Discrete Applied Mathematics 21 (1988) 215–228
North-Holland

KEY STORAGE IN SECURE NETWORKS

Chris J. MITCHELL
Hewlett Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, England, United Kingdom

Fred C. PIPER
Royal Holloway and Bedford New College, London University, Egham Hill, Egham, Surrey TW20 0EX, England, United Kingdom

Received 30 January 1987
Revised 2 June 1987

In this paper the key storage problem associated with the provision of secure communications between every pair of users in a large network is described, and a possible method of alleviating the problem is discussed. This method, based on the use of finite incidence structures with special properties called key distribution patterns, is shown to generalize earlier work in the area. The more general formulation of the storage saving scheme contained here enables use to be made of the extensive body of knowledge already existing on the theory of block designs. From this theory we are able to extract a number of new families of examples of potentially useful key distribution systems.

Keywords. Key management, cryptography, network security, key distribution.

1. Introduction

Suppose there exists a network of v nodes, $P_1, P_2, \ldots, P_v$ say, where each node wishes to have the facility to communicate with each other node in a secure way. As an immediate consequence, each pair of users $\{P_i, P_j\}$ requires a distinct cryptographic key known to them but to no other user.

If conventional (i.e. symmetric or private key) cryptography is being used, then the key management problem is commonly solved by using a key distribution centre (KDC). This KDC knows a distinct key encrypting key for each of the users in the network. When a pair of users wish to communicate securely, the KDC manufactures a key to be used by this pair of users, and then sends it to these users encrypted under their respective key encrypting keys.

However, this scheme requires an online KDC and a network which is responsive enough to enable keys to be distributed only when they are actually needed. It is not difficult to imagine situations where this is not a viable assumption. In such circumstances one solution would be for every user to be equipped in advance with a separate key for use with each other user in the network. Note that a KDC would

almost certainly still be required to coordinate all the key manufacturing and distribution processes.

This type of system clearly requires each user to store $v-1$ keys and usually for the KDC to store $\frac{1}{2}v(v-1)$ keys. In large networks, where it might also be necessary to store "old versions" of keys, the total storage requirement could increase to some multiple of $\frac{1}{2}v(v-1)$. Ultimately, these requirements could give rise to considerable storage problems at both the KDC and at the user node. Possible solutions to this problem have been discussed by a number of authors, e.g. Blom [2, 3], and Jansen [8]; we consider further solutions in the rather more general context previously outlined in a recent paper, [9], where the limitations of Jansen's construction were noted.

We propose the use of a certain special kind of *finite incidence structure* to resolve this problem. Each user is then issued with a relatively small set of "subkeys", and each key to be used by a pair of users is made up from a combination of some of these subkeys. Note that Blom's ideas, [2, 3], do not precisely fit this type of model since he assumes the existence of some kind of algebraic structure on the subkeys. To proceed we require some notation.

A *finite incidence structure* $\mathscr{K}=(\mathscr{P}, \mathscr{B}, I)$ consists of two finite non-empty sets $\mathscr{P}$ and $\mathscr{B}$ and an *incidence relation* I where $I \subset \mathscr{P} \times \mathscr{B}$. We conventionally let $|\mathscr{P}|=v$ and $|\mathscr{B}|=b$, and call the elements of $\mathscr{P}$ *points* and the elements of $\mathscr{B}$ *blocks*. If $(P, x) \in I$, where $P \in \mathscr{P}$ and $x \in \mathscr{B}$, then we say that P *is incident with* x. It is often convenient to consider the set of points incident with a block x, or the set of blocks incident with a point P, and we use (x) and (P) respectively to denote these sets. Hence we write $(P_i) \cap (P_j)$ for the set of blocks incident with both P_i and P_j.

As well as using v and b for the total number of points and blocks respectively, we write $r(i)$ for $|(P_i)|$, i.e. the number of blocks incident with P_i, and $k(j)$ for $|(x_j)|$. Finally, we also let $\lambda(i, j)=|(P_i) \cap (P_j)|$ and $s(i, j)=|(x_i) \cap (x_j)|$.

If every block is incident with the same number of points (i.e. $k(i)=k$ for some constant k) and no two blocks are incident with the same set of points then $\mathscr{K}$ is called a *design*, and these special incidence structures have been well studied, particularly because of their applications in statistical design of experiments. The interested reader is referred to two recent books on this subject, [1, 7]; where relevant we use here the notation of Hughes and Piper, [7], and unless otherwise stated, all results on designs used here can be found in their book. In line with common practice in design theory, if every point is incident with the same number of blocks, then we write r for this number (i.e. $r=r(j)$ for all j).

If $\mathscr{K}$ is a finite incidence structure with $v \geq 3$, then we call $\mathscr{K}$ a *key distribution pattern* (KDP) iff the following property holds:

Property 1.1. *If* $P_i, P_j \in \mathscr{P}$ *then* $(P_i) \cap (P_j) \subset (P_m)$ *iff* $i=m$ *or* $j=m$.

To use the notion of a KDP we now identify our set of network nodes with $\mathscr{P}$ and a set of subkeys with $\mathscr{B}$, where $(\mathscr{P}, \mathscr{B}, I)$ is a KDP. Then the key to be used

by users P_i and P_j to communicate with one another is made up from a combination of the subkeys in $(P_i) \cap (P_j)$, and since we have a KDP, Property 1.1 implies that no other user knows all the subkeys in this set. To combine the set of subkeys to make an N-bit link key one might typically define each subkey to be an N-bit vector over GF(2), and combine the subkeys using some sort of "one way function".

Before proceeding we attempt to justify our insistence that $v \geq 3$. If $v = 2$, then there is really no key distribution problem in this context; note also that, given $v \geq 3$, Corollary 2.3 below implies that $b \geq 3$.

In addition, note that Property 1.1 has a simple geometrical interpretation. The axiom is precisely equivalent to demanding that the incidence structure has line size 2 (in the language of design theory, a *line* through points A and B is the set of points contained in the intersection of the point sets (x), for all blocks $x \in (A) \cap (B)$.

