An Optimal Construction

Here, we present a construction of optimal $g$-USS schemes for any $g \in \mathcal{F}$. Essentially, we divide any $g \in \mathcal{F}$ into a set of truncated linear functions $g_1, g_2, \ldots, g_N$ for some $N$ such that $g(l) = \sum_{j=1}^{N} g_j(l)$ for $0 \le l \le n$, called a *decomposition of* $g$. Based on this decomposition, the secret $S$ is given by a vector of random variables $S_1, S_2, \ldots, S_N$ with

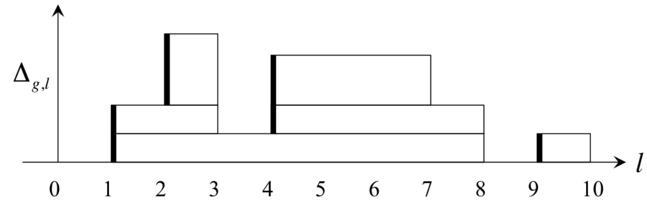


Fig. 1. An example of $\Delta_{g,l}$ filled with rectangles.

$\mathbf{H}(S_j) = g_j(n)\mathbf{H}(S)$.[1] The optimal $g$-USS scheme consists of classical optimal threshold and ramp schemes for $g_j$ (i.e., $g_j$-USS schemes) on the random variable $S_j$ with $1 \le j \le N$. The total amount of information each player receives is given by the sum of the values of $\Delta_{g_j}\mathbf{H}(S)$.

We draw the values of $\Delta_{g,l}$ rather than $g$. As $\Delta_{g,l}$ is the difference, it also preserved under addition; that is, if $g(l) = g'(l) + g''(l)$ for every $l$, then

$$\Delta_{g,l} = \Delta_{g',l} + \Delta_{g'',l}.$$

The classical threshold and ramp schemes (i.e., USS schemes for truncated linear access functions) are depicted as rectangles whose height is also the amount of information each player receives. Its width can be arbitrary long. Any such rectangle with rational height, including one with zero height, can be realized [18]. Fig. 1 shows an example of values of $\Delta_{g,l}$. The thick vertical lines show the positive values of $\Delta_{g,l} - \Delta_{g,l-1}$; their total sum is the lower bound given in Theorem 1. The graph can be filled with rectangles (thus, the independent combination of corresponding USS schemes gives a scheme with the given values of $\Delta_{g,l}$); the total height of these rectangles is equal to the thick lines.

We first present a procedure to fill $\Delta_{g,l}$ with rectangles corresponding to truncated linear access functions $g_1, \ldots, g_N$ so that the total height of these rectangles is equal to the sum of positive values of $\Delta_{g,l} - \Delta_{g,l-1}$. We then show a construction of $g$-USS schemes from $g_j$-USS schemes with $1 \le j \le N$ and prove its optimality.

We say that $g_h$ is a truncated linear function *corresponding to a rectangle* with starting point $l_L$, end point $l_R$, and height $H_h$ if

$$g_h(l) = \begin{cases} 0, & \text{for } 0 \le l < l_{\rm L}, \\ H_h \cdot (l - l_L), & \text{for } l_L \le l \le l_R, \\ H_h \cdot (l_R - l_L), & \text{for } l_R < l \le n. \end{cases} \quad (12)$$

When filling the values of $\Delta_{g,l}$, we start from the bottom, so that the width is extended as much as possible. This is reasonable because ramp schemes with longer ramp runs are more efficient in terms of the share entropy. The proposed procedure, denoted by $\Pi$, takes $g \in \mathcal{F}$ as an input and outputs a finite set of truncated linear functions $\mathcal{F}_g \subset \mathcal{F}$, such that $g = \sum_{g_h \in \mathcal{F}_g} g_h$, as follows.

Filling procedure $\Pi(g)$

Init. Set $h := 0$ and $\mathcal{F}_g := \emptyset$.

Repeat Steps 1–3 until $g = 0$. Then, output $\mathcal{F}_g$.

