CLASSIFICATION OF IDEAL HOMOMORPHIC THRESHOLD SCHEMES OVER FINITE ABELIAN GROUPS*

(Extended Abstract)

Yair Frankel Yvo Desmedt

Department of EE & CS
University of Wisconsin — Milwaukee
Milwaukee, WI 53201
U. S. A.

Abstract

Threshold schemes allow any t out of l individuals to recompute a secret (key). General sharing schemes are a generalization. In homomorphic sharing schemes the "product" of shares of the keys gives a share of the product of the keys. We prove that there exist infinitely many Abelian groups over which there does *not* exist an *ideal homomorphic* threshold scheme. Additionally we classify *ideal homomorphic* general sharing schemes. We discuss the potential impact of our result on the construction of general sharing schemes.

1 Introduction

General secret sharing schemes [3, 14, 9] provide a means to distribute *shares* of a secret (key) k so that any subset of individuals (shareholders) specified by an access structure can recompute the secret. Threshold schemes [3, 14] have an access structure where t out of l individuals can recompute the secret. Besides using threshold schemes to recompute a secret, they are used, for example, in fault tolerant computing [13].

*This work has been supported by NSF Grant NCR-9106327.

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 25-34, 1993.

Many threshold schemes such as [5, 11, 12, 14] work over a finite field. However, other structures such as the groups Z_n^*, elliptic curves and Z_n^{+1} (groups of integers modulo n with Jacobi symbol $+1$) are often used in cryptography. Giving secrets and maintaining group operations is therefore useful. Homomorphic threshold schemes over a finite Abelian group have been used in several cryptographic schemes. Indeed homomorphic threshold schemes over a finite Abelian group have been used to set up secret ballot election schemes [1]. Existing threshold authentication (and threshold signature) schemes [6] are also based on them. These have shown the usefulness of homomorphic threshold schemes over a finite Abelian group.

To guarantee that a threshold scheme is secure Stinson and Vanstone [17] speak about perfect threshold schemes. *Perfect* threshold schemes do not reveal anything about the secret k when $t-1$ shares are used. Let $\mathcal{S}$ be the set of all possible shares and $\mathcal{K}$ be the set of possible secrets (keys). A threshold scheme is called *ideal* when it is perfect and when $|\mathcal{S}|$ equals $|\mathcal{K}|$, $|\mathcal{S}|$ is the cardinality of the set $\mathcal{S}$.

Benaloh [1] defined homomorphic threshold schemes as those having the property that when $s_i \in \mathcal{S}$ is i's share of $k \in \mathcal{K}$ and $s_i' \in \mathcal{S}$ is i's share of $k' \in \mathcal{K}$, then $s_i \cdot s_i'$ is i's share of $k * k'$ and for such threshold schemes t shareholders can reconstruct $k * k'$ using their $s_i \cdot s_i'$.

To keep storage requirements restricted it is important to make the size of the shares in a sharing scheme as small as possible. It is well known that in perfect general sharing schemes the size of the share must be at least as large as the size of the key. Therefore ideal sharing schemes have been studied extensively. Unfortunately, ideal sharing schemes cannot be made for all access structures [2]. The maximum l for an ideal threshold scheme is dependent on t and $|\mathcal{K}|$ [11]. Other results on ideal sharing schemes encompasses a classification for ideal sharing schemes [4] and the fact that without having public information no threshold scheme can be made ideal [17]. Observe that Shamir's threshold scheme [14] and others [5, 11, 12] are homomorphic and schemes satisfying this property are becoming important.

In this paper we study *ideal homomorphic* threshold and general sharing schemes where the key space is a finite Abelian group. On the first look it seems that this study would only result in a combination of earlier obtained results. Unexpectedly we are able to exemplify a set of secrets (keys) $\mathcal{K}$ that when it

forms a group and one insists that the threshold scheme is homomorphic then there does not exists an ideal threshold scheme (see Section 4). Moreover we can give infinitely many examples of this. In threshold schemes the maximum l is dependent on t and the cardinality of $\mathcal{K}$ [11]. However, in *homomorphic* threshold scheme the maximum l is a dependent on t and the algebraic structure of $\mathcal{K}$.

The results in this paper will make protocols which use homomorphic threshold schemes over a finite Abelian group (*e.g.*, see [1, 6]) more practical. For instance, being able to use an ideal scheme has a direct implication on the practicality of protocol using the homomorphic threshold scheme.

