Applications of finite geometries to information security

Christine M. O'Keefe
Department of Pure Mathematics
The University of Adelaide
GPO Box 498, Adelaide, SA 5001
AUSTRALIA

Abstract *Many problems in information security can be resolved using combinatorial structures, primarily geometries. In fact, often the most efficient solutions known are provided by schemes based on geometries. In this expository article we look at two problems in information security and discuss proposed geometrical solutions. In addition, we generalise two known constructions for Key Distribution Patterns, using Laguerre planes. The generalisation has the potential to provide new examples of Key Distribution Patterns, as well as simplifying the proofs of the constructions considerably.*

1. Introduction

This paper gives an introduction to some applications of finite geometries to information security. Section 1 describes the general framework of these applications and discusses why finite geometries might be useful in this context. In sections 2 and 3 we look at two applications in more detail, surveying known results on *secret sharing schemes* and on *key distribution patterns* which make use of finite geometries. Finally, section 4 contains the extensions of some known constructions of key distribution patterns (KDPs) into certain finite geometries known as Laguerre planes. These generalisations have the advantage that the verification of the KDP property is easier in the Laguerre plane context. Further, if there is a Laguerre plane of non-prime power order (currently an unsolved problem) then the generalisations give new examples of KDPs.

The field of information security is largely driven by the need to provide information security functions for a society which is increasingly dependent on digital information and communication. In particular, two structures designed to

provide some of these functions are secret sharing schemes and key distribution patterns.

Informally, a *secret sharing scheme* is a means by which only certain predetermined subsets of a set of authorised participants can access a secret. The secret could be either a piece of information, a key for a cryptosystem or a key allowing control of some action. Since we can think of the participants as points and the subsets with access to the secret as blocks, we immediately see that we can model such schemes with incidence structures. Just why we might want to use geometries for these incidence structures will be discussed in Section 2.

One of the most difficult and important problems facing users of cryptographic systems is the problem of key management, since a cryptosystem is useless or worse than useless if its keys have been compromised. *Key management* principles and procedures seek to provide a secure method of distributing keys among a number of participants in a cryptographic scheme. Section 3 investigates a natural way of modelling a key distribution pattern as a design. It has been found that geometry has played a part in the construction of some efficient key distribution patterns, in particular, [14] gave two constructions of Key Distribution Patterns based on families of conics in finite affine planes. In Section 4 we generalise these by providing constructions in any Laguerre plane. If there are Laguerre planes of non-prime power order (currently an unsolved problem) then the generalisation gives new examples of Key Distribution Patterns. In any case the constructions and the proofs are much easier in the general (Laguerre plane) setting.

Perhaps one of the first questions we should ask is, *Why should finite geometries be involved in the study of information security?* Do finite geometries just provide "nice" examples, or is there some intrinsic reason why they appear in efficient solutions to many of the problems in information security? Of course it would be extremely difficult to answer this question in general, so I will attempt to give what I believe are some partial answers, with supporting evidence.

It is extremely difficult to define the term 'finite geometry', and I prefer not to do so. However, examples of finite geometries include the finite projective and affine spaces and the finite inversive, Laguerre and Minkowski planes mentioned in this article.

The first thing to say is that it is easy to see why we should deal with *finite* objects. We have a finite number of participants, messages, bits, and so on, so we are talking about finite, or discrete, mathematics. Thus, we are mainly concerned with the *Why geometries?* part of the question.

We have already hinted at something which is possibly part of the answer. As soon as we have a set of elements and distinguished subsets of them, we have an incidence structure. If we are lucky, the properties that we require, say fixed parameters or interactions of the subsets, might force the incidence structure to be a design, or even a geometry. The properties of the problem might be best modelled by a geometry, with its levels of interaction between components of various types, as seen in the application to secret sharing schemes discussed in Section 2. Beutelspacher [3] pointed out that the complex structure of geometries can provide efficient models for hierarchical systems and structures.

In any case, usually we are looking for a *good* solution to our problem, for a suitable definition of good. Designs and, to a greater extent, geometries have a great deal of symmetry and have well-determined interactions between their components. Hence it is not inconceivable that geometries, with their rich structure, might provide good solutions to problems.

In [3], Beutelspacher gave an additional argument. He pointed out that geometries are often examples of more general structures with *extreme* values of parameters, that is, with parameters at an extreme of their possible values. Often these extreme cases are the ones we prefer, for practical reasons.

An added bonus is that the performance of a geometrical solution to a problem resides in the properties of the geometry itself, rather than in some hard problem (such as factoring a large integer) whose performance status changes over time. More precisely, a scheme is *unconditionally secure* if its security is independent of the computing power and effort an unauthorised opponent is willing to use to improperly break the scheme. In general, we might expect schemes constructed from geometrical structures to provide unconditional security or performance, rather than the conditional security provided by hard number-theoretical problems. We shall see that, in many situations, this is indeed the case.

A scheme which is based on a geometry inherits all the structure of the underlying geometry. As a consequence, it is found in practice that a geometrical scheme is easy to construct and easy to implement. In general there is less storage required, as much of the information resides in the geometrical structure, hence does not need to be stored.

