Key Predistribution Scheme Using Affine Planes and Blom's Scheme

Alexey Urivskiy
Moscow Institute of Physics and Technology
Dolgoprudnyi, Russia
Email: ourivski@mail.ru

***Abstract*—In this paper we discuss the problem of designing a key predistribution scheme (KPS). We present a composite deterministic KPS based on "multiple key spaces" construction principle. As building blocks for it we take a KPS generated by affine planes and the well-known Blom's scheme. The analysis of the resulting scheme shows its high global connectivity and resilience against nodes' compromise. The KPS can be constructed and flexibly tuned in a wide range of design parameters.**

I. Introduction

To provide security services like confidentiality and authenticity in a network in almost all cases it is sufficient to establish a secret key for every pair of nodes. One of the well-known solutions to the problem of key establishment for large-scale networks, especially consisting of nodes with very limited resources like sensor networks, is to use *key predistribution schemes* (KPS). In a KPS a trusted authority at a setup stage generates a set of secret keys (or other keying material) $\mathcal{K}$ called a key space (or a key pool). Each node j is given a subset of keys $\mathcal{S}_j \subset \mathcal{K}$ — the node's key ring (or key block), which is stored in node's memory. After that the trusted authority quits. The distributed data allow predefined groups of nodes to compute common keys. In what follows we only are interested in the keys for pairs of nodes. The pairwise key k_{ij} for nodes i and j is computed by $k_{ij} = f(S_i, j) = f(S_j, i)$, where f is some publicly specified key derivation function.

There several somewhat contradictory characteristics (measures) describing the quality of a KPS and its applicability to a particular environment. Let us discuss only the most important characteristics.

a) Storage: Nodes' memory is usually constrained so the number of keys stored by each node (the size of the node's key ring) should be kept as small as possible.

b) Connectivity: This defines the ability of the KPS to form secure path between nodes. We distinguish two types of KPSs. If two nodes share a key with some probability less than 1, such schemes are called *probabilistic*. Probabilistic schemes were originally introduced in [1]. Otherwise, if it is guaranteed by the KPS that any pair of nodes are able to establish a common key, the KPS is called *deterministic*.

In a probabilistic scheme if two nodes, say j_x and j_y, have have no common key, the pair attempts, through a path-key establishment protocol, to find a sequence of intermediate nodes $j_u, \ldots, j_v$ such that every pair of adjacent nodes in the path $j_x, j_u, \ldots, j_v, j_y$ have a common key. In practice only short paths, e. g. including 2 or 3 hops, are of interest.

This distinction between deterministic and probabilistic schemes is a measure of *global connectivity*, which describes the ability of the network to become globally connected as a whole. In some environments, however, more appropriate are measures of *local connectivity*, describing the ability of a node to form secure paths within its close neighborhood. Local connectivity is usually considered within some nodes' deployment model and physical connection between nodes.

c) Resilience (security): A typical attack on a KPS assumes that the adversary randomly captures a set of nodes, and get access to all keys of those nodes. The captured nodes are called *compromised nodes*, and their keys are called *compromised keys*.

There is no single measure for resilience of KPSs. For deterministic schemes a notion of w-security seems most appropriate. A KPS is called *w-secure*, if given a specified pair of nodes, any coalition of w or fewer other nodes, pooling together their key blocks, can do no better at computing the pairwise key of these two than guess the key without any keying material whatsoever.

Remember, however, that when more than w nodes are compromised, then two innocent nodes may still establish a secure path through intermediate nodes. Thus, every deterministic KPS by nodes' compromise will eventually turn into a probabilistic one. For probabilistic schemes a more suitable measure of resilience [2] is the probability that the direct link between two innocent nodes is affected after c other nodes are compromised.

d) Complexity (efficiency): There are several processes involved in practical application of a KPS, including system setup, shared key discovery, path-key establishment, common key computation, etc. Some of them depend only on the KPS, some others are affected by node deployment model and application scenarios. It is desirable that all of them be as efficient as possible.

The art of designing a good KPS is to efficiently balance all those characteristics or to find a trade-off between them. There are a huge amount of results is the area of key predistribution. For survey of recent results see for example [3] and [4].