In Section 2 we overview the necessary definitions. In Section 3 we prove that $\mathcal{S}(\cdot)$ is isomorphic to $\mathcal{K}(*)$ in any ideal homomorphic general sharing scheme over a group $\mathcal{K}(*)$. Using this property a classification of ideal homomorphic threshold schemes over a finite Abelian group is made in Section 4. A link between a geometric general sharing scheme [16] and homomorphic general sharing schemes is established in Section 5.

2 Background and notation

We now introduce formal definitions and notation used in this paper. When $\mathcal{A}$ is a set, $|\mathcal{A}|$ will denote the cardinality of the set. We now overview the definition of threshold schemes [3, 14] and homomorphic threshold schemes [1].

Definition 1 A *threshold scheme* contains two algorithms, one which creates shares of a secret key $k \in \mathcal{K}$ for l individuals so that any t individuals (t is fixed and $t \leq l$) can regenerate the secret using the second algorithm, yet less than t individuals cannot using any method. Let $\mathcal{A} = \{1, \ldots, l\}$ and $\mathcal{S}$ be the set of possible shares[1]. The distributor generates the tuple $S_{\mathcal{A}} = (s_1, \ldots, s_l)$ where $s_i \in \mathcal{S}$ and the public directory $\mathcal{X}_{\mathcal{A}} = \{x_i \mid i \in \mathcal{A}\}$.

More formally, a t-out-of-l threshold scheme satisfies:

1. $\forall \mathcal{B} \subset \mathcal{A}$ where $|\mathcal{B}| = t - 1$ holds: if $\mathsf{H}(k) \neq 0$ then $0 < \mathsf{H}(k \mid S_{\mathcal{B}}, \mathcal{X}_{\mathcal{A}}) \leq \mathsf{H}(k)$ for H the entropy function [8] and if $S_{\mathcal{A}} = (s_1, \ldots, s_l)$ then $S_{\mathcal{B}} =$

[1] A more general definition allows the set of shares to be different for each shareholder $i \in \mathcal{A}$ [2, 7]. All our results remain valid for the more general definition. To avoid heavy notation we assume the set of shares are identical.

$(s_{i_1}, \ldots, s_{i_{|\mathcal{B}|}})$ where $\mathcal{B} = \{i_1, \ldots, i_{|\mathcal{B}|}\}$.

2. $\forall \mathcal{B} \subset \mathcal{A}$ where $|\mathcal{B}| = t$, there exists a function $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}}$ such that $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}}(S_\mathcal{B}) = k$.

Schemes in which for any $\mathcal{B} \subset \mathcal{A}$ with $|\mathcal{B}| = t-1$ holds that $\mathsf{H}(k|S_\mathcal{B}, \mathcal{X}_\mathcal{A}) = H(k)$ are called *perfect*. When a sharing scheme is perfect and $|\mathcal{K}|/|\mathcal{S}| = 1$, it is called an *ideal* sharing scheme.

Definition 2 Let "$\cdot$" be a binary operation over $\mathcal{S}$ (so $\mathcal{S}$ is closed under "$\cdot$") and "$*$" be a binary operation over $\mathcal{K}$. If $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}}$ is a homomorphism from $\mathcal{S}^t(\cdot)$ to $\mathcal{K}(*)$ for each $\mathcal{B} \subset \mathcal{A}$ with $|\mathcal{B}| = t$, then the threshold scheme is called a homomorphic threshold scheme[2].

The above definitions can be easily modified to general sharing schemes allowing for any access structure.

3 Structure of shares

We first analyze the structure of $\mathcal{S}(\cdot)$ in an ideal general sharing scheme where $\mathcal{K}(*)$ is a group. We note that the definition of homomorphic threshold scheme is very general and does *not* even state whether $\mathcal{S}(\cdot)$ has any special properties such as being a group. The same statement can be made about homomorphic general sharing schemes.

Theorem 1 *If the key space $\mathcal{K}(*)$ of an ideal homomorphic t-out-of-l threshold scheme is a finite group, then the share space $\mathcal{S}(\cdot)$ is isomorphic to $\mathcal{K}(*)$.*

Proof. In any ideal threshold scheme when $s_{i_1}, \ldots, s_{i_t} \in \mathcal{S}$ then $S_\mathcal{B} = (s_{i_1}, \ldots, s_{i_t})$ is a valid tuple of shares. Clearly, if $S'_\mathcal{B} = (s'_{i_1}, \ldots, s'_{i_t})$ is a valid tuple of shares then $S''_\mathcal{B} = (s_{i_1}, s'_{i_2}, \ldots, s'_{i_t})$ is also for the scheme to perfect. Repeating this process for $i_2, \ldots, i_t$ proves that *any* combination of t elements of $\mathcal{S}$ can be valid as t shares.

[2] If the threshold scheme is not perfect then the above definition must be slightly adapted.

