Practical Approaches to Varying Network Size in Combinatorial Key Predistribution Schemes

Kevin Henry[1], Maura B. Paterson[2], and Douglas R. Stinson[1(✉)]

[1] David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada
k2henry@cs.uwaterloo.ca, dstinson@math.uwaterloo.ca
[2] Department of Economics, Mathematics and Statistics, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK
m.paterson@bbk.ac.uk

Abstract. Combinatorial key predistribution schemes can provide a practical solution to the problem of distributing symmetric keys to the nodes of a wireless sensor network. Such schemes often inherently suit networks in which the number of nodes belongs to some restricted set of values (such as powers of primes). In a recent paper, Bose, Dey and Mukerjee have suggested that this might pose a problem, since discarding keyrings to suit a smaller network might adversely affect the properties of the scheme.

In this paper we explore this issue, with specific reference to classes of key predistribution schemes based on transversal designs. We demonstrate through experiments that, for a wide range of parameters, randomly removing keyrings in fact has a negligible and largely predictable effect on the parameters of the scheme. In order to facilitate these computations, we provide a new, efficient, generally applicable approach to computing important properties of combinatorial key predistribution schemes.

We also show that the structure of a resolvable transversal design can be exploited to give a deterministic method of removing keyrings to adjust the network size, in such a way that the properties of the resulting scheme are easy to analyse. We show that these schemes have the same asymptotic properties as the transversal design schemes on which they are based, and that for most parameter choices their behaviour is very similar.

Keywords: Wireless sensor network · Key predistribution scheme · Combinatorial design

1 Introduction

In this paper, we consider *wireless sensor networks* (WSNs) consisting of a large number m of identical sensor nodes that are randomly deployed over a

D. Stinson's research is supported by NSERC discovery grant 203114-11.

T. Lange, K. Lauter, and P. Lisoněk (Eds.): SAC 2013, LNCS 8282, pp. 89–117, 2014.
DOI: 10.1007/978-3-662-43414-7_5,

target area. After deployment, each node communicates in a wireless manner with other nodes that are within communication range, thus forming an ad hoc network. Due to the wireless nature of the communication, it is desirable for cryptographic tools to be used for provision of secrecy, data integrity, and/or authentication. The nodes' restricted computational ability and battery power mean that, in many situations, it is preferable to use symmetric algorithms rather than relying on more computationally-intensive public key techniques. This requires nodes to share keys; one standard approach to providing such keys is the use of a *key predistribution scheme* (KPS), in which keys are stored in the nodes' keyrings prior to deployment. For example, in the seminal scheme of Eschenauer and Gligor [4], the keys are randomly drawn from a common keypool.

After the nodes have been deployed, nodes that are within communication range execute a *shared key discovery* protocol to determine which keys they have in common. Two nodes that share at least η keys (for some predetermined *intersection threshold* $\eta \geq 1$) use all their common keys to derive a new key that is used to secure communication between them. This is referred to as a secure *link* between these nodes. There exists a large quantity of literature relating to the construction of KPSs for WSNs; surveys include [2,7,10].

KPSs based on combinatorial structures such as designs or codes have been studied as an alternative to random schemes (see [6,9] for surveys of combinatorial schemes). Such schemes have several advantages over the random schemes: for instance, they make it possible to prove the scheme has desirable properties relating to connectivity and resilience, they enable more efficient discovery of shared keys, and they reduce the amount of randomness required when instantiating the schemes [5].

Key predistribution schemes for WSNs are typically evaluated using certain metrics that relate to the performance of the resulting networks. Firstly, it is desirable to restrict the total amount of memory each node must use for storing keys/keying material. Secondly, after the nodes have been deployed, it is desirable for there to be as many secure links as possible between neighbouring nodes, so as to increase the (secure) *connectivity* of the resulting network. The extent to which a KPS facilitates achieving this objective is frequently measured in terms of the quantity Pr_1, which denotes the probability that any two given nodes share at least η common keys.

Finally, we wish to measure the scheme's ability to withstand adversarial attack. A widely studied attack model, which we follow in this paper, is that of *random node capture* [4], where the adversary can eavesdrop on all communication in the network, and can also comprise random nodes in order to extract any keys/keying material they contain. The *resilience* of a KPS in the face of an attacker is expressed in terms of the quantity $\mathsf{fail}(s)$, which is defined to be the probability that a randomly chosen link is broken when an attacker compromises s nodes uniformly at random, and then extracts their keys.

For simplicity, we focus particularly on $\mathsf{fail}(1)$ in this work. In this case, a link $\{A, B\}$ is broken by another node C when $A \cap B \subseteq C$, where A, B and C denote the sets of keys held by the three corresponding nodes.

There is an inherent tension between the need to provide good connectivity and the need to maintain a high level of resilience without requiring an excessive number of keys to be stored. Designing a KPS involves finding a scheme that delivers a good tradeoff between these properties, and which is sufficiently flexible to be useful for a range of practical choices of parameters such as network size, available storage and desired level of security.

One feature of combinatorial schemes that could be viewed as a drawback is the fact that, due to the structure of the combinatorial object used, the number of nodes in the scheme may be required to be of a particular form, such as a power of a prime, for example. If the number n of nodes in the network in which we wish to employ such a scheme is not of this form, then the most commonly suggested remedy is to take the smallest number of that form that is larger than n, and simply select some (randomly chosen) subset of n keyrings from the resulting scheme (e.g., see [5]). In a recent paper [1], Bose, Dey and Mukerjee have suggested that removing keyrings in this manner from a combinatorial scheme may adversely affect its properties, thus negating some of the main benefits of such schemes. Instead, they propose a deterministic KPS in which various block designs are combined to give a scheme in which the number of keyrings can be varied directly in a more flexible manner.

In this paper, we examine more closely the actual effects of removing keyrings from a combinatorial KPS. We focus specifically on the family of schemes proposed by Lee and Stinson based on transversal designs [5], since they have been shown to behave well for a wide range of parameters [9]. In Sect. 2, we exploit the structure of resolvable transversal designs to propose a deterministic method for selecting keyrings to remove from the schemes of Lee and Stinson without unduly affecting their performance. The properties of these modified schemes are easy to analyse using the framework established in [9], and we exploit this feature to compare their performance directly with the combinatorial schemes from which they were derived, demonstrating that they yield a family of schemes with a flexible choice of parameters whose properties compare favourably with those of existing schemes.

In addition, for a broad range of parameter choices, we consider networks consisting of various numbers of nodes with keyrings chosen uniformly at random from transversal design KPSs, and we compute the mean and standard deviation of the resulting values of the security and performance metrics for these schemes. The results, given in Sect. 3.2, demonstrate that the change in these metrics as keyrings are removed is in fact very limited, and largely predictable.

Computing properties of schemes obtained by randomly deleting some number of keyrings from a combinatorial scheme can be time-consuming. Therefore, in Sect. 4 we describe a new approach to facilitate the efficient evaluation of metrics for connectivity and resilience in general KPSs. This approach is based on some new formulas for these metrics that are of independent interest.

1.1 Overview of the Construction and Analysis of Combinatorial Key Predistribution Schemes

A *set system* $(X, \mathcal{A})$ consists of a finite set X of *points*, together with a finite set $\mathcal{A}$ of subsets of X, which are known as *blocks*. A set system can be used to construct a KPS by associating each key in a certain keyspace with an element of X and each node with an element of $\mathcal{A}$, so that a node is preloaded with the keys that correspond to points lying in its corresponding block. The point x acts as a *key identifier* for the corresponding secret key. Key identifiers (and which nodes hold which key identifiers) are public information, whereas the values of the keys are secret (known only to the nodes that hold them).

Example 1. Let

$$\begin{aligned} X &= \{1,2,3,4,5,6,7,8,9\}, \quad \text{and} \\ \mathcal{A} &= \{123, 456, 789, 147, 258, 369, \\ &\qquad 159, 267, 348, 168, 249, 357\}. \end{aligned}$$

Then $(X, \mathcal{A})$ is a set system in which there are nine points and twelve blocks. Each block contains three points. The associated KPS will have 12 nodes, each of which possesses three of the nine secret keys.

It is easy to see that, in this model, the Eschenauer-Gligor scheme [4] is obtained when the underlying set system consists of n random k-subsets of the v-set X. On the other hand, combinatorial key predistribution schemes are typically based on set systems arising from combinatorial objects with nice properties that ensure the resulting schemes perform well and are amenable to analysis. Particular examples of combinatorial objects that have been proposed for use in key distribution in this way include projective planes, generalised quadrangles, configurations, common intersection designs, transversal designs of strength 2 or 3, partially balanced incomplete block designs, inversive planes [3], orthogonal arrays, Reed-Solomon codes, mutually-orthogonal Latin squares, and rational normal curves in projective spaces (see [9] for a survey and analysis of such schemes).

In this paper, we focus mainly on transversal designs, which we define now.

Definition 1. *Let t, n and k be positive integers such that $t \leq k \leq n$. A* transversal design TD(t,k,n) *is a triple $(X, \mathcal{H}, \mathcal{A})$, where X is a finite set of cardinality kn, $\mathcal{H}$ is a partition of X into k parts (called* groups*) of size n and $\mathcal{A}$ is a set of k-subsets of X (called* blocks*), which satisfy the following properties:*

1. *$|H \cap A| = 1$ for every $H \in \mathcal{H}$ and every $A \in \mathcal{A}$, and*
2. *every subset of t elements of X from t different groups occurs in exactly one block in $\mathcal{A}$.*

The parameter t is called the strength of the transversal design.

