QUADERNI

Università degli Studi di Siena
DIPARTIMENTO DI ECONOMIA POLITICA

STEFANO VANNUCCI

On Perfect Secret Sharing Schemes and Coalitional Game Forms

n. 316 - Marzo 2001

On Perfect Secret Sharing Schemes and Coalitional Game Forms

Stefano Vannucci
Dipartimento di Economia Politica,
Universita' di Siena
Piazza S. Francesco 7, 53100 Siena
e-mail: vannucci@unisi.it

January 25, 2001

Abstract

It is shown that *Perfect* Secret Sharing Schemes are *Simple* Weak Effectivity Functions. Namely, for any finite set K of keys and any finite set N of participants the set of all Perfect Secret Sharing Schemes having 0-normalized security level $\#K-1$ is characterized as the set of all *Simple* Weak Effectivity Functions on *(N,K)*: *perfection* in secret sharing turns out to have *simplicity* as its nice game-theoretic counterpart. It also follows that Perfect Secret Sharing Schemes do admit *universal* implementation procedures using 1-threshold schemes as elementary 'building blocks'.

JEL Classification Numbers 025,026

1 Introduction

In real-life situations, efficiency considerations may variously dictate either *disclosure* or *protection* of privately held information. The information revelation problem i.e. elicitation of private information by means of suitable incentive schemes has always been a central theme in the literature on mechanism design, at least since the beginnings of the modern game-theoretic approach back in the early '70s. In an information revelation problem (e.g. in auctions or voting) individual agents and/or coalitions of agents must be induced to share some of their 'secret', privately held information with the service provider i.e. the agency responsible for computing and possibly enforcing the decision mechanism's outcomes.

By contrast, the *reverse* situation –where *the service provider assigns to agents and/or coalitions some private information* (e.g. a private key, or parts of it) *which is meant to be kept as a secret by its legitimate holders*– raises a few interesting issues which are best addressed within the theoretical framework of *distributed cryptography.* However, it transpires that the management and transmission of secret/confidential information is also of considerable significance from a *game-theoretic* perspective, and of growing practical importance due to the ever increasing role of electronic information processing in social and economic interactions. Here, the basic problem is of course ensuring that access rights are not abused i.e. that *the entitled agents are able to protect their secret against possible insiders' or outsiders' attacks.* Thus, the issue is *protection* –as opposed to revelation–*of private information.* A particularly interesting version of this problem obtains when the secret itself is to be *shared* among a *coalition* of agents.

A *secret sharing scheme (SSS)* is a rule for *apportioning* some *secret* information among participants in such a way that certain 'legal' sets of agents which comprise the *access structure* of the scheme– and *only* them– have *joint* access to the relevant data (the 'secret'). An SSS is *perfect* whenever *any* 'illegal' coalition of agents –no matter how many shares are legally accessible to its members–cannot do any better than a coalition of outsiders, i.e. –typically–randomly guessing the secret among the (publicly known) set of admissible data or keys. The reciprocal of the *probability of deception* –that is the probability of successful random guessing– provides then a well-defined measure of the *security level* of the scheme.

It has been known since the late '80s that perfect SSSs do exist *for any prescribed security level* and *any access structure* (see e.g. Benaloh, Leichter(1990)): in particular, several examples which admit a natural implementation via modular arithmetic and combinatorial geometric structures have been designed and studied (see e.g. Simmons(1992), Stinson(1995), Menezes,van Oorschott,Vanstone (1997), Beutelspacher,Rosenbaum(1998)). However, a few questions remain that– to the best of my knowledge– have not been explicitly addressed in the extant cryptographic literature, namely:

- How can the class of *all* possible perfect SSSs at *any* security level be described? Is it amenable to any 'convenient' characterization?

- Is it possible to implement *all* access structures at any fixed security level using some perfect SSS as a unique elementary 'building' block or different (sets of) 'building blocks' are required in order to implement distinct access structures and/or to achieve distinct security levels?

It turns out that the foregoing issues can be readily addressed and solved by expressing them in a suitable *coalitional game-theoretic format.* This is most conveniently done relying on *weak effectivity functions (WEFs). A WEF* is a map that attaches to each coalition S the set of all outcome-subsets into which S is able to 'force' the final outcome.Thus, a WEF can also be characterized as an outcome-subsets-parameterized family of *simple games* i.e. sets of (locally) *'winning' coalitions.* A WEF is *simple* if such a family of *simple* *games* reduces to a *unique set of (almost) globally 'winning' coalitions. It will be shown in the present note that–for any finite set K of keys and any finite set N of agents–* the set of all perfect SSSs does indeed correspond precisely to the set of all simple WEFs on (N, K). Now, it can be shown that any simple WEF is representable as the intersection of a finite set of weighted simple WEFs. Since any weighted simple EF admits a 'perfect' implementation (either modular-arithmetical or combinatorial geometric), it follows that –in principle– repeated application of the latter can be used as the *basic component of a universal implementation procedure for perfect SSSs of arbitrary access structure and security level.*