Beutelspacher [3] noted that, in most applications, only the *structure* of the geometry is used. Often a question that arises in an application will translate to a geometrical problem, usually depending only on the incidences of the structure. Also, the applications concentrate on projective spaces over finite fields, perhaps

for the reason that they are well understood and calculations can be performed efficiently.

2. Secret Sharing Schemes

First, let's give a more precise definition of a secret sharing scheme. We adopt the terminology used in [14], due largely to Simmons.

The set $\mathcal{P}$ of *participants* in a secret sharing scheme are those who are authorised to take part in the scheme. The *secret* is the piece of information to be protected, or the action whose initiation is to be controlled, and the set of all possible secrets is the *secret set*. Given $\mathcal{P}$, the *access structure* Γ of a secret sharing scheme is a specification of those subsets of $\mathcal{P}$ which are authorised to determine the secret.

The final component of a secret sharing scheme is the security. The *security* s is defined to be the reciprocal of the maximum, taken over all subsets of $\mathcal{P}$ not in Γ of the probability that an unauthorised set of participants obtains the secret.

Hence we see that a secret sharing scheme on a participant set $\mathcal{P}$ is determined by the pair (Γ, s). In practice the participants are each issued with a *share,* and the shares of a set of participants are used to determine whether the set of participants is authorised.

An access structure (and hence any scheme with that access structure) is *monotone* if every set of participants which contains a subset in the access structure is itself in the access structure, that is,

$$A \in \Gamma \text{ and } A \subseteq A' \subseteq \mathcal{P} \Rightarrow A' \in \Gamma.$$

Non-monotone schemes have been considered to model situations in which there is a power of veto, see [4], but here we restrict our attention to monotone schemes.

We think of a secret sharing scheme, then, as the abstract notion of its access structure and security. A *construction* for a secret sharing scheme is some concrete realisation of the scheme. Usually, a construction for a scheme is a mapping of the shares and secret onto the elements of some incidence structure so that the properties of the scheme are reflected by the properties of the incidence structure, see Example 2.1.

It should be clear that, given a secret sharing scheme with access structure Γ and security s, there may be many different constructions for the scheme, see, for example, [15] and its references. The most elementary construction is the one which uses the complete listing of all subsets in the access structure. When a group of people tries to access the secret the list of authorised sets has to be checked. We hope to find more efficient algorithms than this one.

2.1 Example Suppose that we are given a participant set $\mathcal{P}$ where $|\mathcal{P}| = v \geq 3$. Suppose we wish to construct a secret sharing scheme with security 100 and with access structure Γ which is all subsets of $\mathcal{P}$ of size at least 3. (In fact this is a $(3, v)$-threshold scheme, where a (k, n)-*threshold scheme* is a secret sharing scheme on n participants whose access structure is the collection of subsets of $\mathcal{P}$ of size at least k, see [15].) It is easy to see that Γ is monotone. We now give a construction for this scheme.

In $PG(3, q)$, choose the points of a line l to be the secret set (this line l is assumed to be public knowledge). We assume that each secret in the secret set is used with equal probability. Once a secret S (point of l) is chosen, let π be a plane through S and meeting l only in S. We choose a set $\mathcal{K}$ of points on π such that $\mathcal{K} \cup \{S\}$ is a $(v+1)$-arc of π (that is, $\mathcal{K} \cup \{S\}$ is a set of $v+1$ points, no three collinear). The share of each participant is the coordinate triple of one point of $\mathcal{K}$. Note that the maximum size of a k-arc in π is $q+1$ if q is odd and $q+2$ if q is even (see [8], 8.1.3); so immediately we see that we must have q large enough, say $q \geq v+1$.

Now when at least three participants get together, their shares span the plane π. This group of participants can therefore determine the point S of intersection of the plane π with the line l and so recover the secret.

We consider the security of this construction. An unauthorised set of participants (a group of one or two participants) has as shares either a point of $PG(3, q)$ or two points spanning a line of $PG(3, q)$, not through S. This unauthorised set, in attempting to determine the secret, can do no better than just to guess S, knowing only that it lies on l. Since there are $q+1$ points on a line in $PG(3, q)$, so we can obtain a security of 100 by choosing $q \geq 99$.

We now consider some desirable properties of secret sharing schemes. An *outsider* in a secret sharing scheme is a non-participant in the scheme. A scheme is *perfect* if the probability that an outsider can improperly obtain the secret is at most the reciprocal of the security. In other words, the probability that an unauthorised set can improperly obtain the secret is no better than that of an

outsider. The construction given in Example 2.1 is perfect, since an outsider can at best guess the point S on l, with probability $1/(q+1)$, equal to the best an unauthorised set of participants can do.

Further, it is clear that the scheme of Example 2.1 is unconditionally secure, since the security is independent of the amount of computing power and effort that an opponent is willing to expend in order to improperly obtain the secret. They can do no better than just guess the secret among the points of l.

There are many geometrical constructions, such as Example 2.1, for secret sharing schemes with monotone access structure. Such constructions generally have the property that they are perfect and unconditionally secure. In addition, they are easy to construct and to implement. Also, since the geometrical structure can quickly check whether a subset is authorised, it is unnecessary to keep a list of the subsets in the access structure, so the storage requirements are generally quite low. For these reasons we introduce the definition of a geometric construction for a secret sharing scheme.