To conclude these introductory remarks we exhibit the existence of some KDPs.

Example 1.2. Suppose $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ is defined by:

$$\mathcal{P} = \{P_1, P_2, \ldots, P_v\}, \qquad \mathcal{B} = \{x_{ij} : 1 \leq i < j \leq v\},$$

$$(P_i, x_{st}) \in I \quad \text{iff} \quad i = s \text{ or } i = t$$

Then this corresponds exactly with the case where each pair of users is provided with a unique key. This is what we call the *trivial* KDP on v points, since using this KDP is equivalent to not using a KDP system at all. In the notation of design theory $\mathcal{K}$ is a trivial 2-$(v, 2, 1)$ design.

Example 1.3. Suppose $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ is defined by

$$\mathcal{P} = \{P_1, P_2, \ldots, P_v\}, \qquad \mathcal{B} = \{x_1, x_2, \ldots, x_v$$

and

$$(P_i, x_j) \in I \quad \text{iff} \quad i \text{ is not equal to } j.$$

In this case $|(P_i) \cap (P_j)| = v - 2$, and $(P_i) \cap (P_j)$ contains all blocks except x_i and x_j. It is immediately clear that $\mathcal{K}$ is a KDP. In the notation of design theory, $\mathcal{K}$ is a trivial 2-$(v, v-1, v-2)$ design.

Example 1.4. Suppose $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ is a 2-$(v, k, 2)$ design satisfying $b = v$ (and hence $r = k$ and $v = \frac{1}{2}(k^2 - k + 2)$; then $\mathcal{K}$ is normally called a *biplane*. A discussion of biplanes can be found in [7, Chapter 3]; [6, Chapter 15] contains a complete listing of all the known non-isomorphic biplanes (of which there are only 17, the largest having $k = 13$). Any 2-(v, k, λ) design satisfying $b = v$ is usually referred to as a *symmetric* design, and in such a design any two blocks always have λ points in common. So, in a biplane, any two blocks have 2 points in common, and it is then immediate to see that a biplane must be a KDP.

We now consider three different ways in which two KDPs can be joined to give a new larger KDP. The proofs that these constructions actually give KDPs can be found in a more general setting in Section 3 below.

Construction 1.5. Suppose that $\mathcal{K}=(\mathcal{P}_\mathcal{K}, \mathcal{B}_\mathcal{K}, I_\mathcal{K})$ and $\mathcal{L}=(\mathcal{P}_\mathcal{L}, \mathcal{B}_\mathcal{L}, I_\mathcal{L})$ are KDPs having $v_\mathcal{K}$, $b_\mathcal{K}$ and $v_\mathcal{L}$, $b_\mathcal{L}$ points and blocks respectively. This construction combines these two KDPs to give a new KDP with $v_\mathcal{K}+v_\mathcal{L}$ points and $b_\mathcal{K}\cdot b_\mathcal{L}$ blocks, and which we will denote by $\mathcal{M}=(\mathcal{P}_\mathcal{M}, \mathcal{B}_\mathcal{M}, I_\mathcal{M})$.

Let

$$\mathcal{P}_\mathcal{M}=\mathcal{P}_\mathcal{K}\cup\mathcal{P}_\mathcal{L}, \qquad \mathcal{B}_\mathcal{M}=\{(x, y): x\in\mathcal{B}_\mathcal{K},\ y\in\mathcal{B}_\mathcal{L}\}$$

and define $I_\mathcal{M}$ as follows. If $P\in\mathcal{P}_\mathcal{M}$, then P is incident with block (x, y) iff either $P\in\mathcal{P}_\mathcal{K}$ and P is incident with x in $\mathcal{K}$, or $P\in\mathcal{P}_\mathcal{L}$ and P is incident with y in $\mathcal{L}$. More informally we write $\mathcal{B}_\mathcal{M}=\{x\cup y: x\in\mathcal{B}_\mathcal{K}, y\in\mathcal{B}_\mathcal{L}\}$, where the incidence is "inherited" from $\mathcal{K}$ and $\mathcal{L}$, and where by the *union* $x\cup y$ of two blocks we mean the block z with the property that $(z)=(x)\cup(y)$.

Construction 1.6. Suppose that $\mathcal{K}=(\mathcal{P}_\mathcal{K}, \mathcal{B}_\mathcal{K}, I_\mathcal{K})$ and $\mathcal{L}=(\mathcal{P}_\mathcal{L}, \mathcal{B}_\mathcal{L}, I_\mathcal{L})$ are KDPs having $v_\mathcal{K}$, $b_\mathcal{K}$ and $v_\mathcal{L}$, $b_\mathcal{L}$ points and blocks respectively. This construction combines these two KDPs to give a new KDP with $v_\mathcal{K}+v_\mathcal{L}-1$ points and $b_\mathcal{K}+r_\mathcal{K}(i)(b_\mathcal{L}-1)$ blocks (where $r_\mathcal{K}(i)$ is the number of blocks incident with a chosen point from $\mathcal{P}_\mathcal{K}$), and which we will denote by $\mathcal{M}=(\mathcal{P}_\mathcal{M}, \mathcal{B}_\mathcal{M}, I_\mathcal{M})$.

First choose some $P_i\in\mathcal{P}_\mathcal{K}$, and let $\mathcal{P}_\mathcal{M}=(\mathcal{P}_\mathcal{K}-\{P_i\})\cup\mathcal{P}_\mathcal{L}$. Now divide the blocks of $\mathcal{K}$ into two subclasses, namely those which are incident with P_i and those which are not, and call these classes $\mathcal{Q}$ and $\mathcal{R}$ respectively (note that $\mathcal{Q}\cup\mathcal{R}=\mathcal{B}_\mathcal{K}$). We now set

$$\mathcal{B}_\mathcal{M}=\mathcal{R}\cup\{x\cup y-\{P_i\}: x\in\mathcal{Q}, y\in\mathcal{B}_\mathcal{L}\},$$

where the union of blocks is defined precisely as in the previous example, and the incidence relation is derived directly from the incidence relations in $\mathcal{K}$ and $\mathcal{L}$.