2 The model

To begin with, a few basic definitions concerning key establishment protocols must be introduced. Let N be a finite set of *agents* or *participants*, K a finite set of possible *secret keys* to be shared. A *secret sharing scheme (SSS)* for (N, K) is a tuple $\mathbf{S}$ $=(\mathcal{S}, \alpha, \pi, h)$ consisting of a *share space* S (typically a non-empty finite set 'with structure', e.g. a finite projective space–see the definition below– or more generally an object of a suitably chosen concrete category), a *sharing rule* $\alpha : K \times N \to \mathcal{S}$ (with *canonical extension* $\alpha^* : K \times P(N) \to \bigcup_{T \subseteq N} \mathcal{S}^T$ as defined by the following rule: for any $T \subseteq N$, $\alpha^*(k, T) = (\alpha(k, i) : i \in T))$, a *pooling function* $\pi : \bigcup_{T \subseteq N} \mathcal{S}^T \to P(\mathcal{S})$ such that $\pi((x_i)_{i \in S}) \subseteq \pi((x'_i)_{i \in T})$ whenever $(x_i)_{i \in S} \in \mathcal{S}^S, (x'_i)_{i \in T} \in \mathcal{S}^T$, $S \subseteq T$ and $x_i = x'_i$ for any $i \in S$, and a *(semi-neutral) recovering function* $h : P(\mathcal{S}) \to P(K)$ such that for any $k_1, k_2 \in K$, $K_1, K_2 \subseteq K$, $A, B \subseteq \mathcal{S}$, and $T \subseteq N$: $A \subseteq B$ entails $h(B) \subseteq h(A)$, $k \in h(\pi(\alpha^*(k, T)))$, $\{k\} = h(\pi(\alpha^*(k, N)))$, $K_1 = h(\pi(\alpha^*(k_1, T))$ and $K_2 = h(\pi(\alpha^*(k_2, T))$ entail $\#K_1 = \#K_2$, and $h(\emptyset) = K$ (this last requirement reflects the typical assumption that the key set K be *public knowledge*).

Remark 1 *It should be noticed here that the 'fine-grained' definition of an SSS proposed above is* not *standard. Indeed, SSSs are variously presented in the cryptographic literature, to an extent that makes it difficult to single out a standard definition.The most common usage consists in identifying SSSs with their sharing rules as defined above, while leaving implicit the pooling and recovering functions. I find, however, that the more detailed –if perhaps clumsier– definition offered here has some distinct advantages. Moreover, the results presented below might be appropriately reformulated according to the 'coarser' definition.*

The *access structure* of an SSS $\mathbf{S}$ $=(\mathcal{S}, \alpha, \pi, h)$ for (N, K) is the bipartition $(L(\mathbf{S}), L^c(\mathbf{S}))$ of $P(N)$ into *legal* and *illegal* coalitions (or authorized and unauthorized subsets), respectively, where the set of legal coalitions is given by $L(\mathbf{S}) = \{S \subseteq N : \text{for any } k \in K,\ h(\pi(\alpha^*(k, S))) = \{k\}\}$. Notice that–by definition of the recovering function h– the set $L(\mathbf{S})$ of legal coalitions of an access structure amounts to an *order filter* of $(P(N), \supseteq)$, i.e.a subset of $P(N)$ such that for any $S, T \subseteq N$, if $T \supseteq S$ and $S \in L(\mathbf{S})$ then $T \in L(\mathbf{S})$ (and conversely any order filter of $(P(N), \supseteq)$ uniquely identifies a possible access structure with N as set of participants).

An SSS $\mathbf{S}$ for (N, K) is said to be a *(rational) threshold SSS* if there exist $t \in \mathbb{R}_+$, and $w : N \to \mathbb{R}_+$ ($t \in \mathbb{Q}_+$ and $w : N \to \mathbb{Q}_+$) such that $L(\mathbf{S}) = \left\{S \subseteq N : \sum_{i \in S} w(i) \geq t\right\}$: the corresponding access structure is also said to be a *threshold access structure.* The *(normalized) security level* of a $\mathbf{S} = (\mathcal{S}, \alpha, \pi, h)$ is given by the (rational) number $p_{\mathbf{S}}^{-1} - 1$, where

$$p_{\mathbf{S}} = \max \left\{ \begin{array}{c} m \in \mathbb{Z}_+ : \text{there exist } S \in L^c(\mathbf{S}), K' \subseteq K, k \in K' \text{ such that} \\ K' = h(\pi(\alpha^*(k, S))), \text{ and } m = (\# K')^{-1} \end{array} \right\}$$

denotes the *probability of deception*, i.e. the maximum probability of access to the secret on the part of an illegal coalition (under equiprobability of key-choice on the part of the key-dealing agency).