We note that transversal designs are equivalent to other familiar combinatorial objects such as orthogonal arrays and maximum distance separable (MDS) codes; see [9, Sect. 2.7] for further discussion on these equivalences.

Example 2. Lee and Stinson [5] proposed a family of combinatorial KPSs based on transversal designs $\mathrm{TD}(2, k, p)$. The set systems they use can be constructed explicitly as follows:

For p a prime and k an integer with $2 \leq k \leq p$ we construct a $\mathrm{TD}(2, k, p)$ by letting the points be all elements of the form (a, b) where $a \in \{0, 1, \ldots, k-1\}$ and $b \in \mathbb{Z}_p$. The transversal design has p^2 blocks, which are given by the sets of the form

$$A_{i,j} = \{(x, ix + j \pmod p) | 0 \leq x \leq k-1\}.$$

This construction can be generalised in an obvious way by replacing $\mathbb{Z}_p$ by the finite field $\mathrm{GF}(n)$. Hence, we can obtain a transversal design $\mathrm{TD}(2, k, n)$ with n^2 blocks for any prime power n. It is straightforward to show that in this scheme any two nodes share either 1 key or 0 keys; as such we specify that $\eta = 1$ and hence two neighbouring nodes form a secure link if they share one common key.

To construct a transversal design of strength 3 (a $\mathrm{TD}(3, k, p)$) the points are taken to be all elements of the form (a, b) where $a \in \{0, 1, \ldots, k-1\}$ and $b \in \mathbb{Z}_p$, as before. For each of the p^3 polynomials f in $\mathbb{Z}_p[x]$ of degree at most 2 we obtain a block by taking the set of points of the form

$$A_f = \{(x, f(x) \pmod p) | 0 \leq x \leq k-1\}.$$

Once again, we can replace $\mathbb{Z}_p$ by the finite field $\mathrm{GF}(n)$ in this construction and obtain a $\mathrm{TD}(3, k, n)$ for any prime power n. Two nodes in this scheme share either 0, 1 or 2 keys. Hence we can choose to use an intersection threshold of either $\eta = 1$ or $\eta = 2$ for specifying the minimum number of keys that must be shared by two nodes before they can form a secure link.

The values of $\mathsf{fail}(1)$ and Pr_1 for these schemes, in the case of strength 2 with $\eta = 1$ and strength 3 with $\eta = 1$ or $\eta = 2$, are given in Table 1.

For the transversal designs $\mathrm{TD}(t, k, n)$ for both $t = 2$ and $t = 3$ described above, the points of the design can be partitioned into k subsets H_i, for $0 \leq i \leq k-1$, by setting

$$H_i = \{(i, b) | b \in \mathrm{GF}(n)\}.$$

These sets H_i are known as the *groups* of the transversal design. It is straightforward to show that each subset of t points of the transversal design from t different groups occur together in exactly one block of the transversal design.

Example 3. Bose et al. [1] proposed a family of KPSs obtained by combining η designs that are the duals of designs derived from association schemes. For the sake of clarity, we will restrict ourselves to the specific instantiation in which the designs are all copies of a $\mathrm{TD}(2, k, n)$.

In the case of $\eta = 1$, the Bose et al. scheme instantiated with a $\mathrm{TD}(2, k, n)$ coincides exactly with Lee and Stinson's transversal design scheme.

For $\eta = 2$, they take two copies of a $\mathrm{TD}(2, k, n)$ and construct a new set system by letting the set of points be the union of the sets of points of each of the designs, and by letting the blocks be given by all possible unions of the form $B_1 \cup B_2$ where B_1 is a block of the first $\mathrm{TD}(2, k, n)$ and B_2 is a block of the second $\mathrm{TD}(2, k, n)$. This scheme has $2kn$ points, and n^4 blocks. Each block contains $2k$ points, and two blocks intersect in either 0, 1, 2, k, or $k + 1$ points.

As observed in [5], combinatorial schemes possess several distinct advantages as compared to random schemes such as Eschenauer-Gligor:

- the deterministic nature and regular structure of combinatorial schemes ensure that the precise values of metrics of the scheme such as $\mathsf{fail}(1)$ and Pr_1 can be computed exactly, rather than simply the expected value of these quantities;
- combinatorial schemes reduce the quantity of random numbers that must be generated in setting up the scheme;
- most importantly, for many combinatorial schemes, their regular structure leads to very efficient algorithms for performing tasks such as shared key discovery once the nodes are deployed.

As such, combinatorial schemes can represent an efficient and effective way of establishing keys in many WSN scenarios.

A survey and analysis of many existing combinatorial schemes was carried out in [9]. The concept of a *partially balanced t-design* (PBtD) was introduced, and explicit formulas for evaluating $\mathsf{fail}(1)$ and Pr_1 were given for any combinatorial scheme that can be constructed from a PBtD.

Definition 2. *For positive integers v, k, t and λ_i with $0 \leq i \leq t - 1$, a $t - (v, k, \lambda_0, \lambda_1, \ldots, \lambda_{t-i})$*-partially balanced t-design *is a pair $(X, \mathcal{A})$ with the following properties:*

1. *X is a finite set whose elements are referred to as* points*, and $\mathcal{A}$ is a finite set of k-subsets of X; its elements are referred to as* blocks*.*
2. *There are λ_0 blocks in $\mathcal{A}$.*
3. *For $1 \leq i \leq t - 1$, each subset of i points of X occurs in either no blocks, or in exactly λ_i blocks.*
4. *For $t \leq i \leq k$, each subset of i points occurs in either 0 or 1 blocks.*

Paterson and Stinson [9] showed that a wide range of existing combinatorial KPSs (including KPSs constructed from transversal designs) could be modelled as PBtDs. The advantage of doing so is that the properties of these schemes can easily be evaluated and compared with the aid of the formulas given in [9]. The resulting values for a range of schemes are given in Table 1. The transversal-design based schemes described in Example 2 were shown to provide a good degree of flexibility for the construction of KPSs relative to other PBtDs, since they are easily constructed for a wide range of useful parameters, the block size

can be chosen independently of the network size, and the values of t and η can also be varied independently.

The KPSs of Bose et al. [1] are not PBtDs, and hence they cannot be analysed directly using the approach of [9]. One of the motivations behind their schemes is to provide constructions that can yield KPSs for a flexible choice of network size; in [1], they note that "the number of nodes need not be of the particular forms p^2 or p^3, with p prime or prime power". The traditional view of combinatorial construction of KPSs is that, provided a range of parameters is available, then if a specific network size n is desired it suffices to choose parameters to give a scheme that suits a network of size greater than n and simply discard the unneeded keyrings. Bose et al. [1] object (with particular reference to [5]) that "if we then discard the unnecessary node allocations to get the final scheme for use, this final scheme will not preserve the Pr_1 and $\mathsf{fail}(s)$ values of the original scheme and hence the properties of the final scheme in this regard can become quite erratic" [1]. One main goal of our paper is to refute this statement.

1.2 Outline of the Paper

In Sect. 2, we present two approaches to increasing the flexibility of combinatorial predistribution schemes based on transversal designs. One approach is randomized and the other is deterministic. In Sect. 3, we perform extensive comparisons of our generalized constructions to the original transversal design schemes. In Sect. 4, we derive new formulas that facilitate the computation of metrics for connectivity and resilience for arbitrary key predistribution schemes based on set systems. Finally, Sect. 5 is a short conclusion.

2 Two Approaches to Varying the Network Size in KPSs based on Transversal Designs

In this section we consider two distinct approaches to varying the network size in the transversal design-based KPSs of Lee and Stinson. One option is to use the standard approach of randomly removing blocks from the design.

Scheme 1 (Random scheme). *Suppose a KPS is desired for a network containing m nodes. Let n be the smallest prime power satisfying $n^2 \geq m$. Then by constructing a* $\mathrm{TD}(2, k, n)$ *and selecting a subset of m blocks uniformly at random we obtain a set system that can be used to provide a KPS for the network.*

Similarly, we can construct a KPS for this network based on a transversal design of strength 2 by taking n to be the smallest prime power with $n^3 \geq m$, and then selecting m blocks uniformly at random from the set of blocks of a $\mathrm{TD}(3, k, n)$.

The benefits of such an approach include its simplicity and the fact that it can be applied for any value of m. It is a very natural approach, given that it mirrors precisely the commonly anticipated situation in which a small number of

nodes may fail or run out of power after deployment. We will see that this scheme performs well in practice: in Sect. 3.2 we demonstrate that for a wide range of parameter choices, restricting to a random subset of blocks of a $\mathrm{TD}(2, k, n)$ does not adversely affect the expected performance of schemes based on these designs. Furthermore, we still retain some desirable properties of combinatorial schemes such as efficient shared key discovery.

One of the other underlying motivations of using combinatorial designs to construct KPSs is the fact that their deterministic and highly structured nature allows us to guarantee the values they attain for metrics such as $\mathsf{fail}(1)$ and Pr_1. If blocks are deleted at random, we lose these guarantees, even though diminished performance is very unlikely. In this section we propose a second technique, to overcome this possible drawback. We demonstrate how to exploit the structure of transversal designs in order to select subsets of the blocks *deterministically* in such a way that the precise performance of the resulting structure is straightforward to evaluate. Specifically, we will make use of *resolvable transversal designs* to accomplish this objective.

