Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks

Seyit A. Çamtepe, Bülent Yener

***Abstract*— Key distribution is one of the most challenging security issues in wireless sensor networks where sensor nodes are randomly scattered over a hostile territory. In such a sensor deployment scenario, there will be no prior knowledge of post deployment configuration. For security solutions requiring pairwise keys, it is impossible to decide how to distribute key pairs to sensor nodes before the deployment. Existing approaches to this solution are to assign more than one key, namely a key-chain, to each node. Key-chains are randomly drawn from a key-pool. Either two neighboring nodes have a key in common in their key-chain, or there is a path, called key-path, among these two nodes where each pair of neighboring nodes on this path has a key in common. Problem in such a solution is to decide on the key-chain size and key-pool size so that every pair of nodes can establish a session key directly or through a path with high probability. The size of the key-path is the key factor for the efficiency of the design. This paper presents novel,** *deterministic* **and** *hybrid* **approaches based on** *Combinatorial Design* **for key distribution. In particular, several** *block design* **techniques are considered for generating the key-chains and the key-pools.**

Comparison to probabilistic schemes shows that our combinatorial approach produces better connectivity with smaller key-chain sizes.

Department of Computer Science, Rensselaer Polytechnic Institute, TROY, NY 12180, email: camtes@cs.rpi.edu.

Department of Computer Science, Rensselaer Polytechnic Institute, TROY, NY 12180, email: yener@cs.rpi.edu.

I. Introduction

In this work, we consider a sensor network in which sensor nodes need to communicate with each other for data processing and routing. We assume that the sensor nodes are distributed to the target area in large numbers and their location within this area is determined randomly. These type of sensor networks are typically deployed in adversarial environments, including military applications where a large number of sensors may be dropped from airplanes.

The security between a pair of sensor nodes requires establishment of a pairwise *secret key*. A key pre-distribution scheme is required where keys are uploaded to sensors before the deployment. Since the network topology is unknown prior to deployment, the keys loaded into the sensors must be carefully selected so to increase the probability that two neighboring sensor nodes have at least one key in common. Nodes that do not share a key directly may use a path where each pair of nodes on the path shares a key. The average length of this path, called *average key-path*, is an important performance metric and design consideration.

The common approach is to assign each sensor node multiple keys, *randomly* drawn from a key-pool, to construct a *key-chain* to ensure that either two neighbor nodes have a key in common in their key-chain, or there is a key-path. Thus the challenge is to decide on the key-chain size and key pool size so that every pair of nodes can establish a session key directly or through a path.

Eschenauer *et al.* [9] propose a *random key pre-distribution scheme* where tens to hundreds of keys are uploaded to sensors before the deployment. In their solution, initially a large key pool of P and the key identities are generated. For each sensor, k keys are randomly drawn from the key-pool P without replacement. These k keys and their identities form a *key-chain* which is loaded in to memory of the sensor node. Two neighboring nodes compare list of identities of keys in their key-chain. Since only the identities are exchanged, this process can take place without any privacy mechanism. Eschenauer *et al.* also propose to employ *Merkle Puzzle* [13] similar approach to secure key identities. After key identity exchange, common key(s) are used to secure the link in between two sensor nodes. It may be the case that some of the neighboring nodes may not be able to find a key in common. These nodes may communicate securely through other nodes, through other secured links. It is very important to select correct values for key-chain size and key-pool size so that graph generated after key distribution is connected. Chan *et al.* [3] propose a modification to the basic scheme of Eschenauer *et al.* [9]. They increase the amount of key overlap required for key-setup. That is, q common keys are needed instead of one to be able to secure the communication between two neighboring nodes.

Random-pairwise key scheme in [3], is a modification of the pairwise key scheme. It is based on *Erdos and Renyi's* work; to achieve probability p of any two nodes are connected, in a network of n nodes, each node needs only to store a random set of np pairwise keys instead of $n-1$. Slijepcevic *et al.* [17] propose that each sensor node shares a list of master keys, a random function and a seed. Every sensor uses shared random function and shared seed to select a network wise or group wise master key.

In [16], [23], [6], [7], [4], [2] a network architecture where there are one or more base-stations is considered. These base-stations are considered as powerful in resource and sensor nodes are clustered around them. Each sensor node shares a key with each base-station to secure sensor node to base-station and base-station to sensor node unicast communication. Authentication mechanism for the broadcasts from base-station to sensor nodes is considered in [16], [6], [7], [12], [4]. They propose modified versions of *TESLA* where a verifiable key, which is used to encrypt a message, is disclosed later then the message broadcasted.

A. Our Contributions and Organization of this Work

The main contribution of this work is the *deterministic* and *hybrid* approaches to the key distribution problem. In particular, we bring in a novel construction methodology from *Combinatorial Design Theory* to address this problem. Although there are some applications of Combinatorial Designs in cryptography [19], [20], [21], and in network design [25], [22], best to our knowledge this work is the first to apply design theory to key distribution. Our analysis indicate that deterministic approach has strong advantages over the randomized ones since it (i) increases the probability that two nodes will share a key, and (ii) decreases the key-path length.

This paper is organized as follows: In Section II we provide a brief background to the combinatorial designs used in this work without exceeding the scope of this paper. In Section III we introduce our key distribution construction and explain the mapping from design theory to this practical problem. In Section IV we address scalability issues. In Section V, we present our analysis and comparison with randomized methods. Finally, in Section VI we conclude.

II. Background on Combinatorial Designs

A *Balanced Incomplete Block Design (BIBD)* is an arrangement of *v* distinct objects into *b* blocks such that each block contains exactly *k* distinct objects,

each object occurs in exactly *r* different blocks, and every pair of distinct objects occurs together in exactly λ blocks. The design can be expressed as (v, k, λ), or equivalently (v, b, r, k, λ), where:

$$\lambda\ (v-1)\ =\ r\ (k-1)$$
$$b\ k\ =\ v\ r$$

A. Symmetric BIBD

A *BIBD* is called *Symmetric BIBD* or *Symmetric Design* when $b = v$ and therefore $r = k$ [5], [1], [10], [24]. A *Symmetric Design* has four properties: every block contains $k = r$ elements, every element occurs in $r = k$ blocks, every pair of elements occurs in λ blocks and every pair of blocks intersects in λ elements.

Example 1: Consider $(v, k, \lambda) = (7, 3, 1)$, or equivalently $(v, b, r, k, \lambda) = (7, 7, 3, 3, 1)$, *Symmetric Design*. Let $S = \{1, 2, 3, 4, 5, 6, 7\}$ be the set of $|S| = v = 7$ objects. There are $b = 7$ blocks such that each block contains $k = 3$ objects. Every object occurs in $r = 3$ blocks. Every pair of distinct objects occurs in $\lambda = 1$ blocks and every pair of blocks intersects in $\lambda = 1$ objects. The blocks of the *Symmetric Design* are:

$$\{1,2,3\}\ \{1,4,5\}\ \{1,6,7\}\ \{2,4,6\}$$
$$\{2,5,7\}\ \{3,4,7\}\ \{3,5,6\}$$

In this paper, we are interested in a subset of Symmetric Designs, called a *Finite Projective Plane*. A *Finite Projective Plane* consists of a finite set P of points and a set of subsets of P, called lines. For an integer *n* where $n \geq 2$, *Finite Projective Plane* of order *n* has four properties: (i) every line contains exactly $n+1$ points, (ii) every point occurs on exactly $n+1$ lines, (iii) there are exactly n^2+n+1 points, and (iv) there are exactly n^2+n+1 lines. If we consider lines as blocks and points as objects, then a *Finite Projective Plane* of order *n* is a *Symmetric Design* with parameters $(n^2+n+1, n+1, 1)$ [5], [1].

