Redistribution of mechanical secret shares

Yvo Desmedt[1], Rei Safavi-Naini[2], and Huaxiong Wang[3]

[1] Department of Computer Science, Florida State University, USA
Dept. of Mathematics, Royal Holloway, University of London, UK
email: desmedt@cs.fsu.edu
[2] School of IT and CS, University of Wollongong, Australia
email: rei@uow.edu.au
[3] Department of Computing, Macquarie University, Australia
email: hwang@comp.mq.edu.au

Abstract. Vaults are used extensively in the financial world. Some of these vaults use a secret sharing scheme in which the shares are mechanical keys. Reorganization of a corporation sometimes requires to change the access structure of those authorized to open the vault. Although changing access structure is studied in the context of secret sharing schemes, the techniques are inadequate in the case that the shares are mechanical keys. For example, some schemes require that an existing secret sharing scheme (vault in our case) be fitted with new sets of shares (mechanical keys in our case). That is a number of share sets (key sets) be produced that open the same vault. Making such a modification to a mechanical vault is very expensive, if at all possible. We study how one can redistribute secret shares only by using copying of these shares, which is the only operation one can allow to deal with mechanical shares without changing the mechanical vault mechanism.
Keywords: secret sharing, combinatorics, cover-free family

1 Introduction

The downsizing of dot-com's has made several investors question the importance of e-banking, e-cash, etc. Moreover, recent terrorist attacks have demonstrated the need for protection of our mechanical assets. In the light of these events we question whether the recent research in cryptography has overemphasized the electronic aspect of security.

Although our financial world has become heavily computerized, large amounts of old-fashioned cash are still around and need protection. Moreover several financial institutes (such as banks) offer vaults to clients to store valuables such as jewelry, stocks and bonds. Cyber crime often receives a lot of press, but financial institutes are still vulnerable to old-fashioned theft. An example of a \$13.7 million theft is the case of Charlotte [11] in 1998. What is special about this theft is that it was done by a *single* insider who had access to the vault.

To avoid such thefts financial institutes usually require that two keys given to two different people are needed to open a vault. From a cryptographic aspect the security of a single vault is a 2-out-of-2 secret sharing scheme [4, 19]. Note

that often individual safes are in a vault room behind a locked main armored door where two keys given to two different people are needed to open this main armored door. *Such measures clearly generate more complex access structures.* Although access structures of mechanical secret sharing schemes are equivalent to data based ones, there are major differences with secret sharing schemes in the usual cryptographic setting. When shares are data one may have, for example, homomorphic secret sharing schemes [2]. Such algebraic operations on secret shares have been useful for a broad number of applications, such as threshold cryptography. Therefore, one may conclude that cryptography cannot play a major role on addressing mechanical security, e.g. mechanical secrets' shares. However, in this paper we will demonstrate that techniques used extensively in cryptography can sometimes be used for mechanical security.

We believe that applying cryptography to security problems outside the internet is not only an interesting academic exercise, but recent terrorist attacks have clearly demonstrated the need for protecting against the threats outside the cyber world and the need to examine the usefulness of our techniques in a broader context. In this paper we focus on mechanical secret sharing which is commonly used in financial institutions.

We consider the problem of how a financial institute can reorganize the access structure to a mechanical secret sharing scheme. To be precise, given shares of an ℓ-out-of-v mechanical secret sharing scheme, how can we reorganize it into a t-out-of-n one. One approach is to redesign the safe mechanism, which is quite expensive. Therefore, we study how to achieve this goal without such a redesign. Here, we can only work with the shares that this time are keys without algebraic properties! The only "operation" we allow on mechanical shares is that these are copied. Note that prior work on redistribution of secret sharing, such as [9, 1, 13, 10, 17] is not applicable to mechanical share redistribution.

In this paper we will first discuss in Section 3 our approach. We will see that our problem is equivalent to the construction of what we call a strong cover-free family, a special type of cover-free families that is a concept introduced by Erdös-Frankl-Furedi [12]. We will see that several concepts that have been used extensively in modern cryptography, such as universal hash-functions, can be used to construct strong cover-free families (see Section 4). To evaluate how good our constructions are, in Section 5 we discuss bounds on strong cover-free families. We conclude in Section 6.

2 Preliminaries

This section can be skipped by the reader familiar with secret sharing.

Definition 1. *Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a group of n participants and let $\mathcal{K}$ denote the set of secrets. We assume P_i's share is selected from the set $\mathcal{S}_i$. A (t, n)-threshold scheme (or also called a t-out-of-n secret sharing scheme) is a pair of algorithms: the* dealer algorithm $\mathcal{D}$ *and the* combiner algorithm $\mathcal{C}$*. For a secret from $\mathcal{K}$ and a randomly chosen element of $\mathcal{R}$, the dealer algorithm applies*

the mapping

$$\mathcal{D} : \mathcal{K} \times \mathcal{R} \to \mathcal{S}_1 \times \ldots \times \mathcal{S}_n$$

to assign shares to participants in $\mathcal{P}$. The combiner algorithm takes the shares of a subset $B \subseteq \mathcal{P}$ of participants and if the set $B \subseteq \mathcal{P}$ and $|B| \geq t$ it returns the secret.

$$\mathcal{C} : \bigcup_{P_i \in A} \{\mathcal{S}_i\} \to \mathcal{K}.$$

$\mathcal{K}, \mathcal{S}_i$ corresponds random variables $\mathbf{K}$ and $\mathbf{S}_i$. A secret sharing scheme is perfect if for all $(i_1, i_2, \ldots, i_{t-1})$ where $1 \leq i_j \leq n$:

$$\text{prob}(\mathbf{K} = k \mid \mathbf{S}_{i_1} = s_{i_1}, \mathbf{S}_{i_2} = s_{i_2}, \ldots \mathbf{S}_{i_{t-1}} = s_{i_{t-1}}) = \text{prob}(\mathbf{K} = k).$$

The most known (t, n) secret sharing scheme using algebra is Shamir's scheme [19]. Since we focus on mechanical secret sharing, we do not survey it.
One measure for efficiency of the secret sharing scheme can be through the notion of share expansion.

Definition 2. *Under the above notation, we define the share expansion of a secret share scheme as*

$$\rho = \max_{1 \leq i \leq n} \frac{\log |\mathcal{S}_i|}{|\mathcal{K}|}.$$

Throughout this paper, all logarithms are to the base 2, unless otherwise indicated.