2.1 Resolvable Transversal Designs of Strength 2

Definition 3. *A transversal design* $TD(2, k, n)$ *is said to be* resolvable *if it is possible to partition the blocks of the design into sets* $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n$*, such that each point of the design belongs to precisely one block in each set. The sets* $\mathcal{B}_i$ *are known as* parallel classes *of the design.*

Resolvable transversal designs have previously been exploited for constructing KPSs suited for networks where there is group deployment of nodes; see [8]. The transversal design KPSs proposed by Lee and Stinson do not require the resolvability property; however, the transversal designs $\mathrm{TD}(2, k, n)$ used in [5] are in fact resolvable.

Example 4. For the $\mathrm{TD}(2, k, n)$ described in Example 2, the parallel classes of blocks are given by

$$\mathcal{B}_i = \{\mathcal{A}_{i,j} | j \in \mathrm{GF}(n)\}, i \in \mathrm{GF}(n).$$

It is straightforward to see that no point lies in two distinct blocks of a given parallel class, since if a point (x, y) were in blocks $\mathcal{A}_{i,j}$ and $\mathcal{A}_{i,h}$, this would imply that $y = ix + j$ and also $y = ix + h$, whence $j = h$.

A resolvable transversal design $\mathrm{TD}(2, k, n)$ has n parallel classes with n blocks in each class. We propose using such designs for key predistribution as follows:

Scheme 2 (Linear scheme). *We construct a set system for use in a KPS by starting with a resolvable* $TD(2, k, n)$*, where* n *is a prime power. Let* ℓ *be an integer between 1 and* n*. Select* ℓ *parallel classes of blocks of the design, and let the blocks in these parallel classes be the blocks of the set system. We refer to the resulting set system as a* $\overline{\mathrm{TD}}(2, k, n, \ell)$*.*

As each parallel class contains n blocks, this means that Scheme 2 yields a KPS with ℓn keyrings. This number can be varied as required by choosing an appropriate value of ℓ: roughly speaking, we require that $n \geq \sqrt{m}$ and $\ell \approx m/n$. One nice feature of this method of choosing blocks is that the resulting incidence structure is in fact a PBtD, and hence its properties can be determined in a straightforward manner simply by using the formulas given in [9]. We now perform this analysis to show that Scheme 2 performs well even for comparatively small values of ℓ.

Theorem 1. *A* $\overline{\mathrm{TD}}(2, k, n, \ell)$ *is a* 2-$(kn, k, \ell n, \ell)$-*PBtD*

Proof. Take ℓ parallel classes of blocks from a resolvable TD$(2, k, n)$, and let $\mathcal{A}$ be the set of blocks in these parallel classes. Let X be the set of points in the TD$(2, k, n)$; we note that X contains kn points. Now, $\mathcal{A}$ contains $\lambda_0 = \ell n$ blocks, each containing k points. Every point of X is contained in precisely one block in each parallel class, and hence is contained in precisely $\lambda_1 = \ell$ blocks of $\mathcal{A}$. Furthermore, since each pair of points in X is contained in either 0 or 1 blocks of the TD$(2, k, n)$, it follows that any pair of points is contained in either 0 or 1 blocks of $\mathcal{A}$. Thus $(X, \mathcal{A})$ satisfies all the properties of a 2-$(kn, k, \ell n, \ell)$-PBtD.

The values of $\mathsf{fail}(1)$ and Pr_1 for a PBtD are easy to compute systematically using the explicit formulas given in [9]. For a given block B of a PBtD and a point C on that block, denote by $\mu'(1)$ the number of blocks A of the PBtD such that $A \cap B = \{C\}$ (it was shown in [9] that this value is independent of the choice of point and block.) Define a *link* to be a pair of blocks with nonempty intersection. We let L denote the total number of links in a PBtD, we let α denote the number of links in which a given block B is contained, and we let β denote the number of links $\{A, C\}$ with $B \neq A, C$ such that $A \cap C \subset B$ (again, these values do not depend on the specific choice of B). Then, applying the formulas of [9] to a 2-$(kn, k, \ell n, \ell)$-PBtD, we have:

$$\begin{aligned}
\mu'(1) &= \lambda_1 - 1 = \ell - 1, \\
\alpha &= k\mu'(1) = k(\ell - 1), \\
\beta &= \mu'(1)\left(\frac{\lambda_1}{2} - 1\right) k = (\ell - 1)\left(\frac{\ell}{2} - 1\right) k, \\
L &= \frac{b\alpha}{2} = \frac{\ell n k(\ell - 1)}{2}, \\
\mathsf{fail}(1) &= \frac{\beta}{L - \alpha} = \frac{\ell - 2}{\ell n - 2}, \\
\mathsf{Pr}_1 &= \frac{\alpha}{b - 1} = \frac{k(\ell - 1)}{\ell n - 1}.
\end{aligned}$$

In the case where $\ell = n$, a $\overline{\mathrm{TD}}(2, k, n, \ell)$ is simply a TD$(2, k, n)$, and hence Scheme 2 is a generalisation of the corresponding scheme of Lee and Stinson. The formulas computed above for $\mathsf{fail}(1)$ and Pr_1 can be seen to agree with the corresponding formulas for Lee and Stinson's scheme in the case where $\ell = n$.

2.2 Transversal Designs of Higher Strength

Just as in the case of transversal designs of strength 2, it is possible to deterministically select subsets of blocks from transversal designs of higher strength, such as the $\mathrm{TD}(3, k, n)$ suggested for use in key predistribution by Lee and Stinson, in a way that allows flexibility in the number of keyrings of the resulting scheme, while still maintaining good performance. We begin by illustrating a useful approach to partitioning the blocks of the $\mathrm{TD}(3, k, n)$ described in Example 2.

Example 5. Let n be a prime power and let X be the set of points of one of the $\mathrm{TD}(3, k, n)$ whose construction is described in Example 2. We can partition the blocks of this design into sets $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n$ by defining

$$\mathcal{B}_i = \{\mathcal{A}_f | f(x) = ix^2 + ax + b \text{ for some } a, b \in \mathrm{GF}(n)\}, i \in \mathrm{GF}(n).$$

We show, for each i, that the incidence structure $(X, \mathcal{B}_i)$ is a $\mathrm{TD}(2, k, n)$, with the same groups as the original $\mathrm{TD}(3, k, n)$. Suppose this is not the case. Then there is a pair $\{(x, A), (y, B)\}$ (where $x \neq y$) that appears in two blocks of the same $\mathcal{B}_i$. So we have

$$ix^2 + ax + b = A = ix^2 + cx + d \quad \text{and} \quad iy^2 + ay + b = B = iy^2 + cy + d.$$

From this, we get

$$ax + b = cx + d \quad \text{and} \quad ay + b = cy + d.$$

Since $x \neq y$, we have $a = c$, which implies $b = d$. Therefore the two blocks coincide and we have a contradiction.

Scheme 3 (Quadratic scheme). *Let n be a prime power. Starting with a $TD(3, k, n)$, we define a set system by letting ℓ be an integer between 1 and n, selecting ℓ of the sets $\mathcal{B}_i$, and letting $\mathcal{A}$ be the set of blocks in these ℓ sets. We refer to the incidence structure $(X, \mathcal{A})$ as a $\overline{\mathrm{TD}}(3, k, n, \ell)$. Using a $\overline{\mathrm{TD}}(3, k, n, \ell)$ for constructing a KPS in the standard way yields a scheme with ℓn^2 keyrings, for which we can choose an intersection threshold of either $\eta = 1$ or $\eta = 2$.*

As before, this method of selecting blocks yields a structure that is easy to analyse:

Theorem 2. *A $\overline{\mathrm{TD}}(3, k, n, \ell)$ is a 3-$(kn, k, \ell n^2, \ell n, \ell)$-PBtD.*

Proof. A $\overline{\mathrm{TD}}(3, k, n, \ell)$ consists of a set of kn points, together with ℓ disjoint sets of n^2 blocks of k points, and thus has ℓn^2 blocks in total. Every point of the $\overline{\mathrm{TD}}(3, k, n, \ell)$ is contained in n blocks in each of these sets, and therefore is contained in ℓn blocks in total. If a pair of points belong to a group of the underlying $\mathrm{TD}(3, k, n)$ then they do not occur together in any block of the $\overline{\mathrm{TD}}(3, k, n, \ell)$. If two points lie in different groups, then in each of the ℓ sets $\mathcal{B}_i$ there is precisely one block that contains them. Thus any pair of points occurs together in either 0 or ℓ blocks of the $\overline{\mathrm{TD}}(3, k, n, \ell)$. Finally, any set of three points occur together in either 0 or 1 blocks of the $\mathrm{TD}(3, k, n)$ and thus also occur together in 0 or 1 blocks of the $\overline{\mathrm{TD}}(3, k, n, \ell)$.