An (equally distributed) *SSS* $\mathbf{S}$ =$(\mathcal{S}, \alpha, \pi, h)$ for (N, K) is said to be *perfect* (*at (normalized) security level* $q \in \mathbb{Q}_+$) if

i) $h(\pi(\alpha^*(k, S))) = h(\pi(\alpha^*(k, T)))$ for any $S, T \in L^c(\mathbf{S}), k \in K$, and

ii) $[\# h(\pi(\alpha^*(k, S)))]^{-1} = q + 1$ *for all* $S \in L^c(\mathbf{S})$.

Hence, *a perfect SSS is equally protected against outsiders' and insiders' possible attacks.*

The following construct will also be used in the sequel.

Let $\{\mathbf{S}_j = (\mathcal{S}_j, \alpha_j, \pi_j, h_j) : j \in J\}$ be a finite family of perfect SSSs for (N, K). Then, the *product SSS* $\bigotimes_{j \in J} \mathbf{S}_j = (\mathcal{S}^J, \alpha^J, \pi^J, h^J)$ of $\{\mathbf{S}_j : j \in J\}$ is defined as follows:

$\mathcal{S}^J \cong \prod_{j \in J} \mathcal{S}_j$, for any $j \in J$;

$\alpha^J : K \times N \to \mathcal{S}^J$ is defined by the rule $\alpha^J(k, i) = \prod_{j \in J} \alpha_j(k_j, i)$, and similarly

$\pi^J : \bigcup_{T \subseteq N} (\mathcal{S}^J)^T \to P(\mathcal{S}^J)$ is defined as $\pi((\mathcal{S}^J)^T) = \prod_{j \in J} \pi_j((\mathcal{S}_j^T))$, while

$h^J : P(\mathcal{S}^J) \to P(K)$ is defined by the following rule

$$h^J(Y) = \left\{ \begin{array}{c} \{k\} \text{ if for any } j \in J : \\ h_j(\left\{s_j \in \mathcal{S}_j : \text{there exists } ((s_j^*)_{j \in J}) \in Y \text{ s.t. } s_j^* = s_j\right\}) = \{k\}, \text{ and} \\ K \text{ otherwise} \end{array} \right\}$$

.

Moreover, the *security level* of $\bigotimes_{j \in} \mathbf{S}_j$is defined as $\max \left\{ p_{\mathbf{S}_j}^{-1} : j \in J \right\} - 1$.

Let us now turn to the relevant *coalitional game-theoretic* notions. A *weak effectivity function (WEF)* on player set N and outcome set X is a function $E : P(N) \to P(P(X))$ such that : (WEF 1) $E(\emptyset) = \emptyset$; (WEF 2) $X \in E(S)$ for any $S \subseteq N, S \neq \emptyset$; (WEF 3) $E(N) \supseteq E(S)$ for any $S \subseteq N$; (WEF 4) $\emptyset \notin E(S)$ for any $S \subseteq N$.

Remark 2 *Clearly enough, WEFs amount to a slight generalization of* effectivity functions (EFs) *(see e.g. Abdou,Keiding(1991)). Indeed, an EF on* (N, X) *is a WEF such that* $E(N) = P(X) \setminus \{\emptyset\}$ *.*

Moreover, a WEF E on (N, X) is *monotonic* if for any $S, T \subseteq N$, $A, B \subseteq X$: $[A \in E(S)$ and $S \subseteq T$ entail $A \in E(T)]$ and $[A \in E(S)$ and $A \subseteq B$ entail $B \in E(S)]$, and *simple* if there exist an order filter $\mathcal{W}$ of $(P(N), \supseteq)$,

$\emptyset \neq \mathcal{W} \neq P(N)$, $A^* \in P(X) \setminus \{\emptyset\}$, and an order filter $\mathcal{Y}$ of $(P(X), \supseteq)$ with $\mathcal{Y} \supseteq \{A \subseteq X : A \supseteq A^*\}$ such that for any $S \subseteq N, A \subseteq X : A \in E(S)$ if and only if either $[S \in \mathcal{W}$ and $A \in \mathcal{Y}]$ or $[S \neq \emptyset$ and $A \supseteq A^*]$: in that case we also write $E = E(\mathcal{W}, \mathcal{Y}, A^*)$. A simple WEF $E(\mathcal{W}, \mathcal{Y}, A^*)$ is (rational) *threshold simple* if $\mathcal{W}$ is *a (rational) linear threshold order filter* i.e. there exist a (rational) *scalar* weight-function $w : N \to \mathbb{R}_+$ $(w : N \to \mathbb{Q}_+)$ and a (rational) *scalar* threshold or quota $q \in \mathbb{R}_+$ $(q \in \mathbb{Q}_+)$ such that $S \in \mathcal{W}$ if and only if $\sum_{i \in S} w(i) \geq q$:the pair (q, w) is also said to be a *representation* of $E(\mathcal{W}, \mathcal{Y}, A^*)$. Furthermore, a simple WEF E is said to be $(1, n)-threshold$ if it admits a representation $(1, w)$ where w is a $\{0, 1\}$-valued weight function.