In this paper, we present a deterministic key predistribution scheme which is a combination of two different KPSs: the one based on a special class of combinatorial designs, called

affine planes, and the well-known Blom's scheme. The type of KPS construction called multi space KPS and is quite popular [11]. Our main result is a full theoretical analysis of global connectivity of the scheme.

II. Affine-plane-generated KPS

Combinatorial objects are natural to consider when constructing a KPS. Since they are regular structures many characteristics of the KPS can be computed or quite precisely estimated.

The first use of combinatorial structures in key predistribution was proposed in works by Mitchell and Piper [5]. The next wave of interest was raised by research of distributed sensor networks, and the use of combinatorial designs was proposed Camtepe and Yener [6]. Since that a lot of results have been obtained, see further [7] and [8]. In this paper, we use a special class of combinatorial designs called affine planes as a KPS.

A. Affine planes

We briefly remind the results on affine planes [9]. A t-(v, k, λ) design is an arrangement of v distinct elements (called points) into blocks, each comprising k points, such that every t points occur in exactly λ different blocks. Every element occurs in exactly r different blocks. The total number of blocks is $b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$.

We will only be interested in designs with $t = 2$. By definition, an affine plane of order m is a 2-$(m^2, m, 1)$ design with $m \geq 2$. Denote the plane as $S(m^2, m, 1)$.

So it is defined on the set of $v = m^2$ points, there are $b = m^2 + m$ blocks, every block contains $k = m$ points. every point occurs in $r = m + 1$ distinct blocks.

An affine plane can be represented by its incidence matrix $\mathbf{A} = [a_{ij}]$, which is a $b \times v$ binary matrix such that $a_{ij} = 1$ if j-th point is in the i-th block, otherwise $a_{ij} = 0$.

It is known that affine planes exist whenever m is a power of a prime. And there are polynomial-complexity algorithms for creating incidence matrices of affine planes (see e.g. [9]).

B. KPS

Consider an incidence matrix of an affine plane as the incidence matrix of a KPS. The points of the plane turn into nodes, the blocks correspond to keys. (Note, however, that usually the opposite binding is used: the points correspond to keys, while blocks — to nodes.) In thus defined KPS every pair of nodes share a key. And there is only one key for the pair. So this KPS is a deterministic one. The KPS is globally defined by a single parameter m. For the sake of brevity we will call such a KPS the *Affine*(m).

The incidence matrix of any KPS defines a key-sharing graph. The vertices of the graph are nodes. Two vertices are connected by an edge if the corresponding nodes share a key. If the key-sharing graph is connected, then a secure (multi-hop) path between any two nodes could be found. The key sharing graph of Affine(m) is connected with all one-hop paths between nodes.

However the common key of a pair is not unique to that pair, and $m - 2$ other nodes shares the same key. Compromising a node means compromising all its keys. This equivalent to exclusion of the corresponding vertex and edges from the graph.

If a single node a is compromised, the links for $(m^2 - 1)(m - 2)/2$ different pairs out of total $(m^2 - 1)(m^2 - 2)/2$ possible pairs not including a are compromised either.

If nodes are compromised sequentially, one by one, at some moment the graph becomes disconnected — there will at least two nodes having no key-path between them. Let us define *the connectivity breaking threshold* s as the minimal number of nodes to be compromised, so that the key-sharing graph of a KPS becomes disconnected. In other words, if *arbitrary* $s - 1$ nodes are compromised, then the key-sharing graph of the KPS remains connected.

III. Global connectivity of Affine(m)

Two natural questions concerning the key-sharing graph given by a KPS are (i) what is the connectivity breaking threshold s, (ii) how long are the key-paths between innocent nodes if $\ell < s$ nodes are compromised. For the graph given by the Affine(m) we will answer both questions below.

Lemma 1: Consider Affine(m). Suppose some nodes together with the keys belonging to them are compromised. The key-sharing graph of the scheme remains connected as long as every node holds at least two noncompromised keys. The longest key-path between two nodes includes at most 2 hops.