Given a block design $D = (v, k, \lambda)$ with a set S of $|S| = v$ objects and $B = \{B_1, B_2, \ldots, B_b\}$ of $|B| = b$ blocks where each block includes exactly k objects, *Complementary Design* $\overline{D}$ has the complement blocks $\overline{B_i} = S - B_i$ as its blocks for $1 \leq i \leq b$. $\overline{D}$ is a block design with parameters $(v, b, b-r, v-k, b-2r+\lambda)$ where $(b-2r+\lambda > 0)$ [1, Theorem 1.1.6]. If $D = (v, k, \lambda)$ is a *Symmetric Design*, then $\overline{D} = (v, v-k, v-2r+\lambda)$ is also a *Symmetric Design* [1, Corollary 1.1.7].

Example 2: Consider Symmetric Design $D = (v, k, \lambda) = (7, 3, 1)$ of *Example-1*. Complementary Design of this design is $\overline{D} = (v, v-k, b-2r+\lambda) = (7, 4, 2)$. Given the same set S of $|S| = v = 7$ objects, there are $b = 7$ blocks such that each block contains $v - k = 4$ objects. Every object occurs in $b-r = 4$ blocks. Every pair of distinct objects occurs in $b - 2r + \lambda = 2$ blocks and every pair of blocks intersects in $b-2r+\lambda = 2$ objects. The blocks of the *Complementary Design* are:

$$\{4,5,6,7\}\ \{2,3,6,7\}\ \{2,3,4,5\}\ \{1,3,5,7\}$$
$$\{1,3,4,6\}\ \{1,2,5,6\}\ \{1,2,4,7\}$$

B. Finite Generalized Quadrangle

A *Finite Generalized Quadrangle (GQ)* is an incidence structure $S = (P, B, I)$ where P and B are disjoint and nonempty sets of points and lines respectively, and for which *I* is a symmetric point-line incidence relation satisfying the following axiom:

1) Each point is incident with $t+1$ lines $(t \geq 1)$ and two distinct points are incident at most one line,
2) Each line is incident with $s+1$ points $(s \geq 1)$ and two distinct lines are incident with at most one point,
3) If x is a point and L is a line not incident (I) with x, then there is a unique pair $(y, M) \in PXB$ for which $x\ I\ M\ I\ y\ I\ L$.

In this work, we are interested in three known GQ's as defined in [14], [8], [11], [15]: two GQs are from the *Projective Space* $PG(4, q)$ and $PG(5, q)$ of order q, third one is from $PG(4, q^2)$ of order q^2. Let function

f be an *irreducible binary quadratic*, then the three GQs can be defined as follows:

1) $GQ(s,t) = GQ(q,q)$ from $PG(4,q)$ with canonical equation $x_0^2 + x_1x_2 + x_3x_4 = 0$:
$$GQ(q,q) \Rightarrow \begin{cases} s = t = q \\ v = b = (q+1)(q^2+1) \end{cases}$$

2) $GQ(s,t) = GQ(q,q^2)$ from $PG(5,q)$ with canonical equation $f(x_0,x_1) + x_2x_3 + x_4x_5 = 0$:
$$GQ(q,q^2) \Rightarrow \begin{cases} s = q \\ t = q^2 \\ v = (q+1)(q^3+1) \\ b = (q^2+1)(q^3+1) \end{cases}$$

3) $GQ(s,t) = GQ(q^2,q^3)$ from $PG(4,q^2)$ with canonical equation $x_0^{q+1} + x_1^{q+1} + ... + x_d^{q+1} = 0$:
$$\text{GQ}(q^2,q^3) \Rightarrow \begin{cases} s = q^2 \\ t = q^3 \\ v = (q^2+1)(q^5+1) \\ b = (q^3+1)(q^5+1) \end{cases}$$

Consider $GQ(s,t) = GQ(q,q)$ where $s = t = q$. We can consider lines as blocks and points as objects meaning that there are $v = b = (q+1)(q^2+1)$ blocks and objects where each block contains $s+1 = q+1$ objects and where each object is contained in $t+1 = q+1$ blocks.

Example 3: Consider $GQ(s,t) = GQ(2,2)$ for $q = 2$. There are $v = b = 15$ blocks and objects where each block contains $s+1 = 3$ objects and where each object is contained in $t+1 = 3$ blocks. Assume that $S = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$ is the set of objects, then the blocks are:

$$\begin{gathered} \{0,3,4\}\ \{0,7,8\}\ \{0,11,12\}\ \{1,3,5\}\ \{1,7,9\} \\ \{1,11,13\}\ \{2,3,6\}\ \{2,7,10\}\ \{2,11,14\}\ \{4,9,14\} \\ \{4,10,13\}\ \{5,8,14\}\ \{5,10,12\}\ \{6,8,13\}\ \{6,9,12\} \end{gathered}$$

Consider blocks $\{0,3,4\}$ and $\{1,7,9\}$. They don't share an object, but there are three other blocks that share an object with both: (i) block $\{0,7,8\}$ by sharing objects *0* and *7,* (ii) block $\{1,3,5\}$ by sharing objects *3* and *1,* and (iii) block $\{4,9,14\}$ by sharing objects *4* and *9*.

Example 4: Consider $GQ(s,t) = GQ(2,2)$ design of *Example-3*. *Complementary Design* of this design will have $b = 15$ blocks where each block has $v - s - 1 = 12$ objects.

$$\begin{gathered} \{1,2,5,6,7,8,9,10,11,12,13,14\} \\ \{1,2,3,4,5,6,9,10,11,12,13,14\} \\ \{1,2,3,4,5,6,7,8,9,10,13,14\} \\ \{0,2,4,6,7,8,9,10,11,12,13,14\} \\ \{0,2,3,4,5,6,8,10,11,12,13,14\} \\ \{0,2,3,4,5,6,7,8,9,10,12,14\} \\ \{0,1,4,5,7,8,9,10,11,12,13,14\} \\ \{0,1,3,4,5,6,8,9,11,12,13,14\} \\ \{0,1,3,4,5,6,7,8,9,10,12,13\} \\ \{0,1,2,3,5,6,7,8,10,11,12,13\} \\ \{0,1,2,3,5,6,7,8,9,11,12,14\} \\ \{0,1,2,3,4,6,7,9,10,11,12,13\} \\ \{0,1,2,3,4,6,7,8,9,11,13,14\} \\ \{0,1,2,3,4,5,7,9,10,11,12,14\} \\ \{0,1,2,3,4,5,7,8,10,11,13,14\} \end{gathered}$$

III. Combinatorial Design to Key Distribution

In the following two sections, we describe how *Symmetric Designs* and *Generalized Quadrangles* are used to generate key-chains for the sensors in a sensor network.

A. Mapping from Symmetric Design to Key Distribution

In this work, we are interested in *Finite Projective Plane* of order *n* which is a *Symmetric Design (Symmetric BIBD)* with parameters $(n^2+n+1, n+1, 1)$.