Finally, the next definition establishes the basic link between SSSs and WEFs as required for the ensuing analysis.

Let $\mathbf{S}$ =$(\mathcal{S}, \alpha, \pi, h)$ be an SSS for (N, K); then, for any $k \in K$ the characteristic WEF $E_k^{\mathbf{S}}$ of $\mathbf{S}$ at k is defined by the following rule: for any *non-empty* $S \subseteq N$, $E_k^{\mathbf{S}}(S) = \{A \subseteq K : A \supseteq h(\pi(\alpha^*(k, S)))\}$,and $E_k^{\mathbf{S}}(\emptyset) = \emptyset$. Consistency of the foregoing terminology is in fact established through the following

Claim 3 *Let* $\mathbf{S} = (\mathcal{S}, a, \pi, h)$ *be an SSS for* (N, K)*. Then* $\left\{E_k^{\mathbf{S}} : k \in K\right\}$ *is a family of monotonic WEFs on* (N, K)*.*

Proof. By definition of $E_k^{\mathbf{S}}$ and h, $K \in E_k^{\mathbf{S}}(S)$ for any $S \in P(N) \setminus \{\emptyset\}$ and any $k \in K$, while $\emptyset \in E_k^{\mathbf{S}}(S)$ entails–again by definition of $E_k^{\mathbf{S}}$ and h–$h(\pi(\alpha^*(k, S))) = \emptyset$, a contradiction in view of the fact that $\emptyset \neq h(\pi(\alpha^*(k, N))) \subseteq h(\pi(\alpha^*(k, S)))$. Also –by definition of h, π, α^*– for any $S \subseteq N$

$h(\pi(\alpha^*(k, N))) \subseteq h(\pi(\alpha^*(k, S)))$, whence

$E_k^{\mathbf{S}}(N) = \{A \subseteq D : A \supseteq h(\pi(\alpha^*(k, N)))\} \supseteq \{A \subseteq D : A \supseteq h(\pi(\alpha^*(k, S)))\} = E_k^{\mathbf{S}}(S)$.

Thus, for any $k \in K$, $E_k^{\mathbf{S}}$ is indeed a WEF on (N, K). Moreover, monotonicity of $E_k^{\mathbf{S}}$ also follows immediately from the definition. ■

We are now ready to introduce our representation result

Proposition 4 *Let* $\mathbf{S}$ *be an SSS for* (N, K)*.Then,* $\mathbf{S}$ *is a* perfect *SSS if and only if –for any* $k \in K$– $E_k^{\mathbf{S}}$ *is a* simple *WEF on* (N, K)*. In particular,* $\mathbf{S}$ *is perfect* at security level q *if and only if* $E_k^{\mathbf{S}} = E_k^{\mathbf{S}}(L(\mathbf{S}), \{A \subseteq K : k \in A\}, K^*)$ *with* $k \in K^*$ *and* $\#K^* = q + 1$*.*

Proof. Let $\mathbf{S} = (\mathcal{S}, \alpha, \pi, h)$ be an SSS for (N, K) and $(L(\mathbf{S}), L^c(\mathbf{S}))$ its access structure.

Now, suppose $\mathbf{S}$ is *perfect* at security level q. Then, for any k there exists $K^* \subseteq K$, $K^* \ni k$, $\#K^* = q + 1$ such that for any $S \subseteq N$

$$h(\pi(\alpha^*(k, S))) = \left\{ \begin{array}{c} \{k\} \text{ if } S \in L(\mathbf{S}) \\ K^* \text{ if } S \in L^c(\mathbf{S}) \end{array} \right\} .$$

Hence, by definition of $E_k^{\mathbf{S}}$, for any non-empty $S \subseteq N$

$$E_k^{\mathbf{S}}(S) = \left\{ \begin{array}{c} \{A \subseteq K : k \in A\} \text{ if } S \in L(\mathbf{S}) \\ \{A \subseteq K : A \supseteq K^*\} \text{ if } S \in L^c(\mathbf{S}) \end{array} \right\}.$$

Since clearly $\emptyset \notin E_k^{\mathbf{S}}(S) \supseteq E_k^{\mathbf{S}}(T) \ni K$ for any $S \in L(\mathbf{S}), T \in L^c(\mathbf{S})$, it follows that $E_k^{\mathbf{S}}$ is indeed a *simple WEF* on (N, K). In particular, for any $k \in K$

$E_k^{\mathbf{S}} = E_k^{\mathbf{S}}(L(\mathbf{S}), \{A \subseteq K : k \in A\}, K^*)$.