This allows us to use the formulas of [9] to compute $\mathsf{fail}(1)$ and Pr_1. Defining $\mu'(2)$ to be the number of blocks C whose intersection with a given block B is a given set $S \subset B$ of two points, we have

$$\begin{aligned}\mu'(2) &= \lambda_2 - 1 = \ell - 1,\\ \mu'(1) &= \lambda_1 - 1 - (k-1)\mu'(2) = \ell n - 1 - (k-1)(\ell-1).\end{aligned}$$

For a KPS with intersection threshold $\eta = 2$ we have

$$\begin{aligned}\alpha &= \binom{k}{2}\mu'(2) = \binom{k}{2}(\ell-1),\\ \beta &= \mu'(2)\left(\frac{\lambda_2}{2}-1\right)\binom{k}{2} = (\ell-1)\left(\frac{\ell}{2}-1\right)\binom{k}{2},\\ L &= \frac{b\alpha}{2} = \frac{\ell n^2(\ell-1)}{2}\binom{k}{2},\\ \mathsf{fail}(1) &= \frac{\beta}{L-\alpha} = \frac{\ell-2}{\ell n^2-2},\\ \mathsf{Pr}_1 &= \frac{\alpha}{b-1} = \frac{k(k-1)(\ell-1)}{2(\ell n^2-1)}.\end{aligned}$$

Using intersection threshold $\eta = 1$ gives

$$\begin{aligned}\alpha &= k\mu'(1) + \binom{k}{2}\mu'(2) = k(\ell n - 1) - \binom{k}{2}(\ell-1),\\ \beta &= \mu'(1)\left(\frac{\lambda_1}{2}-1\right)k + \mu'(2)\left(\frac{\lambda_2}{2}-1\right)\binom{k}{2},\\ &= (\ell n - 1 - (k-1)(\ell-1))\,k\left(\frac{\ell n}{2}-1\right) + (\ell-1)\left(\frac{\ell}{2}-1\right)\binom{k}{2},\\ L &= \frac{b\alpha}{2} = \frac{\ell n^2\left(k(\ell n-1) - \binom{k}{2}(\ell-1)\right)}{2},\\ \mathsf{fail}(1) &= \frac{\beta}{L-\alpha} = \frac{2(\ell n-1)(\ell n-2) - (k-1)(\ell-1)(2\ell n-\ell-2)}{(\ell n^2-2)(2\ell n-2-(k-1)(\ell-1))},\\ \mathsf{Pr}_1 &= \frac{\alpha}{b-1} = \frac{k(2\ell n-2-(k-1)(\ell-1))}{2(\ell n^2-1)}.\end{aligned}$$

In the case where $\ell = n$, a $\overline{\mathrm{TD}}(3,k,n,\ell)$ is simply a $\mathrm{TD}(3,k,n)$ and Scheme 2 is a generalisation of the corresponding scheme of Lee and Stinson. When $\ell = n$, the formulas computed above for $\mathsf{fail}(1)$ and Pr_1 agree with the corresponding formulas for Lee and Stinson's scheme.

2.3 Finer Control Over the Number of Blocks

Scheme 3 provides KPSs with ℓn^2 keyrings by selecting ℓ disjoint sets of n^2 blocks from a $\mathrm{TD}(3,k,n)$. Each of these sets of blocks is in fact a resolvable

$\mathrm{TD}(2, k, n)$. Thus, if a more fine-grained choice of network size is required, it would be possible to choose ℓ sets of blocks, together with m parallel classes of blocks from an $(\ell+1)^{\text{th}}$ copy of a $\mathrm{TD}(2, k, n)$. This would yield a network with $\ell n^2 + mn$ keyrings; appropriate choices of ℓ and m thus allow the network size to be adjusted to the nearest multiple of n. The resulting combinatorial structure would be a 3-$(kn, k, \ell n^2 + mn, \ell n + m, \ell + 1)$-PB$t$D, and hence could be analysed in a similar manner to the schemes based on a $\overline{\mathrm{TD}}(3, k, n, \ell)$.

3 Analysis and Comparisons of the New Constructions with Previous Schemes

In this section, we compare the new schemes (Scheme 1, 2 and 3) with the transversal design schemes from which they were derived. Recall that Scheme 1 consists of random blocks chosen from a transversal design, while Scheme 2 and Scheme 3 are deterministic schemes consisting of specified blocks from transversal designs of strength 2 and 3, respectively.

First, Table 1 summarizes the formulas for six deterministic schemes. The six schemes considered in Table 1 (denoted A–F) are the following:

A: Scheme 2, based on a $\overline{\mathrm{TD}}(2, k, n, \ell)$
B: Scheme 3, based on a $\overline{\mathrm{TD}}(3, k, n, \ell), \eta = 2$
C: Scheme 3, based on a $\overline{\mathrm{TD}}(3, k, n, \ell), \eta = 1$
D: Scheme 2, based on a $\mathrm{TD}(2, k, n)$ (i.e., Scheme 2 with $\ell = n$)
E: Scheme 3, based on a $\mathrm{TD}(3, k, n), \eta = 2$ (i.e., Scheme 3 with $\ell = n$)
F: Scheme 3, based on a $\mathrm{TD}(3, k, n), \eta = 1$ (i.e., Scheme 3 with $\ell = n$)

Table 1. Metrics for some transversal design based schemes

Scheme	Pr_1	$\mathsf{fail}(1)$
A.	$\dfrac{k(\ell-1)}{\ell n - 1}$	$\dfrac{\ell - 2}{\ell n - 2}$
B.	$\dfrac{k(k-1)(\ell-1)}{2(\ell n^2 - 1)}$	$\dfrac{\ell - 2}{\ell n^2 - 2}$
C.	$\dfrac{k(2\ell n - 2 - (k-1)(\ell-1))}{2(\ell n^2 - 1)}$	$\dfrac{2(\ell n - 1)(\ell n - 2) - (k-1)(\ell-1)(2\ell n - \ell - 2)}{(\ell n^2 - 2)(2\ell n - 2 - (k-1)(\ell-1))}$
D.	$\dfrac{k}{n+1}$	$\dfrac{n-2}{n^2-2}$
E.	$\dfrac{k(k-1)}{2(n^2+n+1)}$	$\dfrac{n-2}{n^3-2}$
F.	$\dfrac{k(2n-k+3)}{2(n^2+n+1)}$	$\dfrac{2n^3 + (4-2k)n^2 + (k-5)n + 2k - 6}{(2n-k+3)(n^3-2)}$

In Sect. 3.1, we briefly discuss asymptotic comparisons between the deterministic schemes A–F, using the formulas in Table 1. In Sect. 3.2, these formulas are evaluated for a range of parameter choices to provide a direct comparison with the corresponding values for equivalent parameter choices in Scheme 1 (the Random Scheme).

3.1 Asymptotic Comparisons

It is interesting to compare Scheme 2 and Scheme 3 to the transversal design schemes on which they are based. In Scheme 2 and Scheme 3, we have an additional parameter $\ell \leq n$ (the original schemes correspond to $\ell = n$). Suppose $c < 1$ is a positive real number and we take $\ell = cn$. We compute the ratio of the values of Pr_1 for schemes labelled A and D in Table 1 using the formulas given there:

$$\frac{\mathsf{Pr}_1(\text{scheme } A)}{\mathsf{Pr}_1(\text{scheme } D)} = \frac{\frac{k(cn-1)}{cn^2-1}}{\frac{k}{n+1}} = \frac{(cn-1)(n+1)}{cn^2-1}.$$

As $n \to \infty$, it is easy to see that this ratio approaches 1.

Thus, for example, if we use only $n/1000$ of the n parallel classes, the connectivity of the partial scheme is asymptotically the same as the transversal design scheme on which it is based. A similar result holds for resilience, as can be seen by computing the ratios of the relevant $\mathsf{fail}(1)$ values. Furthermore, a similar phenomenon is observed for Scheme 3, for both $\eta = 1$ and $\eta = 2$, i.e., when we use the formulas for the schemes labelled B and E, as well as for the schemes labelled C and F. We summarize this as follows.

Theorem 3. *Let $0 < c < 1$ and let $\ell = cn$ in scheme A, B or C from Table 1. Then*

$$\lim_{n\to\infty} \frac{\mathsf{Pr}_1(\text{scheme } A)}{\mathsf{Pr}_1(\text{scheme } D)} = \lim_{n\to\infty} \frac{\mathsf{fail}(1)(\text{scheme } A)}{\mathsf{fail}(1)(\text{scheme } D)} = 1,$$

$$\lim_{n\to\infty} \frac{\mathsf{Pr}_1(\text{scheme } B)}{\mathsf{Pr}_1(\text{scheme } E)} = \lim_{n\to\infty} \frac{\mathsf{fail}(1)(\text{scheme } B)}{\mathsf{fail}(1)(\text{scheme } E)} = 1,$$

and

$$\lim_{n\to\infty} \frac{\mathsf{Pr}_1(\text{scheme } C)}{\mathsf{Pr}_1(\text{scheme } F)} = \lim_{n\to\infty} \frac{\mathsf{fail}(1)(\text{scheme } C)}{\mathsf{fail}(1)(\text{scheme } F)} = 1.$$

3.2 Comparisons for Explicit Parameter Choices

In this section, we compare the random and deterministic schemes we have presented. We consider transversal designs of strengths 2 and 3 that are appropriate for maximum network sizes of (approximately) 5000 nodes and 24000 nodes:

- The transversal designs yielding maximum network size 5000 (approximately) are TD(2,15,71) and TD(3,15,17); note that $71^2 = 5041$ and $17^3 = 4913$. Here the block size is 15, which means that nodes will each store 15 keys.
- The transversal designs for maximum network size 24000 (approximately) are TD(2,25,157) and TD(3,25,29); note that $157^2 = 24649$ and $29^3 = 24387$. Here the block size is 25, which means that nodes will each store 25 keys.