1) Mapping: We assume a distributed sensor network where there are *N* sensor nodes. Sensor nodes communicate with each other and require pairwise keys to secure their communication. Each sensor has a *key-chain* of *K* keys which is stored to its ROM before the deployment. Keys are selected from a set *P* of *key-pool*. To secure the communication between them, a pair of sensor nodes need to have χ keys in common in their key-chain. Based on this, we define mapping given in Table-I

Symmetric Design		**Key Distribution**
Object Set (S)	$\rightarrow$	Key-Pool (P)
Object Set Size ($\|S\| = v = n^2 + n + 1$)	$\rightarrow$	Key-Pool Size ($\|P\|$)
Blocks	$\rightarrow$	Key-Chains
Number of Blocks ($b = n^2 + n + 1$)	$\rightarrow$	Number of Key-Chains (N)
Number of Blocks ($b = n^2 + n + 1$)	$\rightarrow$	Number of Sensor Nodes (N)
Number of Objects in a Block ($k = n + 1$)	$\rightarrow$	Number of Keys in a Key-Chain (K)
Number of Blocks that an Object is in ($r = n + 1$)	$\rightarrow$	Number of Key-Chains that a Key is in
Two Blocks share ($\lambda = 1$) Objects	$\rightarrow$	Two Key-Chains share (χ) Keys

TABLE I

Mapping from Symmetric Design to Key Distribution

For a sensor network of N nodes, with total of N key-chains, a Symmetric Design with $b \geq N$ blocks needs to be constructed by using set S with $|S| = v = b$ objects. That means, $b = v = n^2 + n + 1 \geq N$ for a prime power n [5], [1]. Each object in S can be associated with a distinct random key, and each block can be used as a key-chain. That provides $b \geq N$ key-chains each having $K = k = n + 1$ keys. Symmetric Design guarantees that any pair of blocks has λ objects in common, meaning that any pair of key-chains, or equivalently sensor nodes, has $\chi = \lambda$ keys in common.

2) Construction: There are several methods to construct *Symmetric Designs* of the form $(n^2+n+1, n+1, 1)$. In this project, we use a *complete set* of $(n-1)$ *Mutually Orthogonal Latin Squares (MOLS)*. A *Latin Square* on n symbols is an $n \times n$ array such that each of the n symbols occurs exactly once in each row and each column. The number n is called the *order of the square*. If $A = (a_{ij})$ and $B = (b_{ij})$ are any two $n \times n$ arrays, the *join* of A and B is a $n \times n$ array whose $(i, j)^{th}$ element is the pair (a_{ij}, b_{ij}). The Latin Squares A and B of order n are *Orthogonal* if all entries of the join of A and B are distinct. Latin Squares $A_1, A_2, ..., A_r$ are *Mutually Orthogonal* $(MOLS)$ if they are orthogonal in pairs. For prime power n, a set of $(n-1)$ MOLS of order n is called a *Complete Set* [5], [1]. A complete set of $(n-1)$ MOLS can be used to construct *Affine Plane* of order n which is an $(n^2, n, 1)$ design. *Affine Plane* of order *n* can be converted to *Projective Plane* of order *n* which is a $(n^2+n+1, n+1, 1)$ *Symmetric Design*. The construction algorithm can be summarized as follows:

1) Given a network size of *N*, find a prime power n where $n^2 + n + 1 \geq N$,
2) Generate a complete set of $(n-1)$ MOLS of order *n* [1, Theorem 5.1.1],
3) Construct the Affine Plane of order *n* from the MOLS [1, Theorem 1.3.5],
4) Construct the Projective Plane of order *n* from the Affine Plane [1, Theorem 1.2.5].

3) Analysis: Symmetric Design has a very nice property that, any pair of blocks shares exactly one object. Probability of key share between any pair of nodes is $P_{SYM} = 1$, so that *Average Key Path Length* is 1.

Symmetric Design of the form $(n^2+n+1, n+1, 1)$ is not a scalable solution itself. Given a fixed key-chain size $k = n + 1$, it can support network sizes of N where $N \leq n^2 + n + 1$. For networks smaller than n^2+n+1, simply some of blocks may not be used still preserving key sharing probability $P_{SYM} = 1$. For the networks where $N > n^2 + n + 1$, key-chain size must be increased, that is, n must be increased to next prime power. Due to the memory limitations in a sensor node, this may not be a good solution. Moreover, such an increase in n may produce designs which can support much bigger networks than required. In probabilistic key distribution schemes, it is always

possible to increase size of key-pool for a fixed key-chain size to increase the number of key-chains. But, such an approach sacrifices key share probability and requires better connectivity at underlying physical network. It is possible to merge deterministic and probabilistic designs to inherit advantages of both. Later in Section-IV, we propose *Hybrid* of Symmetric and Probabilistic Designs to cope with scalability problems. basically, we use n^2+n+1 blocks of the Symmetric Design and select uniformly at random remaining $N-(n^2+n+1)$ blocks among the $(k=n+1)$-subsets of the Complementary Symmetric Design.

B. Mapping from Generalized Quadrangles to Key Distribution

In this work, we are interested in three known $GQ(s,t)$: $GQ(q,q)$, $GQ(q,q^2)$ and $GQ(q^2,q^3)$. Table-II gives details about their parameters.

1) Mapping: Consider a sensor network of N nodes where each node requires a *key-chain* having *K* keys coming from a *key-pool* P. Assume also that, not all pairs of neighboring nodes need to share a key directly, they can communicate through a secure path on which every pair of neighboring nodes shares a key. GQ can be used to generate key-chains for such networks. Namely, points in GQ can be considered as the keys and lines as the key-chains. Mapping between GQ and Key Distribution is given in Table-III.

In GQ, there are $(t+1)$ lines passing through a point, and a line has $(s+1)$ points. That means, a line shares a point with exactly $t(s+1)$ other lines. Moreover, if two lines, say lines A and B, do not share a point, then for each point pt_A on line A, there is a point pt_B on line B such that there exist a line C passing through both points pt_A and pt_B. That means, if two lines A and B do not share a point, there are $(s+1)$ distinct lines which share a point with both lines A and B. In terms of Key Distribution, it means that, a block shares a key with $t(s+1)$ other blocks. Additionally, if two blocks do not share a key, there are $(s+1)$ other blocks sharing a key with both.

2) Construction: The three $GQ(s,t)$'s used in this work are incidence relations between points and lines in a *Projective Space* $PG(d,q)$ and $PG(d,q^2)$ with dimension d. Points of the space are vectors with $(d+1)$ elements of the form $(x_0,x_1,x_2,\ldots,x_d)$ where $x_i<q$ for $PG(d,q)$ and $x_i<q^2$ for $PG(d,q^2)$. They hold the projective plane equations given in Table-IV.

We use irreducible binary quadratic $f(x_0,x_1)=dx_0^2+x_0x_1+x_1^2$ for $GQ(q,q^2)$ as given in Table-IV. Our construction algorithm can be summarized as follows:

1) Given network size of *N*, find a prime power q where:
$$b=q^3+q^2+q+1 \;\geq\; N \text{ for } GQ(q,q)$$
$$b=q^5+q^3+q^2+1 \;\geq\; N \text{ for } GQ(q,q^2)$$
$$b=q^8+q^5+q^3+1 \;\geq\; N \text{ for } GQ(q^2,q^3).$$
2) Find all points in Projective Space $PG(4,q)$ for $GQ(q,q)$, $PG(5,q)$ for $GQ(q,q^2)$ and $PG(4,q^2)$ for $GQ(q^2,q^3)$. That is, find all points holding given canonical equation.
3) Construct bilinear groups of size $s+1$ from v points, that is, find $s+1$ points which are on the same line. Note that each point is incident to $t+1$ lines.

3) Analysis: In a $GQ(s,t)$, there are $b=(t+1)(st+1)$ lines and a line intersects with $t(s+1)$ other lines. Thus, in a design generated from a GQ, a block shares an object with $t(s+1)$ other blocks. Probability P_{GQ} that two blocks shares at least one object, or equivalently, probability P_{GQ} that a pair of nodes share at least one key is:

$$P_{GQ} \;=\; \frac{t(s+1)}{b} \;=\; \frac{t(s+1)}{(t+1)(st+1)}.$$

Table-V lists key share probabilities for the three GQ.