Conversely, let $\left\{E_k^{\mathbf{S}} : k \in K\right\}$ be a family of *simple* WEFs on (N, K). Then, for any $k \in K$ there exist an order filter $\mathcal{W}_k$ of $(P(N), \supseteq)$ with $\emptyset \neq \mathcal{W}_k \neq P(N)$, an order filter $\mathcal{Y}_k$ of $(P(K), \supseteq)$, and a nonempty set K_k^*, $k \in K_k^* \subseteq K$ such that for any *non-empty* $S, T \subseteq N$, $S \notin \mathcal{W}_k, T \in \mathcal{W}_k$:

$E_k^{\mathbf{S}}(T) = \mathcal{Y}_k \supseteq \{A \subseteq K : A \supseteq K_k^*\} = E_k^{\mathbf{S}}(S)$.

It follows that –by definition of $E_k^{\mathbf{S}}$–for any $S \notin \mathcal{W}_k$:

$\{A \subseteq K : A \supseteq h(\pi(\alpha^*(k, S)))\} = E_k^{\mathbf{S}}(S) = \{A \subseteq K : A \supseteq K_k^*\}$

whence $h(\pi(\alpha^*(k, S))) = K_k^*$

(indeed, suppose not; then, either $h(\pi(\alpha^*(k, S)) \parallel K_k^*$ or w.l.o.g. $h(\pi(\alpha^*(k, S))) \supset K_k^*$: in both cases $K_k^* \in \{A \subseteq K : A \supseteq K_k^*\} \setminus \{A \subseteq K : A \supseteq h(\pi(\alpha^*(k, S)))\})$.

Hence $\mathbf{S}$ is *perfect* with security level $q' = (\# K_k^*) - 1$ as required. ■

Apart from providing a convenient game-theoretic characterization of *all* perfect SSS at *any* security level, the foregoing Proposition also entails that *there exist 'universal" procedures which can 'uniformly' implement perfect SSS of arbitrary access structure using a unique most elementary threshold SSS as a 'building block'.* In order to substantiate that claim we shall refer to a prominent special class of implementations of perfect SSSs, namely (projective) combinatorial *geometric* schemes.

Remark 5 *Since threshold schemes are sufficient to generate perfect SSSs of any access structure and security level, one might also use the well -known Shamir's perfect threshold SSS which relies instead on modular addition as opposed to combinatorial projective structures (see e.g. Stinson(1995)). Indeed, Shamir threshold scheme –the very first example of a* perfect *SSS – is arguably as intuitively appealing and elegant as typical geometric threshold perfect schemes are, and is informationally efficient or* 'ideal' *(i.e. its* information rate– *the rate of the size of the key space to the size of the biggest individual share space– is* 1*, which is provably the* optimum *rate for perfect schemes). However, the basic Shamir scheme is known to be* manipulable *in the following sense: a cheater may transmit* false *information concerning his share and use knowledge of the correspondingly* incorrect *key in order to recover* by himself *the true key by using his* true *share. By contrast standard combinatorial geometric threshold schemes are typically* nonmanipulable *in that sense. Given the game-theoretic emphasis of the present note, I take that circumstance–over and above the undeniable simplicity and elegance of such geometric schemes– to be an almost compelling reason to choose combinatorial projective threshold schemes as the basic reference schemes in what follows.*

Unfortunately enough, a presentation of geometric threshold schemes requires a quite massive amounts of new definitions: they are provided below for the sake of completeness.

An *incidence structure* is a tuple $\mathbb{G}=(\mathbf{P},\mathbf{B},\Im)$ where $\mathbf{P},\mathbf{B}$ are *disjoint* sets (the sets of *points* and *blocks* –or *lines*–, respectively) and $\Im \subseteq (\mathbf{P}\cup\mathbf{B})^2$ is a *reflexive and symmetric* binary relation, the *incidence relation* on $\mathbf{P}\cup\mathbf{B}$. An incidence structure $\mathbb{G}=(\mathbf{P},\mathbf{B},\Im)$ is a *projective space* if the following properties hold:

(P1) (Line axiom): for any $P,Q\in\mathbf{P}$, if $P\neq Q$, then there exists $L\in\mathbf{B}$ –also denoted by (PQ)– such that $\Im\supseteq\{(P,L),(Q,L)\}$,and for any $L'\in\mathbf{B}$, $\Im\supseteq\{(P,L),(Q,L),(P,L'),(Q,L')\}$ entails $L=L'$.

(P2) (Points-on-a-line axiom): for any $L\in\mathbf{B}$ there exist $P,Q,R\in\mathbf{P}$, such that $\#\{P,Q,R\}=3$ and $\Im\supseteq\{(P,L),(Q,L),(R,L)\}$

(P3) (Veblen-Young No-parallelism axiom): for any $P,Q,R,S\in\mathbf{P}$ such that $\#\{P,Q,R,S\}=4$, if $(PQ)\cap(RS)\neq\emptyset$ then $(PR)\cap(QS)\neq\emptyset$

Furthermore, a projective space is said to be *nondegenerate* if the following condition is also satisfied

(P4) (Nondegeneracy axiom): $\#\mathbf{B}\geq 2$.