[1] If $g(n) < 1$, $S$ is a vector of $N+1$ random variables $S_1, S_2, \ldots, S_N, S_{N+1}$, where $S_{N+1}$ is a temporal random variable controlling the amount of exceed information so that $\mathbf{H}(S_{N+1}) = (1 - g(n)) \cdot \mathbf{H}(S)$.

Step 1. $h := h + 1$. Find the first position $l$ such that $\Delta_{g,l} > 0$, where $0 \leq l < n$, and set $l_{\mathrm{L}}$ to this point. Extend the width of the rectangle as much as possible by finding the first position $l$ such that $\Delta_{g,l} = 0$, where $l_{\mathrm{L}} < l \leq n$, and setting $l_{\mathrm{R}}$ to this point. Extend the height as much as possible by setting

$$H_h \triangleq \min\{\Delta_{g,l} | l_{\mathrm{L}} \leq l < l_{\mathrm{R}}\}.$$

Step 2. Set $g_h$ as the truncated linear function corresponding to the rectangle with starting point $l_L$, end point $l_R$, and height $H_h$.

Step 3. Set $g := g - g_h$ and $\mathcal{F}_g := \mathcal{F}_g \cup \{g_h\}$. □

The proposed procedure must terminate for any input $g \in \mathcal{F}$, because in each execution of Steps 1–3, $\Delta_{g,l}$ is decreased to zero for at least one position $l$ with $l_{\mathrm{L}} \leq l < l_{\mathrm{R}}$; thus the procedure terminates after at most $n$ iterations. For the case in Fig. 1, the first rectangle is a rectangle with $(l_{\mathrm{L}}, l_{\mathrm{R}}) = (1, 8)$, and $\Delta_{g,l}$ is decreased to zero at $l = 3$. The second rectangle is one with $(l_{\mathrm{L}}, l_{\mathrm{R}}) = (1, 3)$, and rectangles with $(l_{\mathrm{L}}, l_{\mathrm{R}}) = (2, 3)$, $(4, 8)$, $(4, 7)$, and $(9, 10)$ follow in order. Then, $\Delta_{g,l}$ is decreased to zero for all positions.

The next theorem guarantees that the proposed procedure returns an optimal output.

*Theorem 2:* For any access function $g \in \mathcal{F}$, the output $\mathcal{F}_g$ of $\Pi(g)$ satisfies

$$\sum_{g_h \in \mathcal{F}_g} \Delta_{g_h} = \sum_{j=1}^{M} \Delta_{g,\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{g,\check{l}_j},$$

where $M$ denotes the number of local maximum gradients of $g$; and $\hat{l}_j$ with $1 \leq j \leq M$ (resp. $\check{l}_j$ with $1 \leq j < M$) denotes the point on which the gradient is the $j$-th local maximum of $g$ (resp. the $j$-th local minimum of $g$).

*Proof:* From Eq. (8), it holds that $\sum_{j=1}^{M} \Delta_{g,\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{g,\check{l}_j} = \sum_{l=0}^{n-1} (\Delta_{g,l} - \Delta_{g,l-1})^+$. For each iteration of the procedure, the remainder is always in $\mathcal{F}$ (i.e., a monotonically increasing function). Thus, it is enough to prove that for any $g \in \mathcal{F}$,

$$\sum_{l=0}^{n-1} (\Delta_{g,l} - \Delta_{g,l-1})^+ = \Delta_{g_1} + \sum_{l=0}^{n-1} (\Delta_{g',l} - \Delta_{g',l-1})^+ \quad (13)$$

where $g' = g - g_1$.

From Step 2, it follows that $\Delta_{g_1,l} = H_h > 0$ if $l_{\mathrm{L}} \leq l < l_{\mathrm{R}}$ and otherwise $\Delta_{g_1,l} = 0$. Then, $\Delta_{g',l} = \Delta_{g,l} - \Delta_{g_1}$ if $l_{\mathrm{L}} \leq l < l_{\mathrm{R}}$ and otherwise $\Delta_{g',l} = \Delta_{g,l}$. Thus, for every $l \neq l_{\mathrm{L}}, l_{\mathrm{R}}$,