We analyse and compare the behaviour of Scheme 1, Scheme 2 and Scheme 3 for the parameters listed above; in particular, we evaluate $\mathsf{fail}(1)$ and Pr_1 for these schemes. In the case of Scheme 2 and Scheme 3, we have used the formulas from Table 1 to obtain these values. For each choice of n and k, we evaluated

$\mathsf{fail}(1)$ and Pr_1 for the schemes based on a $\overline{\mathrm{TD}}(2,k,n,\ell)$ or $\overline{\mathrm{TD}}(3,k,n,\ell)$ with $\eta = 1, 2$, for every ℓ between 2 and n inclusive. In the case of Scheme 1, for each network size m, we constructed 100 random instances of the KPS and we computed the exact values of $\mathsf{fail}(1)$ and Pr_1 for each of these 100 instances.

The results of these calculations are presented in graphical form in Figs. 1, 2, 3, 4, 5 and 6. In these figures, we plot the connectivity or resilience of a random scheme and a corresponding deterministic scheme. The solid lines, labelled "random", refer to Scheme 1; the dashed lines, labelled "parallel", refer to Scheme 2 or Scheme 3. The dotted lines, labelled "σ", indicate the standard deviation of the values computed for Scheme 1 over the 100 trials (since the standard deviations are quite small, these lines are very close to the bottom of the graphs). The value m is the number of blocks in the associated set system (i.e., the number of nodes in the network).

In the case of Scheme 1, we also computed the maximum and minimum values of $\mathsf{fail}(1)$ and Pr_1 obtained over the 100 trials, for each value of m. As well, we

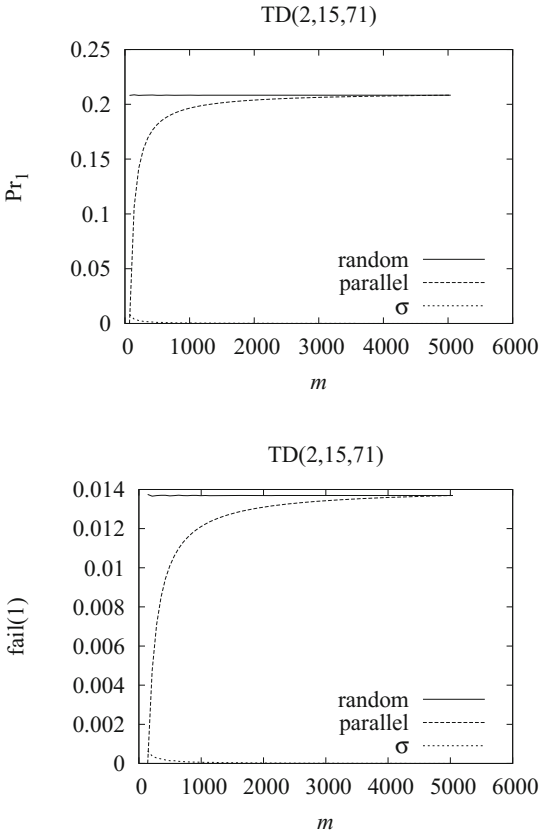

Fig. 1. Connectivity and resilience of KPSs derived from TD(2,15,71)

have tabulated the mean and standard deviation over the 100 samples. In these two tables, the network size is $m = \ell n = 71\ell$. This data is presented, for the schemes derived from a TD(2,15,71), in Tables 3 and 4 in the Appendix.

Some of the main observations we can draw from these results are as follows:

- In Figs. 1–6, the plots of the values of fail(1) or Pr_1 as blocks are selected uniformly from a TD$(2, k, n)$ or TD$(3, k, n)$ (Scheme 1) are all essentially a horizontal line, indicating that on average the values of fail(1) and Pr_1 do not change greatly, even if the number of blocks selected is quite small. This is entirely to be expected: fail(1) and Pr_1 by definition are quantities that represent an average over all the keyrings in the network, so taking the average over smaller, uniformly selected subsets of keyings should not affect these values too much. The average values computed in our experiments are in fact very close to the exact average values that are computed theoretically.
- One quantity of particular interest here is the standard deviation of fail(1) and Pr_1 for Scheme 1, since this determines the extent to which a particu-

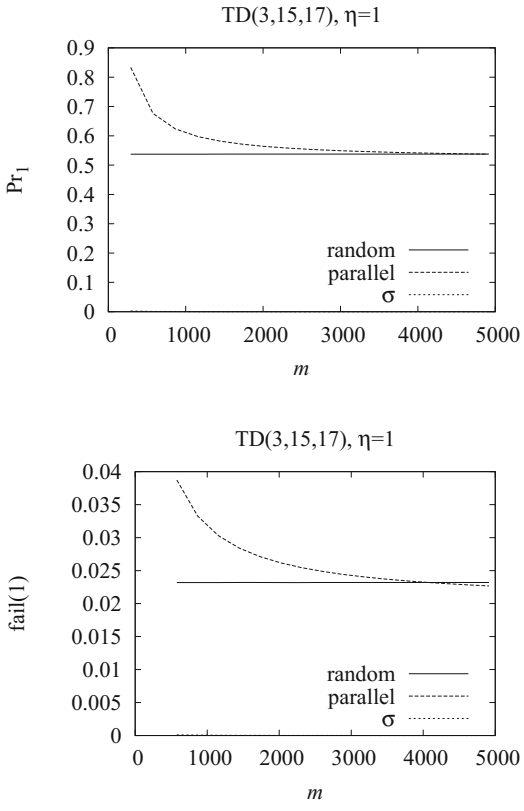

Fig. 2. Connectivity and resilience of KPSs derived from TD(3,15,17) with $\eta = 1$

lar random choice of subnetwork may have $\mathsf{fail}(1)$ or Pr_1 values that differ from the average values for the scheme as a whole. Naturally, the standard deviation of these values increases slightly when the number blocks is very small. However, we can see from Figs. 1–6 that these standard deviations are still extremely low, especially in the case of schemes obtained from the larger designs. Moreover, there is a very low range of values of $\mathsf{fail}(1)$ and Pr_1 encountered in our experiments. This is evident from Tables 3 and 4 in the Appendix, for the schemes derived from a TD(2,15,71). Schemes derived from other transversal designs exhibit similar behaviour in terms of the variability of these metrics. Thus we see that in practice, selecting random subsets of the keyrings is unlikely to have much of an effect on the values of $\mathsf{fail}(1)$ and Pr_1 for the scheme.

– In Scheme 2, when the number ℓ of parallel classes is very small, the value of Pr_1 is low, due to the fact that no two blocks within a given parallel class have any points in common. Nevertheless, Figs. 1 and 4 demonstrate that this value grows rapidly as ℓ increases, and soon approaches the Pr_1 value

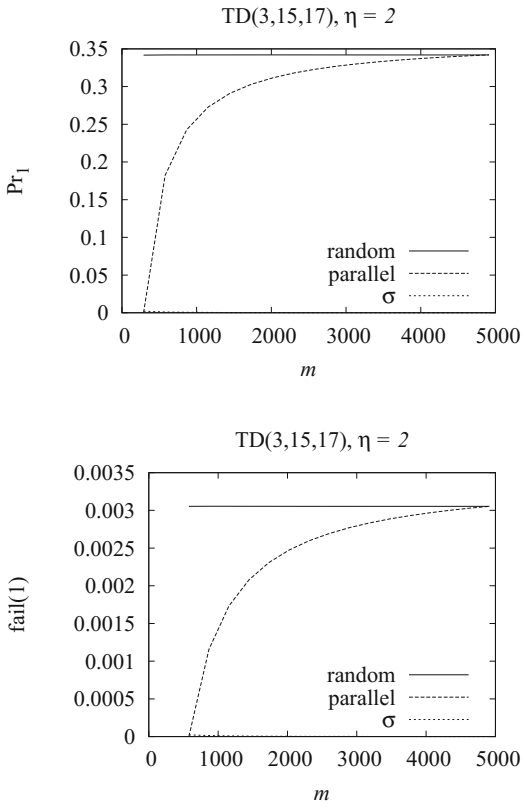

Fig. 3. Connectivity and resilience of KPSs derived from TD(3,15,17) with $\eta = 2$

attained by Scheme 1. On the other hand, for Scheme 2, the value of fail(1) is also low initially, and similarly becomes closer to that of Scheme 1 as ℓ increases. Thus we see that the properties of Scheme 2 and Scheme 1 are very similar in practice, for even moderately large values of ℓ.

- Figures 3 and 6 show that Scheme 3 with intersection threshold $\eta = 2$ exhibits a similar behaviour to that of Scheme 2: the Pr_1 and fail(1) values are low when ℓ is small, but increase rapidly as ℓ becomes larger. The reason for this is entirely analogous: for any given set $\mathcal{B}_i$ of blocks, no two of the blocks in that set intersect in two points, and hence for $\eta = 2$ there are no secure links formed between nodes whose keyrings are derived from such blocks.
- Figures 2 and 5 are interesting, as they show a slightly different behaviour pattern for Scheme 3 in the case of intersection threshold $\eta = 1$. Here the Pr_1 and fail(1) values are in fact higher when ℓ is small, and then decrease for larger values of ℓ, eventually approaching the properties of Scheme 1. This is explained by the fact that two blocks within the same set $\mathcal{B}_i$ have probability $\frac{k}{n+1}$ of sharing a common key (cf. Table 2), which is higher (for the parameters under consideration) than the average probability $\frac{k(2n-k+3)}{2(n^2+n+1)}$ that two blocks chosen uniformly from a $\mathrm{TD}(3, k, n)$ share at least one key. As in previous cases, it is clear from these graphs that once a reasonable number of the sets $\mathcal{B}_i$ are chosen, the properties of Scheme 3 are very close to those of Scheme 1.