Proof: Consider some innocent node a. Assume that two edges, say E_1 and E_2 are incident to a. The corresponding blocks of the plane are $A_1 = \{a, a_2, a_3, \ldots, a_m\}$ and $A_2 = \{a, a_{m+1}, a_{m+2}, \ldots, a_{2m-1}\}$.

Consider arbitrary innocent node $b \neq a$. What are the paths between a and b? Consider two cases.

Case 1. If $b \in A_1$ or $b \in A_2$, then a and b are incident to the same edge, and there is a 1-hop path between a and b in the key-sharing graph.

Case 2. Assume $b \notin A_1$ and $b \notin A_2$.

It is known [10] that in an affine plane for any block A and a point $x \notin A$ there is a unique block B containing x such that $A \cap B = 0$.

According to this property there is a unique block B_1 such that $b \in B_1$ and $B_1 \cap A_1 = 0$. But according to the condition of the lemma there are at least two blocks B_1 and B_2 containing b. So we conclude that $A_1 \cap B_2 = c_1$. Then between a and b there is a 2-hop path through c_1.

Moreover by the same property $B_1 \cap A_2 = c_2 \neq 0$ and $c_2 \neq c_1$. Otherwise there would be two blocks A_1 and A_2 containing both a and c_1 which contradicts the property of the affine plane. ■

The proof of the lemma gives us a useful corollary.

Corollary 1: If the key-sharing graph of the Affine(m) is connected after some nodes' compromise, then two innocent nodes either connected by a 1-hop key-path or at least by two different 2-hop key-paths.

The following lemma gives the exact answer, when the condition of lemma 1 holds.

Lemma 2: The key-sharing graph of Affine(m) stays connected as long as no more than $m-1$ nodes have been compromised.

Proof: Consider an arbitrary node a. There are exactly $r = m+1$ blocks $A_1, A_2, \ldots, A_{m+1}$ in the plain containing a. According to the properties of the plain for every node $b \neq a$ there is only one block A_j containing both a and b. If b is compromised, then A_j is compromised. If some $m-1$ different nodes are compromised, then at most $m-1$ blocks containing a is compromised. So there is at least $r-(m-1) = 2$ noncompromised blocks left which contain a, and thus according to the lemma 1 the remaining key-sharing graph is connected. ∎

What happens if more than $m-1$ nodes are compromised? There are sets m nodes, whose compromise will partition the network into at least $m-1$ segments of size at most m. A particular such set is a set of m nodes that are in same block of the affine plane. Thus, we proved the following theorem.

Theorem 1: The KPS generated by $S(m^2, m, 1)$ affine plain has the connectivity breaking threshold equal to m.

Example 1: Consider an affine plane $S(1024, 32, 1)$ giving a KPS for $N = 1024$ nodes. Every node stores $m+1 = 33$ keys. Two innocent nodes will find a secure path of length at most 2 as long as no more than $m-1 = 31$ other nodes are compromised.

IV. BAffine(w, N) — Multiple Spaces KPS

Affine-plane-generated KPSs have very moderate connectivity breaking threshold. A known approach to increase the resilience of a KPS against nodes' compromise is to combine two KPS to create the so called "multiple spaces" KPS [11], [12]. In a multiple spaces scheme, each key in the first KPS (which is now called "outer" scheme) is replaced by keying information for the second scheme, called "inner", scheme.

Suppose that in the outer scheme every key belongs to k_{out} nodes and every node stores r_{out} keys. Suppose further that in the inner scheme the node stores $r_{in}(p)$ keys if there are p nodes in the scheme. So in the the resulting (composite) scheme the node has to store $r = r_{out} \cdot r_{in}(k_{out})$. Taking Affine($m$) as the outer scheme we get $r = (m+1)r_{in}(m)$ keys. The obvious restriction is $r \leq N-1$, otherwise the trivial KPS where every pair of node share a unique key would be absolutely better. Since $N = m^2$, then $r_{in}(m) \leq m-1$. If a w-secure deterministic set-intersection KPS is taken, then theoretically $r_{in}(m) \sim w \log_2 m$ [13]. From this we obtain $w \leq \frac{\sqrt{N}}{\log_2 \sqrt{N}}$ which is not flexible enough for practical applications.