Comparison of Symmetric and GQ Designs for Key Distribution: We are interested in five metrics when comparing the designs: (i) object share, the number of objects shared between any pair of blocks, (ii) block

GQ(s,t)	s	t	b	v
$GQ(q,q)$	q	q	q^3+q^2+q+1	q^3+q^2+q+1
$GQ(q,q^2)$	q	q^2	$q^5+q^3+q^2+1$	q^4+q^3+q+1
$GQ(q^2,q^3)$	q^2	q^3	$q^8+q^5+q^3+1$	$q^7+q^5+q^2+1$

TABLE II

The $GQ(s,t)$ parameters.

Generalized Quadrangle $GQ(s,t)$		**Key Distribution**
Point Set (P)	$\rightarrow$	Key-Pool (P)
Point Set Size ($\|S\| = v = (s+1)(st+1)$)	$\rightarrow$	Key-Pool Size ($\|P\|$)
Line Set (B)	$\rightarrow$	Key-Chains
Number of Lines ($\|B\| = b = (t+1)(st+1)$)	$\rightarrow$	Number of Key-Chains (N)
Number of Lines ($\|B\| = b = (t+1)(st+1)$)	$\rightarrow$	Number of Sensor Nodes (N)
Number of Points on a Line ($s+1$)	$\rightarrow$	Number of Keys in a Key-Chain (K)
Number of Lines that a Point is incident ($t+1$)	$\rightarrow$	Number of Key-Chains that a Key is in
Two Lines share (≤ 1) points	$\rightarrow$	Two Key-Chains share (χ) Keys

TABLE III

Mapping from GQ to Key Distribution

GQ	PG	Points	Canonical Equation for PG
$GQ(q,q)$	$PG(4,q)$	(x_0,x_1,x_2,x_3,x_4)	$x_0^2+x_1x_2+x_3x_4=0$
$GQ(q,q^2)$	$PG(5,q)$	$(x_0,x_1,x_2,x_3,x_4,x_5)$	$f(x_0,x_1)+x_2x_3+x_4x_5=0$
$GQ(q^2,q^3)$	$PG(4,q^2)$	(x_0,x_1,x_2,x_3,x_4)	$x_0^{q+1}+x_1^{q+1}+x_2^{q+1}+x_3^{q+1}+x_4^{q+1}=0$

TABLE IV

Projective Space equations

GQ	Pairwise Key Sharing Probability
$GQ(q,q)$	$P_{QQ}=\frac{q^2+q}{q^3+q^2+q+1}$
$GQ(q,q^2)$	$P_{QQ^2}=\frac{q^3+q^2}{q^5+q^3+q^2+1}$
$GQ(q^2,q^3)$	$P_{Q^2Q^3}=\frac{q^5+q^3}{q^8+q^5+q^3+1}$

TABLE V

Pairwise Key Sharing Probabilities

size, the number of objects in a block, (iii) object-pool size, the number of objects in the key-pool, (iv) number of blocks, and (v) scalability of the design.

In turns of object share, Symmetric Design guarantees exactly one common object between any pair of blocks. In GQ, any pair of blocks may either directly share an object or, shares an object through a third block. When object-pool size, number of blocks and block size parameters are fixed, Probabilistic key distribution scheme performs worst among all. In Section-V we provide detailed comparisons of object share probabilities among all designs.

In turns of object-pool size and number of blocks, with the same block size, GQ makes use of a larger object-pool and generates more blocks than Symmetric Design. Probabilistic key distribution scheme can make use of any object-pool size to create any number

of blocks. For the block size of $k = q+1$ and a prime number q:

- $GQ(q, q)$ generates $q^3 + q^2 + q + 1$ blocks by using object-pool of size $q^3 + q^2 + q + 1$,
- $GQ(q, q^2)$ generates $q^5 + q^3 + q^2 + 1$ blocks by using object-pool of size $q^4 + q^3 + q + 1$,
- Symmetric Design generates q^2+q+1 blocks by using object-pool of size $q^2 + q + 1$.

Moreover, for the block size of $k = q^2 + 1$ and a prime number q:

- $GQ(q^2, q^3)$ generates $q^8+q^5+q^3+1$ blocks by using object-pool of size $q^7 + q^5 + q^2 + 1$,
- Symmetric Design generates $(q^2)^2 + q^2 + 1$ blocks by using object-pool of size $(q^2)^2 + q^2 + 1$.

Probabilistic key distribution is the most scalable solution. But it must be kept in mind that, use of very small object-pool increases the probability of object share between any pair of blocks by decreasing the security in that; number of the objects (keys) need to be discovered by the adversary decreases. Similarly, use of very large object pool decreases the probability of object share between any pair of blocks by increasing the security. Therefore scalability of probabilistic key distribution scheme is usable up to some degree. Next, in Section-IV, we propose Hybrid Symmetric and GQ Designs which provide solutions as scalable as probabilistic key distribution schemes, yet taking advantages of underlying GQ and Symmetric Designs.

IV. Hybrid Designs for Scalable Key Distributions

The main drawback of the combinatorial approach comes from the difficulty of their construction. Given a desired number of sensor nodes or a desired number of keys in the pool, we may not be able to construct a combinatorial design for the target parameters.

In this work, we present a novel approach called *Hybrid Design* which combines deterministic and probabilistic constructions of the original design. We will consider two Hybrid Designs: *Hybrid Symmetric Design* and *Hybrid GQ Design*. By using Symmetric or GQ Design and its complement, we preserve useful properties of combinatorial design yet taking advantage of flexibility and scalability of probabilistic approaches to support any network sizes.

A. Mapping

Consider a sensor network where there are N nodes, therefore N key-chains are required. Due to memory limitations, key-chains can have at most K keys coming from key-pool P. We can employ Hybrid Design for the cases where there is no known combinatorial design technique to generate design with N nodes for the given key-chain size K. Basically, Hybrid Design finds largest prime power n such that $k \leq K$ and generates N blocks of size k where objects come from object set S of size $|S| = v$. The b of N blocks are generated by base Symmetric or GQ Design and $N-b$ blocks are randomly selected among k-subsets of the Complementary Design blocks. We define mappings as in Table-VII.

B. Construction

For a given key-chain size K and network size N, Hybrid Design first generates the Base Symmetric or GQ Design D with largest possible prime power n where $k \leq K$. Base Symmetric or GQ Design D generates b blocks of size k. Table-VI lists the relation between block size k and number of blocks b for the prime power n. Next step is to generate Complementary Design $\overline{D}$ where there are b blocks of size $v - k$. Table-VI lists the parameters of the Complementary Designs. Due to the fact that $v - k > k$ for Symmetric and GQ designs, blocks of the Complementary Design can not be used as the key-chains, but their subsets can. To scale the base design up to given network size, Hybrid Design

Design	**k**	**r**	**b**	**v**
$Symmetric$	$n+1$	$n+1$	n^2+n+1	n^2+n+1
$Complementary\ Symmetric$	n^2	n^2	n^2+n+1	n^2+n+1
$GQ(n,n)$	$n+1$	$n+1$	n^3+n^2+n+1	n^3+n^2+n+1
$Complementary\ GQ(n,n)$	n^3+n^2	n^3+n^2	n^3+n^2+n+1	n^3+n^2+n+1
$GQ(n,n^2)$	$n+1$	n^2+1	$n^5+n^3+n^2+1$	n^4+n^3+n+1
$Complementary\ GQ(n,n^2)$	n^4+n^3	n^5+n^3	$n^5+n^3+n^2+1$	n^4+n^3+n+1
$GQ(n^2,n^3)$	n^2+1	n^3+1	$n^8+n^5+n^3+1$	$n^7+n^5+n^2+1$
$Complementary\ GQ(n^2,n^3)$	n^7+n^5	n^8+n^5	$n^8+n^5+n^3+1$	$n^7+n^5+n^2+1$