We conclude that removal of keyrings from a KPS based on transversal designs, whether randomly or deterministically as in Scheme 2 or 3, causes no undue disruption to the behaviour of the scheme.

4 An Efficient New Approach to Calculating Connectivity and Resilience for Arbitrary Set Systems

In this section, we describe a new approach to facilitate the efficient evaluation of metrics for connectivity and resilience in general KPSs. We were motivated to do this in order to compute the metrics of our random scheme that consists of random subsets of blocks of a transversal design. Suppose we start with any set system $(X, \mathcal{A})$ having blocks of size k. Denote $b = |\mathcal{A}|$. Suppose the maximum intersection of any two blocks in $\mathcal{A}$ is $t-1$. (In a given application, the value of t may already be known beforehand. However, if it were not already known, it could be computed as the first step of the process we are about to describe.)

For $|C| = i$ where $\eta \leq i \leq t-1$, define λ_C to be the number of blocks $A \in \mathcal{A}$ containing all the points in C. It will turn out that we can compute Pr_1 and fail(1) fairly easily if we know all the λ_C values. This has at least two desirable consequences:

1. For various types of "structured" set systems (for example, a partially balanced t-design) we know the relevant λ_C's and so we can compute formulas for Pr_1 and fail(1) in a straightforward manner.

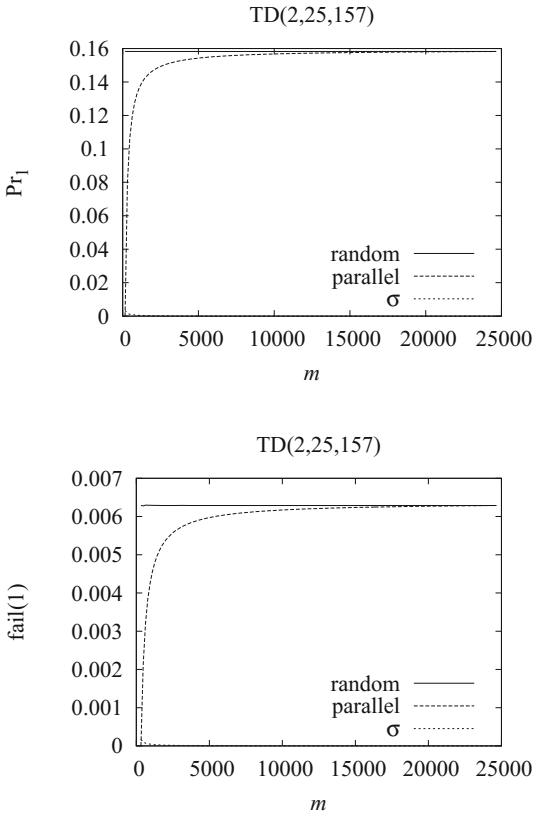

Fig. 4. Connectivity and resilience of KPSs derived from TD(2,25,157)

2. For an arbitrary "unstructured" set system, we can use this approach to compute Pr_1 efficiently. In a "naive" approach, we would probably examine all pairs of blocks to see which pairs form links, which would already require time $\Theta(b^2)$. However, it is straightforward to tabulate all the relevant λ_C values in time $\Theta(b)$, and then apply the formulas we derive, in order to compute Pr_1. This will be discussed further in Sect. 4.3.

4.1 Formulas for Connectivity

For a set of points C with $|C| \geq \eta$, define a *C-link* to be a set of two nodes $\{A, B\}$ such that $A \cap B = C$. The number of C-links is denoted by $\lambda'(C)$; therefore,

$$\lambda'(C) = |\{\{A, B\} : A, B \in \mathcal{A}, A \cap B = C\}|.$$

The next lemma follows easily from the principle of inclusion-exclusion.

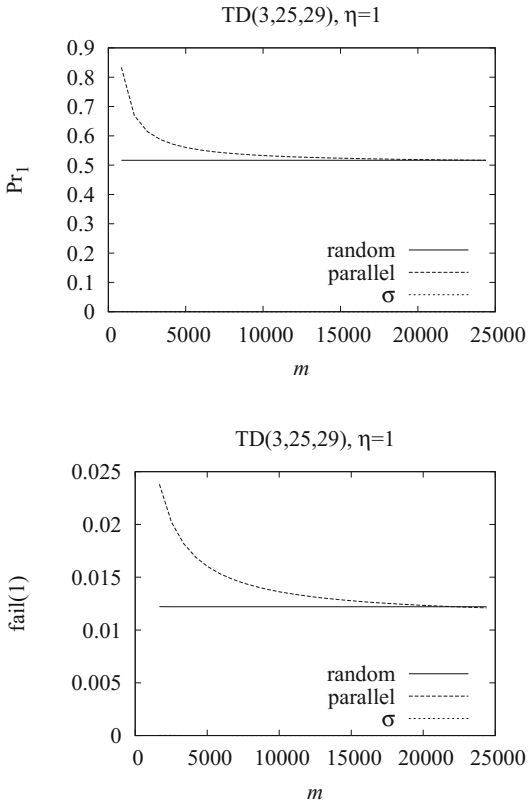

Fig. 5. Connectivity and resilience of KPSs derived from TD(3,25,29) with $\eta = 1$

Lemma 1. *If* $|C| = i \leq t-1$, *then*

$$\lambda'(C) = \sum_{D \subseteq X \setminus C, |D| \leq t-1-i} (-1)^{|D|} \binom{\lambda_{C \cup D}}{2}. \tag{1}$$

In particular, $\lambda'(C) = \binom{\lambda_C}{2}$ *if* $|C| = t-1$.

Define an *i-link* to be any C-link where $|C| = i$. For $\eta \leq i \leq t-1$, let L_i denote the number of i-links (or course, there are no i-links with $i \geq t$). For $\eta \leq i \leq t-1$, it is clear that

$$L_i = \sum_{|C|=i} \lambda'(C). \tag{2}$$

The quantity

$$L = \sum_{i=\eta}^{t-1} L_i \tag{3}$$

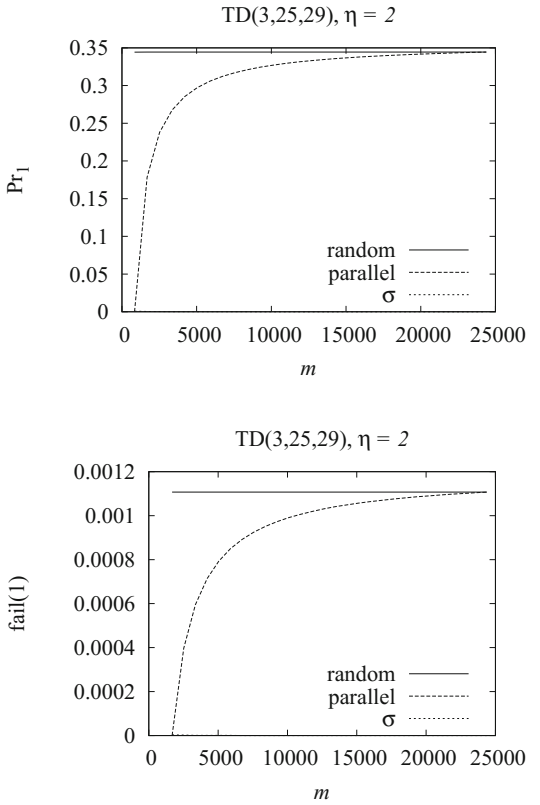

Fig. 6. Connectivity and resilience of KPSs derived from TD(3,25,29) with $\eta = 2$

is the total number of links. From this, it immediately follows that

$$\mathsf{Pr}_1 = \frac{L}{\binom{b}{2}}. \tag{4}$$

Define

$$q_i = \sum_{|C|=i} \binom{\lambda_C}{2}. \tag{5}$$

We now provide a useful formula for L_i.

Lemma 2. *For $\eta \leq i \leq t-1$, we have that*

$$L_i = \sum_{j=i}^{t-1} (-1)^{j-i} \binom{j}{i} q_j. \tag{6}$$

Proof. In view of (2), we need to sum (1) over all C with $|C| = i$. When we do this, each possible term $(-1)^{|D|}\binom{\lambda_{C\cup D}}{2}$ is included in the sum $\binom{|C\cup D|}{|C|} = \binom{|D|+i}{i}$ times.

For $\eta \le i \le t-1$, let

$$a_i = \sum_{j=\eta}^{i} (-1)^{i-j} \binom{i}{j}. \tag{7}$$

Then we have the following.

Theorem 4.

$$L = \sum_{i=\eta}^{t-1} a_i q_i, \tag{8}$$

where the q_i's and a_i's are defined in (5) and (7), respectively.

Proof. We sum the formula (6) as i ranges from η to $t-1$. The number of times q_i is included in the sum is easily seen to be equal to a_i.

We present some applications of the formula (8) for small values of t and η in Table 2.

Table 2. Applications of Theorem 4

t	η	L
2	1	q_1
3	2	q_2
3	1	$q_1 - q_2$
4	3	q_3
4	2	$q_2 - 2q_3$
4	1	$q_1 - q_2 + q_3$
5	4	q_4
5	3	$q_3 - 3q_4$
5	2	$q_2 - 2q_3 + 3q_4$
5	1	$q_1 - q_2 + q_3 - q_4$

Now, applying (8) and (4), we have the following formula for Pr_1.

