Efficient Multiplicative Sharing Schemes

Simon R. Blackburn[*] [**], Mike Burmester[*], Yvo Desmedt[***] and Peter R. Wild[*]

Abstract. Multiplicative threshold schemes are useful tools in threshold cryptography. For example, such schemes can be used with a wide variety of practical homomorphic cryptosystems (such as the RSA, the El Gamal and elliptic curve systems) for threshold decryption, signatures, or proofs. The paper describes a new recursive construction for multiplicative threshold schemes which makes it possible to extend the number of users of such schemes for a relatively small expansion of the share size. We discuss certain properties of the schemes, such as the information rate and zero knowledge aspects.

The paper extends the Karnin–Greene–Hellman bound on the parameters of ideal secret sharing schemes to schemes which are not necessarily ideal and then uses this as a yardstick to compare the performance of currently known multiplicative sharing schemes.

1 Introduction

Secret sharing — the process of distributing a secret key amongst several participants so that only certain subsets of these participants can recover any information about the key — has been intensively studied since its invention by Blakley [2] and Shamir [13] in the late 1970's. The more specific notion of homomorphic secret sharing was introduced by Benaloh [1] in the context of creating secret ballot election schemes and can be used to achieve secret sharing without a mutually trusted authority. In such schemes, binary operations are defined on the set of keys and the set of shares in such a way that the process of a collection of participants pooling their shares to recompute the key may be regarded as a homomorphism from the set of n-tuples of shares to the set of keys. This paper is concerned with the design of sharing schemes which possess a close analogue of the homomorphic property known as the multiplicative property. In multiplicative sharing schemes there is a multiplication defined on the set K of all possible keys such that the recomputation of the key can be achieved by multiplying together appropriate elements of K derived from some of the participants' shares (see Section 2 for a formal definition). Any ideal homomorphic sharing

[*] Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom. E-mail addresses: s.blackburn@vms.rhbnc.ac.uk, m.burmester@vms.rhbnc.ac.uk, p.wild@vms.rhbnc.ac.uk.

[**] This author is supported by an E.P.S.R.C. Advanced Fellowship.

[***] Dept. EE & CS, Univ. of Wisconsin – Milwaukee, P.O. Box 784, WI 53201 Milwaukee, U.S.A. Email address: desmedt@cs.uwm.edu. This author was supported by N.S.F. NCR-9508528 and the E.P.S.R.C.

U. Maurer (Ed.): Advances in Cryptology - EUROCRYPT '96, LNCS 1070, pp. 107-118, 1996.

scheme automatically satisfies the multiplicative property [7, 8]. Such schemes have played a crucial role in threshold cryptography and function sharing — see for example [3, 6, 4]. Threshold cryptography refers to the study of schemes which share the ability to compute a cryptographic function analogously to the way threshold secret sharing schemes share a secret. One application, for example, allows shareholders to co-sign messages non-interactively. In the process of co-signing, users divulge only enough information to allow the co-signature of a particular message and nothing more — for example, no information about their secret shares is revealed. This property is achieved by requiring that the secret sharing scheme has such properties as being zero-knowledge (the computational equivalent of perfect sharing).

In applications where K can be regarded as the additive group of a finite field, multiplicative and homomorphic zero-knowledge threshold schemes exist that are ideal [13] (i.e. the size of the shares is the same as the size of the key). But in many applications K cannot be regarded in this way (for example in the context of RSA based threshold schemes) and known multiplicative and homomorphic zero-knowledge threshold schemes have a large share expansion (the reciprocal of the information rate). Indeed in the Desmedt–Frankel zero-knowledge t out of n threshold scheme [7], which is multiplicative and homomorphic, the shares are roughly n times larger than the key. Although the scheme in [4] has only a $\log_2 n$ expansion of the shares when $t = 2$, its performance when t is only moderately larger is poor.

The goal of this paper is to present multiplicative zero-knowledge threshold schemes for which the share expansion is substantially better than for competing schemes. The schemes we present are also homomorphic if the group K is abelian. We also consider an inequality of Karnin, Greene and Hellman [12] which bounds the number n of participants of an ideal t out of n secret sharing scheme in terms of t and the size q of the set of shares. We extend their bound to the case when the scheme is not necessarily ideal.

The paper is organised as follows. Section 2 contains some basic definitions and introduces the notation that we use in the remainder of the paper. In Section 3 we extend the Karnin–Greene–Hellman bound from the situation of ideal threshold schemes to the general case. The result will be used in Section 5 to prove that if t and the order of K are held constant, our threshold schemes are asymptotically optimal as $n \to \infty$. All our schemes are recursive in nature (cf. [4]) — we construct a t out of n scheme by using several copies of a t out of ℓ scheme for some $\ell < n$. This recursive construction is given in Section 4. An analysis of the share expansion of the schemes, the zero-knowledge properties, and a discussion of the performance of the schemes can be found respectively in Sections 5, 6 and 7.