A *geometric construction* for a secret sharing scheme (Γ, s) on a participant set $\mathcal{P}$ is a construction in which the possible secrets and the shares are subspaces in a projective space $PG(n,q)$. The secret set is usually also a subspace and the possible secrets are subspaces of the secret set. Further, the construction is such that a subset of participants in $\mathcal{P}$ is in Γ if and only if the subspace of $PG(n,q)$ spanned by the points contained in their shares contains the secret. The value of q must be large enough to accommodate the number of participants with the given access structure among the subspaces of $PG(n,q)$. The security is achieved by choosing a value of q large enough, as in Example 2.1, to ensure a large enough number of secrets, each chosen with equal probability. In fact Example 2.1 is a geometric construction for the secret sharing scheme given there, as the secret set is a line, the secrets are points on that line and the shares are points of $PG(3,q)$. In addition, a set of participants is in Γ if and only if their shares span the plane π which contains the secret S.

So far we have not considered the existence of constructions for given secret sharing schemes. Also, if we prefer geometric constructions (for the reasons indicated above), we are lead to consider the following questions:

1. Given a secret sharing scheme with a monotone access structure, is it possible to find a construction for it? Is there an algorithm to find the construction?

2. Must there always be a perfect construction?

3. Must there always be a perfect, geometric construction?

In 1987, Ito, Saito and Nishizeki [9] showed that any secret sharing scheme with monotone access structure can be realised with a perfect construction, and gave an algorithm using the underlying structure of a (k, k)-threshold scheme. In 1990, Benaloh and Leichter [1] gave a different algorithm for such a construction, again using threshold schemes. Further, Simmons [16] conjectured in 1990 that any secret sharing scheme with monotone access structure could be realised with a perfect, geometric construction.

The proof of this conjecture was given in 1992 by Simmons, Jackson and Martin [11], who exhibited an algorithm for constructing a perfect, geometric secret sharing scheme for any given monotone access structure. This algorithm basically translates the algorithms given in [9] and [1] into geometric language, and shows that the construction can be found based on the manipulation of Boolean logical expressions. More precisely, an algorithm is given which operates on a logical description of the access structure to produce another logical expression that uniquely defines a geometrical construction for the scheme.

Now we know that any secret sharing scheme with a monotone access structure can be constructed with a perfect, geometric scheme. The next question to ask is, are these schemes any good in practical situations?

There are several performance or efficiency measures proposed for constructions of secret sharing schemes, see, for example, [5] or [6]. These are largely based on the aim of minimising the size of the shares issued to each participant. Unfortunately the perfect, geometric constructions for secret sharing schemes arising from the Simmons, Jackson and Martin algorithm do not perform very well according to these measures, see the conclusion of [11]. Importantly, however, it is still true that given a secret sharing scheme with a monotone access structure then geometric constructions are among the best known according to the proposed measures.

Thus we see that we have an algorithmic way of providing a perfect, geometric construction for a secret sharing scheme with monotone access structure, but these schemes are not very efficient in practice. However, as discussed in [10], since geometric constructions worked out on a case-by-case basis have been found to be good in practice, what is needed is an algorithm for finding a good (perfect, geometric) construction for a secret sharing scheme with a monotone access structure.

3. Key Distribution Patterns

The security of a cryptosystem, either symmetric or public key, is determined under the fundamental assumption that a possible opponent has complete knowledge of the algorithm being used. This is called *Kerckhoff's assumption,* and the consequence of this assumption is that the security of a cryptographic system resides entirely in the key. It follows that *key management,* the theory of secure generation, distribution and storage of cryptographic keys, is of prime importance.

Most of the solutions proposed so far use a *key distribution centre,* or KDC, to generate and distribute the keys. The KDC would probably also be required to store, for some period of time, the keys which it generates.

Consider a network of $v \geq 3$ nodes $P_1, P_2, \ldots, P_v$, each of which must be able to communicate with any other node in a secure way. (The case $v = 2$ is trivial, as only a single key is required.) We assume that this communication is done via a *symmetric* cryptosystem, that is, each pair of nodes P_i, P_j must be in possession of a common (secret) key K_{ij} which they use for encryption and decryption of the messages sent between them. One way to achieve this would be to distribute to each pair of nodes a key, unique to that pair. We call this the *trivial* system for key distribution. In this system, the KDC would need to generate (and possibly store) $v(v-1)/2$ secret keys and we require each node to store $v-1$ keys. This system has the advantage that, after the initial key distribution, each node is ready to communicate with each other node. The main disadvantage is that a large amount of key storage is required at each node and at the KDC.

An alternative to the above system would be for the KDC to generate a key for a pair of communicating nodes only when it is required, and destroy the key after each use. The storage required is quite small, since each node need only store a key for communicating with the KDC plus the session keys for the nodes with which it is currently communicating. The problems of the responsiveness of the KDC (it is no good waiting half an hour for a key for an urgent message), the delay in communication and the bottleneck situation created by the large amount of communication traffic with the KDC currently seem difficult to resolve.