Construction 1.7. Suppose that $\mathcal{K}=(\mathcal{P}_\mathcal{K}, \mathcal{B}_\mathcal{K}, I_\mathcal{K})$ and $\mathcal{L}=(\mathcal{P}_\mathcal{L}, \mathcal{B}_\mathcal{L}, I_\mathcal{L})$ are KDPs having $v_\mathcal{K}$, $b_\mathcal{K}$ and $v_\mathcal{L}$, $b_\mathcal{L}$ points and blocks respectively. This construction combines these two KDPs to give a new KDP $\mathcal{M}=(\mathcal{P}_\mathcal{M}, \mathcal{B}_\mathcal{M}, I_\mathcal{M})$ with $v_\mathcal{K}+v_\mathcal{L}-2$ points and $b_\mathcal{K}+b_\mathcal{L}+(r_\mathcal{K}(i)-1)(r_\mathcal{L}(j)-1)-1$ blocks, where $r_\mathcal{K}(i)$ is the number of blocks incident with a chosen point P_i from $\mathcal{P}_\mathcal{K}$, and $r_\mathcal{L}(j)$ is the number of blocks incident with a chosen point Q_j from $\mathcal{P}_\mathcal{L}$.

First let

$$\mathcal{P}_\mathcal{M}=(\mathcal{P}_\mathcal{K}-\{P_i\})\cup(\mathcal{P}_\mathcal{L}-\{Q_j\}).$$

Now divide the blocks of $\mathcal{K}$ into two subclasses, namely those which are incident with P_i and those which are not, and call these classes $\mathcal{Q}_\mathcal{K}$ and $\mathcal{R}_\mathcal{K}$ respectively (note that $\mathcal{Q}_\mathcal{K}\cup\mathcal{R}_\mathcal{K}=\mathcal{B}_\mathcal{K}$). Similarly divide the blocks of $\mathcal{L}$ into two subclasses, namely those which are incident with Q_j and those which are not, and call these classes $\mathcal{Q}_\mathcal{L}$ and $\mathcal{R}_\mathcal{L}$ respectively (note that $\mathcal{Q}_\mathcal{L}\cup\mathcal{R}_\mathcal{L}=\mathcal{B}_\mathcal{L}$). We now set

$$\mathcal{B}_\mathcal{M}=\mathcal{R}_\mathcal{K}\cup\mathcal{R}_\mathcal{L}\cup\{(x-\{P_i\})\cup(y-\{Q_j\}): x\in\mathcal{Q}_\mathcal{K}, y\in\mathcal{Q}_\mathcal{L}\}.$$

These examples and constructions show that there are many nontrivial KDPs. We now need some way of assessing the relative usefulness of these KDPs in terms of the amount of storage space that they can save. Three primary objectives must be firstly to minimize the total number of subkeys, i.e. to minimize b (which determines the amount of storage required at the KDC), secondly to minimize the total storage required at all the network nodes, i.e. to minimize $r(1)+r(2)+\cdots+r(v)$ and thirdly to minimize the maximum storage required at any one node, i.e. to minimize $\max\{r(i)\}$. Different situations may require other measures of usefulness.

It should now be clear that, of the three construction methods described above, Construction 1.7 is potentially the most useful, since the KDPs constructed this way will have smaller b for given v, which is one of our chief objectives. We conclude these introductory remarks by giving a small example of Construction 1.7; note that this example is unrealistically small.

Example 1.8. Let $\mathscr{H}$ and $\mathscr{L}$ both be 2-(7, 4, 2) designs, i.e. 7-point biplanes. Suppose that

$$\mathscr{P}_{\mathscr{H}}=\{P_1, \quad ,P_7\}, \qquad \mathscr{P}_{\mathscr{L}}=\{Q_1,\ldots,Q_7\}$$
$$\mathscr{B}_{\mathscr{H}}=\{x_1,\ldots,x_7\}, \qquad \mathscr{B}_{\mathscr{L}}=\{y_1,\ldots,y_7\},$$

and let the blocks of $\mathscr{H}$ and $\mathscr{L}$ be incident with the following sets of points: x_1 with $\{P_3, P_5, P_6, P_7\}$, x_2 with $\{P_2, P_4, P_5, P_6\}$, x_3 with $\{P_1, P_4, P_6, P_7\}$, x_4 with $\{P_2, P_3, P_4, P_7\}$, x_5 with $\{P_1, P_2, P_5, P_7\}$, x_6 with $\{P_1, P_2, P_3, P_6\}$, x_7 with $\{P_1, P_3, P_4, P_5\}$, y_1 with $\{Q_3, Q_5, Q_6, Q_7\}$, y_2 with $\{Q_2, Q_4, Q_5, Q_6\}$, y_3 with $\{Q_1, Q_4, Q_6, Q_7\}$, y_4 with $\{Q_2, Q_3, Q_4, Q_7\}$, y_5 with $\{Q_1, Q_2, Q_5, Q_7\}$, y_6 with $\{Q_1, Q_2, Q_3, Q_6\}$ and y_7 with $\{Q_1, Q_3, Q_4, Q_5\}$.

If we "choose" points P_1 and Q_1, then the incidence structure $\mathscr{M}$ obtained using Construction 1.7 has point set

$$\mathscr{P}_{\mathscr{M}}=\{P_2,\ldots P_7, Q_2, \quad ,Q_7.$$

(i.e. $v=14$) and block set

$$\mathscr{B}_{\mathscr{M}}=\{x_1, x_2, x_4, y_1, y_2, y_4\}\cup\{z_{ij}=x_i\cup y_j-\{P_1, Q_1\}: i,j=3, 5, 6, 7\}$$

(i.e. $b=22$). Each point is incident with 10 blocks, e.g. Q_4 is incident with blocks y_2, y_4, z_{33}, z_{53}, z_{63}, z_{37}, z_{73}, z_{57}, z_{67}, z_{77}.