2 Definitions and Notation

Informally, a perfect t out of n threshold scheme is a scheme in which a collection of n users (called participants) are each given a share (which may, for example, be a finite string or an element of a finite field). The shares are chosen such that any t of the participants can pool their shares to compute some secret piece of information (called the key) and such that the knowledge of at most $t-1$ of the shares gives absolutely no information about the key.

We define our notation as follows. Let P be a set of n participants which we identify with the set $\{1, 2, \ldots, n\}$. Let K be a finite set whose elements we call keys and suppose that K has two or more elements (to avoid trivialities). Let S be a finite set of order q whose elements we call shares[4]. Finally, let V be the set of all n-tuples of elements from S, where each n-tuple is indexed by the elements of P.

Definition 1. A t out of n threshold scheme consists of two algorithms. The *distribution algorithm* $\mathcal{D}$ is a probabilistic algorithm which takes as input an element $k \in K$. It randomly generates an element $(s_1, s_2, \ldots, s_n) \in V$ according to some distribution depending on k. The algorithm then distributes share s_i to participant i. The *reconstruction algorithm* $\mathcal{R}$ is an algorithm which takes as input an element $(s_1, s_2, \ldots, s_n) \in V$ with up to $n-t$ erasures (i.e. up to $n-t$ of the components $s_1, \ldots, s_n$ have been omitted). It outputs a key $k \in K$. The pair $(\mathcal{D}, \mathcal{R})$ is a *perfect* t *out of* n *threshold scheme* if the following two conditions are satisfied.

1. Any t participants may use algorithm $\mathcal{R}$ to reconstruct the key. More formally, if $c \in V$ is a possible output from algorithm $\mathcal{D}$ when $k \in K$ is input, then algorithm $\mathcal{R}$ outputs k when the element c with up to $n-t$ erasures is input.
2. No information is revealed about the key k by knowing up to $t-1$ of the participants' shares. More formally, suppose that X is a random variable taking values in K according to some distribution. Let Y_i (where $i \in P$) be random variables taking values in S defined by the distribution on the set of shares given to participant i when algorithm $\mathcal{D}$ is run on input X. Then the variable X is independent of the joint distribution of the variables $Y_{i_1}, \ldots, Y_{i_{t-1}}$ for all $i_1, \ldots, i_{t-1} \in P$.

We remark that, since S and K are finite, Condition 2 is equivalent to Equation (2) in the paper of Karnin, Green and Hellman [12]. All schemes that we consider are perfect, that is, satisfy Condition 2 above, so from now on we drop this term and just refer to t out of n threshold schemes.

In this paper we concentrate on multiplicative threshold schemes [4].

Definition 2. Let $(\mathcal{D}, \mathcal{R})$ be a t out of n threshold scheme for which the key space K is a finite group[5] with respect to the operation "$*$". The scheme $(\mathcal{D}, \mathcal{R})$

[4] In this paper we assume, for simplicity, that all participants receive shares taken from the same set S. The results of the paper easily extend to the situation where the share sets associated with each participant are allowed to differ.

[5] The definitions and results in this paper can easily be extended to the case when K is a finite quasigroup.

is *multiplicative* over $(K, *)$ if for all sets $B = \{i_1, i_2, \ldots, i_t\}$ of t distinct participants there exists a family $f_{i_1,B}, f_{i_2,B}, \ldots, f_{i_t,B}$ of functions from S to K and a public ordering $i_1, i_2, \ldots, i_t$ of the elements of B with the following property. For all keys $k \in K$ and shares $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$ that have been distributed to B by algorithm $\mathcal{D}$ on input k, we may express k in the form:

$$k = f_{i_1,B}(s_{i_1}) * f_{i_2,B}(s_{i_2}) * \cdots * f_{i_t,B}(s_{i_t}). \tag{1}$$

Note that multiplicative schemes only impose a group structure on the set of keys K — no group structure on the set of shares S is assumed. This is in contrast to the notion of homomorphic schemes [1].

2.1 An Example

We illustrate the concept of a multiplicative threshold scheme and its use in threshold cryptography with the following example. Let q be a prime and let $K = (\mathbb{F}_q, +)$ be the additive group of the field $\mathbb{F}_q$ of q elements. The Shamir threshold scheme [13] over $\mathbb{F}_q$ is a multiplicative scheme over K. Indeed, in the Shamir t out of n threshold scheme, Lagrange interpolation allows the secret $k \in K$ to be written as

$$k = e_{i_1,B}s_{i_1} + e_{i_2,B}s_{i_2} + \cdots + e_{i_t,B}s_{i_t}$$

where B is a set of t participants $\{i_1, i_2, \ldots, i_t\}$ who hold shares $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$, and $e_{i_1,B}, e_{i_2,B}, \ldots, e_{i_t,B}$ are elements of $\mathbb{F}_q$ which may be calculated from public information about the subset B. Thus, in this case, $f_{i_j,B}(s_{i_j}) = e_{i_j,B}s_{i_j}$ for $j = 1, \ldots, t$.