For this reason, we will concentrate our attention on combinatorial models similar to the trivial system of initial distribution of keys to each pair of nodes. In other words, we seek a system under which each node can communicate with each other node without first needing to contact the KDC, but we require that the key storage needed at each node should be as small as possible. Mitchell and Piper [13] have proposed an elegant solution in which each node is issued with a relatively

small number of *subkeys* (binary strings of a specified length) and each key used by a pair of nodes is generated from a combination of some of these subkeys. This combination is usually a one-way function to ensure that an opponent obtaining a secret key would be unable to recover the subkeys.

Suppose we think of the set of nodes as the set $\mathcal{P}$ of *points* and the set of subkeys as the set $\mathcal{B}$ of *blocks* of a (finite) incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$. A point is *incident* with a block if the corresponding node posesses the corresponding subkey. The key to be used for communication between two nodes P_1, P_2 is generated from the subkeys in $(P_1) \cap (P_2)$ (where (P) denotes the set of blocks incident with P). We make the following definition, following [12], and identifying the nodes with the points and the subkeys with the blocks.

A *key distribution pattern,* or KDP, on v points is a finite incidence structure $\mathcal{K}$ with $v \geq 3$ and such that, for any two distinct points P_1, P_2 of $\mathcal{K}$, we have

$$(\mathcal{K}1) \qquad (P_1) \cap (P_2) \not\subseteq (Q) \text{ for any } Q \in \mathcal{P} \backslash \{P_1, P_2\}.$$

The condition on the KDP ensures that the key K_{ij} used by the pair of nodes P_1, P_2 cannot be determined from the subkeys of any other node. For if Q is another node, the condition $(\mathcal{K}1)$ ensures that P_1, P_2 share at least one subkey not in the subkey set belonging to Q.

There is an immediate geometrical interpretation of $(\mathcal{K}1)$. If we recall that the *line* on points A, B of $\mathcal{P}$ is the set of points in the intersection of all blocks on A, B; we see that condition $(\mathcal{K}1)$ is equivalent to the condition that each line of $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ has size 2.

It is desirable in an application that each of a pair of nodes be able to determine the common key *non-interactively,* that is, with no interaction between the nodes. This is achieved by a key distribution pattern as follows. The blocks used in the key distribution pattern are really just names for the subkeys, and each node is issued with the values of only those subkeys which it posesses. Then the key distribution pattern is made public information. When a node wishes to communicate with another node it uses the public information to determine the names of the subkeys that it has in common with with that other node, then uses the (private) values of those subkeys to determine the common secret key, using some one-way function.

The trivial system for key distribution proposed above (in which each pair of nodes has a common key) has the trivial $2 - (v, 2, 1)$ design as its KDP. To see

this, let $\mathcal{P} = \{P_1, \ldots, P_v\}$ be the set of points, let $\mathcal{B} = \{x_{ij} \mid 1 \leq i < j \leq v\}$ be a set of subkeys and define $P_i \mathcal{I} x_{jk}$ if and only if $i = j$ or $i = k$. Then, if nodes P_1, P_2 say wish to communicate, each uses the (unique) common subkey x_{12} to determine (via some one-way function) their common key K_{12}.

The problem is to give examples of KDPs with storage requirements at each node as small as possible. The KDP of the trivial $2-(v,2,1)$ design requires storage of $(v-1)$ subkeys at each node, and is the standard with which other KDPs are compared.

As an example, consider the incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ where we have $\mathcal{P} = \{P_1, \ldots, P_v\}$, $\mathcal{B} = \{x_1, \ldots, x_v\}$ and where $P_i \mathcal{I} x_j$ if and only if $i \neq j$ (this is a trivial symmetric $2-(v, v-1, v-2)$ design). Now this design is a KDP on v points, since for any i, j we have $|(P_i) \cap (P_j)| = v-2$ (in fact $(P_i) \cap (P_j)$ contains every block except x_i and x_j) and any third point P_k is incident with only $v-3$ of these $v-2$ blocks, as (P_k) does not contain x_k. Although this KDP only requires a total of v subkeys at the KDC, it still requires the storage of $v-1$ subkeys at each node.

There have been other KDPs proposed. In [12], it is shown that any *biplane* (a $2-(v,k,2)$ design) is a KDP in which the KDC generates v subkeys and in which each node stores only r subkeys where r satisfies $r(r-1) = 2(v-1)$. (To see that a biplane is a KDP, note that every pair of points is incident with exactly two blocks, and any third point is incident with at most one of these two blocks, for if not, there would be a pair of blocks incident with three points.) Quinn [13] gives a construction for KDPs, better than the trivial KDP, using Hadamard matrices.

In terms of the storage requirements, biplanes are 'good' 1-KDPs, but the problem is that there are only a finite number of examples of biplanes known, and the largest of these has only 79 points. Although Mitchell and Piper [12] gave some methods for combining w-KDPs to obtain w-KDPs on a larger number of points, there is still a restriction on the parameters of any example obtained in this way, and possibly some of the performance is lost. Quinn [13] has given a construction of an infinite family of good 1-KDPs based on conics in finite desarguesian projective planes. The storage requirements for these new KDPs both at the KDC and at each node are approximately the same as for the biplane KDP for the same number of nodes and give a significant saving over the storage requirements of the trivial KDP.

The above KDPs protect a key from attack by a single other participant in the system, in the sense that the subkeys at one particular node cannot be used

to generate the key of another pair of users. This idea can be generalised to one which protects each key from attack by a number of participants in collusion, as in [12].

Let $v \geq 3$ and let w be an integer with $1 \leq w \leq v-2$. A *w-KDP* on v points is a finite incidence structure $\mathcal{K}$ with v points such that, for any pair of points P_1, P_2 we have

$$(P_1) \cap (P_2) \not\subseteq \bigcup_{i=1}^{w} (Q_i) \text{ for any points } Q_1, \ldots, Q_w \in \mathcal{P} \backslash \{P_1, P_2\}. \qquad (\mathcal{K}2).$$

This condition $(\mathcal{K}2)$ ensures that P_1 and P_2 share at least one subkey not in any of $(Q_1), \ldots, (Q_w)$. Note that every KDP is a w-KDP for some maximal value of $w \geq 1$, and we use the maximal value of w in claiming that a structure is a w-KDP.

Notice that the trivial KDP on v points is a $(v-2)$-KDP, since any number of nodes, distinct from a given two nodes P_1, P_2, in collusion do not posess the common subkey x_{12} of P_1 and P_2. The trivial symmetric designs and the biplanes are all 1-KDPs. Further, Mitchell and Piper [12] showed that every t-design with $t \geq 3$ is a $(t-2)$-KDP and that every $3-(v,k,\lambda)$ design for which $\lambda_2 > w\lambda$ is a w-KDP.

Mitchell and Piper [12] also pointed out some immediate geometrical consequences of their definition. Recall that if $P \in \mathcal{P}$, the *external structure* $\mathcal{K}^P$ of $\mathcal{K}$ at P is the incidence structure with point set $\mathcal{P} \backslash \{P\}$ and block set $\{B \in \mathcal{B} \mid P \notin B\}$. It is not difficult to show (see [12]) that if $w \geq 1$ then an incidence structure $\mathcal{K}$ is a $(w+1)$-KDP if and only if $\mathcal{K}^P$ is a w-KDP for each $P \in \mathcal{P}$.

Mitchell [11] has discussed the effectiveness of using 3-designs as KDPs. In particular, we consider an *inversive plane* of order q, that is, a $3-(q^2+1, q+1, 1)$ design. The following results, giving an example of the usefulness of external structures, are stated in [13]:

3.1 Construction [13], 3.1.7 An inversive plane of order q is a q-KDP on q^2+1 points with $q(q^2+1)$ subkeys and $q(q+1)$ subkeys at each node.

Proof: It is easy to see that an inversive plane has q^3+q blocks and $q(q+1)$ blocks on a point. Since two points lie on $q+1$ blocks, and any three points lie on a unique block, it follows that the blocks on a pair of points cannot be contained in the union of the blocks on any q other points. □

3.2 Construction [13], 3.3.4 Let P be any point of an inversive plane $\mathcal{I}$ of order q. Then $\mathcal{I}^P$ is a $(q-1)$-KDP on q^2 points with $q^2(q-1)$ subkeys and q^2-1 subkeys at each node.

Proof: It is clear that $\mathcal{I}^P$ has q^2 points and $q^3+q-(q(q+1))=q^3-q^2$ blocks, with each pair of points on $q(q+1)-(q+1)=q^2-1$ blocks on a point. The result follows from the result of Mitchell and Piper. □

Thus the external structure of an inversive plane at one of its points provides a KDP with slightly better storage requirements than those of the inversive plane KDP. Notice, however, that one node is lost. Constructions 3.1 and 3.2 give infinite families of KDPs, as there is an inversive plane of every prime power order, see [7]. It is an unsolved problem in finite geometry whether there are any inversive planes of non-prime power order.

Quinn [13] also gave constructions of new w-KDPs using families of conics in finite desarguesian affine planes. We discuss these constructions further in Section 4. All of these are examples of KDPs which have significantly better key storage requirements than the trivial KDP.

Quinn noted the following open problems. Let $\mathcal{K}$ be a w-KDP on v points. We require lower bounds for the following, as functions of v and w:
(1) the average (bit) storage at a node
(2) the total (bit) storage.

Also, we also need an upper bound (as a function of v) for
(3) w, the number of colluding nodes which can be protected against while still having reasonable storage.

Once good bounds are known, the problem will be to find KDPs near or attaining these bounds.

In conclusion, we have seen that not only do geometrical objects provide examples of KDPs, but geometrical concepts such as lines, external structures, have a role to play in the theory of KDPs.

4. Laguerre planes and w-KDPs

We have already seen that inversive planes give rise to w-KDPs as in Constructions 3.1 and 3.2. In this section we give constructions of w-KDPs using other so-called circle geometries, *the Laguerre planes.*

Quinn [13] 3.5.6 and 3.5.8 gave constructions for two families $\mathcal{K}_3(q,u)$ and $\mathcal{K}_4(q,u,t)$ of $(u-1)$-KDPs on q^2 nodes, where q is a prime power, using lines and families of conics in u copies of the desarguesian affine plane of order q. In fact her constructions are particular cases of the following more general constructions, 4.1 and 4.2, for w-KDPs in any Laguerre plane of order s. For geometrical preliminaries needed in this section, see [7] or [8] and [2] or [17].

A *(finite) Laguerre plane* is an incidence structure of *points, lines,* and *circles* satisfying:

(i) each point is on a unique line, and a line and a circle have a unique common point

(ii) any three points, no two collinear, lie on a unique circle

(iii) if P and Q are two non-collinear points and if $\mathcal{C}$ is a circle containing P but not Q then there is exactly one circle $\mathcal{C}'$ incident with P, Q and having only P in common with $\mathcal{C}$

(iv) there exist a point P and a circle $\mathcal{C}$ not containing P, and each circle contains at least three points.

Given a Laguerre plane, there is an integer s such that each circle has $s+1$ points. We call s the *order* of the Laguerre plane, which we then denote by $\mathcal{L}(s)$. It follows easily that a Laguerre plane $\mathcal{L}(s)$ has $s(s+1)$ points, $s+1$ mutually disjoint lines and s^3 circles. Each line has s points, there is a unique line and s^2 circles on a point and there are s circles on a pair of points.

Given a w-KDP $\mathcal{K}$ on v points, we let b denote the *total storage* of $\mathcal{K}$, where the total storage is the total number of subkeys in $\mathcal{K}$. Also, we let r denote the *node storage,* that is, the number of subkeys held at each node in $\mathcal{K}$. In general, good KDPs seek to minimise these storages, with a low value of r possibly more desirable than a low value of b.

4.1 Construction Choose u collinear points $R_1, \ldots, R_u$ in $\mathcal{L}(s)$, where $2 \leq u \leq s$. Let $\mathcal{K}_1 = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be the incidence structure with *points* the points of $\mathcal{L}(s)$ not on the line containing the points R_i, *blocks* the circles of $\mathcal{L}(s)$ containing R_i for some i together with the pairs $\{P_i, P_j\}$ where P_i, P_j are collinear in $\mathcal{L}(s)$. Then $\mathcal{K}_1$ is a $(u-1)$-KDP on s^2 points with $b = us^2 + s^2(s-1)/2$ and $r = us + s - 1$.

Each pair of points in $\mathcal{K}_1$ lies on 1 or u common blocks.

Proof: First we show that $\mathcal{K}_1$ satisfies the property $(\mathcal{K}2)$ given in Section 3 for $w = u - 1$. Let P_1, P_2 be points of $\mathcal{K}_1$. If P_1, P_2 are collinear in $\mathcal{L}(s)$ then $(P_1) \cap (P_2)$ is just the block $\{P_1, P_2\}$, which is not in (Q) for any $Q \in \mathcal{P} \backslash \{P_1, P_2\}$, hence is not in the union of the sets (Q_i) for any $u - 1$ points $Q_1, \ldots, Q_{u-1} \in \mathcal{P} \backslash \{P_1, P_2\}$ and condition $(\mathcal{K}2)$ is satisfied. If P_1, P_2 are not collinear in $\mathcal{L}(s)$, then $(P_1) \cap (P_2)$ is the set of u circles on the three points P_1, P_2, R_i for each $i = 1, \ldots, u$. Suppose that condition $(\mathcal{K}2)$ is not satisfied, so there is a collection of $u - 1$ points $Q_1, \ldots, Q_{u-1} \in \mathcal{P} \backslash \{P_1, P_2\}$ such that

$$(P_1) \cap (P_2) \subseteq \bigcup_{i=1}^{u-1} (Q_i).$$

It follows that there are two circles, on P_1, P_2, R_i and P_1, P_2, R_j say, which are contained in (Q_k) for some $1 \leq k \leq u - 1$. But then these circles have three points in common, namely P_1, P_2, Q_k, contrary to the property (ii) of a Laguerre plane.

Finally we check the parameters. The number of points is the number of points of $\mathcal{L}(s)$ not on a line, which is $s^2 + s - s = s^2$. The number b is the number of circles on the points $R_1, \ldots, R_u$ plus the number of pairs $\{P_i, P_j\}$ of collinear points. This is $us^2 + s^2(s-1)/2$. Also, r is the number of circles on a fixed point P_i and one of the points $R_1, \ldots, R_u$ plus the number of pairs $\{P_i, P_j\}$ where P_j is collinear with P_i, which is $us + s - 1$. □

4.2 Construction Choose u collinear points $R_1, \ldots, R_u$ in $\mathcal{L}(s)$, where $2 \leq u \leq s$. Let $\pi_1, \ldots, \pi_t$ be $t \geq 2$ permutations of the set $\mathcal{P}$ of points of $\mathcal{L}(s)$ not lying on the line containing the points R_i and with the additional property that

for each ordered pair (i, j) with $1 \leq i, j \leq t$ and for each pair P_1, P_2 of points in $\mathcal{P}$ if $\pi_i(P_1)$ is collinear with $\pi_i(P_2)$ then $\pi_j(P_1)$ is not collinear with $\pi_j(P_2)$.

Let $\mathcal{K}_2 = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be the incidence structure as follows. The *points* are the points of $\mathcal{P}$, the *blocks* are the sets $\pi_i^{-1}(\mathcal{C}_j)$ for some $i \in \{1, \ldots, t\}$ and where $\mathcal{C}_j$ is a circle through the point R_j for some $j \in \{1, \ldots, u\}$. (Note that some blocks may not be distinct.) Then $\mathcal{K}_2$ is a $(u-1)$-KDP on s^2 points with $b = tus^2$ and $r = tus$. Each pair of points lies on either $(t-1)u$ or tu common blocks.

Proof: We show that $\mathcal{K}_2$ satisfies the property $(\mathcal{K}2)$ given in Section 3 for $w = u - 1$. Let P_1, P_2 be points of $\mathcal{K}_2$. By the properties of the permutations, it follows that either $\pi_i(P_1)$ is not collinear with $\pi_i(P_2)$ for any $i = 1, \ldots, t$ or that $\pi_k(P_1)$ is collinear with $\pi_k(P_2)$ for exactly one value $k \in \{1, \ldots, t\}$ (and so $\pi_i(P_1)$ is not collinear with $\pi_i(P_2)$ for any $i \in \{1, \ldots, t\} \backslash \{k\}$). If $\pi_i(P_1)$ is not collinear

with $\pi_i(P_2)$ for some value i then $(P_1) \cap (P_2)$ contains the set of blocks $\pi_i^{-1}(\mathcal{C}_j)$ where $\mathcal{C}_j$ is a circle through $\pi_i(P_1), \pi_i(P_2), R_j$ for each $j \in \{1, \ldots, u\}$ (a total of u blocks). It follows that for any pair of points P_1, P_2 then $(P_1) \cap (P_2)$ contains either $(t-1)u$ or tu circles on P_1 and P_2. Although some of these circles may be repeated, $(P_1) \cap (P_2)$ contains at least u distinct circles, one through each of $R_1, \ldots, R_u$. As in the proof of Construction 4.1, if condition $(\mathcal{K}2)$ is not satisfied, there is a collection of $u-1$ points $Q_1, \ldots, Q_{u-1} \in \mathcal{P} \backslash \{P_1, P_2\}$ such that

$$(P_1) \cap (P_2) \subseteq \bigcup_{i=1}^{u-1} (Q_i).$$

It follows that there are at least two circles, on the points $\pi_i(P_1), \pi_i(P_2), R_i$ and the points $\pi_i(P_1), \pi_i(P_2), R_j$ say, which are contained in (Q_k) for some $1 \leq k \leq u-1$. But then these circles have three points in common, namely $\pi_i(P_1), \pi_i(P_2), Q_k$, contrary to the property (ii) of a Laguerre plane.

We calculate the parameters of this w-KDP. The number of points is the number of points of $\mathcal{L}(s)$ not on a line, which is s^2. The number b is t times the number of circles on one of the points $R_1, \ldots, R_u$, which is tus^2. Also, r is t times the number of circles on a fixed point and one of the points $R_1, \ldots, R_u$, which is $us + s - 1$. □

If the w-KDP $\mathcal{K}_2$ has no repeated blocks, then it is in fact a $((t-1)u-1)$-KDP, and in general $\mathcal{K}_2$ will be a w-KDP for some maximum value w with $u-1 \leq w \leq ((t-1)u-1)$. For ease of notation we refer to $\mathcal{K}_2$ as a $(u-1)$-KDP.

There is an infinite family of Laguerre planes known, see [2] or [17]. In particular, let $\mathcal{O}$ be an oval in a plane $PG(2,q)$ embedded in $PG(3,q)$, where q is a power of a prime, let $P \in PG(3,q) \backslash PG(2,q)$ and let T denote the cone which projects $\mathcal{O}$ from P. The set of points $\mathcal{P} = T \backslash P$, the set of lines through P and a point of $\mathcal{O}$ and the set of intersections of T with the planes in $PG(3,q)$ not through P form a Laguerre plane $\mathcal{L}(\mathcal{O})$ of order q. A Laguerre plane isomorphic to a $\mathcal{L}(\mathcal{O})$ is called *ovoidal,* and is *classical* if the oval is an irreducible conic. It follows that the constructions 4.1 and 4.2 provide an infinite family of q-KDPs on q^2 points, for q a power of a prime.

Further, many w-KDPs on different numbers of points can be constructed using 4.1 or 4.2. If we require a w-KDP on v points, we choose $s^2 \geq v$ such that there is a Laguerre plane of order s and construct a w-KDP on s^2 points. If $s^2 > v$, there will be nodes which are not presently used. Such nodes could be added to the network later as required. As a penalty, the total and node storages increase.

We now investigate how these constructions generalise the constructions in [13] 3.5.6 and 3.5.8. Given a point Q of the Laguerre plane $\mathcal{L}(s)$, the *internal structure* $\mathcal{L}_Q$ at Q is the incidence structure with *points* the points of $\mathcal{L}(s)$ not collinear with Q, *lines* the lines of $\mathcal{L}(s)$ not containing Q and the circles of $\mathcal{L}(s)$ containing Q. Under the incidence induced by the incidence of $\mathcal{L}(s)$, this is an affine plane of order s, and we note that each internal structure of a classical Laguerre plane is desarguesian.

It is not difficult to see that Quinn's coordinate-based constructions are actually performed in the internal structures of a classical Laguerre plane at the points $R_1, \ldots, R_u$ of the constructions. Thus they follow from the Constructions 4.1 and 4.2 in the special case that $\mathcal{L}(s)$ is classical. Since all Laguerre planes of order s will give rise to KDPs on s^2 nodes with the same storage requirements, if s is a power of a prime then it is probably expedient to use the classical Laguerre plane and the coordinatisations exhibited in [13]. However the constructions and proofs of the w-KDP property are easier using the methods introduced in this section. In addition, if there are Laguerre planes of non-prime power order (currently an unsolved problem in finite geometry), then Constructions 4.1 and 4.2 will give new examples of w-KDPs.

Quinn, [13] 3.4.7, has addressed the general problem of the existence of such a set of permutations as required in Construction 4.2. As a corollary, it follows that the set $\mathcal{P}$ of points of a Laguerre plane not on a fixed line certainly admits at least 2 and at most $s+1$ such permutations. (If the Laguerre plane is classical then $s+1$ permutations are admitted.) The value $t = 2$ certainly minimises the number of subkeys stored at the KDC and at each node for given values of s and u. However further analysis of the number of bits needed for the keys and subkeys is required to determine whether $t = 2$ also minimises the bit storage requirements, see [13].

In conclusion, we note that the w-KDPs found in Constructions 4.1 and 4.2 may also be useful in practice, since they are easy to implement and have significantly lower storage requirements than the trivial KDP, as exhibited in the following table.

In the table, m is the maximum number of subkeys used to determine each key (namely, the maximum value of $|(P_1) \cap (P_2)|$ in the w-KDP). The first rows of the table (above the bar) give restrictions on the parameters of the w-KDP and the rows below the bar give properties of the w-KDPs.

	$\mathcal{K}_1$	$\mathcal{K}_2$
u	$2 \leq u \leq s$	$2 \leq u \leq s$
t		$2 \leq t \leq s+1$
w	$u-1$	$u-1$
max v	s^2	s^2
r	$us+(s-1)$	tus
b	$us^2 + \frac{s^2(s-1)}{2}$	tus^2
m	u	tu

To compare, recall that the trivial KDP on s^2 points will have $r = (s^2-1)$, $b = s^2(s^2-1)/2$ and $m = 1$. If small values of w are acceptable, we can achieve a much lower key storage and total storage using the geometrical w-KDPs $\mathcal{K}_1$ and $\mathcal{K}_2$.

Acknowledgements: The author wishes to thank Keith Martin for useful discussions about many facets of information security.

The author also acknowledges the support of the Australian Research Council.

5. References

[1] J. Benaloh and J. Leichter, Generalized Secret Sharing and Monotone Functions, Crypto '88, Santa Barbara, CA, August 21–25, 1988, in *Advances in Cryptology,* Ed. by G. Goos and J. Hartmanis, Vol. 403, Springer-Verlag , Berlin, 1990, 27–35.

[2] W. Benz, *Vorlesungen über Geometrie der Algebren,* Springer-Verlag, Berlin-Heidelberg, 1973.

[3] A. Beutelspacher, Applications of finite geometry to cryptography, *Geometries, Codes and Cryptography,* Ed. by G. Longo, M. Marchi and A. Sgarro, CISM Courses and Lectures No. 313, Springer-Verlag, Wien - New York 1990, 161–186.

[4] A. Beutelspacher, How to say 'no', **in** Lecture notes in computer science 434; Advances in cryptology; Proc. Eurocrypt '89, Berlin: Springer-Verlag, 1990, 491–496.

[5] G. Blundo, E. de Santis, D.R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, J. Cryptology, to appear.

[6] E.F. Brickell and D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, to appear, *J. Cryptology.*

[7] P. Dembowski, Finite Geometries, Springer, Berlin, 1968.

[8] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, Oxford, 1978.

[9] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proceedings IEEE Global Telecommunications Conference, Globecom '87,* IEEE Communications Soc. Press (1987), 99–102.

[10] W.-A. Jackson and K.M. Martin, Geometric secret sharing schemes and their duals, preprint (1991).

[11] C.J. Mitchell, Combinatorial techniques for key storage reduction in secure networks. Technical memo, Hewlett Packard Laboratories, Bristol, 1988.

[12] C.J. Mitchell and F.C. Piper, Key storage in secure networks, *Discrete Applied Mathematics* **21** (1988), 215–228

[13] K.A.S. Quinn, *Combinatorial Structures with Applications to Information Theory* PhD Thesis, RHBNC, University of London, 1991.

[14] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their application, Chapter 9 in *Contemporary Cryptology: The Science of Information Integrity,* Ed. by G.J. Simmons, IEEE Press, New York, 1992, 441–497.

[15] G.J. Simmons, Geometric shared secret and/or shared control schemes, Crypto '90, Santa Barbara, CA, August 11-15, 1990, *Advances in cryptology,* Vol 537 Ed. by S.A.Vanstone, Springer-Verlag, Berlin, 1991, 216–241.

[16] G.J. Simmons, W.A. Jackson and K. Martin, The geometry of shared secret schemes, *Bull. I.C.A.* **1** (1991), 71–88.

[17] J.A. Thas, Circle geometries and generalized quadrangles, *Finite Geometries,* Dekker, New York, 1985, 327–352.

(Received 1/9/92)