Let $s \in \mathcal{S}$ and $\eta_{\mathcal{B},\mathcal{X}_A}(s,\ldots,s) = k \in \mathcal{K}$. For the threshold scheme to be perfect one needs that $\eta_{\mathcal{B},\mathcal{X}_A}(s,\ldots,s,\mathcal{S}) = \mathcal{K}$. First $s \cdot \mathcal{S} = \mathcal{S}$ since $\eta_{\mathcal{B},\mathcal{X}_A}(s,\ldots,s) * \eta_{\mathcal{B},\mathcal{X}_A}(s,\ldots,s,\mathcal{S}) = \eta_{\mathcal{B},\mathcal{X}_A}(s\cdot s,\ldots,s\cdot s, s\cdot\mathcal{S}) = k * \mathcal{K} = \mathcal{K}$. Since $s \cdot \mathcal{S} = \mathcal{S}$ and $\mathcal{S}$ is finite, there exist an element e_x for every $x \in \mathcal{S}$ such that $x \cdot e_x = x$. From this we note that $\eta_{\mathcal{B},\mathcal{X}_A}(e_x,\ldots,e_x) = 1 \in \mathcal{K}$ since $\eta_{\mathcal{B},\mathcal{X}_A}(x,\ldots,x) = \eta_{\mathcal{B},\mathcal{X}_A}(x\cdot e_x,\ldots,x\cdot e_x)$. Now, $\eta_{\mathcal{B},\mathcal{X}_A}(x,\ldots,x,y) = \eta_{\mathcal{B},\mathcal{X}_A}(x\cdot e_x,\ldots,x\cdot e_x, y\cdot e_x) = \eta_{\mathcal{B},\mathcal{X}_A}(x,\ldots,x,y\cdot e_x)$. Since $|\mathcal{S}| = |\mathcal{K}|$ and the scheme is perfect, $y \cdot e_x = y$. Thus e_x is a right identity element. Similarly we can prove a left identity element. So there exists an identity element $1 \in \mathcal{S}$. Let $\psi_{i,\mathcal{B},\mathcal{X}_A}(x) = \eta_{\mathcal{B},\mathcal{X}_A}(1,\ldots,1,x)$ where x is the i^{th} share. The mapping $\psi_{i,\mathcal{B},\mathcal{X}_A}$ is a homomorphism from $\mathcal{S}$ to $\mathcal{K}$. Observe that $\psi_{i,\mathcal{B},\mathcal{X}_A}$ is onto because the scheme is perfect. The fact that $|\mathcal{S}| = |\mathcal{K}|$ implies $\psi_{i,\mathcal{B},\mathcal{X}_A}$ is bijective. Because $\psi_{i,\mathcal{B},\mathcal{X}_A}(x\cdot(y\cdot z)) = \psi_{i,\mathcal{B},\mathcal{X}_A}((x\cdot y)\cdot z)$ and because $\psi_{i,\mathcal{B},\mathcal{X}_A}$ is bijective, we must have that $\mathcal{S}(\cdot)$ is associative and therefore $\mathcal{S}(\cdot)$ is a group. □

A *monotone access structure* satisfies the property that when a set of shareholders $\mathcal{B}$ can recompute a secret then any superset $\mathcal{B}' \supset \mathcal{B}$ can also recompute the secret. Careful examination of the above proof indicates the following.

Corollary 1 *If the key space $\mathcal{K}(*)$ of an ideal homomorphic monotone general sharing scheme is a finite group, then the share space $\mathcal{S}(\cdot)$ is isomorphic to $\mathcal{K}(*)$.*

4 Classification

Due to [11], in any threshold scheme there is the following bound on l: $l_{\text{MAX}} \leq |\mathcal{K}| + t - 2$. Theorem 1 can be used to find a bound for l_{MAX} for ideal homomorphic threshold schemes.

Theorem 2 *Let $\mathcal{K}(*)$ be a finite Abelian group. There is an ideal homomorphic t-out-of-l threshold scheme with key space $\mathcal{K}(*)$ if and only if for each Sylow subgroup $G(*)$ of $\mathcal{K}(*)$ there is an ideal homomorphic t-out-of-l threshold scheme with key space $G(*)$.*