This multiplicative scheme may be used to provide threshold decryption in the El Gamal public key cryptosystem as follows (see [5]).

Let p be a prime and let q be a prime divisor of $p - 1$. Let g be an element of $\mathbb{F}_p$ of multiplicative order q. Let $k \in K$ and put $y = g^k$. The value y is the public key (corresponding to secret key k) used to encrypt messages so that only a threshold of t participants holding shares of k can decrypt the corresponding cryptograms.

To encrypt a message block $m \in \mathbb{F}_p$, a value r is chosen at random in K and cryptogram (R, c) is formed, where $R = g^r$ and $c = zm$ with $z = y^r$. A set B of t participants $i_1, i_2, \ldots, i_t$ decrypt (R, c) as follows. Individually, using their secret shares, they calculate $z_{i_j} = R^{e_{i_j,B}s_{i_j}}$ for $j = 1, \ldots, t$. Provided q is large, these values $z_{i_1}, z_{i_2}, \ldots, z_{i_t}$ may be made public without compromising $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$. From these values, $z = z_{i_1}z_{i_2}\cdots z_{i_t}$ may be calculated and $m = cz^{-1}$ recovered. Thus the cryptogram is decrypted (by a threshold of participants) while the secret key k and shares $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$ remain secret.

Schemes which are multiplicative over the group of units of the integers modulo n can be used in conjunction with RSA to achieve threshold decryption and signature schemes (see [7] for a description of suitable schemes). Note that the Shamir scheme can no longer be used in this situation because there is no natural way of regarding the group of units of the integers modulo n as a field.

Schemes which are multiplicative over a non-abelian group are useful in zero-knowledge proofs which utilise joint knowledge of a graph isomorphism (see [4]). Multiplicative schemes are especially useful in this last situation, as suitable homomorphic schemes do not always exist [9].

Because of the above applications, it is desirable to construct multiplicative threshold schemes for a wide range of groups. Note that, for such schemes to be practical, a multiplicative scheme should be computationally feasible. Moreover, one must take care that the computational information required to carry out the multiplicative scheme efficiently does not compromise any public key system used as part of the application. For example, the factorisation of n should not be required in RSA based schemes. Thus one should check in any given situation whether the use of a given multiplicative scheme is appropriate. Such issues motivate the study of zero-knowledge techniques, see Section 6.

3 Extending the Karnin–Greene–Hellman bound

Karnin, Greene and Hellman established [12, Theorem 5] that for an ideal t out of n threshold scheme where the set of shares has order q, the inequality $n \leq q + t - 2$ always holds, provided that $t \geq 2$. They used a correspondence between ideal schemes and Maximum Distance Separable codes together with a bound on the lengths of such codes due to Singleton [14]. The aim of the present section is to show that this bound holds for schemes which are not necessarily ideal — our method of proof is of necessity quite different.

Theorem 3. *Let $t \geq 2$ and suppose there exists a perfect t out of n threshold scheme where the shares are taken from a set of order q. Then*

$$n \leq q + t - 2. \tag{2}$$

Proof: We may realise a 2 out of $n - (t - 2)$ threshold scheme using a t out of n scheme by making public the shares of a fixed set of $t - 2$ participants in the t out of n scheme. Thus the existence of a t out of n scheme implies the existence of a 2 out of $n - (t - 2)$ scheme. So in order to prove (2), it suffices to show that for a 2 out of n threshold scheme with shares taken from a set of order q, we have

$$n \leq q. \tag{3}$$

Suppose, for a contradiction, that there exists a 2 out of n threshold scheme $(\mathcal{D}, \mathcal{R})$ with a share set of order q and such that $n \geq q + 1$. Recall that the algorithm $\mathcal{D}$ proceeds by generating an element $c \in V$ and distributing the ith component of c to participant i. For $k \in K$, define C_k to be the set of all $c \in V$ generated by algorithm $\mathcal{D}$ with positive probability when k is given as input. If $k, k' \in K$ are distinct keys and $c \in C_k, c' \in C_{k'}$, then c and c' can agree in at most one component, because two components uniquely determine the key in a 2 out of n threshold scheme.