$$\Delta_{g',l} - \Delta_{g',l-1} = \Delta_{g,l} - \Delta_{g,l-1}.$$

From the definition of $l_{\mathrm{L}}, l_{\mathrm{R}}$, it holds that $\Delta_{g',l_{\mathrm{L}}-1} = \Delta_{g,l_{\mathrm{L}}-1} = 0$ and $\Delta_{g',l_{\mathrm{R}}} = \Delta_{g,l_{\mathrm{R}}} = 0$. Thus, we have

$$\begin{aligned}
&(\Delta_{g',l_{\mathrm{L}}} - \Delta_{g',l_{\mathrm{L}}-1})^+ \\
&\quad = (\Delta_{g,l_{\mathrm{L}}} - \Delta_{g_1}) - 0 \\
&\quad = (\Delta_{g,l_{\mathrm{L}}} - \Delta_{g,l_{\mathrm{L}}-1})^+ - \Delta_{g_1},
\end{aligned}$$

while

$$\begin{aligned}
(\Delta_{g',l_{\mathrm{R}}} - \Delta_{g',l_{\mathrm{R}}-1})^+ &= (0 - \Delta_{g',l_{\mathrm{R}}-1})^+ = 0, \\
(\Delta_{g,l_{\mathrm{R}}} - \Delta_{g,l_{\mathrm{R}}-1})^+ &= (0 - \Delta_{g,l_{\mathrm{R}}-1})^+ = 0.
\end{aligned}$$

Summarizing the above equations, we have

$$\begin{aligned}
&(\Delta_{g',l} - \Delta_{g',l-1})^+ \\
&\quad = \begin{cases} (\Delta_{g,l_{\mathrm{L}}} - \Delta_{g,l_{\mathrm{L}}-1})^+ - \Delta_{g_1}, & \text{for } l = l_{\mathrm{L}}, \\ (\Delta_{g,l} - \Delta_{g,l-1})^+, & \text{for } l \neq l_{\mathrm{L}}. \end{cases} \quad (14)
\end{aligned}$$

By summing Eq. (14) for $0 \leq l < n$, we get Eq. (13). ■

The following theorem presents a construction of USS for any access function $g \in \mathcal{F}$ based on a decomposition of $g$.

*Theorem 3:* For any access function $g \in \mathcal{F}$ and any truncated linear access functions $g_1, \ldots, g_N \in \mathcal{F}$ such that $g(l) = \sum_{j=1}^{N} g_j(l)$ for $0 \leq l \leq n$, there is a $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ satisfying

$$\mathbf{H}(\xi_i) = \sum_{j=1}^{N} \Delta_{g_j} \mathbf{H}(S). \quad (15)$$

*Proof:* Let $\alpha_j = g_j(n)$. Let $k_j$ and $L_j$ be the ramp end and ramp run of $g_j$, respectively. Let $(S_j, \xi_{j,1}, \ldots, \xi_{j,n})$ be optimal $(k_j, L_j, n)$-ramp schemes where $S_1, \ldots, S_N$ are mutually independent and $\mathbf{H}(S_j) = \alpha_j \mathbf{H}((S_1, \ldots S_N))$. Define $S = (S_1, \ldots, S_N)$ and $\xi_i = (\xi_{1,i}, \ldots, \xi_{N,i})$ for $i \in P$. Because $\alpha_j$ is in $\mathbb{Q}_{[0,1]}$, there is an integer $\beta$ and a prime $q$ such that $\beta_j = \alpha_j \beta$ are also integers, and $L_j$ divides $\beta_j$ and optimal $(k_j, L_j, n)$-ramp schemes can be constructed for $\hat{S}_j = \mathrm{GF}(q^{\beta_j})$ [5], [18]. We note that $\beta = \sum_{j=1}^{N} \beta_j$ and $\hat{S} = \mathrm{GF}(q^{\beta})$.