Corollary 1.

$$\mathsf{Pr}_1 = \frac{\sum_{i=\eta}^{t-1} a_i q_i}{\binom{b}{2}}. \tag{9}$$

4.2 Formulas for Resilience

Recall that a C-link is a set of two nodes $\{A, B\}$ such that $A \cap B = C$. The number of C-links is $\lambda'(C)$ and the number of nodes that break the C-link $\{A, B\}$ is $\lambda_C - 2$. The probability that the C-link $\{A, B\}$ is broken by the compromise of a random node not in the link is $(\lambda_C - 2)/(b - 2)$. Averaging over all L links, we obtain the following formula for $\mathsf{fail}(1)$, which can be viewed as a generalisation of [9, Corollary 4.6]:

$$\mathsf{fail}(1) = \frac{1}{L} \sum_{\{C:\eta \le |C| \le t-1\}} \frac{(\lambda_C - 2)\lambda'(C)}{b-2}. \tag{10}$$

In order to compute $\mathsf{fail}(1)$ using (10), we first need to evaluate the expression $\sum \lambda_C \lambda'(C)$. Substituting (1) into this sum, we have

$$\begin{aligned} \sum_{\{C:\eta \le |C| \le t-1\}} \lambda_C \lambda'(C) &= \sum_{\{C:\eta \le |C| \le t-1\}} \left(\lambda_C \sum_{D \subseteq X \setminus C, |D| \le t-1-i} (-1)^{|D|} \binom{\lambda_{C \cup D}}{2} \right) \\ &= \sum_{\{E:\eta \le |E| \le t-1\}} \left(\binom{\lambda_E}{2} \sum_{\{C:\eta \le |C|, C \subseteq E\}} (-1)^{|E|-|C|} \lambda_C \right), \end{aligned}$$

letting $E = C \cup D$. As a result, we obtain the following.

Lemma 3.

$$\sum_{\{C:\eta \le |C| \le t-1\}} \lambda_C \lambda'(C) = \sum_{\{E:\eta \le |E| \le t-1\}} \mu_E \binom{\lambda_E}{2}, \tag{11}$$

where

$$\mu_E = \sum_{\{C:\eta \le |C|, C \subseteq E\}} (-1)^{|E|-|C|} \lambda_C. \tag{12}$$

For future use, we mention a couple of special cases of (12):

$$\mu_E = \begin{cases} \lambda_E & \text{if} |E| = \eta \\ \lambda_E - \sum_{x \in E} \lambda_{E \setminus \{x\}} & \text{if} |E| = \eta + 1. \end{cases} \tag{13}$$

Next, applying (3) and (2) we have that

$$\sum_{\{C:\eta \le |C| \le t-1\}} 2\lambda'(C) = 2L. \tag{14}$$

Now we can state our main formula.

Theorem 5.

$$\mathsf{fail}(1) = \frac{1}{L(b-2)} \left(\sum_{\{E:\eta \le |E| \le t-1\}} \mu_E \binom{\lambda_E}{2} \right) - \frac{2}{b-2}. \tag{15}$$

Proof. The result follows immediately from (10), (11) and (14).

4.3 Computing Connectivity and Resilience

Suppose we are given a set system $(X, \mathcal{A})$, where $b = |\mathcal{A}|$. As previously mentioned, we assume that value of the parameter t is already known. Here are the steps that would be followed to compute Pr_1 and $\mathsf{fail}(1)$.

1. Compute all the values λ_C for $\eta \le |C| \le t-1$. This can be done efficiently as follows:
   (a) Initialise $\lambda_C \leftarrow 0$ for all relevant C.
   (b) For every block $A \in \mathcal{A}$ and for every $C \subseteq A$ such that $\eta \le |C| \le t-1$, set $\lambda_C \leftarrow \lambda_C + 1$.

   (For fixed values of η and t, we observe that the λ_C's can be computed in time $\Theta(b)$ by this method.)
2. Compute all the values μ_C for $\eta \le |C| \le t-1$, using the formula (12).
3. Compute the values q_i for $\eta \le i \le t-1$, using the formula (5).
4. Compute L using the formula (8).
5. Compute $\mathsf{Pr}_1 = L/\binom{b}{2}$ and compute $\mathsf{fail}(1)$ using the formula (15).

Remark. If we only wanted to compute Pr_1, then step 2 could be omitted.

4.4 Examples

Here are some small examples to illustrate the application of the formulas we have developed.

Example 6. Suppose $X = \{1, \ldots, 6\}$ and

$$\mathcal{A} = \{\{123\}, \{124\}, \{125\}, \{456\}, \{136\}\}.$$

It easy to check that $t = 3$ in this design. Then we have

$$\begin{array}{l} \lambda_{12} = 3\ \lambda_{13} = 2\ \lambda_{14} = 1\ \lambda_{15} = 1\ \lambda_{16} = 1\ \lambda_{23} = 1 \\ \lambda_{24} = 1\ \lambda_{25} = 1\ \lambda_{26} = 0\ \lambda_{34} = 0\ \lambda_{35} = 0\ \lambda_{36} = 1 \\ \lambda_{45} = 1\ \lambda_{46} = 1\ \lambda_{56} = 1 \\ \hline \lambda_1 = 4\ \ \lambda_2 = 3\ \ \lambda_3 = 2\ \ \lambda_4 = 2\ \ \lambda_5 = 2\ \ \lambda_6 = 2 \end{array}$$

It is easy to compute $q_1 = 13$ and $q_2 = 4$. When $\eta = 1$, we have $L = q_1 - q_2 = 9$ and $\mathsf{Pr}_1 = 9/10$; when $\eta = 2$, we have $L = q_2 = 4$ and $\mathsf{Pr}_1 = 4/10$.

In order to compute $\mathsf{fail}(1)$, we also need to compute the μ_C's. First, suppose $\eta = 2$. Then $\mu_C = \lambda_C$ for $|C| = 2$, and

$$\mathsf{fail}(1) = \frac{1}{4 \times 3}\left(3\binom{3}{2} + 2\binom{2}{2}\right) - \frac{2}{3} = \frac{1}{4}.$$

When $\eta = 1$, we need to compute λ_C when $|C| = 1, 2$. When $|C| = 1$, we have $\mu_C = \lambda_C$. When $|C| = 2$, we use (13) to compute μ_C:

$$\begin{array}{l} \mu_{12} = -4\ \mu_{13} = -4\ \mu_{14} = -5\ \mu_{15} = -5\ \mu_{16} = -5\ \mu_{23} = -4 \\ \mu_{24} = -4\ \mu_{25} = -4\ \mu_{26} = -5\ \mu_{34} = -4\ \mu_{35} = -4\ \mu_{36} = -3 \\ \mu_{45} = -3\ \mu_{46} = -3\ \mu_{56} = -3 \end{array}$$

$$\mathsf{fail}(1) = \frac{1}{9 \times 3}\left(4\binom{4}{2} + 3\binom{3}{2} + 4 \times 2\binom{2}{2} - 4\binom{3}{2} - 4\binom{2}{2}\right) - \frac{2}{3} = \frac{7}{27}.$$

Here is an example with $t = 4$. We just compute Pr_1 for this example.

Example 7. Suppose $X = \{1, \ldots, 9\}$ and

$$\mathcal{A} = \{\{1234\}, \{1235\}, \{1367\}, \{5678\}, \{4789\}\}.$$

Here $t = 4$ and we compute $q_1 = 14$, $q_2 = 7$ and $q_3 = 1$. When $\eta = 1$, we have $L = q_1 - q_2 + q_3 = 8$ and $\mathsf{Pr}_1 = 4/5$; when $\eta = 2$, we have $L = q_2 - 2q_3 = 5$ and $\mathsf{Pr}_1 = 1/2$; and when $\eta = 3$, we have $L = q_3 = 1$ and $\mathsf{Pr}_1 = 1/10$.

5 Conclusion

We have provided two methods of increasing the flexibility of combinatorial key predistribution schemes. These methods are discussed and evaluated in reference to the transversal design schemes introduced in [5]. The first method is to exploit the underlying structure of transversal designs to explicitly describe a wide range of "partial" designs whose properties can easily be analysed using existing formulas [9]. The schemes based on these partial designs have properties very similar to the transversal design schemes from which they are derived. The second method (e.g., see [5]) is to randomly delete blocks from a specified set system. We show by running extensive experiments that this method also does not affect performance adversely, which contradicts assertions made in [1]. Finally, we develop some new formulas that facilitate the efficient computation of metrics of KPS derived from arbitrary set systems. These formulas were useful in the experiments we carried out, but they may have additional applications in the theoretical study of combinatorial KPS for wireless sensor networks.