Let X be a random variable taking values uniformly in the set of keys K. Let Y be the random variable taking values in V formed by applying algorithm $\mathcal{D}$

to X, and for all $i \in \{1, \ldots n\}$ let Y_i be its ith component. For $k \in K$, define Y^k to be the random variable taking values in $C_k \subseteq V$ with probability distribution equal to the distribution of elements $c \in V$ generated by algorithm $\mathcal{D}$ when the key k is input, and for all $i \in \{1, \ldots, n\}$ let Y_i^k be the ith component of Y^k. Since Y_i and X are independent, we may note that $Prob(Y_i^k = s) = Prob(Y_i = s \mid X = k) = Prob(Y_i = s)$. So $Prob(Y_i^k = s) = Prob(Y_i^{k'} = s)$ for all $s \in S$ and all $k, k' \in K$. Let $k, k' \in K$ be distinct keys. Define $\delta : S \times S \to \mathbb{Z}$ by

$$\delta(s, s') = \begin{cases} 1 \text{ if } s = s' \text{ and} \\ 0 \text{ if } s \neq s'. \end{cases}$$

Let $Z_i^{k,k'}$ be a random variable defined by $Z_i^{k,k'} = \delta(Y_i^k, Y_i^{k'})$. Let E denote the expected value function. Since our scheme is perfect, we find

$$\begin{aligned} E(Z_i^{k,k'}) &= Prob(Y_i^k = Y_i^{k'}) = \sum_{s \in S} Prob(Y_i^k = s) \cdot Prob(Y_i^{k'} = s) \\ &= \sum_{s \in S} \left(Prob(Y_i^k = s)\right)^2 \geq \frac{1}{q}. \end{aligned}$$

So

$$E(\sum_{i=1}^{q+1} Z_i^{k,k'}) = \sum_{i=1}^{q+1} E(Z_i^{k,k'}) \geq \frac{q+1}{q} > 1.$$

This implies that there exist $c \in C_k$ and $c' \in C_{k'}$ such that c and c' agree in more than one component (indeed, they agree in more than one of their first $q + 1$ components). This is the contradiction that we have been seeking, so the inequality (3), and therefore the inequality (2), follow. □

4 A Recursive Construction

We describe a method for constructing a t out of ℓ^d threshold scheme whenever ℓ is a prime power such that

$$\ell \geq \binom{t}{2}(d-1) \tag{4}$$

by using a t out of ℓ threshold scheme. The t out of ℓ^d scheme is multiplicative provided that the t out of ℓ scheme is.

Let $(\mathcal{D}, \mathcal{R})$ be a t out of ℓ threshold scheme, where ℓ is a prime power. Let S be the set of shares of the scheme $(\mathcal{D}, \mathcal{R})$ and identify the set P of participants of the scheme with the finite field $\mathbb{F}_\ell$ of order ℓ. Suppose that d is a positive integer such that $\ell \geq \binom{t}{2}(d-1)$ and set $b = \binom{t}{2}(d-1)$. We define a t out of ℓ^d threshold scheme $(\mathcal{D}', \mathcal{R}')$ as follows.

The shares of our new scheme will be taken from the set $S' = S^{b+1}$, the set of all $(b+1)$-tuples of shares from $(\mathcal{D}, \mathcal{R})$. We identify the set P' of participants in our new scheme with the set of polynomials of degree less than d with coefficients in $\mathbb{F}_\ell$. If $f(X) = \sum_{i=0}^{d-1} a_i X^i \in P'$, then define $f(\infty) = a_{d-1}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_b$ be distinct elements of $\mathbb{F}_\ell$ and let $\alpha_0 = \infty$.

We define the distribution algorithm $\mathcal{D}'$ as follows. On being given $k \in K$, algorithm $\mathcal{D}'$ executes algorithm $\mathcal{D}$ a total of $b+1$ times, to produce elements $c^0, c^1, c^2, \ldots, c^b \in S^\ell$. The random input used by $\mathcal{D}$ in each execution should be independent of the random inputs used by previous executions. For each $j \in \{0, \ldots, b\}$, we may write $c^j = (c^j_\alpha)_{\alpha \in \mathbb{F}_\ell}$ for some elements $c^j_\alpha \in S$. The algorithm then distributes the share $c'_f \in S'$ to $f \in P'$ where c'_f is defined by

$$c'_f = (c^0_{f(\infty)}, c^1_{f(\alpha_1)}, c^2_{f(\alpha_2)}, \ldots, c^b_{f(\alpha_b)}).$$

We define the reconstruction algorithm $\mathcal{R}'$ as follows. Let $f_1, f_2, \ldots, f_t$ be distinct participants. The algorithm $\mathcal{R}'$ must recompute the key $k \in K$ given the shares $c'_{f_1}, c'_{f_2}, \ldots, c'_{f_t}$. The algorithm $\mathcal{R}'$ begins by trying to find an integer $i \in \{0, 1, \ldots, b\}$ such that the elements $f_1(\alpha_i), f_2(\alpha_i), \ldots, f_t(\alpha_i)$ are distinct. Such an integer i always exists, by the following argument. Consider the polynomial h defined by

$$h = \prod_{1 \leq u < v \leq t} (f_u - f_v).$$

Then h is a nonzero polynomial of degree at most b. We consider two cases separately.