Proof. It is well known that each Abelian group $\mathcal{K}$ is isomorphic to $G_1 \times G_2 \times \cdots \times G_c$ where the G_i are all the different Sylow subgroups[3] in $\mathcal{K}$. Let $\psi_{i,\mathcal{B},\mathcal{X}_\mathcal{A}}$ be as in the proof of Theorem 1. Note that to $k \in \mathcal{K}$ corresponds an (k', k'') where $k' \in G_1$ and $k'' \in G_2 \times \cdots \times G_c$, similarly due to Theorem 1, $s_i \in \mathcal{S}$ corresponds to (s_i', s_i'') $(1 \leq i \leq l)$. So, $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}} : \mathcal{S}^t \rightarrow \mathcal{K}$ corresponds to $\eta'_{\mathcal{B},\mathcal{X}_\mathcal{A}} : (G_1 \times (G_2 \times \cdots \times G_c))^t \rightarrow G_1 \times (G_2 \times \cdots \times G_c)$ and similarly we define $\psi'_{i,\mathcal{B},\mathcal{X}_\mathcal{A}}$. Because $\psi'_{i,\mathcal{B},\mathcal{X}_\mathcal{A}}$ gives a group isomorphism and because the G_j are Sylow subgroups we have $\psi'_{i_t,\mathcal{B},\mathcal{X}_\mathcal{A}}((s'_{i_t}, 1)) = (k'_t, 1)$. Observe that $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}}(s_{i_1}, \ldots, s_{i_t}) = \prod_{j \in \mathcal{B}} \psi_{j,\mathcal{B},\mathcal{X}_\mathcal{A}}(s_j)$. One can now prove that $\eta'_{\mathcal{B},\mathcal{X}_\mathcal{A}}((s'_{i_1}, 1), \ldots, (s'_{i_t}, 1)) = (k', 1)$ for some k'. Similarly $\eta'_{\mathcal{B},\mathcal{X}_\mathcal{A}}((1, s''_{i_1}), \ldots, (1, s''_{i_t})) = (1, k'')$. When $\eta'_{\mathcal{B},\mathcal{X}_\mathcal{A}}((s'_{i_1}, s''_{i_1}), \ldots, (s'_{i_t}, s''_{i_t})) = (a, b)$ then $a = k' \in G_1$ and $b = k'' \in G_2 \times \cdots \times G_c$, because $\eta'_{\mathcal{B},\mathcal{X}_\mathcal{A}}$ is a function. So this induces an ideal homomorphic t-out-of-l threshold scheme with key space $\mathcal{K}' \cong G_1$. A similar argument is made for each G_i $(2 \leq i \leq c)$.

Moreover, if there exists an ideal threshold scheme for each G_i $(1 \leq i \leq c)$ then there exists one for the key space $\mathcal{K} \cong G_1 \times G_2 \times \cdots \times G_c$. □

Corollary 2 *There exists an infinite number of Abelian groups $\mathcal{K}$ for which there does* not *exist an ideal homomorphic threshold scheme when $l > 2$, even when $l < |\mathcal{K}|$ and $t = 2$.*

Proof. Let $\mathcal{K}(*) \cong Z_2 \times Z_{q_2^{\omega_2}} \times \cdots \times Z_{q_c^{\omega_c}}(+)$ where $q_i \neq 2$ are primes and $q_i \neq q_j$ for $i \neq j$. Due to [11] the maximum l in a threshold scheme over $\mathcal{K}$ is $l_{\mathsf{MAX}} \leq |\mathcal{K}| + t - 2$. Due to Theorem 2, when $t = 2$ in an ideal homomorphic threshold scheme then $l \leq 2$ for our $\mathcal{K}$. □

Careful examination of the proof for Theorem 2 indicates that the theorem can be generalized to any monotone access structure.

Corollary 3 *Let $\mathcal{K}(*)$ be a finite Abelian group. Then there is an ideal homomorphic monotone general sharing scheme with key space $\mathcal{K}$ if and only if for each Sylow subgroup G of $\mathcal{K}$ there is an ideal homomorphic monotone general sharing scheme for key space G.*

[3] A Sylow p-subgroup of $\mathcal{K}$, p prime, is a subgroup whose order is the largest power of p which divides the order of $\mathcal{K}$ [10].

Corollary 4 *Let $\mathcal{K}(*)$ be a finite Abelian group. If there is an ideal homomorphic t-out-of-l threshold scheme with key space $\mathcal{K}$, then for each characteristic subgroup[4] G of $\mathcal{K}$ there is an ideal homomorphic t-out-of-l threshold scheme with key space G.*

Proof. Restrict the shares to G and use the fact that $\eta_{\mathcal{B},\mathcal{X}_\mathcal{A}}(s_{i_1},\ldots,s_{i_{|\mathcal{B}|}}) = \prod_{j\in\mathcal{B}} \psi_{j,\mathcal{B},\mathcal{X}_\mathcal{A}}(s_j)$ (because ideal threshold schemes are erasure codes [11]). □

Corollary 4 implies that there is *no* ideal homomorphic 2-out-of-3 threshold scheme when the key space is $Z_4(+)$, but there is one when the key space is $Z_2 \times Z_2(+)$. So insisting on having a homomorphic scheme does make it not ideal.