It is clear that $(S, \xi_1, \ldots, \xi_n)$ is an SS scheme. For any subset $A \subseteq P$, letting $l = |A|$,

$$\begin{aligned}
\mathbf{H}(S|\xi_A) &= \sum_{j=1}^{N} \mathbf{H}(S_j | (\xi_{j,i})_{i \in A}) \\
&= \sum_{j=1}^{N} (1 - \alpha_j^{-1} g_j(l)) \mathbf{H}(S_j) \\
&= \sum_{j=1}^{N} \alpha_j (1 - \alpha_j^{-1} g_j(l)) \mathbf{H}(S) \\
&= (1 - g(l)) \mathbf{H}(S)
\end{aligned}$$

from the properties of the optimal ramp schemes used. Thus, Eq. (5) holds, and $(S, \xi_1, \ldots, \xi_n)$ is a $g$-USS scheme. Similarly, it holds that

$$\begin{aligned}
\mathbf{H}(\xi_i) &= \sum_{j=1}^{N} \mathbf{H}(\xi_{j,i}) \\
&= \sum_{j=1}^{N} \alpha_j^{-1} \Delta_{g_j} \mathbf{H}(S_j) \\
&= \sum_{j=1}^{N} \Delta_{g_j} \mathbf{H}(S)
\end{aligned}$$

from the optimality of the used ramp schemes. Thus, Eq. (15) holds. ■

The next theorem guarantees the existence of an optimal USS scheme for any access function $g \in \mathcal{F}$.

*Theorem 4:* For any access function $g \in \mathcal{F}$, there is a $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ satisfying

$$\mathbf{H}(\xi_i) = \left( \sum_{j=1}^{M} \Delta_{g,\hat{l}_j} - \sum_{j=1}^{M-1} \Delta_{g,\check{l}_j} \right) \mathbf{H}(S),$$

where $M$ denotes the number of local maximum gradients of $g$; and $\hat{l}_j$ with $1 \leq j \leq M$ (resp. $\check{l}_j$ with $1 \leq j < M$) denotes the point at which the gradient is the $j$-th local maximum (resp. the $j$-th local minimum).

*Proof:* From Theorems 2 and 3, the equality holds. This means that $\mathbf{H}(\xi_i)$ in the proposed construction achieves the lower bound of Theorem 1. ∎

The optimal $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ with $\hat{S} = \mathrm{GF}(q^{\beta})$ consists of optimal $g_j$-USS schemes $(S_j, \xi_{j,1}, \ldots, \xi_{j,n})$ with $\hat{S}_j = \mathrm{GF}(q^{\beta_j})$ where $\Pi(g) = \{g_j\}$, $q$ is a prime, and $\beta, \beta_j > 0$ are integers such that $\beta_j/\beta = g_j(n)$ and $L_j | \beta_j$. Thus, the size of the domain of secrets depends on $\Pi(g) = \{g_j\}$. We briefly discuss the size of the domain of secrets from two points of view. One is a necessary size of the domain for a given access function (which must be very large), and the other is that for a given length of the secret (e.g., 128-bit values). For a given $g$, let $g_j(n) = \gamma'_j/\gamma_j$ for some integers $\gamma'_j, \gamma_j > 0$. Consider an extreme case that $\gamma_j$ with $1 \leq j \leq |\Pi(g)|$ are coprime. To satisfy the above requirement, $\beta$ should be divided by $\prod \gamma_j$. It follows that $\beta \geq \prod \gamma_j$. From Steps 1–2 of the filling process $\Pi(g)$, $g_j(n) \leq \Delta_g$. From $\gamma'_j > 0$, we have $\gamma_j \geq \Delta_g^{-1}$. Thus, $\beta \geq \Delta_g^{-|\Pi(g)|}$. This means that the size of the domain of secrets $|\hat{S}| = q^{\beta}$ becomes very large if we allow complex control of leakage with various values of $\Delta_{g,l}$, implying a larger size of the domain of shares $|\hat{S}_j|$. For a given length of secrets, denoted by $\kappa$, if we could prioritize the efficiency over the control of leakage, then we could define $g$, $\hat{S}$, and $\hat{S}_j$ as follows: $g(l) = l/n$, that is, $|\Pi(g)| = 1$ and $g = g_1$ with $(L_1, k_1) = (n, n)$; $\beta$ is the smallest integer such that $\beta \geq \kappa$ and $n|\beta$; $\hat{S} = \mathrm{GF}(2^{\beta})$ and $\hat{S}_1 = \mathrm{GF}(2^{\beta/n})$. It holds that $\beta < n + \kappa$. Thus, $|\hat{S}|$ and $|\hat{S}_1|$ are at most $2^{n+\kappa-1}$ and $2^{1+(\kappa-1)/n}$. The size of the domain of shares $|\hat{S}_j|$ becomes closer to the ideal value $2^{\kappa/n}$ for a larger $\kappa$.