TABLE VI

Parameters k, r, v, b for Symmetric, GQ and their Complementary Designs

Hybrid Symmetric Design		**Key Distribution**
Object Set (S)	$\rightarrow$	Key-Pool (P)
Object Set Size ($\|S\| = v$)	$\rightarrow$	Key-Pool Size ($\|P\|$)
Blocks of base design and selected (k)-subsets from Complementary Design	$\rightarrow$	Key-Chains
Number of blocks from base design (b) + Number of selected (k)-subsets ($N-b$)	$\rightarrow$	Number of Key-Chains (N)
Number of blocks from base design (b) + Number of selected (k)-subsets ($N-b$)	$\rightarrow$	Number of Sensor Nodes (N)
Number of Objects in a Block ($k \leq K$)	$\rightarrow$	Number of Keys in a Key-Chain (K)
Two Blocks share zero or more Objects	$\rightarrow$	Two Key-Chains share (χ) Keys

TABLE VII

Mapping from Hybrid Design to Key Distribution

randomly selects remaining $N-b$ blocks uniformly at random among k-subsets of Complementary Design blocks. Selected k-subsets (blocks) along with the blocks of the base design can be used to support network of size N. Algorithm can be summarized as follows:

1) Given N sensor nodes where each can store key-chain of size K, find largest possible prime power n such that $k \leq K$ for k values given in Table-VI.
2) Generate base design (Symmetric or GQ) D:
   - Generate object pool $P = \{a_1, a_2, ..., a_v\}$ of size v,
   - Generate blocks $B = \{B_1, B_2, \ldots, B_b\}$ where $|B_i| = k$ for $1 \leq i \leq b$.
3) Generate Complementary Design $\overline{D}$ from the base design:
   - Generate blocks $\overline{B} = \{\overline{B_1}, \overline{B_2}, \ldots, \overline{B_b}\}$ where $\overline{B_i} = P - B_i$ and $|\overline{B_i}| = v - k$ for $1 \leq i \leq b$. Block $\overline{B_i}$ includes all objects of P not included in the corresponding block B_i of base design.
4) Generate $N-b$ blocks $H = \{H_1, H_2, \ldots, H_{N-b}\}$, from Complementary Design where $|H_i| = k$ for $1 \leq i \leq N-b$:
   - Consider all k-subsets of all Complementary Design blocks in $\overline{B}$,
   - Randomly select $N-b$ subsets to generate the set H,
   - For each selected k-subset, check all blocks of base design in B and all blocks generated so far in H, accept if it does not exist.
5) Blocks of Hybrid Design are $B \cup H$.

Example 5: Assume that we would like to generate key-chains for a network with $N = 10$ nodes. Assume

also that nodes have very limited memories, so that they can store at most $K = 3$ keys in their key-chains. Hybrid Symmetric Design can be used to generate design for this network. Symmetric Design $(v, k, \lambda) = (7, 3, 1)$ of *Example-1* can be used as the base design to generate $b = 7$ blocks out of $v = 7$ objects where block size is $k = 3$. Blocks of Symmetric Design form the set B=$\{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}\}$. Remaining $N - b = 3$ blocks are selected uniformly at random among the 3-subsets of the Complementary Symmetric Design blocks. The blocks of the Complementary Symmetric Design $\overline{D} = (v, v-k, b-2r+\lambda) = (7, 4, 2)$ is given in *Example-2*. Assume that selected blocks are $\{4,5,6\}$, $\{2,3,6\}$ and $\{1,5,7\}$ which are the 3-subsets of the sets $\{4,5,6,7\}$, $\{2,3,6,7\}$ and $\{1,3,5,7\}$ respectively. These blocks (3-subsets) form the set H=$\{\{4,5,6\}, \{2,3,6\}, \{1,5,7\}\}$. The blocks of the Hybrid Symmetric Design is then $B \cup H$= $\{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}, \{4,5,6\}, \{2,3,6\}, \{1,5,7\}\}$.

C. Analysis

In this section we analyze some important properties of Hybrid Symmetric Designs and Hybrid GQ Designs. We will look for some useful properties coming from underlying combinatorial design. Based on these properties, we will analyze object share probabilities between any pair of blocks in $B \cup H$. Proofs for the properties and theorem are given in the appendix.

1) Hybrid Symmetric Design:

Property 1: For all $B_j \in B$ and $H_i \in H$, $\exists b \in B_j | b \notin H_i$. ■

Property 1 does not hold among the blocks in H. To see that, consider two such blocks H_i and H_j for $i \neq j$. Assume that H_i and H_j are selected among k-subsets of Complementary Design blocks $\overline{B_l}$ and $\overline{B_k}$ respectively. Complementary Design of a Symmetric Design has the property that, any pair of blocks has $n^2 - n$ objects in common. For $n > 2$, when $(n^2 - n) > (n+1)$, it can be the case that randomly selected blocks (k-subsets) H_i and H_j are equivalent.

Property 2: Given key chain size $k = n+1$, Hybrid Symmetric Design can support network sizes up to:

$$\binom{v}{k} = \binom{n^2+n+1}{n+1}.$$

■

This is the maximum network size that simple probabilistic key pre-distribution scheme can support for key-chain size $k = n + 1$ and key-pool size $v = n^2 + n + 1$. Probabilistic scheme can go beyond this limit by simply increasing the key-pool size v for a fixed key-chain size k. To provide the same scalability, we will employ Hybrid GQ Designs and discuss it in next section. For fixed key chain size $k = n+1$, $GQ(n, n^2)$ will be able to generate designs for networks up to:

$$\binom{v}{k} = \binom{n^4+n^3+n+1}{n+1}.$$

This is the upper limit of our deterministic algorithms. Numerically, for key chain size of 4, our Hybrid $GQ(n, n^2)$ Design supports network sizes up to $6.210.820$. It supports $(2,54 \times 10^{14})$ nodes for $k = 6$, $(8,08 \times 10^{22})$ nodes for $k = 8$, $(1,18 \times 10^{32})$ nodes for $k = 10$, $(5,78 \times 10^{41})$ nodes for $k = 12$ and so on.

Consider blocks $B \cup H$ of the Hybrid Symmetric Design. Any pair of blocks selected from this set can be either one of the four compositions. Properties 3 to 6 below give probability of sharing at least one object between pairs in each composition. Property-7 presents probabilities for these compositions to happen. Finally, Theorem-8 presents probability of object share in Hybrid Symmetric Design.

Property 3: The probability P_{BB} that any pair of blocks in set B of Symmetric Design has exactly one object in common is $P_{BB} = 1$. ■

Property 4: Consider any pair of blocks in H

where each one is picked among the subsets of a distinct Complementary Design blocks. The probability P_{HH} that these two blocks have at least one object in common approaches to 1 as n (block size) increases. ■

Property 5: Consider any pair of blocks in H where each of them is picked among the subsets of the same Complementary Design block. The probability P_H that these two blocks have at least one object in common is :

$$P_H = 1 - \frac{\binom{n^2-n-1}{n+1}}{\binom{n^2}{n+1}}.$$

■

Property 6: Consider any pair of blocks $(H_i, B_j) \in H \times B$ where $H_i \in H$ and $B_j \in B$. The probability P_{HB} that these two blocks have at least one object in common is:

$$\frac{\frac{1}{2}n^2 + \frac{3}{2}n + 1}{n^2+n+1} \leq P_{HB} \leq \frac{n^2+2}{n^2+n+1}.$$

■

Property 7: Consider any pairing between N blocks of $B \cup H$ of Hybrid Symmetric Design. Any pair of blocks selected from this set can be either one of the four compositions. Probabilities for these compositions are:

1) $Q_{BB} = \frac{b(b-1)}{N(N-1)}$, Both blocks can be from B
2) $Q_{HB} = \frac{2b(N-b)}{N(N-1)}$, One from B and one from H
3) $Q_H = \frac{(N-b)(N-2b)}{bN(N-1)}$, Both from H and subset of the same Complementary Design block
4) $Q_{HH} = \frac{(b-1)(N-b)^2}{bN(N-1)}$, Both from H and subset of the distinct Complementary Design blocks

where $Q_{BB} + Q_{HB} + Q_H + Q_{HH} = 1$. ■

Thus we have the following theorem:

Theorem 8: Probability P_{HSYM} that any pair of blocks shares a key in Hybrid Symmetric Design is:

$$P_{HSYM} = P_{BB}Q_{BB} + P_{HB}Q_{HB} + P_H Q_H + P_{HH}Q_{HH}$$

■

2) Hybrid GQ Designs:

Property 9: Given key chain size $k = n+1$, Hybrid GQ Design can support network sizes up to:

$$\tbinom{v}{s+1} = \tbinom{(s+1)(st+1)}{s+1}.$$

■

Consider blocks $B \cup H$ of the Hybrid GQ Design. Any pair of blocks selected from this set can be either one of the four compositions. Properties 10 to 13 below give probability of sharing at least one object between pairs in each composition. Property-14 presents probabilities for these compositions to happen. Finally, Theorem-15 presents probability of object share in Hybrid GQ Design.

Property 10: The probability P'_{BB} that any pair of blocks in set B of GQ Design has exactly one object in common is given in Table-V for $GQ(q,q)$, $GQ(q,q^2)$ and $GQ(q^2,q^3)$. ■

Property 11: Consider any pair of blocks in H where each one is picked among the subsets of a distinct Complementary Design blocks. The probability P'_{HH} that these two blocks have at least one object in common approaches to 1 as n (block size) increases. ■

Property 12: Consider any pair of blocks in H where each of them is picked among the subsets of the same Complementary Design block. The probability P'_H that these two blocks have at least one object in common is:

$$P'_H = 1 - \frac{\binom{(s+1)(st-1)}{s+1}}{\binom{st(s+1)}{s+1}}.$$

■

Property 13: Consider any pair of blocks $(H_i, B_j) \in H \times B$ where $H_i \in H$ and $B_j \in B$. The probability P'_{HB} that these two blocks have at least one object in common is:

$$\frac{(s+1)(t-s/2+1)}{(t+1)(st+1)} \leq P'_{HB} \leq \frac{(st-s+t+2)}{(t+1)(st+1)}.$$

■

Property 14: Consider any pairing between N blocks of $B \cup H$ of Hybrid GQ Design. Block pairings and their probabilities are the same as Property-7 for b values listed in Table-II for each $GQ(q,q)$, $GQ(q,q^2)$ and $GQ(q^2,q^3)$. ■

Theorem 15: Probability P_{HGQ} that any pair of blocks shares a key in Hybrid GQ Design is:

$$P_{HGQ} = P'_{BB}Q_{BB} + P'_{HB}Q_{HB} + P'_{H}Q_{H} + P'_{HH}Q_{HH}$$

■

V. Computational Results

We have implemented *Random Key Pre-distribution Scheme* by Eschenauer *et al.* [9], *Symmetric Design*, $GQ(q,q)$, $GQ(q,q^2)$, *Hybrid Symmetric Design*, and compared them with other. In random key pre-distribution scheme, we initially generate a large pool of *P* keys and their identities. For each sensor, we uniformly randomly draw *k* keys from the key-pool *P* without replacement. These *k* keys and key identities form the *key-chain* of a sensor node.

Basically, for a network of size N, we generate N key-chains and assign them to N sensor nodes. Then, we uniformly randomly distribute N nodes in to a 1×1 unit grid. Every wireless sensor has a coverage of radius r where $r = d\ (ln\ N)/N$, every node within this coverage area is assumed to be a neighbor. Note that, parameter d can be used to play with radius r and therefore average degree of the network.

After the deployment, two neighboring nodes compare the keys in their key-chains by using the key id's. If they have a key in common, it is used to secure the communication. If there is no key in common, they try to find a shortest possible path where each pair of nodes on the path shares a key. Length of this path is called *Key Path Length* where *Key Path Length* for two nodes directly sharing a key is 1. *Average Key Path Length* is one of the factor that we use to compare random key pre-distribution scheme with our Combinatorial and Hybrid Design schemes.

Probability p that two key-chains share at least one key is another factor we use in comparison. For random key pre-distribution scheme, for a given key-pool size P and key-chain size k, Eschenauer *et al.* [9] approximate probability p as:

$$P_{RAND} = 1 - \frac{(1-\frac{k}{P})^{2(P-k+1/2)}}{(1-\frac{2k}{P})^{(P-2k+1/2)}}.$$

In Symmetric Design, $P_{SYM} = 1$ since any pair of key chains shares exactly one key. In $GQ(s,t)$, probability of key share P_{QQ} for $GQ(q,q)$, P_{QQ^2} for $GQ(q,q^2)$ and $P_{Q^2Q^3}$ for $GQ(q^2,q^3)$ is given in analysis section of the GQ Design, in Table-V.

Probability of key share P_{HSYM} is given in analysis section of the Hybrid Symmetric Design. Similarly, probability of key share P_{HGQ} for Hybrid GQ Design is given in analysis section of the Hybrid GQ Designs.

Following tables summarize the computational results: (i) analytical solution for probability p that two key-chains share at least one key, and (ii) simulation results for *Average Key Path Length*.

Table-VIII compares Symmetric Design with Random Key Pre-distribution scheme. For the same network size, key-chain size and pool-size, Symmetric Design provides better probability of key share between any two key-chains. Simulation results for average key path length supports this advantage. In Random Key Pre-distribution scheme, a pair of nodes requires go through path of $1,35$ hops on average to share a key and communicate securely. This path length is 1 for Symmetric Design since it guarantees

that any pair of key-chains has exactly one key in common.

Table-IX compares $GQ(q,q)$ with Random Key Pre-distribution scheme. $GQ(q,q)$ decreases key chain size, causing a small decrease in key sharing probability. Analytical solution shows that random key pre-distribution scheme provides slightly better probability of key share between key chains, but $GQ(q,q)$ is still competitive to random key pre-distribution scheme. When two key chains do not share a key, $GQ(q,q)$ guarantees existence of third block which shares a key with both.

Table-X compares $GQ(q,q^2)$ with Random Key Pre-distribution scheme. Generalized Quadrangle provides better key sharing probability and performs better in simulation by producing shorter *Average Key Path Lengths*.

Table-XI compares $GQ(q^2,q^3)$ with Random Key Pre-distribution scheme. Generalized Quadrangle provides much better key sharing probability, we expect that simulation results will produce again much shorter *Average Key Path Length* compared to random key pre-distribution scheme.

Table-XII compares Hybrid Symmetric Design with Random Key Pre-distribution Scheme. Hybrid Symmetric Design makes use of Symmetric Design, yet taking advantages of the scalability of probabilistic approach. Given target network size N and key chain size k for which there is no known design, computational results shows that Hybrid Symmetric Design shows better performance than Probabilistic Design.

VI. Conclusions

In this work we presented novel approaches to the key distribution problem in large scale sensor networks. In contrast with prior work, our approach is combinatorial based on Combinatorial Block Designs. We showed how to map from two classes of combinatorial designs to deterministic key distribution mechanisms. We remarked the scalability issues in the deterministic constructions and proposed hybrid mechanisms. Hybrid constructions combine a deterministic core design with probabilistic extensions to achieve key distributions to any network size.

The analysis and computational comparison to the randomized methods show that the combinatorial approach has clear advantages: (i) it increases the probability of a pair of sensor nodes to share a key, and (ii) decreases the key-path length while provides scalability with hybrid approaches.

References

[1] I. Anderson, "Combinatorial Designs: Construction Methods," Ellis Horwood Limited, 1990.

[2] D.W. Carman, B.J. Matt and G.H. Cirincione, "Energy-efficient and Low-latency Key Management for Sensor Networks", In Proceedings of 23rd Army Science Conference, 2002.

[3] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," In 2003 IEEE Symposium on Research in Security and Privacy, 2003.

[4] M. Chen, W. Cui, V. Wen and A. Woo, "Security and Deployment Issues in a Sensor Network," Ninja Project, A Scalable Internet Services Architecture, Berkeley, http://citeseer.nj.nec.com/chen00security.html, 2000.

[5] C.J. Colbourn, J.H. Dinitz, "The CRC Handbook of Combinatorial Designs," CRC Press, 1996.

[6] J. Deng, R. Han and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado, 2003.

[7] J. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks," 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), 2003.

[8] P. Dembowski, " Finite Geometries," Springer Verlag, 1968.

[9] L. Eschenauer, V. D. Gligor, "A key-management scheme for distributed sensor networks", Proceedings of the 9th ACM conference on Computer and communications security, 2002.

Pool Size (P)	Key Chain Size(k)	Number Sensor Nodes	Random Prob.	Symmetric Prob.	Random Avg. Key Path	Symmetric Avg. Key Path	Avg. Node Degree
100807	318	100807	0.634	1.0	–	1.0	–
10303	102	10303	0,639	1.0	1,35	1.0	56
5113	72	5113	0,642	1.0	1,35	1.0	51
2863	54	2863	0,645	1.0	1,35	1.0	47
1407	38	1407	0,651	1.0	1,34	1.0	42
553	24	553	0,663	1.0	1,33	1.0	35

TABLE VIII

Symmetric Design vs Random Key Pre-distribution

Pool Size (P)	Key Chain Size(k)	Number Sensor Nodes	Random Prob.	$GQ(q,q)$ Prob.	Random Avg. Key Path	$GQ(q,q)$ Avg. Key Path	Avg. Node Degree
7240	20	7240	0,053	0,052	2,68	2,69	205
5220	18	5220	0,060	0,058	2,89	2,88	148
2380	14	2380	0,079	0,076	3,17	3,18	88
1464	12	1464	0,094	0,090	2,73	2,71	81
400	8	400	0,150	0,140	3,61	3,49	32
156	6	156	0,212	0,192	2,82	2,53	25

TABLE IX

Generalized Quadrangle $GQ(q,q)$ vs Random Key Pre-distribution

Pool Size (P)	Key Chain Size(k)	Number Sensor Nodes	Random Prob.	$GQ(q,q^2)$ Prob.	Random Avg. Key Path	$GQ(q,q^2)$ Avg. Key Path	Avg. Node Degree
15984	12	162504	0,0008	0,0089	–	–	
2753	8	17200	0,003	0,022	2,96	2,96	631
756	6	3276	0,010	0,045	3,12	3,22	179
112	4	280	0,056	0,128	5,63	5,49	29
27	3	45	0,190	0,266	2,23	2,14	15

TABLE X

Generalized Quadrangle $GQ(q,q^2)$ vs Random Key Pre-distribution

Pool Size (P)	Key Chain Size(k)	Number Nodes	Random Prob.	$GQ(q^2,q^3)$ Prob.
81276	6	393876	0,000091	0,008251
2440	4	6832	0,002340	0,039519
165	3	297	0,030098	0,134680

TABLE XI

Generalized Quadrangle $GQ(q^2,q^3)$ vs Random Key Pre-distribution

[10] M. Hall, "Combinatorial Theory," Blaisdell Publishing Company, 1967.

[11] J.W.P. Hirschfeld, "Projective Geometries Over Finite Fields," Clarendon Press Oxford, 1979.

[12] D. Liu and P. Ning, "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in

Pool Size (P)	Key Chain Size(k)	Number Sensor Nodes	Random Prob.	Hybrid Sym. Prob.	Random Avg. Key Path	Hybrid Sym. Avg. Key Path	Avg. Node Degree
10303	102	10500	0,632	0,99	1,36	1,01	56
5113	72	5250	0,632	0,99	1,35	1,01	51
2863	54	3000	0,628	0,98	1,35	1,03	47
1407	38	1500	0,627	0,97	1,34	1,04	42
553	24	750	0,547	0,89	1,33	1,15	37
183	14	250	0,563	0,89	1,31	1,14	29

TABLE XII

Hybrid Symmetric Design vs Random Key Pre-distribution

Distributed Sensor Networks", The 10th Annual Network and Distributed System Security Symposium, February 2003

[13] R. Merkle, "Secure Communication over insecure channels," Communications of the ACM, 1978.

[14] S. E. Payne, J. A. Thas, "Finite Generalized Quadrangles," Research Notes in Mathematics, Pitman Advanced Publishing Program, 1984.

[15] D. Pedoe, "An introduction to Projective Geometry," Oxford, 1963.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless Networks Journal (WINE), 2002.

[17] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M. B. Srivastava, "On communication Security in Wireless Ad-Hoc Sensor Network," Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002.

[18] F. Stajano, R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks," AT&T software symposium, 1999.

[19] D. R. Stinson, S. A. Vanstone, "A combinatorial approach to threshold schemes,", Advances in Cryptology - CRYPTO '87, 1987.

[20] D. R. Stinson, "A construction for authentication / secrecy codes from certain combinatorial designs," Advances in Cryptology - CRYPTO '87, 1987.

[21] D. R. Stinson, "Combinatorial characterizations of authentication codes," Advances in Cryptology - CRYPTO '91, 1991.

[22] Y. Song, A. Wool, B. Yener, "Combinatorial Design of Multi-ring Networks with Combined Routing and Flow Control," in Computer Networks Vol.3 No: 3, pp 247-267, 2003.

[23] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for Sensor Networks," CADIP Research Symposium, 2002.

[24] W.D. Wallis, "Combinatorial Desing," Marcel Dekker Inc., 1988.

[25] B. Yener, Y. Ofek, M. Yung, "Combinatorial Design of Congestion Free Networks," In IEEE/ACM Transactions on Networking, Vol. 5, No. 6, pages: 989-1000, December 1997.

APPENDIX

Proof: (Property-1) From the definition of Symmetric Design. Since any pair of blocks shares exactly one object, a block in B can not be the subset of the complement of another block in B.

Consider any block $H_i \in H$. Let H_i be picked among the subsets of block $\overline{B_l}$ which is complementary of Symmetric Design block B_l. Assume that there exist a block $B_j \in B$ where $H_i = B_j$. We know that, $\forall x,\ x \in H_i \mid x \in \overline{B_l}$ and $x \notin B_l$. That means, blocks B_j and B_l do not share an object, contradicting the fact that B_j and B_l are blocks of Symmetric Design. Therefore, all blocks in H are distinct from the blocks of the Symmetric Design. ■

Proof: (Property-2) This can be shown by using definition of Symmetric Design. For any set of k objects from the object pool P, if it is not one of the

blocks in B, there is an upper bound for the number of blocks in B that objects of this set can appear in. This upper bound is less than the total number of Symmetric Design blocks. There are blocks in B that this set does not share an object, but is a subset of their complements.