3 Our approach

We first give an informal description of how to reorganize a mechanical secret sharing scheme. We then discuss this formally.
We assume we have a mechanical ℓ-out-of-v perfect secret sharing scheme $(\mathcal{D}_0, \mathcal{C}_0)$ and we want to reorganize it into a perfect t-out-of-n $(\mathcal{D}, \mathcal{C})$ one. Assume that shareholder P_i' $(1 \leq i \leq v)$ in $(\mathcal{D}_0, \mathcal{C}_0)$ has a mechanical share a_i in the ℓ-out-of-v secret sharing scheme. We now need to give a share s_j to shareholder P_j $(1 \leq j \leq n)$ in $(\mathcal{D}, \mathcal{C})$. Since the only allowable operation is to make copies of a_i, s_j can only be a collection of mechanical shares. So s_j can be described using a set B_j of indexes of shares a_i of which P_j received a copy. To guarantee that the resulting $(\mathcal{D}, \mathcal{C})$ sharing scheme is a t-out-of-n one, we need

for the combiner algorithm that if t shareholders P_j put their shares together, they jointly have ℓ mechanical shares of the old $(\mathcal{D}_0, \mathcal{C}_0)$ scheme.

to guarantee perfectness that if $t-1$ shareholders P_j put their shares together, they jointly have at the most $\ell - 1$ shares of the old $(\mathcal{D}_0, \mathcal{C}_0)$ scheme.

We now describe this formally. We first introduce the new concept of a strong cover-free family, a special case of a cover-free family [12] (as proven in Theorem 12).

Definition 3. *A* strong cover-free family *is a set system* $(X, \mathcal{B})$ *such that the following properties are satisfied:*

1. $X = \{x_1, \ldots, x_v\}$ *called* points*;*
2. $\mathcal{B} = \{B_1, \ldots, B_n\}$ *is a set of* n *subsets of* X*, called* blocks *(*$B_i \subseteq X$*);*
3. *For any* Δ *and any* $\Lambda \subseteq \{1, \ldots, n\}$ *with* $|\Delta| = t$ *and* $|\Lambda| = t - 1$*:*

$$|\cup_{i \in \Delta} B_i| > |\cup_{j \in \Lambda} B_j|. \tag{1}$$

We will call $(X, \mathcal{B})$ *a* (v, n, t)*-strong cover-free family (or* $(v, n, t) - SCFF$ *for short).*

The idea behind our new construction is to combine an existing threshold scheme and a SCFF to construct a new threshold scheme. The construction works as follows.

1. Assume $(X, \mathcal{B})$ is a (v, n, t)-SCFF. Let ℓ be a integer such that $\min_{\Delta} |\cup_{i \in \Delta} B_i| \geq \ell > \max_{\Lambda} |\cup_{i \in \Lambda} B_i|$ where Δ runs through all t-subsets of $\{1, \ldots, n\}$ and Λ runs through all $(t-1)$- subsets of $\{1, \ldots, n\}$. Since $(X, \mathcal{B})$ is a SCFF, such ℓ exists.
2. Assume there is a (ℓ, v) threshold scheme $(\mathcal{D}_0, \mathcal{C}_0)$. For a secret $k \in \mathcal{K}$, the v shares of $(\mathcal{D}_0, \mathcal{C}_0)$ are $a_1, \ldots, a_v$.
3. Define a (t, n) threshold scheme for n participants $P_1, \ldots, P_n$ by constructing n shares $\mathbf{s}_1, \ldots, \mathbf{s}_n$ as the ordered (ordered by their index) multiset $\mathbf{s}_i = \{a_j \mid \text{if and only if } x_j \in B_i\}$ and assigning $\mathbf{s}_i$ to the participants P_i for all $1 \leq i \leq n$.

We denote the resulting (t, n) scheme as $(\mathcal{D}, \mathcal{C})$ and prove the following result.

Theorem 1. *If* $(\mathcal{D}_0, \mathcal{C}_0)$ *is perfect, then* $(\mathcal{D}, \mathcal{C})$ *is perfect.*

Proof. Clearly, any t participants, $P_{i_1}, \ldots, P_{i_t}$ say, have $|\mathbf{s}_{i_1} \cup \cdots \cup \mathbf{s}_{i_t}| \geq \ell$ shares from the v share of the (ℓ, v) threshold scheme $(\mathcal{D}_0, \mathcal{C}_0)$. From the choice of ℓ, we know that t participants can reconstruct the secret by applying the combiner algorithm $\mathcal{C}_0$. Next, any $t - 1$ participants have no extra information about k provided $(\mathcal{D}_0, \mathcal{C}_0)$ is perfect. Indeed, assume that $P_{i_1}, \ldots, P_{i_{t-1}}$ want to recover the secret by using their shares $\mathbf{s}_{i_1} \cup \cdots \cup \mathbf{s}_{i_{t-1}} \subseteq \{a_1, \ldots, a_v\}$. Since $|\mathbf{s}_{i_1} \cup \cdots \cup \mathbf{s}_{i_{t-1}}| < \ell$ and the underlying (t, v) scheme $(\mathcal{D}_0, \mathcal{C}_0)$ is perfect, the claim follows.

Note that the share expansion ρ of $(\mathcal{D}, \mathcal{C})$ is determined by the share expansion ρ_0 of $(\mathcal{D}_0, \mathcal{C}_0)$ and the parameters of the (v, n, t)-SCFF $(X, \mathcal{B})$. We have $\rho \leq \max_{1 \leq i \leq n} |B_i| \rho_0$. In particular, if $(\mathcal{D}_0, \mathcal{C}_0)$ is *ideal*, i.e. $\rho_0 = 1$ and $|B_i| = r$ for all $1 \leq i \leq n$, then $\rho = r$.