Now, let $\mathbb{P}=(\mathbf{P},\mathbf{B},\Im)$ be a projective space. A *linear subset* of $\mathbb{P}$ is a set $\mathbf{P}'\subseteq\mathbf{P}$ such that $(RS)\subseteq\mathbf{P}'$ for any $R,S\in\mathbf{P}'$,and the *linear subspace* generated by any set $\mathbf{Q}\subseteq\mathbf{P}$ is

$$\langle\mathbf{Q}\rangle=\bigcap\{\mathbf{U}\subseteq\mathbf{P}:\mathbf{U}\text{ is a linear subset of }\mathbb{P}\text{ such that }\mathbf{Q}\subseteq\mathbf{U}\}.$$

Moreover, the *(linear) subspace* of a projective space $\mathbb{P}$ generated by a linear subset $\mathbf{P}'\subseteq\mathbf{P}$ is a –possibly degenerate– projective space $\mathbb{P}'=(\mathbf{P}',\mathbf{B}_{\mathbf{P}'},\Im_{\mathbf{P}'})$ where $\mathbf{B}_{\mathbf{P}'}=\{L\in\mathbf{B}:P\in\mathbf{P}'$ for any P s.t. $(P,L)\in\Im\}$, and $\Im'=\Im\cap(\mathbf{P}'\cup\mathbf{B}_{\mathbf{P}'})^2$. An *independent set* of points of a projective space $\mathbb{P}=(\mathbf{P},\mathbf{B},\Im)$ is a set of points $\mathbf{Q}\subseteq\mathbf{P}$ such that for any $\mathbf{Q}'\subseteq\mathbf{Q}$, and any $P\in\mathbf{Q}\setminus\mathbf{Q}'$, $P\notin\langle\mathbf{Q}'\rangle$. An independent set $\mathbf{Q}$ of points of a projective space $\mathbb{P}=(\mathbf{P},\mathbf{B},\Im)$ is a *basis* of $\mathbb{P}$ if $\langle\mathbf{Q}\rangle=\mathbf{P}$. It can be shown that all the bases of a projective space have the same cardinality (see e.g. Batten(1997), Beutelspacher, Rosenbaum(1998)). A projective space $\mathbb{P}$ has *dimension d* –also written $\dim\mathbb{P}=d$– if the (common) cardinality of its bases is $d+1$. A *hyperplane* of a d-dimensional projective space $\mathbb{P}$ is a $(d-1)$-dimensional subspace of $\mathbb{P}$. A set $\mathbf{Q}\subseteq\mathbf{P}$ of points of a d-dimensional projective space $\mathbb{P}=(\mathbf{P},\mathbf{B},\Im)$ is *in general position* if $\#\mathbf{Q}\geq d+1$ and any $\mathbf{Q}'\subseteq\mathbf{Q}$ such that $\#\mathbf{Q}'=d+1$ is a basis of $\mathbb{P}$.

It can be shown that 'almost' any $d-$dimensional projective space $(d\geq 2)$ is isomorphic to the (projective) space $\mathbb{P}(V_{\mathcal{R}})$ which results from taking as *points* the 1-dimensional vector subspaces of a suitable $d+1$-dimensional (left) vector space $V_{\mathcal{R}}$ over a division ring $\mathcal{R}$, as *lines* the 2-dimensional vector subspaces of $V_{\mathcal{R}}$, and positing $\Im=\bigcup\{\subseteq,\supseteq\}$ (recall that a *division ring* is a tuple $\mathcal{R}=(\mathbf{R},+,\cdot,0,1)$ such that i) $(\mathbf{R},+,0)$ is a commutative group i.e. $+$ is an associative, commutative binary operation on $\mathbf{R}$ with identity element 0, and such that every element $x\in\mathbf{R}$ has an inverse; ii)$(\mathbf{R}\setminus\{0\},\cdot,1)$ is a (not necessarily commutative) group i.e. $\cdot$ is an associative binary operation on $\mathbf{R}$ with identity element 1, and such that every $x\in\mathbf{R}\setminus\{0\}$ has a bilateral inverse and iii) for any $x,y,z\in\mathbf{R}$ the right and left distributive identities $[x\cdot(y+z)=(x\cdot y)+(x\cdot z)]$ and $[(y+z)\cdot x=(y\cdot x)+(z\cdot x)]$ hold). If a projective space $\mathbb{P}$ is indeed isomorphic to $\mathbb{P}(V_{\mathcal{R}})$, then it is said to be *coordinatized by* $\mathcal{R}$ (see again Beutelspacher, Rosenbaum (1998)). If a projective space $\mathbb{P}$ is coordinatized by a division ring $\mathcal{R}$, then each point of $\mathbb{P}$ may be characterized by its *homogeneous coordinates* i.e. equivalence classes of (vector) coordinates of points in $V_{\mathcal{R}}$ (with equivalence relation $\approx$ defined by the rule $(a_1, .., a_{d+1}) \approx (b_1, .., b_{d+1})$ iff there exists $\alpha \in \mathcal{R}, \alpha \neq 0$ such that $a_i = \alpha b_i$, $i = 1, .., d+1$).