Firstly, suppose that $\deg h \leq b - 1$. Since h can have at most $\deg h$ roots, there exists an integer $i \in \{1, 2, \ldots, b\}$ such that $h(\alpha_i) \neq 0$. But for any $\alpha \in \mathbb{F}_\ell$, $h(\alpha) = 0$ if and only if $f_u(\alpha) = f_v(\alpha)$ for some distinct $u, v \in \{1, 2, \ldots, t\}$. So the values $f_1(\alpha_i), f_2(\alpha_i), \ldots, f_t(\alpha_i)$ are distinct, as required.

We now consider the case when $\deg h = b$. This condition implies that $\deg(f_u - f_v) = d - 1$ for all u and v such that $1 \leq u < v \leq t$. But $\deg(f_u - f_v) = d - 1$ if and only if $f_u(\infty) \neq f_v(\infty)$. So the elements $f_1(\infty), f_2(\infty), \ldots, f_t(\infty)$ are distinct and we may take $i = 0$.

The algorithm $\mathcal{R}'$ now extracts the ith component from each of the shares $c'_{f_1}, \ldots, c'_{f_t}$ to obtain the set $c^i_{f_1(\alpha_i)}, \ldots, c^i_{f_t(\alpha_i)}$. Now $f_1(\alpha_i), f_2(\alpha_i), \ldots, f_t(\alpha_i)$ are distinct elements of P, so the algorithm $\mathcal{R}'$ possesses t distinct components of the element $c^i \in S^l$ and can use algorithm $\mathcal{R}$ to reconstruct the key $k \in K$.

Theorem 4. *The scheme $(\mathcal{D}', \mathcal{R}')$ is a perfect t out of ℓ^d threshold scheme, provided that $(\mathcal{D}, \mathcal{R})$ is a perfect t out of ℓ threshold scheme. The scheme $(\mathcal{D}', \mathcal{R}')$ is also multiplicative or homomorphic, provided that this is also true of the scheme $(\mathcal{D}, \mathcal{R})$.*

The argument above shows that algorithm $\mathcal{R}'$ reconstructs the key from t distinct shares, so any t participants can recover the key. Furthermore, any $t-1$ participants possess at most $t-1$ components of each of the elements $c^0, c^1, c^2, \ldots, c^b$, so are unable to deduce any information about the key k. It is also clear that the scheme $(\mathcal{D}', \mathcal{R}')$ is multiplicative if $(\mathcal{D}, \mathcal{R})$ is, for in this case the algorithm $\mathcal{R}'$ uses the multiplicative algorithm $\mathcal{R}$ in its final step. A similar remark holds for the homomorphic property.

4.1 Geometric interpretation

For the reader familiar with normal rational curves the following provides a geometrical description of our construction. (The construction above was originally found by using this geometrical approach and so we include this interpretation in the hope that it might prove a fruitful perspective in future. However, readers unfamiliar with finite geometry may skip this subsection without prejudicing their understanding of the remainder of the paper).

We identify the participants of the threshold scheme $(\mathcal{D}', \mathcal{R}')$ with the points of the affine geometry $\mathrm{AG}(d, \ell)$ of dimension d over $\mathbb{F}_\ell$. The coordinates of a point correspond to the coefficients of a polynomial of degree at most $d-1$. A parallel class of this geometry consists of ℓ mutually disjoint hyperplanes. We identify these hyperplanes with the participants of the threshold scheme $(\mathcal{D}, \mathcal{R})$. The $b+1$ executions of $(\mathcal{D}, \mathcal{R})$ correspond to $b+1$ parallel classes. Points in the same hyperplane of a given parallel class are given the share for that hyperplane in the corresponding execution of $(\mathcal{D}, \mathcal{R})$ to obtain their share (a $(b+1)$-tuple) in $(\mathcal{D}', \mathcal{R}')$.

The property required of the $b+1$ parallel classes is that any t points should belong to distinct hyperplanes of some parallel class. If this is the case then these t participants can use their shares of the corresponding execution of $(\mathcal{D}, \mathcal{R})$ to reconstruct the key. There is a correspondence between the parallel classes of $\mathrm{AG}(d, \ell)$ and the hyperplanes of the projective space $\mathrm{PG}(d-1, \ell)$ that is the hyperplane at infinity of $\mathrm{AG}(d, \ell)$. Two points belong to different hyperplanes of a parallel class if and only if the line joining them does not meet $\mathrm{PG}(d-1, \ell)$ in a point of the hyperplane corresponding to the parallel class. Our objective is achieved if the $b+1$ hyperplanes in $\mathrm{PG}(d-1, \ell)$ are chosen on a dual normal rational curve.