Appendix

Table 3. Resilience of random KPSs derived from TD(2,15,71)

ℓ	$\mathsf{fail}(1)$ (mean)	$\mathsf{fail}(1)$ (std. dev.)	$\mathsf{fail}(1)$ (min)	$\mathsf{fail}(1)$ (max)
2	0.013749	0.000642	0.011989	0.015357
3	0.013660	0.000381	0.012879	0.014684
4	0.013687	0.000278	0.013134	0.014481
5	0.013702	0.000234	0.013158	0.014362
6	0.013704	0.000179	0.013294	0.014108
7	0.013676	0.000140	0.013338	0.014077
8	0.013687	0.000136	0.013356	0.014063
9	0.013707	0.000109	0.013418	0.013950
10	0.013690	0.000094	0.013476	0.013964
11	0.013682	0.000077	0.013505	0.013850
12	0.013698	0.000071	0.013552	0.013897
13	0.013696	0.000068	0.013517	0.013836
14	0.013685	0.000058	0.013558	0.013820
15	0.013691	0.000055	0.013528	0.013841
16	0.013685	0.000055	0.013586	0.013830
17	0.013694	0.000053	0.013583	0.013862
18	0.013692	0.000044	0.013579	0.013800
19	0.013694	0.000042	0.013602	0.013808
20	0.013694	0.000042	0.013582	0.013812
21	0.013693	0.000037	0.013588	0.013780
22	0.013694	0.000033	0.013602	0.013792
23	0.013687	0.000034	0.013603	0.013760
24	0.013693	0.000031	0.013632	0.013780
25	0.013692	0.000025	0.013614	0.013746
26	0.013690	0.000026	0.013592	0.013749
27	0.013690	0.000025	0.013631	0.013743
28	0.013692	0.000021	0.013630	0.013737
29	0.013691	0.000019	0.013633	0.013730
30	0.013688	0.000019	0.013639	0.013729
31	0.013693	0.000020	0.013655	0.013749
32	0.013693	0.000018	0.013645	0.013732
33	0.013693	0.000016	0.013661	0.013752
34	0.013693	0.000016	0.013659	0.013737
35	0.013695	0.000014	0.013667	0.013724
36	0.013691	0.000014	0.013655	0.013727
37	0.013694	0.000012	0.013664	0.013725
38	0.013694	0.000015	0.013664	0.013735
39	0.013693	0.000012	0.013662	0.013726
40	0.013691	0.000012	0.013668	0.013720
41	0.013693	0.000011	0.013668	0.013726
42	0.013695	0.000013	0.013664	0.013726

Table 3. (*Continued*)

ℓ	$\mathsf{fail}(1)$ (mean)	$\mathsf{fail}(1)$ (std. dev.)	$\mathsf{fail}(1)$ (min)	$\mathsf{fail}(1)$ (max)
43	0.013693	0.000010	0.013674	0.013725
44	0.013693	0.000009	0.013664	0.013712
45	0.013692	0.000008	0.013673	0.013715
46	0.013694	0.000007	0.013679	0.013715
47	0.013693	0.000007	0.013679	0.013709
48	0.013693	0.000008	0.013676	0.013715
49	0.013693	0.000007	0.013676	0.013710
50	0.013693	0.000007	0.013673	0.013710
51	0.013694	0.000005	0.013682	0.013709
52	0.013693	0.000006	0.013679	0.013705
53	0.013694	0.000005	0.013683	0.013707
54	0.013694	0.000005	0.013681	0.013704
55	0.013694	0.000004	0.013683	0.013707
56	0.013693	0.000004	0.013683	0.013703
57	0.013693	0.000004	0.013681	0.013706
58	0.013693	0.000003	0.013683	0.013704
59	0.013693	0.000003	0.013684	0.013698
60	0.013693	0.000003	0.013685	0.013700
61	0.013693	0.000002	0.013688	0.013698
62	0.013693	0.000002	0.013688	0.013700
63	0.013693	0.000002	0.013687	0.013702
64	0.013693	0.000002	0.013689	0.013697
65	0.013693	0.000001	0.013689	0.013697
66	0.013693	0.000001	0.013690	0.013697
67	0.013693	0.000001	0.013691	0.013696
68	0.013693	0.000001	0.013692	0.013695
69	0.013693	0.000000	0.013692	0.013694
70	0.013693	0.000000	0.013693	0.013694
71	0.013693	0.000000	0.013693	0.013693

Table 4. Connectivity of random KPSs derived from TD(2,15,71)

ℓ	Pr_1 (mean)	Pr_1 (std. dev.)	Pr_1 (min)	Pr_1 (max)
1	0.208129	0.008217	0.185111	0.228169
2	0.208647	0.003964	0.197283	0.218659
3	0.208178	0.002706	0.202719	0.215121
4	0.208296	0.001944	0.204200	0.213159
5	0.208403	0.001608	0.204138	0.212795
6	0.208455	0.001297	0.204861	0.211721
7	0.208241	0.001010	0.205467	0.210976
8	0.208214	0.000963	0.205741	0.210926
9	0.208424	0.000790	0.206175	0.210355
10	0.208313	0.000695	0.206834	0.210374

Table 4. (*Continued*)

ℓ	Pr_1 (mean)	Pr_1 (std. dev.)	Pr_1 (min)	Pr_1 (max)
11	0.208234	0.000541	0.206914	0.209409
12	0.208359	0.000501	0.207433	0.209764
13	0.208359	0.000477	0.207073	0.209418
14	0.208284	0.000427	0.207436	0.209333
15	0.208332	0.000422	0.207219	0.209515
16	0.208267	0.000397	0.207473	0.209335
17	0.208340	0.000391	0.207518	0.209341
18	0.208324	0.000329	0.207455	0.209105
19	0.208339	0.000311	0.207681	0.209109
20	0.208333	0.000309	0.207523	0.209267
21	0.208333	0.000277	0.207566	0.209007
22	0.208340	0.000243	0.207638	0.209064
23	0.208282	0.000248	0.207686	0.208775
24	0.208336	0.000230	0.207860	0.208999
25	0.208327	0.000184	0.207737	0.208744
26	0.208307	0.000198	0.207572	0.208763
27	0.208309	0.000186	0.207903	0.208706
28	0.208322	0.000160	0.207863	0.208648
29	0.208314	0.000145	0.207887	0.208595
30	0.208295	0.000146	0.207896	0.208618
31	0.208337	0.000148	0.208046	0.208760
32	0.208330	0.000136	0.207953	0.208620
33	0.208334	0.000125	0.208096	0.208799
34	0.208331	0.000122	0.208052	0.208685
35	0.208344	0.000109	0.208120	0.208560
36	0.208318	0.000109	0.208046	0.208621
37	0.208338	0.000094	0.208113	0.208588
38	0.208338	0.000114	0.208114	0.208655
39	0.208330	0.000089	0.208108	0.208568
40	0.208316	0.000091	0.208140	0.208556
41	0.208336	0.000086	0.208144	0.208569
42	0.208345	0.000098	0.208104	0.208569
43	0.208331	0.000074	0.208187	0.208585
44	0.208334	0.000065	0.208109	0.208480
45	0.208328	0.000060	0.208179	0.208492
46	0.208335	0.000053	0.208232	0.208499
47	0.208334	0.000053	0.208223	0.208458
48	0.208331	0.000058	0.208205	0.208499
49	0.208330	0.000050	0.208211	0.208460
50	0.208332	0.000051	0.208178	0.208459
51	0.208339	0.000041	0.208246	0.208457
52	0.208332	0.000042	0.208226	0.208426

Table 4. (*Continued*)

ℓ	Pr_1 (mean)	Pr_1 (std. dev.)	Pr_1 (min)	Pr_1 (max)
53	0.208338	0.000034	0.208256	0.208440
54	0.208339	0.000036	0.208245	0.208418
55	0.208336	0.000033	0.208255	0.208437
56	0.208333	0.000030	0.208256	0.208410
57	0.208334	0.000028	0.208241	0.208427
58	0.208329	0.000026	0.208255	0.208417
59	0.208331	0.000023	0.208262	0.208371
60	0.208332	0.000021	0.208273	0.208386
61	0.208333	0.000017	0.208295	0.208371
62	0.208335	0.000017	0.208291	0.208387
63	0.208334	0.000016	0.208285	0.208397
64	0.208332	0.000012	0.208301	0.208361
65	0.208332	0.000010	0.208305	0.208360
66	0.208332	0.000009	0.208312	0.208360
67	0.208333	0.000007	0.208316	0.208358
68	0.208334	0.000005	0.208321	0.208347
69	0.208333	0.000003	0.208324	0.208343
70	0.208333	0.000002	0.208329	0.208339
71	0.208333	0.000000	0.208333	0.208333

References

1. Bose, M., Dey, A., Mukerjee, R.: Key predistribution schemes for distributed sensor networks via block designs. Des. Codes Crypt. **67**(1), 111–136 (2013)
2. Çamtepe, S.A., Yener, B.: Key distribution mechanisms for wireless sensor networks: a survey. Technical Report TR-05-07, Rensselaer Polytechnic Institute (2005)
3. Dong, J., Pei, D., Wang, X.: A key predistribution scheme based on 3-designs. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 81–92. Springer, Heidelberg (2008)
4. Eschenauer, L., Gligor, V.: A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47. ACM (2002)
5. Lee, J., Stinson, D.R.: On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. ACM Trans. Inf.Syst. Secur. **11**(2), 1–35 (2008). (Article No. 1)
6. Martin, K.M.: On the applicability of combinatorial designs to key predistribution for wireless sensor networks. In: Chee, Y.M., Li, Ch., Ling, S., Wang, H., Xing, Ch. (eds.) IWCC 2009. LNCS, vol. 5557, pp. 124–145. Springer, Heidelberg (2009)
7. Martin, K.M., Paterson, M.B.: An application-oriented framework for wireless sensor network key establishment. Electron. Notes Theor. Comput. Sci. **192**(2), 31–41 (2008)
8. Martin, K.M., Paterson, M.B., Stinson, D.R.: Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. ACM Trans. Sens. Netw. **7**(2), 1–27 (2010). (Article No. 11)

9. Paterson, M.B., Stinson, D.R.: A unified approach to combinatorial key predistribution schemes for sensor networks. Des. Codes Crypt. **71**, 433–457 (2014)
10. Xiao, Y., Rayi, V.K., Sun, B., Du, X., Hu, F., Galloway, M.: A survey of key management schemes in wireless sensor networks. Comput. Commun. **30**(11–12), 2314–2341 (2007)