It can be shown that if a d-dimensional projective space $\mathbb{P}$ is coordinatized by a division ring $\mathcal{R}$, then *a most typical instance of a set of points in general position* is provided by the set $\mathcal{C}$ of points of a *normal rational curve* of $\mathbb{P}(V_{\mathcal{R}})$, namely–by definition– by those points whose homogeneous coordinates are either $[(1, r, .., r^d)]_{\approx}$ (with $r \in \mathcal{R}$) or $[(0, 0, .., 0, 1)]_{\approx}$. If the relevant division ring is in particular a *finite field* $\mathcal{F}$ (i.e. $\mathcal{R} = \mathcal{F}$ is finite hence commutative by the classic Wedderburn's theorem) then– for any nonnegative integer d– one may consider the finite vector space $\mathcal{F}^d$ so that $\mathbb{P}(\mathcal{F}^d)$ is a *finite* projective space (coordinatized by $\mathcal{F}$ whose cardinality–recall– may be given by *any* positive power of *any* prime number). Now, it should be recalled here that the sets of points of any two lines in an *arbitrary* projective space are bijective. Hence, in a *finite* projective space $\mathbb{P}(\mathcal{F}^d)$ all the lines comprise an equal number $k+1$ of points where k is the cardinality of $\mathcal{F}$(notice that $k+1 \geq 3$ in accordance with axiom (P2)): then, k is said to be the *order* of $\mathbb{P}(\mathcal{F}^d)$ which is also written $\mathbb{P}(\mathcal{F}^d, k)$ to make this fact explicit.

We are now ready to introduce the basic combinatorial geometric SSSs for threshold access structures that we need for our next result.

Definition 6 (Basic perfect projective threshold SSS) *Let N be a non-empty finite set of participants, $\mathcal{W} \subseteq P(N)$ a rational threshold order filter of $(P(N), \supseteq)$ with weight function w and quota $t = \frac{k_0}{m_0}$, and q any positive (rational) number. Next, consider $\left\{ w(i) = \frac{k_i}{m_i} : i \in N \right\}$, compute the least common multiple M of $\{m_0, m_1, .., m_n\}$ and take a finite projective space $\mathbb{P} = \mathbb{P}(\mathcal{F}^{t^*}, q^*)$ where*

$t^* = M^* \cdot t$ with $M^* = \min\{k \cdot M : k \in \mathbb{N}$ and $k \cdot M \geq \log_2 n\}$, and

$q^* = \min\{p \in \mathbb{N} : p \geq q$ and there exist $n, m \in \mathbb{N}$ such that n is prime and $p = n^m\}$.

Finally, take any point Q of $\mathbb{P}$ (i.e. $Q \in \mathbf{P}(\mathbb{P})$), and any line $L \in \mathbf{B}(\mathbb{P})$ such that $(Q, L) \in \Im(\mathbb{P})$ i.e. $Q \in (L)$ where $(L) = \{P \in \mathbf{P}(\mathbb{P}) : (P, L) \in \Im(\mathbb{P})\}$. Then a basic combinatorial projective threshold SSS $\mathbf{S}^{PG}(\mathcal{W}, q^*) = (\mathcal{S}, \alpha, \pi, h)$ *for $(N, (L))$ (with* access structure $(\mathcal{W}, P(N) \setminus \mathcal{W})$ *and* normalized security level q^*) *is defined as follows:*

let H be a hyperplane of $\mathbb{P}$ such that $Q \in H$ and $(L) \nsubseteq H$, and $\mathcal{C}$ a normal rational curve *of H (see the definition above) such that $Q \in \mathcal{C}$. Then, posit $\mathcal{S} = \mathcal{C}$, take $\alpha : N \to P(\mathcal{C} \setminus \{Q\})$ to be an injective function such that $\# \{\alpha(i)\} = M^* \cdot k_i$ for any $i \in N$, and –for any $S = \{1, .., s\} \subseteq N$– define $\pi(Y_1, .., Y_s) = \bigcup_{i \in S} Y_i$. Finally, $h : P(\mathcal{C}) \to P((L))$ is defined by the rule $h(\{P_{1,..,}P_l\}) = (L) \cup ((L) \cap \langle\{P_1, .., P_l\}\rangle)$.*

Remark 7 *Notice that $\dim H = t^* - 1$ hence $\# \{P_1, .., P_l\} = t^*$ entails $\langle\{P_1, .., P_l\}\rangle = H$. It follows that for any $Y \subseteq P(\mathcal{C})$ such that $\#Y = t^*$ one has $h(Y) = (L) \cap H = \{Q\}$. By contrast, if $\#Y < t^*$ then $\langle Y \rangle \cap (L) = \emptyset$, whence $h(Y) = (L)$.*

Notation 8 *We shall denote by $\mathbb{PGTS}(N)$ the class of basic perfect projective threshold SSSs with set of participants N as described above.*

It is a quite remarkable fact that a very simple $(1, n)-$threshold version of such perfect geometric SSSs defined above can in principle be used as the unique 'building brick' in order to implement perfect SSSs of *any* access structure at *any* security level.