Any d hyperplanes of a dual normal rational curve in $\mathrm{PG}(d-1, \ell)$ are independent so that any point of $\mathrm{PG}(d-1, \ell)$ is on at most $d-1$ hyperplanes belonging to the curve. For any t points of $\mathrm{AG}(d, \ell)$ the $\binom{t}{2}$ lines joining two of them meet $\mathrm{PG}(d-1, \ell)$ in points belonging to at most $\binom{t}{2}(d-1)$ hyperplanes of the dual normal rational curve. Thus if $b = \binom{t}{2}(d-1)$ there exists at least one of the $b+1$ parallel classes with the property that the t points belong to distinct hyperplanes of this class. Since a dual normal rational curve consists of $\ell+1$ hyperplanes we obtain the condition $\ell \geq \binom{t}{2}(d-1)$.

5 Share expansion

Let $(\mathcal{D}, \mathcal{R})$ be a threshold scheme with share set S of order q and a key set K of order m. We define the *share expansion* E of the scheme by $E = (\log q)/(\log m)$. (Thus the share expansion of a scheme is just the reciprocal of its information rate). The share expansion of a scheme is a measure of its inefficiency. For all perfect schemes, the share expansion is at least 1 and it is desirable to construct schemes whose expansion is as close to 1 as possible. Define $s_K(t, n)$ to be the smallest share expansion of a t out of n threshold scheme which is multiplicative over K. Theorem 3 gives the following corollary.

Corollary 5. *Let K be a group of order m. For all integers t and n such that $2 \leq t \leq n$,*

$$s_K(t,n) \geq (\log(n-(t-2)))/\log m.$$

Proof: If the set S of shares has order q, then Theorem 1 states that $n-(t-2) \leq q$. So the share expansion $(\log q)/(\log m)$ of any t out of n scheme which is multiplicative over K is at least $(\log(n-(t-2)))/(\log m)$. □

On the other hand, the construction of the previous section shows that

$$s_K(t,\ell^d) \leq (\tbinom{t}{2}(d-1)+1)s_K(t,\ell)$$

whenever ℓ is a prime power such that $\ell \geq \binom{t}{2}(d-1)$. By using this construction repeatedly, one can show that we may realise a scheme with a share expansion of $O((\log n)^{1+\epsilon})$ as $n \to \infty$ for fixed t and for any $\epsilon > 0$. Comparing this expansion with the bound in the corollary above, we see that this scheme seems to be good when n is large compared with t.

5.1 An Explicit Construction

Analysing the behaviour of our recursive construction when we allow t to vary as well as n is a delicate matter. In general, when the recursive construction is being used several times in order to achieve a scheme with desired parameters t and n, it is better to use the recursive construction a small number of times with values for d as large as possible. In this subsection, we use our recursive construction to produce an explicit t out of n scheme for any values of t and n in the case when K is abelian. Although the explicit scheme will not use our recursive construction in an optimal way, the resulting bound on the achievable share expansion for a multiplicative t out of n scheme will be useful in the next section.

Let t and n be arbitrary integers such that $2 < t \leq n$ and let K be an abelian group. We construct a t out of n threshold scheme as follows. We choose a positive constant a. Let ℓ be the first prime power such that $\ell \geq \binom{t}{2}^{1+a}$. We produce a multiplicative t out of ℓ scheme by using a construction of Desmedt and Frankel [7]. This scheme has a share expansion of less than 2ℓ. We then apply our recursive construction with $d = \lceil \ell/\binom{t}{2} \rceil$ a total of m times where $m = \lfloor \log_d \log_\ell n \rfloor + 1$. Note that we can do this since $\ell \geq \binom{t}{2}(d-1)$. At the end of this process, we have a t out of N scheme where $N = \ell^{d^m} \geq n$. By removing the $N-n$ surplus participants, we have constructed a t out of n scheme which is multiplicative over the abelian group K. One can calculate that the share expansion of this scheme is at most

$$2\ell\left\{\binom{t}{2}d\right\}^m < 16\binom{t}{2}^{2+2a}\left\{\frac{\log n}{(1+a)\log\binom{t}{2}}\right\}^{1+\frac{1}{a}}. \tag{5}$$

When $t = 2$, one may use the same methods to produce a scheme with share expansion at most $4\log n$.

6 Zero Knowledge

In many threshold cryptosystems it is important that the amount of knowledge that participants obtain (individually or jointly in groups) from their shares and any public information is no more than is strictly necessary. The study of zero-knowledge threshold schemes [7] addresses this issue. In this section we analyse our scheme from a computational complexity point of view in order to study its zero-knowledge aspects. For this purpose, we implicitly assume that we are studying a family of schemes indexed by some parameter x taken from a set of finite binary strings — this allows us to talk meaningfully about such notions as polynomial time. For reasons of space, we do not explicitly refer to this parameter (e.g. we use the term 'scheme' for a family of schemes) except when discussing the computational complexity of our algorithms. We assume the computational power of the participants in P is polynomially bounded in $|x|$, the binary length of x, and for a t out of n threshold scheme to be *multiplicative* we require in addition to (1) that a polynomial time (in $|x|$) algorithm exists to compute the operations of the group K and a polynomial time (in $|x|$) algorithm exists that can compute the image of any element of the set of shares S under any one of the family of mappings $\{f_{i,B} : S \to K \mid i \in B\}$. We must also take into account the fact that the distribution algorithm $\mathcal{D}$, given the key, may have to distribute shares to a possibly superpolynomial number of participants, and that in the reconstruction algorithm $\mathcal{R}$ the power of many participants may be combined. For this reason we allow $\mathcal{D}$ (when given k) to run in expected polynomial time in $max\{|x|, n\}$ and $\mathcal{R}$ to run in polynomial time in $max\{|x|, t, |n|\}$.