2. Key distribution patterns: Some theoretical results

Before proceeding to any theoretical results on KDPs we digress briefly to consider a result on systems of subsets of a set. This result will in turn give us some useful inequalities for KDPs. The result quoted here can be found in Bollobás' invaluable book, [4].

Let $\mathcal{B}$ be a finite set of cardinality b, i.e. $|\mathcal{B}| = b$. Also let $\mathcal{P}(\mathcal{B})$ be the set of all subsets of $\mathcal{B}$, i.e. the power set of $\mathcal{B}$, and hence $\mathcal{P}(\mathcal{B})$ has cardinality 2^b. If $\mathcal{S}$ is a subset of $\mathcal{P}(\mathcal{B})$, then $\mathcal{S}$ is known as a *Sperner system* iff $S \subset T$ and $S, T \in \mathcal{S}$ implies $S = T$.

Then we immediately have:

Result 2.1 (Sperner, 1928). *If $\mathcal{S} \subset \mathcal{P}(\mathcal{B})$ ($|\mathcal{B}| = b$) is a Sperner system, then $|\mathcal{S}| \leq {}_bC_{[b/2]}$, where by ${}_mC_n$ we mean the binomial coefficient $m!/n!(m-n)!$. Equality is achieved iff $\mathcal{S}$ is the class of all w-subsets of $\mathcal{B}$, where $w = \frac{1}{2}b$ if b is even and $w = \frac{1}{2}(b-1)$ or $w = \frac{1}{2}(b+1)$ if b is odd.*

The relevance of Sperner systems to KDPs is indicated by the next result.

Lemma 2.2. *If $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ is a finite incidence structure, then $\mathcal{K}$ is a KDP iff $\{(P) \cap (P') : P, P'$ distinct elements of $\mathcal{P}\}$ is a Sperner system of subsets of $\mathcal{B}$.*

Proof. Suppose first that $\mathcal{K}$ is a KDP. Choose $P, P', Q, Q' \in \mathcal{P}$ (P, P' and Q, Q' are distinct pairs) and suppose that $(P) \cap (P') \subset (Q) \cap (Q')$. Then

$$(P) \cap (P') \subset (Q) \quad \text{and} \quad (P) \cap (P') \subset (Q'),$$

and so, by Property 1.1, either $P = Q$ and $P' = Q'$ or $P = Q'$ and $P' = Q$. Hence $\{(P) \cap (P') : P, P'$ distinct elements of $\mathcal{P}\}$ is a Sperner system of subsets of $\mathcal{B}$.

Now suppose that $\{(P) \cap (P') : P, P'$ distinct elements of $\mathcal{P}\}$ is a Sperner system of subsets of $\mathcal{B}$ and suppose also that $(P) \cap (P') \subset (Q)$ for some $P, P', Q \in \mathcal{P}$. Then $(P) \cap (P') \subset (Q) \cap (Q')$ for any $Q' \in \mathcal{P}$, and hence either $P = Q$ or $P' = Q$. Hence $\mathcal{K}$ is a KDP. □

Combining Lemma 2.2 with Result 2.1 gives us immediately:

Corollary 2.3. *If $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ is a KDP, then ${}_vC_2 \leq {}_bC_{[b/2]}$.*

This gives us the following lower bounds on b for small values of v:

v	min b
3	3
4	4
	5
6	6
	7
8	7
9	8

Hence if a KDP exists with $b<v$ then $v\geq 8$. Also note that, for any chosen $i\in\{1, 2, \ldots, v\}$, the set $\{(P_i)\cap(P_j)$: j distinct from $i\}$ forms a Sperner system of subsets of (P_i). Hence, again applying Result 2.1 we have:

Lemma 2.4. *If $\mathcal{K}=(\mathcal{P}, \mathcal{B}, I)$ is a KDP, then*

$$v-1\leq {}_{r(i)}C_{[r(i)/2]} \quad \textit{for every } i\in\{1, 2, \quad, v\}.$$

This gives us the following lower bounds on $r(i)$ for small values of v:

v	min $r(i)$
3	
4	
5	4
6	4
7	4
8	5
9	5

Finally note that it should be clear that if $\mathcal{K}=(\mathcal{P}, \mathcal{B}, I)$ is a KDP then $\{(P)$: $P\in\mathcal{P}\}$ is an *intersecting family* of subsets of $\mathcal{B}$ (where we define an intersecting family of subsets to be one having the property that any two elements of the family will have a non-empty intersection). Hence, by a result from Bollobás, [4, Chapter 7], we know that $v\leq 2^{b-1}$. Unfortunately this bound is always weaker than the bound of Corollary 2.3 and so we do not consider it further here.

Having established these very basic inequalities we consider ways in which we can impose additional structure on the KDPs. We do this with the hope that it will indicate better how to construct examples having desirable properties.

Firstly note that, by Result 2.1, in order to obtain a Sperner system of maximal cardinality it is necessary to choose subsets all having the same size. Hence, by considering Lemma 2.2, it might be possible to maximize v for given b by choosing $\lambda(i, j)=\lambda$ for every i, j.

If $\mathcal{K}$ is a KDP with this property (called ($\bar{\text{R}}$.2) by Dembowski [5, Section 1.1]), then we call $\mathcal{K}$ a *balanced* KDP. In the notation of design theory $\mathcal{K}$ is then a *pairwise balanced design*, and, as is well known (see, for example, [1, Theorem II.2.6]) Fisher's inequality holds for such structures. So we have:

Theorem 2.5 (Generalized Fisher inequality). *If $\mathcal{K}$ is a balanced KDP then $b\geq v$.*

A second way in which we might impose additional structure on a KDP is by assuming that it is a 1-design, i.e. by supposing that $r(i)=r$ for every $i\in\{1, 2, \ldots, v\}$ and $k(j)=k$ for every $j\in\{1, 2, \ldots, b\}$. Then we have:

Lemma 2.6. *If $\mathcal{K}$ is both a KDP and a 1-design, then either $\mathcal{K}$ is a trivial KDP or $r \geq 3$, $k \geq 3$ and $\lambda(i,j) \geq 2$ for every $i, j \in \{1, 2, \ldots, v\}$.*

Proof. If $r=1$ or $k=1$ then $b=v=1$ which contradicts our definition of KDP.