We show that our optimal $g$-USS scheme satisfies a stronger security required by fractional secret sharing introduced in [11]. We recall the definitions of fractional secret sharing in [11].

*Definition 3 (Definition 8 in [11]):* Let $P = \{1, \ldots, n\}$ be a finite set of players and let $m$ be an integer. A function $f : 2^P \to \{0, \ldots, m-1\}$ is monotone if $B \subseteq C$ implies that $f(B) \geq f(C)$. A fractional access structure is a monotone function $f : 2^P \to \{0, \ldots, m-1\}$, with $f(\emptyset) = m - 1$. We say that $f$ is symmetric if $f(B)$ depends only on $|B|$.

*Definition 4 (Definition 9 in [11]):* Let $f : 2^P \to \{0, \ldots, m-1\}$ be a fractional access structure and let $S$ be a finite secret-domain. Let $D$ be a randomized algorithm which outputs a uniformly random $s \in S$ together with an $n$-tuple of shares $(v_1, \ldots, v_n)$. We say that $D$ is a fractional secret-sharing scheme realizing $f$ with secret-domain $S$ if there exists a positive integer $k$ such that the following holds: For every $A \subseteq P$, and any possible share vector $v_A$ of players in $A$, the distribution of $s$ conditioned on the event that players in $A$ receive the shares $v_A$ is uniform over a subset of $S$ of size $f(A) \cdot k + 1$. If the above holds with $k = 1$, we say that $D$ strictly realizes $f$.

*Theorem 5:* For any access function $g \in \mathcal{F}$, there is an optimal $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ that strictly realizes a fractional access structure $f : 2^P \to \{0, \ldots, |\hat{S}| - 1\}$ with secret-domain $\hat{S}$.

*Proof:* From Theorem 4, for any $g \in \mathcal{F}$, there is an optimal $g$-USS scheme $(S, \xi_1, \ldots, \xi_n)$ constructed from $g_j$-USS schemes $(S_j, \xi_{j,1}, \ldots, \xi_{j,n})$ with $1 \leq j \leq N$ where each $g_j$ is a truncated linear function with ramp end $k_j$ and ramp run $L_j$, $\hat{S}_j = \mathrm{GF}(q^{\beta_j})$, and $\hat{S} = \hat{S}_1 \times \cdots \times \hat{S}_N$. Let $\alpha_j = g_j(n)$.

Define $f$ such that $f(A) = |\hat{S}|^{1-g(|A|)} - 1$ for $A \subseteq P$. It is clear that $f$ is symmetric. Because $g(0) = 0$ and $g(|B|) \leq g(|C|)$ for any $B, C \subseteq P$ with $B \subseteq C$, it holds that $f(\emptyset) = |\hat{S}| - 1$ and $f(B) \geq f(C)$ for any $B, C \subseteq P$ with $B \subseteq C$. Thus, $f$ is a symmetric fractional access structure. Similarly, we can define $f_j : 2^P \to \{0, \ldots, |\hat{S}_j| - 1\}$ such that $f_j(A) = |\hat{S}_j|^{1-\alpha_j^{-1} g_j(|A|)} - 1$ for $A \subseteq P$ and prove that $f_j$ is a symmetric fractional access structure.