This claim is made precise by the following

Proposition 9 *Let $\mathcal{W} \subseteq P(N)$ be any order filter of $(P(N), \supseteq)$, and $q \in \mathbb{Q}_+$. Then - for any* finite *set K- there exist $k \in \mathbb{Z}_+$,and (isomorphic) $\mathbf{S}_{1,..,}\mathbf{S}_k \in \mathbb{PGTS}(N)$ such that $\mathbf{S} = \bigotimes_{i=1}^k \mathbf{S}_i$ is a perfect SSS for (N, K) at security level q and with access structure $(\mathcal{W}, P(N) \setminus \mathcal{W})$.*

Proof. First, recall that order filters of $(P(N), \supseteq)$ do essentially correspond to simple games on N . But then, one should also recall that every simple game can be regarded as the intersection of a finite number of threshold or weighted simple games. The construction goes as follows: let $\{T_1, .., T_k\} \subseteq P(N) \setminus \mathcal{W}$ be the set of $\supseteq$-maximal coalitions which are not in $\mathcal{W}$. Then, for any $j = 1, .., k$ posit

$\mathcal{W}_j = \{S \subseteq N : S \setminus T_j \neq \emptyset\}$.

It is easily shown that $\mathcal{W} = \bigcap_{j=1}^k \mathcal{W}_j$

(see e.g. Taylor, Zwicker(1999), Theorem 1.7.2 for more details).

Now, notice that –for each $j-$ $(\mathcal{W}_j, P(N) \setminus \mathcal{W}_j)$ can be regarded as the access structure of a $(1, \#(N \setminus T_j))-$threshold SSS. Hence, take a corresponding $\mathbf{S}_j^{PG}(\mathcal{W}_j, q) \in \mathbb{PGTS}(N)$ having access structure $(\mathcal{W}_j, P(N) \setminus \mathcal{W}_j)$ as defined above. It follows that – by definition– the resulting product SSS $\bigotimes_{j \in J} \mathbf{S}_j^{PG}$ has both security level q and access structure $(\bigcap_{j=1}^k \mathcal{W}_j, P(N) \setminus \bigcap_{j=1}^k \mathcal{W}_j)$ as required. ■

It should be emphasized that the foregoing proposition provides a positive answer to the question raised in the introduction concerning indeed the availability of universal 'monogenic' implementation procedures.

3 Concluding remarks

The main message of the present note is that coalitional game-theoretic notions provide a remarkably natural framework for expressing a few basic ideas and results concerning key distribution protocols and related issues in distributed cryptography. In particular, Proposition 9 above shows that dimension-theoretic considerations concerning coalitional game forms suggest ways to obtain perfect SSSs of arbitrary access structure and security level starting from certain simpler perfect SSSs of one single type. Moreover, a game-theoretic outlook might also provide further interesting criteria for assessing perfect (and non perfect) SSSs. This is however best left as a topic for further research.

References

[1] Abdou J., H. Keiding (1991): *Effectivity Functions in Social Choice.*Dordrecht: Kluwer.

[2] Batten L.M. (1997): *Combinatorics of Finite Geometries (2nd edition).* Cambridge: Cambridge University Press.

[3] Benaloh J., J. Leichter (1990): Generalized Secret Sharing and Monotone Functions, in *Advances in Cryptology-CRYPTO '88. Lecture Notes in Computer Science 403.* Berlin, Heidelberg, New York: Springer Verlag.

[4] Beutelspacher A., U. Rosenbaum (1998): *Projective Geometry. From Foundations to Applications.* Cambridge: Cambridge University Press.

[5] Menezes A.J., P.C. van Oorschot, S.A. Vanstone (1997): *Handbook of Applied Cryptography.* Boca Ralton, FL.:CRC Press.

[6] Simmons G.J. (1992): An Introduction to Shared Secret and/or Shared Control Schemes, in G.J.Simmons(ed.): *Contemporary Cryptology.* New York: IEEE Press.

[7] Stinson D.R. (1995): *Cryptography. Theory and Practice.*Boca Ralton, FL.: CRC Press.

[8] Taylor A.D., W. Zwicker (1999): *Simple Games. Desirability Relations, Trading, Pseudoweightings.* Princeton: Princeton University Press.