If $r=2$, then since we must have $1 \leq \lambda(i,j) < r=2$ for every i and j, $\mathcal{K}$ is a balanced KDP with $\lambda=1$, i.e. $\mathcal{K}$ is a 2-$(v, k, 1)$ design with $r=2$. Hence $b \geq v$, and since $bk=vr$ in a 1-design and $\lambda v(v-1)=bk(k-1)$ in a 2-design, [7], $k \leq r=2$, i.e. $b=v=3$ and $k=r=2$, and $\mathcal{K}$ is the unique trivial KDP having $r=2$.

If $k=2$, then, since no two blocks are incident with the same set of points, every pair of points are incident with a unique block which is itself incident with no other points. Hence $\mathcal{K}$ is balanced, i.e. $\mathcal{K}$ is a 2-$(v, 2, 1)$ design which must be a trivial KDP.

Finally now suppose that $k, r \geq 3$, and suppose that $\lambda(i,j)=1$. If we let $(P_i) \cap (P_j) = \{x_s\}$, then x_s cannot be incident with any other point by the definition of KDP. Hence $r=2$, contradicting our assumption. □

3. Collusion and collusion-resistant key distribution patterns

As Blom, [2], has pointed out this type of system can easily break down if two or more people pool their sets of subkeys. More formally, if $P, P', Q, Q' \in \mathcal{P}$ satisfy $(P) \cap (P') \subset (Q) \cup (Q')$ (where P, P' and Q, Q' are both distinct pairs) then if the users corresponding to Q and Q' pool their sets of subkeys, they have sufficient information to compute the key used by users P and P' to communicate with one another.

This is clearly a most undesirable property, and so we now add an additional constraint in order to construct what we call *collusion-resistant* KDPs.

If $w \geq 1$, then define a *w-collusion resistant KDP* (w-CRKDP) to be a finite incidence structure $\mathcal{K}=(\mathcal{P}, \mathcal{B}, I)$ such that $v \geq 3$, no two blocks are incident with the same set of points, and if $1 \leq i, j \leq v$ and

$$H = \{h(1), h(2), \ldots, h(w)\} \subset \{1, 2, \ldots, v\},$$

then we have:

Property 3.1. $(P_i) \cap (P_j) \subset \bigcup_{s=1}^{w} (P_{h(s)})$ *iff either $i \in H$ or $j \in H$.*

More informally we now have an incidence structure with the following property. For any pair of points, A, B say, the set of blocks with which they are both incident is not contained in the union of the sets of blocks incident with any set of up to w points unless A or B are contained in the set. Hence, in our application, if at most w users pool all their subkeys they will be unable to deduce any of the keys used in the network apart from those which are used by at least one of them.

Note that it should be clear that the definition of 1-CRKDP corresponds precisely

to the previous definition of KDP. We now provide some examples of w-CRKDPs for $w>1$.

Example 3.2. A trivial KDP is clearly a w-CRKDP for every w.

Example 3.3. Suppose $\mathscr{K}$ is a 3-design for which $\lambda_2 > w\lambda_3$. Then $\mathscr{K}$ is a w-CRKDP. We now show why this is true. Suppose that $1 \le i < j \le v$,

$$H = \{h(1), h(2), \ldots, h(w)\} \subset \{1, 2, \ldots, v\} - \{i, j\},$$

and

$$(P_i) \cap (P_j) \subset \bigcup_{s=1}^{w} (P_{h(s)}).$$

By definition

$$|(P_i) \cap (P_j)| = \lambda_2 \quad \text{and} \quad |(P_i) \cap (P_j) \cap (P_{h(s)})| = \lambda_3$$

for every $s \in \{1, 2, \ldots, w\}$. Since we know that $\lambda_2 > w\lambda_3$, we have an immediate contradiction and the desired result follows.

The standard relation amongst the parameters of a 3-design means that the condition $\lambda_2 > w\lambda_3$ is equivalent to assuming that $v > w(k-2)+2$. Also note that in any 3-design $\lambda_2 > \lambda_3$, and hence any 3-design is a KDP; in geometrical terms it should be clear that in a 3-design every line has size 2.

Before considering any further examples we examine some geometrical implications of our definition. We first need some basic definitions.

If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, I)$ is an arbitrary finite incidence structure, and $P \in \mathscr{P}$, then we define the internal structure of $\mathscr{K}$ at P, written $\mathscr{K}_P$, to be the structure having point set $\mathscr{P} - \{P\}$ and block set $\{x \in \mathscr{B} : x \text{ contains } P\}$. In addition we define the external structure of $\mathscr{K}$ at P, written $\mathscr{K}^P$, to be the structure having point set $\mathscr{P} - \{P\}$ and block set $\{x \in \mathscr{B} : x \text{ does not contain } P\}$. We can now state:

Lemma 3.4. *Suppose that $\mathscr{K} = (\mathscr{P}, \mathscr{B}, I)$ is a finite incidence structure. Then if $w \ge 1$, $\mathscr{K}$ is a $(w+1)$-CRKDP if and only if $\mathscr{K}^P$ is a w-CRKDP for every $P \in \mathscr{P}$.*

Proof. First suppose that $\mathscr{K}$ is a $(w+1)$-CRKDP. Choose $P \in \mathscr{P}$, and then choose a further pair of points, C, D say, from $\mathscr{K}^P$. Suppose $\mathscr{W}$ is a further set of w points from $\mathscr{K}^P$. Then $\mathscr{W} \cup \{P\}$ is a $(w+1)$-set of points from $\mathscr{K}$, and hence there is a block incident with both C and D which is not incident with any point from $\mathscr{W} \cup \{P\}$. Since this block is not incident with P it must be a block of $\mathscr{K}^P$, and the result follows.

Now suppose that $\mathscr{K}^P$ is a w-CRKDP for every $P \in \mathscr{P}$. Now choose a pair of points $C, D \in \mathscr{P}$ and further let $\mathscr{X}$ be a set of $w+1$ points from $\mathscr{P}$ (not containing C or D). If we suppose that $Q \in \mathscr{X}$, then we know that $\mathscr{K}^Q$ is a w-CRKDP. Hence there exists a block in $\mathscr{K}^Q$ which is incident with both C and D but which is not

incident with any point from $\mathscr{X}-\{Q\}$. This immediately gives us a block in $\mathscr{K}$ which is incident with C and D but yet is not incident with any point in $\mathscr{X}$. The result follows. □

It is well known that if $\mathscr{K}$ is a t-design, then $\mathscr{K}^P$ is a $(t-1)$-design for any point P from $\mathscr{K}$. Combining this knowledge with Example 3.3 and Lemma 3.4, we immediately have:

Example 3.5. Suppose $\mathscr{K}$ is a $(w+2)$-design, where $w \geq 1$. Then $\mathscr{K}$ is a w-CRKDP.

However, having made this observation we note that the use of t-designs with $t \geq 4$ is of limited value in our context. Unfortunately it is true that, if $t \geq 4$, then $b \geq {}_vC_2$. Hence, if a t-design is used with $t \geq 4$ the number of pieces of information to be stored at the key distribution centre will be at least as great as for the trivial KDP.

Finally we observe that Constructions 1.5, 1.6 and 1.7 can be used to give w-CRKDPs for arbitrary values of w. In each case suppose that $\mathscr{K}$ and $\mathscr{L}$ are w-CRKDPs, and, as proved below, the derived KDP $\mathscr{M}$ is always also a w-CRKDP. Again it should be clear that usually Construction 1.7 is the most useful means of construction.

3.1. Proof that Construction 1.5 gives a w-CRKDP

Choose any two points $A, B \in \mathscr{P}_{\mathscr{M}}$. There are three cases to consider, namely: (i) $A, B \in \mathscr{P}_{\mathscr{K}}$, (ii) $A, B \in \mathscr{P}_{\mathscr{L}}$, and (iii) $A \in \mathscr{P}_{\mathscr{K}}$, $B \in \mathscr{P}_{\mathscr{L}}$. In each case suppose that there exists a w-subset $\mathscr{C} \subset \mathscr{P}_{\mathscr{M}}$ such that every block in $\mathscr{B}_{\mathscr{M}}$ that contains A and B is also incident with at least one element of $\mathscr{C}$. For the purposes of the discussion below let $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$, where $\mathscr{C}_1 \subset \mathscr{P}_{\mathscr{K}}$ and $\mathscr{C}_2 \subset \mathscr{P}_{\mathscr{L}}$.

Case (i). Suppose $x \in \mathscr{B}_{\mathscr{K}}$ is incident with both A and B. Then $x \cup y \in \mathscr{B}_{\mathscr{M}}$ is incident with both A and B, for any $y \in \mathscr{B}_{\mathscr{L}}$. By our assumption all these blocks $x \cup y$ must be incident with at least one element of $\mathscr{C}$. If x is not incident with an element of $\mathscr{C}_1$, then this implies that every block $y \in \mathscr{B}_{\mathscr{L}}$ is incident with at least one element of $\mathscr{C}_2$, a contradiction since $|\mathscr{C}_2| \leq w$. Hence x is incident with a block of $\mathscr{C}_1$, again giving a contradiction since $|\mathscr{C}_1| \leq w$.

Case (ii). Since the definition of $\mathscr{M}$ is completely symmetric in $\mathscr{K}$ and $\mathscr{L}$, this case follows using an identical argument to Case (i).

Case (iii). If $\mathscr{X} \subset \mathscr{B}_{\mathscr{K}}$ contains all the blocks incident with A, and $\mathscr{Y} \subset \mathscr{B}_{\mathscr{L}}$ contains all the blocks incident with B, then the set of blocks of $\mathscr{B}_{\mathscr{M}}$ incident with both A and B is precisely $\{x \cup y: x \in \mathscr{X}, y \in \mathscr{Y}\}$. Hence either every block of $\mathscr{X}$ is incident with at least one point of $\mathscr{C}_1$ or every block of $\mathscr{Y}$ is incident with at least one point of $\mathscr{C}_2$. In either event we again have a contradiction. The result now follows. □

3.2. Proof that Construction 1.6 gives a w-CRKDP

Choose any two points $A, B \in \mathscr{P}_{\mathscr{M}}$. There are three cases to consider, namely: (i) $A, B \in \mathscr{P}_{\mathscr{K}}$, (ii) $A, B \in \mathscr{P}_{\mathscr{L}}$, and (iii) $A \in \mathscr{P}_{\mathscr{K}}$, $B \in \mathscr{P}_{\mathscr{L}}$. In each case suppose that there exists a w-subset $\mathscr{C} \subset \mathscr{P}_{\mathscr{M}}$ such that every block in $\mathscr{B}_{\mathscr{M}}$ that contains A and B is also incident with at least one element from $\mathscr{C}$. For the purposes of the discussion below let $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$, where $\mathscr{C}_1 \subset \mathscr{P}_{\mathscr{K}}$ and $\mathscr{C}_2 \subset \mathscr{P}_{\mathscr{L}}$.

Case (i). Define $\mathscr{C}' \subset \mathscr{P}_{\mathscr{K}}$ by $\mathscr{C}' = \mathscr{C}_1$ if $\mathscr{C} = \mathscr{C}_1$ and $\mathscr{C}' = \mathscr{C}_1 \cup \{P_i\}$ otherwise. Then $\mathscr{C}'$ is a subset of $\mathscr{P}_{\mathscr{K}}$ containing at most w points. Suppose $x \in \mathscr{B}_{\mathscr{K}}$ is incident with both A and B. First suppose that x is incident with P_i. Then $(x - \{P_i\}) \cup y \in \mathscr{B}_{\mathscr{M}}$ is also incident with both A and B and hence with at least one element, Q say, from $\mathscr{C}$. If $Q \in \mathscr{C}_1$ then $Q \in \mathscr{C}'$ and x is incident with Q. If $Q \in \mathscr{C}_2$, then $P_i \in \mathscr{C}'$ and x is incident with P_i, i.e. x is always incident with at least one element of $\mathscr{C}'$. Now suppose that x is not incident with P_i. Then $x \in \mathscr{B}_{\mathscr{M}}$ is also incident with both A and B and hence with at least one element, Q say, from $\mathscr{C}$. Moreover Q must be in $\mathscr{C}_1$ (since $x \in \mathscr{B}_{\mathscr{K}}$), and hence Q is in $\mathscr{C}'$. Hence, regardless of the choice for x it is always incident with at least one element of $\mathscr{C}'$, giving the desired contradiction.

Case (ii). If $\mathscr{Q} \subset \mathscr{B}_{\mathscr{K}}$ is defined as above, and $\mathscr{Y} \subset \mathscr{B}_{\mathscr{L}}$ contains all the blocks incident with both A and B in $\mathscr{L}$, then the set of blocks of $\mathscr{B}_{\mathscr{M}}$ incident with both A and B is precisely $\{x \cup y - \{P_i\} : x \in \mathscr{Q}, y \in \mathscr{Y}\}$. It is then straightforward to see that either every block of $\mathscr{Q}$ is incident with at least one point of $\mathscr{C}_1$ or every block of $\mathscr{Y}$ is incident with at least one point of $\mathscr{C}_2$. However, since $|\mathscr{C}_1|, |\mathscr{C}_2| \leq w$ this gives the desired contradiction.

Case (iii). If $\mathscr{X} \subset \mathscr{B}_{\mathscr{K}}$ contains all the blocks incident with both A and P_i, and $\mathscr{Y} \subset \mathscr{B}_{\mathscr{L}}$ contains all the blocks incident with B, then the set of blocks of $\mathscr{B}_{\mathscr{M}}$ incident with both A and B is precisely $\{x \cup y - \{P_i\} : x \in \mathscr{X}, y \in \mathscr{Y}\}$. Hence either every block of $\mathscr{X}$ is incident with at least one point of $\mathscr{C}_1$ or every block of $\mathscr{Y}$ is incident with at least one point of $\mathscr{C}_2$. In either event we again have a contradiction. The result now follows. □

3.3. Proof that Construction 1.7 gives a w-CRKDP

Choose any two points $A, B \in \mathscr{P}_{\mathscr{M}}$. There are three cases to consider, namely: (i) $A, B \in \mathscr{P}_{\mathscr{K}}$, (ii) $A, B \in \mathscr{P}_{\mathscr{L}}$, and (iii) $A \in \mathscr{P}_{\mathscr{K}}$, $B \in \mathscr{P}_{\mathscr{L}}$. In each suppose that there exists a w-subset $\mathscr{C} \subset \mathscr{P}_{\mathscr{M}}$ such that every block in $\mathscr{B}_{\mathscr{M}}$ that contains A and B is also incident with at least one element from $\mathscr{C}$. For the purposes of the discussion below let $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$, where $\mathscr{C}_1 \subset \mathscr{P}_{\mathscr{K}}$ and $\mathscr{C}_2 \subset \mathscr{P}_{\mathscr{L}}$.

Case (i). Define $\mathscr{C}' \subset \mathscr{P}_{\mathscr{K}}$ by $\mathscr{C}' = \mathscr{C}_1$ if $\mathscr{C} = \mathscr{C}_1$ and $\mathscr{C}' = \mathscr{C}_1 \cup \{P_i\}$ otherwise. Then $\mathscr{C}'$ is a subset of $\mathscr{P}_{\mathscr{K}}$ containing at most w points. Suppose $x \in \mathscr{B}_{\mathscr{K}}$ is incident with both A and B. First suppose that x is incident with P_i. Then $(x - \{P_i\}) \cup (y - \{Q_j\}) \in \mathscr{B}_{\mathscr{M}}$ is also incident with both A and B and hence with at least one ele-

ment, R say, from $\mathscr{C}$. If $R \in \mathscr{C}_1$ then $R \in \mathscr{C}'$ and x is incident with R. If $R \in \mathscr{C}_2$, then $P_i \in \mathscr{C}'$ and x is incident with P_i, i.e. x is always incident with at least one element of $\mathscr{C}'$. Now suppose that x is not incident with P_i. Then $x \in \mathscr{B}_{\mathscr{M}}$ is also incident with both A and B and hence with at least one element, R say, from $\mathscr{C}$. Moreover R must be in $\mathscr{C}_1$ (since $x \in \mathscr{B}_{\mathscr{K}}$), and hence R is in $\mathscr{C}'$. Hence, regardless of the choice for x it is always incident with at least one element of $\mathscr{C}'$, giving the desired contradiction.

Case (ii). Since the definition of $\mathscr{M}$ is completely symmetric in $\mathscr{K}$ and $\mathscr{L}$, this case follows using an identical argument to Case (i).

Case (iii). If $\mathscr{X} \subset \mathscr{B}_{\mathscr{K}}$ contains all the blocks incident with both A and P_i, and $\mathscr{Y} \subset \mathscr{B}_{\mathscr{L}}$ contains all the blocks incident with B and Q_j, then the set of blocks of $\mathscr{B}_{\mathscr{M}}$ incident with both A and B is precisely $\{(x-\{P_i\}) \cup (y-\{Q_j\}): x \in \mathscr{X}, y \in \mathscr{Y}\}$. Hence either every block of $\mathscr{X}$ is incident with at least one point of $\mathscr{C}_1$ or every block of $\mathscr{Y}$ is incident with at least one point of $\mathscr{C}_2$. In either event we again have a contradiction. The result now follows. □

Note that, by introducing a little notation, the relationship between the above three methods of construction can be clarified. If $\mathscr{M}$ is constructed from $\mathscr{K}$ and $\mathscr{L}$ using the method of Construction 1.5 then we write $\mathscr{M} = \mathscr{K} \cdot \mathscr{L}$, and we call $\mathscr{M}$ the *product* of $\mathscr{K}$ and $\mathscr{L}$. Then, the method of Construction 1.6 is simply $\mathscr{M} = \mathscr{K}^P \cup \mathscr{K}_P \cdot \mathscr{L}$, and the method of Construction 1.7 is $\mathscr{M} = \mathscr{K}^P \cup \mathscr{L}^Q \cup \mathscr{K}_P \cdot \mathscr{L}_Q$.

4. Further developments

We have so far considered only the case where pairs of users wish to have the means to communicate securely. This idea can be generalized to the situation where every subset of users of size at most g needs to have a key known only to the members of the group. This key can then be used by the members of the closed user group to send secret messages to all the other members of the group.

For this reason we define a (g, w)-*collusion resistant KDP* ((g, w)-CRKDP) to be a w-CRKDP $\mathscr{K} = (\mathscr{P}, \mathscr{B}, I)$, for which if

$$F = \{f(1), f(2), \ldots, f(g)\} \quad \text{and} \quad H = \{h(1), h(2), \ldots, h(w)\}$$

are arbitrary g- and w-subsets of $\{1, 2, \ldots, v\}$ respectively, then we have:

Property 4.1. $\bigcap_{i=1}^{g} (P_{f(i)}) \subset \bigcup_{j=1}^{w} (P_{h(j)})$ *iff* $F \cap H$ *is non-empty.*

It should be clear from the above definition that a $(2, w)$-CRKDP is precisely the same object as a w-CRKDP.

Before giving examples of these structures we need the following generalization of Lemma 3.4 above:

Lemma 4.2. *Suppose that* $\mathcal{K}=(\mathcal{P}, \mathcal{B}, I)$ *is a finite incidence structure. Then if* $g, w \geq 1$, $\mathcal{K}$ *is a* $(g, w+1)$*-CRKDP if and only if* $\mathcal{K}^P$ *is a* (g, w)*-CRKDP for every* $P \in \mathcal{P}$.

Proof. First suppose that $\mathcal{K}$ is a $(g, w+1)$-CRKDP. Choose $P \in \mathcal{P}$, and then choose a set of g points, $\mathcal{G}$ say, from $\mathcal{K}^P$. Suppose $\mathcal{W}$ is a further (disjoint) set of w points from $\mathcal{K}^P$. Then $\mathcal{W} \cup \{P\}$ is a $(w+1)$-set of points from $\mathcal{K}$, and hence there is a block incident with all the points in $\mathcal{G}$ which is not incident with any point from $\mathcal{W} \cup \{P\}$. Since this block is not incident with P it must be a block of $\mathcal{K}^P$, and the result follows.

Now suppose that $\mathcal{K}^P$ is a (g, w)-CRKDP for every $P \in \mathcal{P}$. Now choose a set of g points $\mathcal{G} \subset \mathcal{P}$ and further let $\mathcal{X}$ be a set of $w+1$ points from $\mathcal{P}$ (disjoint from $\mathcal{G}$). If we suppose that $Q \in \mathcal{X}$, then we know that $\mathcal{K}^Q$ is a (g, w)-CRKDP. Hence there exists a block in $\mathcal{K}^Q$ which is incident with all the points in $\mathcal{G}$ but which is not incident with any point from $\mathcal{X}-\{Q\}$. This immediately gives us a block in $\mathcal{K}$ which is incident with all the points in $\mathcal{G}$ but yet is not incident with any point in $\mathcal{X}$. The result follows. □

Using this lemma we can now show that t-designs provide useful examples of (g, w)-CRKDPs (generalizing Example 3.5 above).

Example 4.3. Any $(g+w)$-design is a (g, w)-CRKDP (where $g, w \geq 1$).

First observe that any $(g+1)$-design is a $(g, 1)$-CRKDP (since $\lambda_g > \lambda_{g+1}$ in any $(g+1)$-design). Now, by noting that if $\mathcal{K}$ is a t-design then $\mathcal{K}^P$ is a $(t-1)$-design for any point P from $\mathcal{K}$, the result follows by induction on w (using Lemma 4.2 above).

5. Conclusions

In this paper we have introduced a number of new concepts, and shown how the theory of incidence structures may be applied to key management problems. Fundamental questions arising out of this work, such as finding optimal solutions to the problems posed by particular situations, will be considered in future papers.

References

[1] Th. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Mannheim, F.R.G., 1985).

[2] R. Blom, Non-public key distribution, in: Advances in Cryptology: Proceedings of Crypto 82 (Plenum Press, New York, 1983) 231–236.

[3] R. Blom, An optimal class of symmetric key generation systems, in: Advances in Cryptology: Proceedings of Eurocrypt 84, Lecture Notes in Computer Science 209 (Springer, Berlin, 1985) 335–338.

[4] B. Bollobás, Combinatorics (Cambridge University Press, Cambridge, England, 1986).
[5] P. Dembowski, Finite Geometries (Springer, New York, 1968).
[6] M. Hall, Jr., Combinatorial Theory (Wiley, New York, 2nd ed., 1986).
[7] D.R. Hughes and F.C. Piper, Design Theory (Cambridge University Press, Cambridge, England, 1985).
[8] C.J.A. Jansen, On the key storage requirements for secure terminals, Comput. Security 5 (1986) 145–149.
[9] C.J. Mitchell and F.C. Piper, The cost of reducing key storage requirements in secure networks, Comput. Security 6 (1987) 339–341.