3.1 An example

It is well known that it is easy to make a $(\ell-1)$-out-of-$(v-1)$ perfect secret sharing scheme from an ℓ-out-of-v one. Indeed, give P_i $(1 \leq i \leq v-1)$ as share $s_i = \{a_i, a_v\}$, where a_i is P_i' share in the ℓ-out-of-v secret sharing scheme. So, this corresponds to a $(v, v-1, \ell-1)$-strong cover-free family.
It is obvious that given a mechanical ℓ-out-of-v perfect secret sharing scheme one cannot redistribute the shares to obtain a t-out-of-n one where $t > \ell$. Indeed, let $\Delta \subseteq \{1, \ldots, n\}$ such that $|\Delta| = t$ and $\Lambda \subseteq \Delta$ such that $|\Lambda| = t-1$. To guarantee perfectness the $t-1$ shareholders in Λ should have at maximum $\ell-1$ shares of the old scheme, so at least $t-\ell$ shareholders in Λ need empty sets B. Let us call Λ' those shareholders in Δ that received an empty set. Then, the shareholders in $\Delta \setminus \Lambda'$ can construct the secret key. However, since $|\Lambda'| \geq t-\ell$ we now have that $|\Delta \setminus \Lambda'| = t - |\Lambda'| \leq \ell < t$ can reconstruct the secret. So, we have a contradiction.
We discuss other such bounds in Section 5. We now discuss constructions.

4 Constructions

The following lemma is essential for most of our later constructions.

Lemma 1. *Let $(X, \mathcal{B})$ be a set system such that*

1. $|B_i| = r$, *for all* $i \in \{1, \ldots n\}$;
2. $|B_i \cap B_j| \leq \mu$, *for all* $i \neq j \in \{1, \ldots, n\}$.

Then $(X, \mathcal{B})$ is a (v, n, t) SCFF provided $\binom{t}{2} < r/\mu$.

Proof. Let Δ and Λ be two subset of $\{1, \ldots, n\}$ such that $|\Delta| = t$ and $|\Lambda| = t-1$. We have $|\cup_{i \in \Delta} B_i| \geq \sum_{i \in \Delta} |B_i| - \sum_{i,j \in \Delta} |B_i \cap B_j| \geq tr - \binom{t}{2}\mu = (t-1)r + (r - \binom{t}{2}\mu) > (t-1)r = \sum_{j \in \Lambda} |B_j| \geq |\cup_{j \in \Lambda} B_j|$.

For a given $(v, n, t) - SCFF$ we know that the new mechanical secret sharing scheme is a t-out-of-n threshold scheme. We call the old scheme a ℓ-out-of-v one. For many of the schemes based on the Lemma 1 one could choose ℓ between

- $(t-1)r + 1$ and
- $tr - \binom{t}{2}\mu$,

as is obvious from the proof of Lemma 1. Since for many of our schemes, it is trivial to compute these values, we leave it to the reader.
Note however, we do not have an efficient algorithm to compute the largest possible ℓ with an $(v, n, t) - SCFF$ (i.e. $\min_{\Delta, |\Delta| = t} |\cup_{i \in \Delta} B_i| - 1$) or the smallest one (i.e. $\max_{\Lambda, |\Lambda| = t-1} |\cup_{i \in \Lambda} B_i|$).

4.1 Constructions from combinatorial designs

In this subsection, we will give some constructions of SCFF from certain combinatorial designs, including μ-designs, packing designs and orthogonal array. Similar constructions for traceability schemes and frameproof codes can be found in [21].

As before, we will use $(X, \mathcal{B})$ to denote a set system in which X is a finite set and $\mathcal{B}$ is a family of subsets of X. The elements of X and $\mathcal{B}$ are called *points* and *blocks*, respectively. A $\mu - (v, r, \lambda)$ *design* is a set system $(X, \mathcal{B})$, where $|X| = v, |B| = r$ for every $B \in \mathcal{B}$, and every μ-subset of X occurs in *exactly* λ blocks in $\mathcal{B}$. We will only be interested in $\mu - (v, r, 1)$ design.

Theorem 2. *If there exists a* $\mu-(v, r, 1)$ *design, then there exists a* $(v, \binom{v}{\mu}/\binom{r}{\mu}, t)$-*SCFF for any* t *satisfying* $\binom{t}{2} < \frac{r}{\mu-1}$.

Proof. It is well known that in a $\mu - (v, r, 1)$ design the number of blocks n is exactly $\binom{v}{\mu}/\binom{r}{\mu}$. Assume there exists a $\mu - (v, r, 1)$ design $(X, \mathcal{B})$. Then for each pair $B_i, B_j \in \mathcal{B}$, we trivially have $|B_i \cap B_j| \leq \mu - 1$. From Lemma 1 the theorem is immediate.

There are many results on existence and constructions of $\mu - (v, r, 1)$ design for $r = 2, 3$ [6]. On the other hand, no $\mu - (v, r, 1)$ design with $v > r > \mu$ is known to exist for $\mu \geq 6$. Furthermore, it is known that for $3 \leq r \leq 5$, a $2 - (v, r, 1)$ design exists if and only if $v \equiv 1$, or $r \bmod (r^2 - r)$. To apply Theorem 2, it is required $r \geq 4$ and so that $\binom{3}{2} < r/(\mu - 1)$, where $\mu = 2$. Since $2-(v, 4, 1)$ design exists for any $v \equiv 1, 4 \bmod 12$, Theorem 2 yields the following result.

Corollary 1. *There exists* $(v, \frac{v(v-1)}{12}, 3) - SCFF$ *for all* $v \equiv 1, 4 \bmod 12$.

A $\mu - (v, r, \lambda)$ *packing design* is a set system $(X, \mathcal{B})$, where $|X| = v, |B| = r$ for every $B \in \mathcal{B}$, and every μ-subset of X occurs in *at most* λ blocks in $\mathcal{B}$. Similar to Theorem 2, we have the following theorem.

Theorem 3. *If there exists a* $\mu - (v, r, 1)$ *packing design having* n *blocks, then there exists a* $(v, n, t) - SCFF$ *if* $\binom{t}{2} < \frac{r}{\mu-1}$.

As we noted previously, no $\mu - (v, r, 1)$ designs are known to exist if $v > r > \mu \geq 6$. However, for any μ, there are infinite classes of packing designs with a "large" number of blocks (i.e. close to $\binom{v}{\mu}/\binom{r}{\mu}$). Such packing designs can also be constructed from orthogonal arrays. Recall [6] that an *orthogonal array* $OA(\mu, r, s)$ is a $r \times s^\mu$ array, with entries from a set of $s \geq 2$ symbols, such that in any μ rows, every μ-tuple with elements from s occurs in these μ rows as an $\mu \times 1$ column vector exactly once. We now use this to prove the following theorem.

Corollary 2. *For any prime power* q *and any integer* $\mu < q$, *there exist* $(q^2 + q, q^\mu, t) - SCFF$ *for any* t *satisfying* $\binom{t}{2} < \frac{q+1}{\mu-1}$.

Proof. In [21], Stinson and Wei showed that if there is an $OA(\mu, r, s)$, then there is a $\mu - (rs, r, 1)$ packing design that contains s^μ blocks. It is well known that for any prime power q with $\mu < q$, there exists an $OA(\mu, q+1, q)$ [6]. It follows that there exists a $\mu - (q^2+q, q+1, 1)$ packing design $(X, \mathcal{B})$. From Theorem 3, we have the theorem.

4.2 Constructions from universal hashing families

The concept of *universal hashing family* was invented by Carter and Wegman [8] and has been the foundations of several applications (see e.g. [24, 18]).
Let $\epsilon > 0$. A multiset H of N functions from a n-set X to a m-set Y is called *ϵ-almost universal* ($\epsilon - AU$ for short) if for any two distinct elements $x_1, x_2 \in X$, there exists at most ϵN functions $h \in H$ such that $h(x_1) = h(x_2)$. Without loss of generality we will assume that $n \geq m$. We call H an $\epsilon - AU(N; n, m)$ hashing family. The following shows that SCFF can be constructed from AU hashing families.

Theorem 4. *If there exists an $\epsilon - AU(N; n, m)$ hashing family, then there exists a (Nm, n, t)-SCFF provided $\binom{t}{2} < 1/\epsilon$.*

Proof. Assume that H is an $\epsilon - AU(N; n, m)$ hashing family from S to T. We construct a set system $(X, \mathcal{B})$ as follows. Set $X = H \times T = \{(h, t) \mid h \in H, t \in T\}$ and $\mathcal{B} = \{B_s \mid s \in S\}$, where for each $s \in S$ we define $B_s = \{(h, h(s)) \mid h \in H\}$. Then it is easy to see that $|X| = Nm$, $|\mathcal{B}| = n$ and $|B_s| = N$ for each $s \in S$. For each pair $B_s, B_{s'} \in \mathcal{B}$, we have

$$\begin{aligned} |B_s \cap B_{s'}| &= |\{(h, h(s)) \mid h \in H\} \cap \{(h, h(s')) \mid h \in H\}| \\ &= |\{h \mid h(s) = h(s'), h \in H\}| \\ &\leq \epsilon N \end{aligned}$$

From Lemma 1, we know that $(X, \mathcal{B})$ is an (Nm, n, t) SCFF if $\binom{t}{2} < \frac{N}{\epsilon N} = \frac{1}{\epsilon}$, and the desired result follows.

$\epsilon - AU$ are strictly related to error-correcting codes (see [3]). Let Y be an alphabet of q symbols. An (N, M, D, q) *code* is a set $\mathcal{C}$ of M vectors in Y^N such that the Hamming distance between any two distinct vectors in $\mathcal{C}$ is at least D. The code is *linear* if q is a prime power, $Y = GF(q)$, and $\mathcal{C}$ is a subspace of the vectorspace $GF(q)^N$. Then we will denote it by an $[N, m, D, q]$ code, where $m = \log_q M$ is the *dimension* of the code.
Let $\mathcal{C}$ be a (N, M, D, q) code, we can define a family of functions $H = \{h_1, \ldots, h_N\}$ from $\mathcal{C}$ to Y by the following

$$(h_1(v), h_2(v), \ldots, h_N(v)) = (v_1, \ldots, v_N)$$

for each $v = (v_1, \ldots, v_N) \in \mathcal{C}$.
The following equivalence is due to Bierbrauer, Johansson, Kabatianskii and Smeets [3].

Theorem 5 ([3]). *If there exists an (N, M, D, q) code, then there exists a $(1 - \frac{D}{N}) - AU(N; M, q)$ hash family. Conversely, if there exists an $\epsilon - AU(N; n, m)$ hash family, then there exists an $(N, n, N(1-\epsilon), m)$ code.*

If we apply the above theorem to Justesen codes (Theorem 9.2.4 [23]), we obtain a (v, n, t)-SCFF $(X, \mathcal{B})$ with $|B_i| = O(\log n)$, for all $B_i \in \mathcal{B}$, and the share expansion of the new scheme in our construction is $O(\log n)$.
Another application of Theorem 5 is to use Reed-Solomon codes. An *extended Reed-Solomon* code is a linear code having parameters $[q, u, q-u+1, q]$, where $u \leq q$ and q is a prime power. Applying Theorem 4 and 5 we have

Corollary 3. *Let q be a prime power and $1 \leq u \leq q$. There exists a (q^2, q^u, t) SCFF, where $t \leq \sqrt{\frac{2q}{u-1}} + 1$.*

Proof. Applying the extended Reed-Solomon codes in Theorem 5, we know that there is a $\frac{u-1}{q} - AU(q, q^u, q)$ hashing family. The result follows immediately from Theorem 4.

Using a recursive construction, Stinson (Theorem 6.1 [20]) proved that there exists an $i/q - AU(q^i; q^{2^i}, q)$ hashing family. This in conjunction with with Theorem 4 gives us an infinite class of SCFFs.

Corollary 4. *Let q be a prime power and let $i \geq 1$ be an integer. Let $t \leq \sqrt{\frac{2q}{i}} + 1$. Then there exists a (q^{i+1}, q^{2^i}, t)-SCFF.*

4.3 Construction based on exponential sums

In [14] Helleseth and Johansson used exponential sums over finite fields to construct strongly universal hashing families and authentication codes, motivated by the universal construction in the previous subsection we show that the exponential sums can be applied to our constructions of SCFF with good parameters. Let $GF(q)$ be a finite field with characteristic p, and let $Tr_{q^m/q}(\alpha)$ be the trace function from $GF(q^m)$ to $GF(q)$ defined by

$$Tr_{q^m/q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Lemma 2 ([14]). *Let $f(x) = \sum_{i=1}^{D} a_i x^i \in GF(q^m)[x]$ be a polynomial of degree D that is not expressed in the form $f(x) = g(x)^p - g(x) + \theta$ for any $g(x) \in GF(q^m)[x], \theta \in GF(q^m)$. Let*

$$N_\alpha(f) = |\{x \in GF(q^m) \mid Tr_{q^m/q}(f(x)) = \alpha\}|.$$

Then $N_\alpha(f) \leq q^{m-1} + (D-1)\sqrt{q^m}$ for any $\alpha \in GF(q)$.

Let $D \leq \sqrt{q^m}$, we define a set $\mathcal{F}_D$ of polynomials with degree less than or equal to D by

$$\mathcal{F}_D = \{f(x) \mid f(x) = a_1 x + a_2 x^2 + \cdots + a_D x^D \in GF(q^m)[x], a_i = 0, \quad \text{whenever} \quad p \mid i\}.$$

Then, $\mathcal{F}_D$ is clearly a $(D-\lfloor D/p \rfloor)$-dimensional vector space over $GF(q^m)$, so we have $|\mathcal{F}_D| = q^{m(D-\lfloor D/p \rfloor)}$. Moreover, it is easy to see that for each $f(x) \in \mathcal{F}_D$, $f(x)$ can not be expressible in the form $f(x) = g(x)^p - g(x) + \theta$, and Lemma 2 can be applied. That is, for each $f(x) \in \mathcal{F}_D$ and $\alpha \in GF(q)$, we have $N_\alpha(f) \leq q^{m-1} + (D-1)\sqrt{q^m}$.
For each $\beta \in GF(q^m)$, we associate a function g_β from $\mathcal{F}_D$ to $GF(q)$ defined by $g_\beta(f) = Tr_{q^m/q}(f(\beta))$.
Denote $\mathcal{G} = \{g_\beta \mid \beta \in GF(q^m)\}$. Let $X = \mathcal{G} \times GF(q)$ and $\mathcal{B} = \{B_f, f \in \mathcal{F}_D\}$, where $B_f = \{(g_\beta, g_\beta(f)) \mid \beta \in GF(q^m)\}$. We will show that such set systems $(X, \mathcal{B})$ are SCFF with some appropriate parameters.

Lemma 3. *$|B_f \cap B_{f'}| \leq q^{m-1} + (D-1)\sqrt{q^m}$, for any $f \neq f' \in \mathcal{F}_D$.*

Proof. As is easy to verify:

$$\begin{aligned} |B_f \cap B_{f'}| &= |\{g_\beta \mid g_\beta(f) = g_\beta(f')\}| \\ &= |\{\beta \mid Tr_{q^m/q}(f(\beta)) = Tr_{q^m/q}(f'(\beta))\}| \\ &= |\{\beta \mid Tr_{q^m/q}(f-f')(\beta) = 0\}| \\ &\leq N_0(f-f') \\ &\leq q^{m-1} + (D-1)\sqrt{q^m} \end{aligned}$$

Combining Lemma 3 and Lemma 1, we have the following result.

Theorem 6. *$(X, \mathcal{B})$ is a $(q^{m+1}, q^{m(D-\lfloor D/p \rfloor)}, t)-SCFF$ provided $\binom{t}{2} \leq q^m/(q^{m-1} + (D-1)\sqrt{q^m})$*

The above theorem results in an infinite class of SCFFs with good parameters. For example, taking $D = q^{m/2-1} + 1$ for any even m, then for any t satisfying $\binom{t}{2} \leq q/2$, applying the above theorem gives a $(q^m, q^{m(q^{m/2-1} - \lfloor q^{m/2-1}/p \rfloor)}, \lfloor \sqrt{2} q^{m/4} \rfloor)-SCFF$ for all even m. A simple approximation yields that there is an infinite class of $(v, n, t) - SCFFs$ in which the parameters satisfy $\log n = C\sqrt{v} \log v$, where C is a fixed constant. We have $(\log n)^2 = C^2 v (\log v)^2 \geq c^2 v$, that is, there exists an infinite class of $(v, n, t) - SCFF$ in which v is $O((\log n)^2)$.

4.4 Constructions based on arcs

An arc is a set system $(X, \mathcal{B})$ such that the intersection of any two blocks (lines) is a single point and the intersection of three blocks is empty [15]. This gives the following result not based on Lemma 1.

Theorem 7. *For each prime power q and each t where $2 \leq t \leq q+1$, there exists an $(q^2+q+1, q+1, t)$-SCFF.*

Proof. As is well known [15] a projective plane allows an $(q^2+q+1, q+1)$ block system as an arc. The blocks are the lines in the arc. So from the definition of an arc we immediately have that the union of a (where $a \leq q+1$) different blocks is exactly $a(q+1) - \binom{a}{2}$ since any two lines have an intersection, but three (or more) blocks of the arc never have. So, t blocks have strictly more points than $t-1$ blocks have, since $t(q+1) - \binom{t}{2} > (t-1)(q+1) - \binom{t-1}{2}$ because $(q+1) > (t(t-1) - (t-1)(t-2))/2 = (t-1)$ which follows from our conditions on t.

This theorem can be extended using n-arcs [25]. An n-arc is a set of n points in the projective geometry $PG(k-1,q)$ such that any k points are linearly independent. An SCFF can be constructed from an n-arc in a way similar to above. parameters of this SCFF will be given in the final version of the paper. We note that the problem of finding a $[n,k,n-k+1]$ maximum distance separable code is equivalent to the problem of finding an n-arc in the projective geometry $PG(k-1,q)$ and it is known that $n \leq q+k-2$.

4.5 Constructions based on the complement

We now discuss SCFF based on applying De Morgan's law to the definition. For a set $A \subseteq X$ we define the complement as $\bar{A} = X \setminus A$.

Lemma 4. *A set system $(X,\mathcal{B}')$, where $\mathcal{B}' = \{B'_1,\ldots,B'_n\}$, for which for all $\Delta \subseteq \{1,\ldots,n\}$ and all $\Lambda \subseteq \{1,\ldots,n\}$ where $|\Delta| = t$ and $|\Lambda| = t-1$ we have*

$$|\cap_{i\in\Delta} B'_i| < |\cap_{i\in\Lambda} B'_i| \tag{2}$$

induces an $(|X|,n,t)$-SCFF $(X,\mathcal{B})$ by taking $B_i = \bar{B'}_i$.

Proof. Suppose that the conditions in the lemma are satisfied. Now take the complement of the left and right hand side of (2) and apply De Morgan's law. It is then easy to see that we obtain (1) in which $B_i = \bar{B'}_i$. The lemma then follows immediately.

We are now discussing SCFF with $\ell = v$. This will imply that we can construct a t-out-of-n secret sharing scheme from a v-out-of-v scheme.

Theorem 8. *Constructing a (t,n)-threshold scheme from a (v,v) scheme using an (v,n,t)-SCFF is equivalent to the following conditions on B_i:*
For any Δ and any $\Lambda \subseteq \{1,\ldots,n\}$ with $|\Delta| = t$ and $|\Lambda| = t-1$:

$$\bigcap_{i\in\Delta} \bar{B}_i = \emptyset \qquad \textit{and} \qquad \bigcap_{i\in\Lambda} \bar{B}_i \neq \emptyset$$

where $\bar{B} = X \setminus B$.

Proof. It is easy to see that the addressed problem of constructing a (t,n) scheme from a (v,v) scheme is equivalent to requiring that for any Δ and any $\Lambda \subseteq \{1,\ldots,n\}$ with $|\Delta| = t$ and $|\Lambda| = t-1$:

$$\bigcup_{i\in\Delta} B_i = X \qquad \text{and} \qquad \bigcup_{i\in\Lambda} B_i \neq X. \tag{3}$$

The rest follows from Lemma 4.

It is now obvious that an arc can be used to design such SCFFs. This gives the following corollary.

Corollary 5. *For each prime power q, there exists an $(q^2+q+1, q+1, 3)$-SCFF that allows to construct a $(3, q+1)$-threshold scheme from a (q^2+q+1, q^2+q+1) scheme.*

Proof. From the definition of an arc we have that any 2 lines of the arc always intersect in one point, but the intersection of any 3 lines of the arc is empty. The rest follows from Theorem 8 and the well known [15] property that a projective plane allows an $(q^2+q+1, q+1)$ block system as an arc.

We now use Lemma 4 to obtain other SCFFs.

Theorem 9. *Any $\mu-(n, r, 1)$-design gives us a $(\binom{n}{\mu}/\binom{r}{\mu}, n, \mu)$-SCFF.*

Proof. Let us take an $\mu-(n, r, 1)$ design $(X', \mathcal{B}')$ (see Section 4.1 for a definition). As is well known, this implies we have exactly $\binom{n}{\mu}/\binom{r}{\mu}$ blocks. A block system where $|X'| = n$ and $|\mathcal{B}'| = a$ corresponds with an $a \times n$ incidence matrix M over $GF(2)$. So, the transpose of M induces a block system where $(X, \mathcal{B}) = (\mathcal{B}', X')$. Now let $a = \binom{n}{\mu}/\binom{r}{\mu}$.
The definition of the design implies that every μ-subset of X' occurs in *exactly* one block in $\mathcal{B}'$. So, an $\mu-1$ subset must occur in more than one block in $\mathcal{B}'$. Using the transpose idea and realizing that the columns of M now correspond to blocks in the new $(X, \mathcal{B}) = (\mathcal{B}', X')$ block system this implies that in the new $(X, \mathcal{B}) = (\mathcal{B}', X')$ block system we have that the intersection of μ blocks in the new $(X, \mathcal{B})$ is 1, and the intersection of $\mu-1$ blocks in the new $(X, \mathcal{B})$ is strictly larger than 1. Using Lemma 4 the theorem follows.

Corollary 6. *This easily extends to $\mu-(n, r, \lambda)$-designs.*

5 Bounds

As noted earlier the efficiency of our new construction relies on the parameters strong cover free family involved in the construction. In this section we will derive some bounds on various parameters of SCFFs.
The following theorem completely characterizes the SCFF when $t = 2$.

Theorem 10. *There exists a $(v, n, 2) - SCFF$ if and only if $n \leq \binom{v}{\lfloor \frac{v}{2} \rfloor}$.*

Proof. Assume that $(X, \mathcal{B})$ is a $(v, n, 2) - SCFF$, then it is easy to see that there do not exist two distinct blocks B_i, B_j such that $B_i \subseteq B_j$, i.e., $(X, \mathcal{B})$ is a *Sperner Family* [6]. It is well-known that there exists a Sperner family consisting of n subsets of a v-set only if $n \leq \binom{v}{\lfloor \frac{v}{2} \rfloor}$ (see [6]). Conversely, we can take all $\lfloor \frac{v}{2} \rfloor$-subsets of a v-set, it is easy to see that it results in a $(v, n, 2)$-SCFF with $n = \binom{v}{\lfloor \frac{v}{2} \rfloor}$, proving the desired result.

Next, we derive a lower bound on v for given n and t.

Theorem 11. *In any $(v, n, t) - SCFF$, we have $v \geq (t-1) \log \frac{n}{t-1}$*

Proof. Assume that $(X, \mathcal{B})$ is a $(v, n, t) - SCFF$. Let $\mathcal{F} = \{\cup_{i\in\Lambda} B_i : \Lambda \subseteq \{1, \ldots, n\} \mid with\ |\Lambda| = t-1, B_i \in \mathcal{B}\}$. We observe that for any $\Lambda \neq \Lambda' \subset \{1, \ldots, n\}$ with $|\Lambda| = |\Lambda'| = t-1$, we have $\cup_{i\in\Lambda} B_i \neq \cup_{j\in\Lambda'} B_j$. Indeed, otherwise assume that there are Λ and Λ' with $|\Lambda| = |\Lambda'| = t-1$ such that $\cup_{i\in\Lambda} B_i = \cup_{j\in\Lambda'} B_j$. Since $\Lambda \neq \Lambda'$, we may assume that there is an element $\ell \in \Lambda'$, but $\ell \notin \Lambda$. It follows $\cup_{i\in\Lambda\cup\{\ell\}} B_i = \cup_{i\in\Lambda'} B_i$ and hence $|\cup_{i\in\Lambda\cup\{\ell\}} B_i| = |\cup_{i\in\Lambda'} B_i|$, which contradicts with the assumption that $(X, \mathcal{B})$ is a $(v, n, t) - SCFF$ since $|\Lambda \cup \{\ell\}| = t$ and $|\Lambda'| = t-1$. So we have $|\mathcal{F}| = \binom{n}{t-1}$. Similarly, it is easy to see that $\mathcal{F}$ is a *Sperner family* [6], that is, for any $F \neq F' \in \mathcal{F}$, we always have $F \not\supseteq F'$. It follows (see [6]) that $|\mathcal{F}| \leq \binom{v}{\lfloor \frac{v}{2} \rfloor}$. Since $\binom{n}{t-1} \geq (\frac{n}{t-1})^{t-1}$ and $\binom{v}{\lfloor \frac{v}{2} \rfloor} \leq 2^v$, we obtain $(\frac{n}{t-1})^{t-1} \leq 2^v$, and so $v \geq (t-1)\log\frac{n}{t-1}$.

The above theorem can be restated as $n \leq (t-1)2^{\frac{v}{t-1}}$, which gives an upper bound on n for given v and t. We now see that a strong cover-free family is a special case of a cover-free family [12].

Theorem 12. *A (v, n, t)-SCFF is a (v, n, t)-cover free family.*

Proof. Assume that $(X, \mathcal{B})$ is a (v, n, t)-SCFF. Let Λ be a subset of $\{1, \ldots, n\}$ such that $|\Lambda| = t-1$, and let $i \notin \Lambda$. Then we have $|\Lambda \cup \{i\}| = t$, and so $|\cup_{j\in\Lambda\cup\{i\}} B_j| > |\cup_{j\in\Lambda} B_j|$. It follows that $B_i \not\subseteq \cup_{j\in\Lambda} B_j$, that is, the union of any $t-1$ blocks in $\mathcal{B}$ can not cover any remaining one in $\mathcal{B}$. Such a set system is called (v, n, t)-cover free family [12].

Corollary 7. *Let $(X, \mathcal{B})$ be a $(v, n, t) - SCFF$ such that $|B_i| = r$ for all $B_i \in \mathcal{B}$. Then $n \leq \binom{v}{m}/\binom{r-1}{m-1}$, where $m = \lceil r/t - 1 \rceil$.*

Proof. Using Theorem 12 and by Proposition 2.1 of [12], the result follows immediately.

We can show that in any SCFF $(X, \mathcal{B})$ where $|X| < |\mathcal{B}|$, the parameter t can not be too large relative to n.

Corollary 8. *In a $(v, n, t) - SCFF$, where $v < n$, we have $t < \sqrt{2n}$.*

Proof. Indeed, assume that $(X, \mathcal{B})$ is a $(v, n, t) - SCFF$. From Theorem 12 we know that $(X, \mathcal{B})$ is a $(v, n, t-1)$-cover-free family. By Proposition 3.4 of [12], we have $n \geq \binom{t+1}{2} > t^2/2$, and the desired result follows.

In [22], it has been shown that for (n, m, t)-CFF with $t \geq 2$, $m \geq c\frac{t^2}{\log t}\log n$ for some constant c which is approximately $1/2$. On the other hand, Erdös *et al* [12] showed that for any $n > 0$, there exists an (n, m, t)-CFF with $m = O(t^2 \log n)$ and $|B_i| = O(t \log n)$. This result is, however, non-constructive. Although Kumar *et al* [16] gave a probabilistic construction of CFF that meets the bound, explicit constructions that can achieve or get close to Erdös *et al* bounds are still of interest.

We are now discussing SCFF with $\ell = v$. This will imply that we can construct a t-out-of-n secret sharing scheme from a v-out-of-v scheme.

Theorem 13. *Constructing a (t,n) scheme from a (v,v) scheme using a (v,n,t)-SCFF is only possible if $v \geq \binom{n}{t-1}$.*

Proof. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the n participants in the considered (t,n) secret sharing scheme, $\Gamma_{t-1} = \{A \mid A \subseteq \mathcal{P}, |A| = t-1\}$. Let $(X, \mathcal{B})$ be the (v,n,t)-SCFF, where P_i is assigned a block $B_i \in \mathcal{B}$. We define a function that associates to a set A in Γ_{t-1} a subset of X that are not the union of the blocks allocated to A, we then prove that any different elements in Γ_{t-1} are mapped to disjoint subset of X. The result then follows directly.
The above claimed function is defined as

$$g : \Gamma_{t-1} \to 2^X,$$

such that for any $A \in \Gamma_{t-1}$, where $A = \{P_{i_1}, \ldots, P_{i_{t-1}}\}$ then

$$g(A) = X \setminus \cup_{j=1}^{t-1} B_{i_j}.$$

For any $A_1, A_2 \in \Gamma_{t-1}$, if $g(A_1) \cap g(A_2) \neq \emptyset$, then there is an element $x_i \in X$ which is in both $g(A_1)$ and $g(A_2)$. So x_i can not be covered by the union of blocks allocated the participants in A_1 and A_2. This contradicts the assumption that the union of t blocks cover X since $|A_1 \cup A_2| \geq t$.

We give a construction to show that the bound in Theorem 13 is tight when $t > 1$. Let $\Gamma_{t-1} = \{A \mid A \subseteq \mathcal{P}, |A| = t-1\}$. Let X be a $\binom{n}{t-1}$-set indexed by the elements in Γ_{t-1}, that is $X = \{X_A \mid A \in \Gamma_{t-1}\}$. For each $1 \leq i \leq n$, we define $B_i = \{X_B \mid P_i \notin B, B \in \Gamma_{t-1}\}$. Let $\mathcal{B} = \{B_1, \ldots, B_n\}$. Then it is straightforward to verify that $(X, \mathcal{B})$ is a $(\binom{n}{t-1}, n, t)$-SCFF, and the claim for the tight bound follows. Note that the case $t = 2$ was already proposed in [7] to obtain a homomorphic secret sharing scheme.

6 Evaluation and conclusions

In the following we translate some of the results in the previous section into constructions of mechanical threshold schemes from old ones. We compute possible values of ℓ which are not necessarily maximal or minimal (see the discussion in 4). Here some possible parameters:

1. For any integer $v \equiv 1, 4 \bmod 12$, an (ℓ, v) scheme results in a $(3, \frac{v(v-1)}{12})$ scheme (Corollary 1). The value $\ell = 9$ is possible for these schemes;
2. For any prime power q and any integer $\mu < q$, a (ℓ, q^2+q) scheme results in (t, q^μ) scheme provided $\binom{t}{2} < \frac{q-1}{\mu-1}$ (Corollary 2). For these, (at least) the following values of ℓ are possible: $(t-1)*(q+1)+1 \leq \ell \leq t*(q+1)-\binom{t}{2}*(\mu-1)$.
3. For any prime power q and integer $i \geq 1$, a (ℓ, q^{i+1}) scheme results in a (t, q^{2^i}) scheme provided $t \leq \sqrt{\frac{2q}{i}} + 1$ (Corollary 4). For these, (at least) the following values of ℓ are possible: $(t-1) * q^i + 1 \leq \ell \leq t * q^i - \binom{t}{2} * i * q^{i-1}$.

4. For any prime power q and even m, a (ℓ, q^m) scheme results in a $(t, q^{cmq^{m/2}})$ scheme provided $q > 2\binom{t}{2}$, where c is some fixed constant (Theorem 6). For these, (at least) the following values of ℓ are possible: $(t-1) * q^m + 1 \leq \ell \leq t * q^m - \binom{t}{2} * (q^{m-1} + q^{m/2-1}\sqrt{q^m})$.

For example using $q = 4$, $\mu = 2$ and the parameters in 2 we can construct a $(2, 16)$ scheme from a $(\ell, 20)$ scheme where $6 \leq \ell \leq 9$. Using the same value of q and $i = 1$ together with the result in 3 we obtain a $(3, 16)$ scheme from a $(9, 16)$ and also a $(2, 16)$ scheme from a $(\ell, 16)$ where $5 \leq \ell \leq 7$.
We point out that constructing new threshold schemes from old ones using SCFF may have other applications such as constructing multiplicative secret sharing schemes which are of high importance in threshold cryptography. It is easy to show that if the old scheme is multiplicative then the new scheme based on SCFF is also multiplicative, and its asymptotic efficiency (share expansion) matches the best known results in [5]. However it is not clear if the SCFF construction can outperform the recursive construction in [5] in other aspects. Comparing the two approaches in constructing multiplicative secret sharing schemes deserves a more careful treatment.

References

1. F. Bao, R. Deng, Y. Han, and A. Jeng. Design and analysis of two basic protocols for use in TTP-based key escrow. *Information Security and Privacy, Second Australian Conference, ACISP '97*, LNCS **1270** (1997), 261–270. Sydney, NSW, Australia, July 7–9.
2. J. C. Benaloh, Secret sharing homomorphisms: Keeping shares of a secret secret, *Advances in Cryptology–Crypto '86,* LNCS, **263**(1986), 251–260.
3. J. Bierbrauer, T. Johansson, G. Kabatianskii and B. Smeets, On families of hash functions via geometric codes and concatenation, *Advances in Cryptology–CRYPTO'93,* LNCS, **773** (1994), 331–342.
4. G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of AFIPS 1979 National Computer Conference*, 48:313–317, 1979.
5. S. R. Blackburn, M. Burmester, Y. Desmedt and P. R. Wild, 'Efficient multiplicative sharing schemes,' in *Advance in Cryptology–Eurocrypt '96*, LNCS, **1070**(1996), 107-118.
6. P. J. Cameron and J. H. Van Lint, Deisigns, Graphs, Codes, and their Links, Cambridge University Press, Cambridge 1991.
7. C. Boyd. Digital multisignatures. In H. Beker and F. Piper, editors, *Cryptography and coding*, pp. 241–246. Clarendon Press, 1989. Royal Agricultural College, Cirencester, December 15–17, 1986.
8. J. L. Carter and M. N. Wegman, Universal classes of hash functions, *Journal of Computer and System Sci.*, **18**(1979), 143–154
9. L. Chen, D. Gollmann, and C. Mitchell. Key escrow in mutually mistrusting domains. *Security Protocols* LNCS **1189** (1997), 139–153.
10. Y. Desmedt and S. Jajodia, Redistributing secret shares to new access structures and its applications, *Preprint*, 1997.
11. J. Diamant and F. Rhee. FBI follows money to 7 close to home, catches Ghantt in Mexico. The Charlotte Observer, March 3, 1998. See also: `http://www.charlotte.com/observer/special/heist/pub/heist.htm`.

12. P. Erdös, P. Frankl, and Z. Furedi, Families of finite sets in which no sets is covered by the union of r others, *Israel Journal of Mathematics,* **51**(1985), 79–89.
13. Y. Frankel and P. Gemmell and P. D. MacKenzie and M. Yung, Optimal Resilience Proactive Public Key Cryptosystems, *38th Annual Symp. on Foundations of Computer Science (FOCS)*, 1997.
14. T. Helleseth and T. Johansson, Universal hash functions from exponential sums over finite fields and Galois Rings, *Advances in Cryptology–Crypto'96*, LNCS, **1109**(1996), 31–44.
15. J. W. P. Hirschfeld. *Projective Geometries over finite fields.* Oxford University Press, N.Y., 1979.
16. R. Kumar, S. Rajagopalan and A. Sahai. Coding constructions for blacklisting problems without computational assumptions, *Advances in Cryptology – CRYPTO '99*, LNCS, **1666**(1999), 609-623.
17. K. Martin, R. Safavi-Naini, and H. Wang, Bounds and techniques for efficient redistribution of secret shares to new access structures, *The Computer Journal*, **42**(8) (1999), 638–649.
18. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. *Proceedings of the twenty first annual ACM Symp. Theory of Computing, STOC*, (1989), 33–43.
19. A. Shamir, How to Share a Secret, *Communications of the ACM*, **22**(1976), 612–613.
20. D. R. Stinson, Universal hashing and authentication codes, *Advances in Cryptology–CRYPTO '91*, LNCS, **576** (1992), 74–85.
21. D. R. Stinson and R. Wei, Combinatorial Properties and Constructions of Traceability Schemes and Frameproof Codes, *SIAM. J. Discrete Math*, **11**(1998)41–53.
22. D. S. Stinson, R. Wei and L. Zhu, Some new bounds for cover-free families, *Journal of Combinatorial Theory, A*, **90**(2000), 224-234.
23. J. H. van Lint, Introduction to Coding Theory, *Graduate Texts in Mathematics*, Vol. **86**, Springer-Verlag, 1992.
24. M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, **22** (1981), 265–279.
25. F. J. MacWilliams and N. J. Sloane. *The Theory of Error-Correcting Codes.* northholland publishing company, 1978.