First, we prove that if the used $(k_j, L_j, n)$-ramp schemes with $1 \leq j \leq N$ are fractional secret sharing schemes strictly realizing $f_j$, then the optimal scheme strictly realizes $f$. Suppose $S_j$ with $1 \leq j \leq N$ are uniform over $\hat{S}_j = \mathrm{GF}(q^{\beta_j})$. This follows that $S$ is uniform over $\hat{S} = \mathrm{GF}(q^{\beta})$. For any $A \subseteq P$, any $s'_j, s''_j \in \hat{S}_j$, and any $v_{j,A} \in \hat{\xi}_{j,A}$, it holds that $\Pr(S_j = s'_j | \xi_{j,A} = v_{j,A}) = \Pr(S_j = s''_j | \xi_{j,A} = v_{j,A})$. From the mutual independency of $S_1, \ldots, S_N$, for any $A \subseteq P$, any $s', s'' \in \hat{S}$, and any $v_A \in \hat{\xi}_A$, it holds that $\Pr(S = s' | \xi_A = v_A) = \Pr(S = s'' | \xi_A = v_A)$ and the number of $s$ with $\Pr(S = s \mid \xi_A = v_A) > 0$ is $\prod_{j=1}^{N} (f_j(A) + 1)$. From $H(S_j) = \alpha_j H(S)$ and the uniformity of $S_1, \ldots, S_N$, it holds that $q^{\beta_j} = q^{\alpha_j \beta}$. Thus, $f_j(A) + 1 = q^{\beta_j(1-\alpha_j^{-1} g_j(|A|))} = (q^{\beta})^{\alpha_j(1-\alpha_j^{-1} g_j(|A|))}$. Because the set $g_1, \ldots, g_N$ is a decomposition of $g$, $\sum_{j=1}^{N} \alpha_j(1 - \alpha_j^{-1} g_j(|A|)) = 1 - g(|A|)$. Thus, $\prod_{j=1}^{N} (f_j(A) + 1) = f(A) + 1$. Then, the distribution of $s$ conditioned on the event that players in $A$ receive the shares $v_A$ is uniform over a subset of $\hat{S}$ of size $f(A) + 1$. That is, the optimal scheme strictly realizes $f$ with secret-domain $\mathrm{GF}(q^{\beta})$.

Then, we prove that the $(k_j, L_j, n)$-ramp scheme $(S_j, \xi_1, \ldots, \xi_n)$ constructed by the Shamir scheme in [5] for $\hat{S}_j = \mathrm{GF}(q^{\beta_j})$ strictly realizes $f_j(A) = |\hat{S}_j|^{1-\alpha_j^{-1} g(|A|)} - 1$ for $A \subseteq P$. For a given secret $s \in \hat{S}_j$, the Shamir scheme in [5] chooses $L_j + n$ distinct elements $c_1, \ldots, c_{L_j}, b_1, \ldots, b_n \in \mathrm{GF}(q^{\beta_j/L_j})$, chooses a random polynomial of degree $k_j - 1$ in $\mathrm{GF}(q^{\beta_j/L_j})[x]$ as $p(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ subject to $(p(c_1), \ldots, p(c_{L_j})) = s$, and outputs shares $v_i = p(b_i)$ with $1 \leq i \leq n$.

For any $A \subseteq P$ with $|A| \geq k_j$ and any shares $v_{j,A} \in \hat{\xi}_{j,A}$, the unique polynomial satisfies the $|A|$ equations on $p$ given by $v_{j,A}$. Thus, the secret is uniquely determined. From the definition of truncated linear functions, $g_j(|A|) = g_j(n) = \alpha_j$. Then, $f_j(A) + 1 = 1$.

For any $A \subseteq P$ with $|A| < k_j - L_j$, any $\upsilon_{j,A} \in \hat{\xi}_{j,A}$, and any secret $s \in \hat{S}_j$, there are $(q^{\beta_j/L_j})^{k_j-L_j-|A|}$ polynomials of degree $k_j - 1$ that satisfy the $|A|$ equations on $p$ given by $\upsilon_{j,A}$ and are equally likely chosen. From the definition of truncated linear functions, $g_j(|A|) = g_j(0) = 0$, and then $f_j(A) + 1 = |\hat{S}_j|$. Thus, in both cases, the distribution of $s$ conditioned on the event that players in $A$ receive the shares $\upsilon_A$ satisfies the requirement.