So we see that as an inner scheme we should either choose some probabilistic KPS or Blom's scheme. Our choice is Blom's scheme, since it is deterministic, with known connectivity, and its security can be controlled and tuned according to the requirements.

We briefly remind the reader the construction of Blom's scheme [14]. There are several equivalent descriptions of it, and we use a polynomial one here. The scheme uses a symmetric bivariate polynomial $P(x, y)$ over a finite field $GF(q)$, that is a polynomial with the property that $P(x, y) = P(y, x)$ for all $x, y \in GF(q)$. A node i is given a univariate polynomial $f_i(y) = P(i, y)$. The common key of nodes i and j is computed as $k_{ij} = f_i(j) = f_j(i)$. Obviously $k_{ij} \in GF(q)$. If P has degree w, then each node has to store $w+1$ coefficients of its polynomial, which are elements of $GF(q)$. If an adversary compromises less than w nodes, then it does not learn any information about keys established between innocent nodes. But if he compromises $w+1$ or more nodes, then it can reconstruct the polynomial P and hence learn all the keys. So Blom's scheme can be constructed as w-secure for any w.

If we take Affine(m) as the outer scheme and w-secure Blom's scheme as the inner one, we obtain a composite scheme defined by two parameters: w and m. Such a scheme we will refer to as BAffine(w, N), where, of course, $N = m^2$.

A. Storage

Blom's construction allows us to build a scheme for any w such that $r_{in} = w+1$ independently of the network size. Hence, in BAffine(w, N) the node stores

$$r(w, N) = (w+1)(m+1) = (w+1)(\sqrt{N}+1)$$

keys. Since we need $r(w, N) \leq N-1$, this limits us to $w \leq m-2$. On the other hand this is a trivial restriction for Blom's scheme with m nodes.

B. Resilience and Connectivity: direct links

In BAffine, every pair of nodes shares exactly 1 key, and thus BAffine is a deterministic KPS. Indeed, since in an affine plane two distinct elements occur together in only one block, so two nodes in BAffine share only one key space. In this key space there is exactly 1 common key for every pair given by the Blom's scheme.

If we are only concerned about 1-hop paths between nodes, then BAffine(w, N) is exactly w-secure. If the adversary can compromise nodes on his choice, then to compromise the direct link between any two nodes he must compromise exactly $w+1$ other nodes, which share with that pair the same key space.

Suppose on the contrary, that the adversary has got no ability to choose which nodes to compromise and compromises them randomly. What is the probability to compromise a direct link between two certain nodes a and b if c other nodes are compromised? Denote this probability as $P(c)$.

If $c \leq w$ then trivially $P(c) = 0$. To compromise the direct link between two nodes it is required to compromise the key space which they share. So at least $w+1$ nodes among all compromised ones must share that key space. There are $\binom{m^2-2}{c}$ ways to choose c nodes for compromise (remember a and b are not among them). There are $\binom{m-2}{z}$ ways to compromise z nodes that share the required key space, and

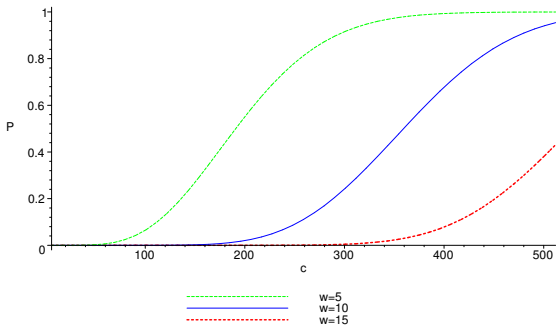

Fig. 1. Probability of compromising a particular link vs the number of compromised nodes

$\binom{m^2-m}{c-z}$ ways to compromise $c-z$ other nodes. Therefore

$$P(c) = \sum_{z=w+1}^{u} \frac{\binom{m-2}{z}\binom{m^2-m}{c-z}}{\binom{m^2-2}{c}}, \quad u = \min(c, m-2) \qquad (1)$$

The graph of $P(c)$ for parameters from example 1 and different w is depicted in figure 1. We see that in some quite broad region of the number of compromised nodes $P(c)$ is extremely small.

C. Global Resilience and Connectivity: multi-hop paths

Consider now secure transmission through multi-hop paths. The following theorem gives the lower bound for the connectivity breaking threshold of BAffine(w, N).

Theorem 2: The connectivity breaking threshold of BAffine(w, N) is

$$s \geq (w+1)\sqrt{N}$$

Proof: Consider a key-sharing graph defined by BAffine. It is a complete graph, with the same vertices and edges as in the graph defined by Affine(m). But in the case of BAffine to compromise a key space the adversary needs to compromise $w+1$ nodes sharing this key space. In lemma 1 it was proved that the key-sharing graph of Affine(m) is connected as long as every nodes holds two noncompromised keys. So in BAffine the key-sharing graph is connected as long as any node enters at least two noncompromised key spaces.

Consider a particular node a in BAffine. a enters $m+1$ different blocks A_i of the affine plane. To compromise a key space in BAffine the adversary has to compromise $w+1$ nodes in some block A_i. So to disconnect the key-sharing graph the adversary has to compromise $w+1$ in each of m blocks A_i, otherwise there will be 2 noncompromised key spaces. Any node other than a is in exactly one of these A_i's according to the property of the affine plane. So the adversary has to compromise at least $(w+1)m = (w+1)\sqrt{N}$ nodes to disconnect the graph. ■

The following lemma gives some more information on the resiliency of BAffine(w, N).

Lemma 3: To completely compromise the node's key ring in BAffine(w, N) at least $(w+1)(\sqrt{N}+1)$ other nodes must be compromised.

Proof: To compromise the key ring of node a the adversary must compromise all key spaces in which a enters. There are $m+1$ such spaces, and in each of them $w+1$ nodes must be compromised. And as discussed before, any node other than a enters those $m+1$ spaces exactly once. ■

Example 2: Suppose we have a network of $N = 1024$ nodes. Assume that every node can store about $r = 200$ keys. We can organize BAffine such that $m = \sqrt{N} = 32$ and $w = \lfloor r/(m+1) - 1 \rfloor = 5$. So we can establish BAffine$(5, 1024)$. It is at least 5-secure scheme. The breaking connectivity threshold is at least $(5+1)\cdot 32 = 192$ nodes and the real size of the key block is $r(5, 1024) = (5+1)\cdot 33 = 198$ keys.

It is interesting to note that when the number of compromised nodes is about the breaking connectivity threshold, the probability to compromise a particular link, when the nodes are compromised at random, is about $1/2$.

D. Length of key-paths

An important question is how fast BAffine degrades from the deterministic KPS, when no nodes are compromised, to a probabilistic one when more and more nodes are being compromised before connectivity breaking threshold is reached. This process can be characterized by an average length L of the key-path in the key-sharing graph between two nodes. Deterministic schemes, where every pair has a common key, have $L = 1$. Probabilistic KPSs have $L > 1$, and L obviously grows with the number of nodes compromised.

Let us estimate L as a function on the number of compromised nodes c for BAffine(w, N). Every key space gives pairwise keys for $m(m-1)/2$ pairs. There are $N(N-1)/2$ different pairs in the network, so a portion of 1-hop links that can be compromised when the key space is compromised is $m(m-1)/N(N-1)$=$1/m(m+1)$. When the key space is compromised 1-hop links disappear, and 2-hop links must be used. As we proved before there are always 2-hop links for BAffine before breaking connectivity threshold s is reached. If ε keys spaces are compromised, so

$$L \leq \frac{1\cdot(m^2+m-\varepsilon)+2\cdot\varepsilon}{m^2+m},$$

where m^2+m is the total number of the key spaces in BAffine.