A t out of n threshold scheme is *perfectly zero-knowledge* if the shares of any $t-1$ or less participants can be simulated perfectly in expected polynomial time bounded by $(t-1)|x|^c$ where c is some constant. Informally, this condition says that $t-1$ participants learn nothing new from their shares and any publicly available information. A t out of n threshold scheme is *perfectly minimal-knowledge* if, given any key $k \in K$, the shares of any $m \geq t$ participants can be simulated perfectly in expected polynomial time bounded by $m|x|^c$, where c is some constant. Informally, this condition says that t or more participants learn no more than is strictly necessary from their shares and any publicly available information. Similar definitions can be formulated for statistical and computational analogues of perfect zero- and minimal-knowledge. For the formal definitions and a more rigourous approach, the reader is referred to [7, 10, 11].

Theorem 6. *Let $(\mathcal{D}, \mathcal{R})$ be a multiplicative t out of ℓ threshold scheme over the group K and let d be polynomially bounded in $|x|$ with $\ell \geq \binom{t}{2}(d-1)$. Then the scheme $(\mathcal{D}', \mathcal{R}')$ constructed in Section 4 is a multiplicative t out of ℓ^d threshold scheme. If, furthermore, t is polynomially bounded in $|x|$ and $(\mathcal{D}, \mathcal{R})$ is perfectly zero-knowledge or minimal-knowledge, then so is $(\mathcal{D}', \mathcal{R}')$. Similar statements can be made for the statistical and computational analogues of perfect zero- and minimal-knowledge.*

Sketch Proof: We use the same notation as in Section 4. First observe that algorithm $\mathcal{R}'$ can certainly find an integer i such that $1 \leq i \leq b$ with the property that all the field elements $f_1(\alpha_i), f_2(\alpha_i), \ldots, f_t(\alpha_i)$ are distinct, since d is polynomially bounded. It follows that $(\mathcal{D}', \mathcal{R}')$ is a threshold scheme.

Next suppose that t is polynomially bounded, that $(\mathcal{D}, \mathcal{R})$ is zero-knowledge and that $f_1, f_2, \ldots, f_{t-1}$ are $t-1$ participants in $(\mathcal{D}', \mathcal{R}')$. The simulator for $(\mathcal{D}', \mathcal{R}')$ runs the simulator for $(\mathcal{D}, \mathcal{R})$ as a black box $b+1$ times, independently. For $i \in \{0, 1, \ldots, b\}$, define $B_i = \{f_1(\alpha_i), f_2(\alpha_i), \ldots, f_{t-1}(\alpha_i)\} \subseteq \mathbb{F}_\ell$, which we regard as a set of participants in $(\mathcal{D}, \mathcal{R})$. For each i, let $\hat{c}^i_{B_i}$ be the vector $(\hat{c}^i_{f_1(\alpha_i)}, \hat{c}^i_{f_2(\alpha_i)}, \ldots, \hat{c}^i_{f_{t-1}(\alpha_i)})$ of simulated shares and let $\hat{c}'_{f_j}$ be defined by $\hat{c}'_{f_j} = (\hat{c}^0_{f_j(\infty)}, \hat{c}^1_{f_j(\alpha_1)}, \ldots, \hat{c}^b_{f_j(\alpha_b)})$, for $1 \leq j \leq t-1$. The components of the shares $\hat{c}'_{f_j}$ are independent and simulate those of the shares c'_{f_j} for the participants $f_1, f_2, \ldots, f_{t-1}$ in $(\mathcal{D}', \mathcal{R}')$, which are also independent. So $\hat{c}'_{f_1}, \ldots, \hat{c}'_{f_{t-1}}$ simulates the shares of $f_1, \ldots, f_{t-1}$. Hence the threshold scheme $(\mathcal{D}', \mathcal{R}')$ is zero-knowledge. The proof for minimal-knowledge is similar and is omitted. □

Corollary 7. *If K is abelian and both t and $\log_2 n$ are polynomially bounded in $|x|$ with $t \geq 2$ then there exists a multiplicative and homomorphic zero- and minimal-knowledge t out of n threshold cryptosystem.*

Proof: The constructions of Subsection 5.1 (with a any positive constant) have share expansion at most $ct^{4+4a}(\log_2 n)^{1+1/a}$, for some constant c. □

If $n = \Theta(2^{|x|})$, but t is polynomially bounded in $|x|$, then the scheme in [7, pp. 673–674] is not zero-knowledge, but Corollary 7 shows that ours is.