5 A general homomorphic sharing scheme

In this section we establish a link between a geometric general sharing scheme [16] and the homomorphic property. Using finite projective geometry, a method to create sharing schemes for any monotone access structure has been developed [16]. Let us briefly review their scheme [16]. In their sharing scheme a public hyperplane V_d intersects with a secret hyperplane V_i at a point which is the secret. Points are given to each shareholder in such a way that they meet the following two conditions. First, when a set of shareholders allowed by the access structure work together, they will be able to generate the secret hyperplane V_i. When a set of shareholders not allowed by the access structure work together, they do not obtain any information about the secret point.

Lemma 1 *Let $\mathcal{K}(*)$ be* any *finite Abelian group. The general sharing scheme in [16] induces a perfect homomorphic sharing scheme with key space $\mathcal{K}$.*

Proof. We modify the scheme developed in [16]. When in [16] the distributor gives a point p_i to shareholders $\{j_1,\ldots,j_{h_i}\}$, the distributor here will give $s_i \in \mathcal{K}$ to shareholders $\{j_1,\ldots,j_{h_i}\}$. Let the total number of such points p_i in [16] be m, then $\prod_{1\le i\le m} s_i = k$ where k is the secret and $s_1,\cdots,s_{m-1}$ have been chosen

[4]Characteristic subgroups are those subgroups that are mapped into themselves by all automorphisms.

as independently random elements in $\mathcal{K}$. The fact that the sharing scheme is perfect follows from the one-time-pad [15]. □

6 Conclusion

Earlier results have demonstrated that homomorphic threshold schemes are useful [1, 6]. A homomorphic *ideal* general sharing scheme where the secret domain is a group has a share domain which is isomorphic to the secret domain. A bound on the maximum l can be made for homomorphic threshold schemes over an Abelian group. This result shows that it is better not to use homomorphic threshold (or sharing) schemes when the homomorphic property is not needed.

Acknowledgment

We thank Mike Burmester (University of London) for discussions about this paper.

REFERENCES

[1] J. C. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pp. 251–260. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[2] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology, Proc. of Crypto '88 (Lecture Notes in Computer Science 403)*, pp. 27–35. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 11–15.

[3] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. Nat. Computer Conf. AFIPS Conf. Proc.*, pp. 313–317, 1979. vol.48.

[4] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2), pp. 123–134, 1991.

[5] G. I. Davida, R. DeMillo, and R. Lipton. Protecting shared cryptographic keys. In *Proceedings of the 1980 Symposium on Security and Privacy*, pp. 100–102. IEEE Computer Society, April 1980. IEEE Catalog No. 80 CH1522-2.

[6] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology, Proc. of Crypto '91 (Lecture Notes in Computer Science 576)*, pp. 457–469. Springer-Verlag, 1992. Santa Barbara, California, U.S.A., August 11-15.

[7] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic general sharing schemes for some key spaces. To be presented at Crypto '92, to appear in: Advances in Cryptology. Proc. of Crypto '92 (Lecture Notes in Computer Science), Springer-Verlag, 1992.

[8] R. G. Gallager. *Information Theory and Reliable Communications*. John Wiley and Sons, New York, 1968.

[9] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structures (in English). In *Proc. IEEE Global Telecommunications Conf., Globecom'87*, pp. 99–102, Washington, DC., 1987. IEEE Communications Soc. Press. Also in "Trans. IEICE Japan" Vol. J71-A, No. 8, 1988 (in Japanese).

[10] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, New York, 2nd edition, 1985.

[11] E. D. Karnin, J. W. Greene, and M. Hellman. On secret sharing systems. *IEEE Tr. Inform. Theory*, 29(1), pp. 35–41, January 1983.

[12] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Comm. ACM*, 24(9), pp. 583–584, September 1981.

[13] M. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM*, 36(2), pp. 335–348, April 1989.

[14] A. Shamir. How to share a secret. *Commun. ACM*, 22, pp. 612–613, November 1979.

[15] C. E. Shannon. Communication theory of secrecy systems. *Bell System Techn. Jour.*, 28, pp. 656–715, October 1949.

[16] G. J. Simmons, W. Jackson, and K. Martin. The geometry of shared secret schemes. *Bulletin of the Institute of Combinatorics and its Applications*, 1, pp. 71–88, 1991.

[17] D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics*, 1(2), pp. 230–236, 1988.