For any $A \subseteq P$ with $k_j - L_j \leq |A| < k_j$, from the definition of $g_j$, $g_j(|A|) = \frac{\alpha_j}{L_j}(|A| - k_j + L_j)$. Therefore, $f_j(A) + 1 = (q^{\beta_j})^{1-(|A|-k_j+L_j)/L_j} = (q^{\beta_j/L_j})^{k_j-|A|}$. For any $\upsilon_{j,A} \in \hat{\xi}_{j,A}$, there are $(q^{\beta_j/L_j})^{k_j-|A|}$ polynomials of degree $k_j - 1$ that satisfy the $|A|$ equations on $p$ given by $\upsilon_{j,A}$ and are equally likely chosen. A different polynomial corresponds to a different secret value. Thus, the distribution of $s$ conditioned on the event that players in $A$ receive the shares $\upsilon_A$ is uniform over a subset of $\hat{S}_j$ of size $(q^{\beta_j/L_j})^{k_j-|A|} = f_j(A) + 1$.

Therefore, our optimal scheme is a fractional secret sharing scheme that strictly realizes $f$ with secret-domain $\mathrm{GF}(q^{\beta})$. ■

The theorem means that our optimal scheme can be used for applications of fractional secret sharing. For instance, the motivated application of fractional secret sharing is that several players share a secret password (e.g., a key which locks a vault) such that the largest subset of cooperating players will be the first to guess the correct password. The uniform distribution does not only give control over the expected number of attempts in an optimal guessing strategy, but also minimizes the variance of the number of such attempts [11]. Our scheme further minimizes the storage required by each player. Thus, both stronger security and higher efficiency are guaranteed.

## V. Conclusion

In this paper, we derived a new lower bound on the entropy of shares for USS schemes. This bound is generally higher than previously known lower bounds, but does not exceed the entropy of the secret. Next, we characterized some classes of access functions in terms of their share entropy. Finally, we presented an optimal construction of USS schemes, which makes the entropy of each share equal to the derived lower bound.

## Acknowledgements

The authors are grateful to the associate editors, Stefan Wolf and Alfred Menezes, for their helpful management. They are also thankful to the referees for their valuable and insightful comments.

## References

[1] L. Bai, "A strong ramp secret sharing scheme using matrix projection," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, New York, NY, USA, Jun. 2006, pp. 652–656.

[2] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. 3rd Int. Conf. Coding Cryptol. (IWCC)*, Qingdao, China, vol. 6639, May/Jun. 2011, pp. 11–46.

[3] A. Beimel and I. Orlov, "Secret sharing and non-Shannon information inequalities," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5634–5649, Sep. 2011.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Manag. Requirements Knowl., Int. Workshop (AFIPS)*, New York, NY, USA, vol. 48, Jun. 1979, pp. 313–317.

[5] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Proc. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, vol. 196, Aug. 1984, pp. 242–269.

[6] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *J. Cryptol.*, vol. 6, no. 3, pp. 157–167, 1993.

[7] L. Csirmaz, "The size of a share must be large," *J. Cryptol.*, vol. 10, no. 4, pp. 223–231, 1997.

[8] O. Ferràs, T. B. Hansen, T. Kaced, and C. Padró. *On the Information Ratio of Non-Perfect Secret Sharing Schemes*. Accessed: Aug. 29, 2017. [Online]. Available: https://eprint.iacr.org/eprint-bin/versions.pl?entry=2014/124

[9] O. Ferrás, T. Hansen, T. Kaced, and C. Padró, "Optimal non-perfect uniform secret sharing schemes," in *Proc. 34th Annu. Int. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, vol. 8617, 2014, pp. 217–234.

[10] M. K. Franklin and M. Yung, "Communication complexity of secure computation," in *Proc. 24th Annu. ACM Symp. Theory Comput. (STOC)*, Victoria, BC, Canada, May 1992, pp. 699–710.

[11] Y. Ishai, E. Kushilevits, and O. Strulovich, "Lossy chains and fractional secret sharing," in *Proc. 30th Int. Symp. Theor. Aspects Comput. Sci. (STACS)*, Feb./Mar. 2013, pp. 160–171.