Any key space (defined by a particular Blom's scheme) can only be compromised when at least $w+1$ nodes entering this space are compromised. Every compromised node enters $m+1$ key spaces. So if c nodes were compromised, then

$$\varepsilon \leq c(m+1)/(w+1)$$

key spaces are broken. Thus the *upper bound* on the average key path length L as a function of c is

$$L(c) \leq \frac{m(w+1)+c}{m(w+1)} = \frac{s+c}{s}, \quad c \leq s$$

So we see that the upper bound grows linearly with the number of compromised nodes. Evidently $L(0) = 1$ since BAffine is deterministic for $c = 0$, and $L(s) \leq 2$ as it was seen before.

And the result is independent of what particular nodes are compromised and whether the adversary compromised them randomly or on his choice.

When nodes are compromised randomly $L(c)$ grows slower than linearly with c. Due to apparent regularity of affine planes, when some number of nodes are compromised the number of colluders entering a key space is almost uniformly distributed. So if a space is compromised almost immediately all spaces are compromised. To compromise all spaces at least s nodes must be compromised. So when nodes are compromised randomly, $L(c) \sim 1$ for $0 \leq c \leq s - \delta$ for some small δ. And only in a narrow region around s does $L(c)$ grow rather fast from 1 to 2. This is also justified by the behavior of $P(c)$ (see (1)).

V. Conclusion

We presented a key predistribution scheme based on two KPSs, the one given by an affine plane $S(m^2, m, 1)$ and a w-secure Blom's scheme. Using "multiple key spaces" approach we obtained from the two a new composite scheme called BAffine(w, N) for the network of size $N = m^2$. The scheme can be constructed for any m such that m is any prime power.

BAffine is a deterministic KPS, i. e. any pair of nodes share a common key. BAffine(w, N) is w-secure. The size of the node's key ring is $(w + 1)(\sqrt{N} + 1)$ keys.

The key sharing graph of BAffine highly resistant to nodes' compromise. Two nodes can always find a secure path between them whenever the adversary compromised no more than any $(w + 1)\sqrt{N} - 1$ nodes. Moreover there is either a direct link or two different 2-hop paths between the pair.

References

[1] L. Eschenauer, V. Gligor, "A Key Management Scheme for Distributed Sensor Networks", In: *Proc. 9th ACM Conference CCS2002*, pp. 41–47, 2002.

[2] J. Lee, D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks". In *Proc. IEEE WCNC'05*, vol. 2, pp. 1200-1205, 2005.

[3] S. A. Camtepe, B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Tech. rep. TR-05-07, Rensselaer Polytechnic Institute*, 2005.

[4] K. M. Martin, M. Paterson, "An application-oriented framework for wireless sensor network key establishment,"' *Electron. Notes Theor. Comput. Sci.* vol. 192, no. 2, pp. 31-41, 2008.

[5] C. J. Mitchell, F. C. Piper, "Key Storage in Secure Networks," *Discrete Applied Mathematics*, vol. 21, no. 3, pp. 215–228, 1988.

[6] S. A. Camtepe, B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," In *Proc. ESORICS 2004*, LNCS vol. 3193, pp. 293-308, Springer, 2004.

[7] J. Lee, D. R. Stinson, "On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs," *ACM Trans. Inform. Syst. Secur*, vol. 11, no. 2, pp. 1-35, 2008.

[8] K. M. Martin, "On the applicability of combinatorial designs to key predistribution for wireless sensor networks," In *Proc. IWCC09*, LNCS vol. 5557, pp. 124-145, Springer, 2009.

[9] D. Stinson, *Combinatorial Designs; Constructions and Analysis*, Springer, 2004.

[10] I. Anderson, *A First Course in Discrete Mathematics*, Springer, 2001.

[11] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inform. Syst. Secur.*, vol. 8, pp. 228- 258, 2005.

[12] R. Wei, J. Wu, 11Product construction of key distribution schemes for sensor networks," In *Proc. SAC 2004*, LNCS vol. 3357, pp. 280-293, Springer, 2005.

[13] K. A. S. Quinn, "Bounds for Key Distribution Patterns," *Journal of Cryptology*, vol. 12, pp. 227–239, 1999.

[14] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," In *Proc. EUROCRYPT'84*, LNCS vol. 209, pp. 335–338, Springer, 1985.