Consider any set C of k objects from object pool P where $C \neq B_i$ and $1 \leq i \leq b$. From the definition of Symmetric Design, we know that, any pair of elements of object pool must be in exactly $\lambda = 1$ block of the Symmetric Design. Moreover, each object must be in $r = k$ blocks. Consider k objects in block C. Consider the case where C shares object with maximum number of blocks. This happens when C shares $k-1$ objects with one of the blocks in B. That means, remaining k^{th} object will appear in other $r = n+1$ blocks of B. Each of $k-1$ objects must be pairing with k^{th} object $\lambda = 1$ time. Therefore, $k-1$ objects will appear alone in $r-2 = n-1$ other blocks. That means, C will share one or more objects with at most:

$$1 + r + (r-1)(r-2) \;=\; n^2 + 2.$$

blocks of in B. But, $|B| = n^2+n+1$ and $n^2+n+1 > n^2+2$ for $n > 1$. That means, $\exists B_j \in B | B_j \cup C = \emptyset$ and $\exists \overline{B_j} \in \overline{B} | C \subseteq \overline{B_j}$. Therefore, Hybrid Design can generate any set of k objects from the object pool P. ■

Proof: (Property-3) This is direct result from definition of Symmetric Design. ■

Proof: (Property-4) Instead of finding the probability, we bound it. Consider blocks H_l and H_k in H which are subsets of $\overline{B_L}$ and $\overline{B_K}$ respectively. Consider random variables X_i and Y_i for $1 \leq i \leq n^2 - n$. X_i takes on value 1 if i^{th} common element in $\overline{B_L}$ is selected. Similarly, Y_i takes on value 1 if i^{th} common element in $\overline{B_K}$ is selected. We are interested in case where X_i and Y_i both takes on value 1, meaning that the i^{th} is selected for both blocks. We define new indicator $Z_i = X_i.Y_i$:

$$E[Z] = \sum_{i=1}^{n2-n} E[Z_i] = \sum_{i=1}^{n2-n} E[X_i]E[Y_i]$$

$$E[Z] = \left(\frac{n+1}{n^2}\right)^2 (n^2 - n) > 1.$$

$E[Z] > 1$ using Markov bound $P(Z \geq 1) \leq E[Z]$ and after checking second moment which shows no significant variance, we conclude that $P(Z \geq 1)$ approaches to 1 as n increases. ■

Proof: (Property-5) Blocks in H are picked uniformly at random among the k-subsets of the Complementary Design blocks. Let $\overline{P_H}$ be the probability that two k-subset of the same Complementary Design block have no objects in common. Let L be the number of all k-subsets of a Complementary Design block of size n^2. A k-subset may pair with $L-1$ other k-subsets and does not share an object with M of them where:

$$P_H = 1 - \overline{P_H} \;,\; M = \binom{n^2-n-1}{n+1} \;,\; L = \binom{n^2}{n+1}$$

$$\overline{P_H} = \frac{M}{L-1} \approx \frac{M}{(L)}.$$

■

Proof: (Property-6) From the definition of Symmetric Design, (i) H_i may be sharing at most two objects with some blocks in B, (ii) H_i may be sharing $k-1$ objects with exactly one of the blocks and share one or two objects with some other blocks in B. In the first case, an object needs to be coupled with $k-1$ objects in $k-1$ different blocks and it needs to be alone in $r-k+1 = 1$ block. Number of the blocks that H_i shares an object with will be:

$$\binom{n+1}{2} + n + 1 = \frac{1}{2}n^2 + \frac{3}{2}n + 1.$$

From the discussion in proof of Property-2, in the second case, H_i will be sharing one or more objects with n^2+2 blocks in B where $|B| = b = n^2+n+1$. Therefore P_{HB} will be:

$$\frac{\frac{1}{2}n^2 + \frac{3}{2}n + 1}{n^2+n+1} \leq P_{HB} \leq \frac{n^2+2}{n^2+n+1}.$$

■

Proof: (Property-7) There are N blocks in block set $B \cup H$ of Hybrid Symmetric Design. Consider a pair of block uniformly randomly selected from this set.

(1) probability Q_{BB} that both blocks are coming from B is:

$$Q_{BB} = \frac{\binom{b}{2}}{\binom{N}{2}} = \frac{b(b-1)}{N(N-1)}.$$

(2) probability Q_{HB} that one block comes from H ($|H| = N - b$) and other from B ($|B| = b$)is:

$$Q_{HB} = \frac{b(N-b)}{\binom{N}{2}} = \frac{2b(N-b)}{N(N-1)}.$$

Note that probability that both blocks are selected from H is:

$$\frac{\binom{N-b}{2}}{\binom{N}{2}} = \frac{(N-b)(N-b-1)}{N(N-1)}.$$

(3) $N - b$ blocks in H are uniformly randomly selected among the k-subset of the b Complementary Design blocks. That means, $(N-b)/b$ blocks are selected among k-subset of each Complementary Design block. Therefore, probability Q_H that both blocks are from H and are subsets of the same Complementary Design block is:

$$Q_H = \frac{(N-b)(N-b-1)}{N(N-1)} \; \frac{b\binom{(N-b)/b}{2}}{\binom{N-b}{2}}$$
$$= \frac{(N-2b)(N-b)}{bN(N-1)}.$$

(4) Probability Q_{HH} that both blocks are from H and are subsets of the distinct Complementary Design block is:

$$Q_{HH} = \frac{(N-b)(N-b-1)}{N(N-1)} \; \left[1 - \frac{b\binom{(N-b)/b}{2}}{\binom{N-b}{2}}\right]$$
$$= \frac{(b-1)(N-b)^2}{bN(N-1)}.$$

■

Proof: (Theorem-8) Consider any pairing between N blocks of $B \cup H$ of Hybrid Symmetric Design. Any pair of blocks selected from this set can be either one of the four compositions given in Property-7 (with probabilities Q_{BB}, Q_{HB}, Q_H and Q_{HH}). Probability of sharing at least one object between pairs of each composition is given in Properties 3, 4, 5 and 6 (P_{BB}, P_{HB}, P_H and P_{HH}). Then, probability P_{HSYM} that any pair of blocks shares at least one key in Hybrid Symmetric Design is:

$$P_{HSYM} = P_{BB}Q_{BB} + P_{HB}Q_{HB} + P_H Q_H + P_{HH}Q_{HH}$$

■

Proof: (Property-9) Similar to proof of Property-2. This can be shown by using definition of GQ Design. For any set of k objects from the object pool P, if it is not one of the blocks in B, there is an upper bound for the number of blocks in B that objects of this set can appear in. This upper bound is less than the total number of GQ Design blocks. There are blocks in B that this set does not share an object, but is a subset of their complements.

Consider any set C of k objects from object pool P where $C \neq B_i$ and $1 \leq i \leq b$. Consider the case where C shares object with maximum number of blocks. From the definition of GQ Design, this happens when set C shares s objects with a block in B. That means, remaining $(s+1)^{th}$ object will appear in other $t+1$ blocks of B. Each of s objects must be pairing with $(s+1)^{th}$ object once. Therefore, s object will appear alone in $t-1$ other blocks. That means, C will share one or more objects with at most:

$$1 + (t+1) + s(t-1) = \; st + t - s + 2.$$

blocks in B. But, there are $(t+1)(st+1)$ blocks in GQ Design and $st^2 + st + t + 1 >> st + t - s + 2$. That means, $\exists B_j \in B | B_j \cup C = \emptyset$ and $\exists \overline{B_j} \in \overline{B} | C \subseteq \overline{B_j}$. Therefore, Hybrid Design can generate any set of k objects from the object pool P. ■

Proof: (Property-11) From the discussion in property-4 it follows. ■

Proof: (Property-12) From the discussion in property-5 it follows. ■

Proof: (Property-13) From the discussion in property-6 it follows. ■

Proof: (Theorem-15) Similar to Theorem-8. From Properties 10, 11, 12, 13 and 14 it follows. ■