7 Discussion

We have presented a recursive construction of threshold schemes that has several useful properties, the property that it preserves the homomorphic and multiplicative nature of the underlying scheme being amongst the most important. The explicit scheme in Subsection 5.1 implies the following.

Corollary 8. *For all constants b such that $0 < b \leq 1/4$, if $t = O(n^{1/4-b})$ then the shares are asymptotically shorter than in the zero-knowledge sharing scheme in [7, pp. 673–674], which has share expansion $\Theta(n)$.*

Proof: If we set $a = 4b$, then the result follows by the proof of Corollary 7. □

It is also obvious that the explicit scheme in Subsection 5.1 is substantially better than the scheme in [7, pp. 673–674] when $t = O((\log_2 n)^b)$ for any constant b — in this case our share expansion is only $O((\log_2 n)^{b'})$ for some constant b'.

When $t > 2$ and n is large compared to t, the recursive construction given in this paper is considerably more efficient than the scheme presented in [4]. In particular, when ϵ is any positive constant, t is constant and $n \to \infty$, the scheme presented here has share expansion of the order of $(\log n)^{1+\epsilon}$ whereas the scheme in [4] has share expansion of at least $c(\log n)^{t-1}$ for some constant c.

Our construction can be combined with existing threshold cryptosystems such as the ones in [3, 4] to make them more efficient (with shorter shares and hence faster computation), whilst maintaining their security.

We conclude by observing that although we were able to prove that our scheme is asymptotically optimal when the order of K and t are constant, the discovery of good bounds on the share expansion of multiplicative or homomorphic zero-knowledge threshold schemes for all parameters K, t and n (and the construction of schemes which meet these bounds) is still an open problem.

References

1. J.C. Benaloh: Secret sharing homomorphisms: Keeping shares of a secret secret. In: A. Odlyzko (ed.): Advances in Cryptology - Crypto '86, Proceedings. Lecture Notes in Computer Science 263. Berlin: Springer 1987, pp. 251–260
2. G.R. Blakley: Safeguarding cryptographic keys. In: Proc. Nat. Computer Conf. AFIPS Conf. Proc., 48, 1979, pp. 313–317
3. A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung: How to share a function securely. In: Proceedings of the twenty-sixth annual ACM Symp. Theory of Computing (STOC), IEEE Press 1994, pp. 522–533. Full paper in preparation (available from authors when completed)
4. Y. Desmedt, G. Di Crescenzo, and M. Burmester: Multiplicative non-abelian sharing schemes and their application to threshold cryptography. In: J. Pieprzyk, R. Safavi-Naini (eds.): Advances in Cryptology - Asiacrypt '94, Proceedings. Lecture Notes in Computer Science 917. Berlin: Springer 1995, pp. 21–32
5. Y. Desmedt and Y. Frankel: Threshold cryptosystems. In: G. Brassard (ed.): Advances in Cryptology - Crypto '89, Proceedings. Lecture Notes in Computer Science 435. Berlin: Springer 1990, pp. 307-315
6. Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In: J. Feigenbaum (ed.): Advances in Cryptology - Crypto '91, Proceedings. Lecture Notes in Computer Science 576. Berlin: Springer 1992, pp 457–469
7. 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)
8. Y. Frankel and Y. Desmedt. Classification of ideal homomorphic threshold schemes over finite Abelian groups. In: R.A. Rueppel (ed.): Advances in Cryptology - Eurocrypt '92, Proceedings. Lecture Notes in Computer Science 658. Berlin: Springer 1993, pp 25–34
9. Y. Frankel, Y. Desmedt and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. In: E.F. Brickell (ed.): Advances in Cryptology - Crypto '92, Proceedings. Lecture Notes in Computer Science 740. Berlin: Springer 1993, pp 549–557
10. Z. Galil, S. Haber, and M. Yung: Minimum-knowledge interactive proofs for decision problems. SIAM J. Comput., 18(4), 711–739 (1989)
11. S. Goldwasser, S. Micali, and C. Rackoff: The knowledge complexity of interactive proof systems. SIAM J. Comput., 18(1), 186–208 (1989)
12. E.D. Karnin, J.W. Greene, and M. Hellman: On secret sharing systems. IEEE Trans. Inform. Theory, 29(1), 35–41 (1983)
13. A.Shamir: How to share a secret. Commun. ACM, 22, 612–613 (1979)
14. R.C. Singleton: Maximal distance q-nary codes. IEEE Trans. Inform. Theory, IT-10, 116–118 (1964)