[12] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Inf. Process. Lett.*, vol. 97, no. 2, pp. 52–57, 2006.

[13] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[14] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, "Nonperfect secret sharing schemes and matroids," in *Proc. Workshop Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Perugia, Italy, vol. 765, May 1994, pp. 126–141.

[15] K. Okada and K. Kurosawa, "Lower bound on the size of shares of nonperfect secret sharing schemes," in *Proc. 4th Int. Conf. Theory Appl. Cryptol. (ASIACRYPT)*, Wollongong, NSW, Australia, vol. 917, Nov./Dec. 1994, pp. 33–41.

[16] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[17] D. R. Stinson, "Decomposition constructions for secret-sharing schemes," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 118–125, Jan. 1994.

[18] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," (in Japanese), *IECE Trans.*, vol. 69, pp. 945–952, Sep. 1985 (Transl.: *Electron. Commun. Jpn. I*, vol. 69, pp. 46–54, Sep. 1986).

[19] K. Yoneyama, N. Kunihiro, B. Santoso, and K. Ohta, "Non-linear function ramp scheme," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Parma, Italy, Oct. 2004, pp. 788–793.

[20] M. Yoshida and T. Fujiwara, "Secure construction for nonlinear function threshold ramp secret sharing," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 1041–1045.

[21] M. Yoshida, T. Fujiwara, and M. Fossorier, "Optimum general threshold secret sharing," in *Proc. 6th Int. Conf. Inf. Theoretic Secur. (ICITS)*, Montreal, QC, Canada, vol. 7412, Aug. 2012, pp. 187–204.

[22] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Telecommunications and Signal Processing). Hoboken, NJ, USA: Wiley, 2006.

**Maki Yoshida** received the M.E. and Ph.D. degrees in informatics and mathematical science from Osaka University, Toyonaka, Osaka, Japan, in 1998 and 2001, respectively. From 2001 to 2013, she was an Assistant Professor at Osaka University. In 2013, she joined National Institute of Information and Communications Technology (NICT). Her research interests include cryptography, information-theoretic security, and computational problems for public-key cryptosystems. She was Program Co-Chair for the 9th International Workshop on Security (IWSEC2014). From 2016 to 2018, she was Director of the Japan Society for Industrial and Applied Mathematics (JSIAM).

**Toru Fujiwara** (S'83–M'86) received the B.E., M.E., and Ph.D. degrees in information and computer science from Osaka University, Toyonaka, Osaka, Japan, in 1981, 1983, and 1986 respectively. In 1986, he joined the faculty of Osaka University. During 1989-1990, he was on leave as a Postdoctoral Fellow in the Department of Electrical Engineering, University of Hawaii, Honolulu, HI, USA. From 1992 to 1997, he was an Associate Professor in the Department of Information and Computer Sciences, Osaka University, where he has been a Professor since 1997. He is currently with the Department of Multimedia Engineering, Graduate School of Information Science and Technology. His current research interests include coding theory and cryptography. He is a Member of the Institute of Electronics, Information and Communication Engineers of Japan, the Information Processing Society of Japan, and the Association for Computing Machinery.

**Marc P. C. Fossorier** (F'06) received the B.E. degree from the National Institute of Applied Sciences (I.N.S.A.) Lyon, France in 1987, and the M.S. and Ph.D. degrees in 1991 and 1994, all in electrical engineering. His research interests include decoding techniques for linear codes, communication algorithms and statistics. Dr. Fossorier was a recipient of a 1998 NSF Career Development award and became IEEE Fellow in 2006. He served as Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2003 to 2006, as Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 1996 to 2003, as Editor for the IEEE COMMUNICATIONS LETTERS from 1999 to 2007, and as Treasurer of the IEEE Information Theory Society from 1999 to 2003. From 2002 to 2007, he was an elected member of the Board of Governors of the IEEE Information Theory Society which he served as Second and First Vice-President. He was Program Co-Chairman for the 2007 International Symposium on Information Theory (ISIT), the 2000 International Symposium on Information Theory and Its Applications (ISITA) and Editor for the Proceedings of the 2006, 2003 and 1999 Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC).