Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 323–328*

Observations on linear key predistribution schemes and their applications to group deployment of nodes

Alexey V. Urivskiy ourivski@mail.ru, urivskiy@infotecs.ru
JSC "InfoTeCS", Moscow, Russia

Abstract. In this paper we discuss key predistribution schemes. In particular, we deal with linear key predistribution schemes which are a generalization of Blom's scheme. We describe how to adapt a general construction to support deployment network nodes in groups. The proposed group-based constructions are evaluated against different attacking strategies.

1 Introduction

A popular research area in cryptographic key management is lightweight distributed environments like wireless ad hoc and sensor networks. It turns out that key predistribution is a suitable solution for them, see surveys [1, 2].

In a *key predistribution scheme* (KPS) a trusted authority at a network setup generates and distributes a set of long-term secret keys $\mathcal{K}$ to a set of nodes. Each node, labeled by index j, is given its own set of keys — the node's key ring (or key block). The distributed keys allow pairs of nodes to compute pairwise (common) keys. After the setup the authority usually quits and, no changes in nodes' key rings is possible.

If a KPS allows every pair of nodes to compute a common key, we call such a scheme *deterministic*. If the pairwise key is not guaranteed for an arbitrary pair, then the KPS is *probabilistic*.

A typical attack on a KPS assumes that the adversary randomly captures a set of nodes. The captured nodes are called *compromised nodes*, and their keys are called *compromised keys*. Collecting the keys of the compromised nodes the adversary tries to compromise pairwise keys of innocent nodes. Alternatively the set of compromised nodes can be considered as a set of malicious colluders.

It is usually required that the pairwise key be secure against a set of colluders of a predefined size. We call a KPS to be *w-secure*, if for any pair of nodes, any coalition of w of fewer other nodes, pooling their key rings, can obtain no information (in information-theoretic sense) about the pairwise key of those two.

Another requirement to consider is storage. Usually the more secure the KPS, the larger amount of data the node has to store for a given network size. However nodes are memory constrained, so a solution with smaller key rings is preferable.

The main challenge when designing a KPS is to balance those somewhat contradicting requirements (there are also many others we do not mention here). Some optimization and useful improvements could be achieved, if additional information on how the network is deployed or the behavior of adversaries could be taken into account.

In this work, we deal with deterministic KPSs of a special type — the so called linear KPS which is a generalization of Blom's KPS [3]. We make some observation on how these KPSs can be constructed so that to support a scenario when nodes naturally or artificially are arranged and deployed in groups.

2 Blom's scheme

We describe Blom's scheme in matrix notation. Let $\mathbf{D}$ be a $(w+1) \times (w+1)$ random symmetric matrix with entries in a finite field $GF(Q)$. The matrix $\mathbf{D}$ is globally kept secret. Let $\mathbf{H}$ be a $(w+1) \times N$ parity check matrix of a Reed-Solomon code over $GF(Q)$. The matrix $\mathbf{H}$ is publicly known.

The j-th node is given the j-th column $\mathbf{a}_j$ of

$$\mathbf{A} = \mathbf{DH}, \tag{1}$$

which he keeps secret. The pairwise key of i-th and j-th nodes is

$$k_{ij} = \mathbf{h}_i^T \mathbf{a}_j = \mathbf{h}_i^T \mathbf{D} \mathbf{h}_j = \mathbf{h}_j^T \mathbf{a}_i, \tag{2}$$

where $\mathbf{h}_i$ is the i-th column of $\mathbf{H}$.

Blom's scheme is deterministic and w-secure. It is also known that the scheme is optimal in terms of storage for a given w. Another important property is that in practice the unbounded scaling is possible: The scheme can include up to Q nodes with typically $Q \geq 2^{80}$. Adding new nodes before the limit is reached does not require rekeying or distributing new keys to the existing nodes.

Due to these positive properties, Blom's scheme is frequently used as a building block in more complex KPSs. On the other hand, Blom's scheme reveals some features which are not always relevant to practice.

First, Blom's scheme is a threshold scheme and satisfies "all-or-nothing" property: No w colluders can get the pairwise key of any pair, but *any* $w+1$ colluders can get pairwise keys of *all the pairs*. However, usually it is expected that the larger the number of colluders, the larger the number of compromised pairwise keys, but not all the keys could be compromised simultaneously.

Second, Blom's scheme follows a homogenous network model: All nodes are considered to be equal in terms of storage, physical resilience etc. It practice, this is almost always not true. Typically nodes are gathered or allocated into some *groups* by one or several criteria.

In this paper, we look at a generalization of Blom's scheme, called *linear* KPSs, and show how to build linear KPSs matching network deployment in groups of nodes.

3 Linear key predistribution schemes

The optimality of Blom's scheme and its threshold behavior are solely defined by the properties of RS-codes. Naturally, it is possible to use other codes. But what will be the effect?

It is quite obvious that a pairwise key in Blom's scheme is a linear combination of random elements of matrix $\mathbf{D}$. So is node's key block $\mathbf{a}_j$. In [4] and [5], Blom's scheme was generalized to the so called *linear* KPS. We formulate the main result of those works as follows.

Theorem 1. *Let* $\mathbf{D}$ *be an* $n \times n$ *random symmetric matrix over* $GF(Q)$*. Let* $\mathbf{H}$ *be some* $n \times N$ *matrix over* $GF(Q)$*. A KPS given by (1) and (2) is* w*-secure if and only if any* $w+1$ *columns of* $\mathbf{H}$ *are linear independent over* $GF(Q)$*.*

The proof is based on the fact that any key can be compromised if it is in a linear span of colluders' keys.

The theorem shows that $\mathbf{H}$ can be a parity check matrix of any $(N, N-n, w+2)$ linear code over $GF(Q)$ to get a w-secure Blom-like scheme. It should be noted however that the smallest size of node's key block (the length of column $\mathbf{a}_j$) is achieved only for MDS codes with distance $w+2 = n+1$. At the same time the threshold property will only be observed for MDS codes as well.

The theorem has a useful corollary.

Corollary 1. *The pairwise key* k_{ij} *of nodes* i *and* j *is compromised against a particular set of colluders* $(\ell_1, \ldots, \ell_c)$ *if and only if* $\mathbf{h}_i$ *or* $\mathbf{h}_j$ *or both are linear dependent on* $\mathbf{h}_{\ell_1}, \ldots, \mathbf{h}_{\ell_c}$*.*

The intrinsic property of any linear KPS is that if a column $\mathbf{h}$ of an innocent node is linear dependent on colluders' columns, then the colluders compromise all pairwise keys of that innocent node. So we may describe the attack of colluders not only against a particular key, but as against the particular node.

By selecting $\mathbf{H}$ with certain properties, or linear dependencies over its columns, we can control the resilience of the linear KPS.

4 Linear KPS for groups of nodes

One of the important scenarios of network deployment is when the nodes are arranged into groups. Grouping can be done according to many different criteria: available computing power, storage, connectivity, physical resilience, geographical location, deployment time, nodes' roles within the network and so on.

A pair of nodes from the same group must definitely possess a pairwise key. The communication between groups is desirable but depends on a particular grouping and the KPS. An important property of linear KPSs, inherited from Blom's one, is that they are deterministic irrespectively of $\mathbf{H}$.

So to obtain a KPS suitable for group deployment scenario one has to select an appropriate $\mathbf{H}$.

4.1 Independent groups

Consider the following quite simple construction of $\mathbf{H}$ appropriate to deployment nodes in independent groups.

Let there be u groups, each of size N_ℓ, so that $\sum_{\ell=1}^{u} N_\ell = N$. Let

$$\mathbf{H}_{ind} = \mathrm{diag}(\mathbf{H}_1, \ldots, \mathbf{H}_u) \tag{3}$$

where $\mathbf{H}_\ell$ is an $(w_\ell + 1) \times N_\ell$ parity check matrix of an $(N_\ell, N_\ell - w_\ell - 1, w_\ell + 2)$ MDS code over $GF(Q)$ corresponding to the ℓ-th group of nodes.

4.1.1 Security analysis

Strictly speaking, the KPS with $\mathbf{H}_{ind}$ is only w-secure for $w = \min_\ell w_\ell$, while the node has to store as many as $n = \sum_\ell (w_\ell + 1)$ keys, as if it were $n-1$-secure Blom's scheme. On the other hand, resiliency degradation in the network highly depends on how the attacker compromises nodes. We consider the properties of the scheme against two attacking strategies. In the first one, the adversary cannot choose from which groups to compromise nodes. And he compromises them by randomly selecting from the whole network. We will call this a *whole network* attacking strategy. In the second strategy, the adversary is only able to compromise nodes by randomly selecting them from particular (fixed or predefined) groups. This strategy is called *group-bounded*.

Working with groups, it is not enough to characterize the coalition of colluders only by its size. We need to know a distribution of colluders among groups. A coalition given by an u-vector $(s_1, s_2, \ldots, s_u)$ is a coalition in which there are s_1 colluders from group 1, s_2 colluders from group 2, and so on.

Whole network strategy. Take any $w_\ell + 1$ columns from $\mathbf{H}_\ell$, $\ell = 1, \ldots, u$. They altogether form a non-singular matrix. Then immediately from corollary 1, we see that *any* $(w_1 + 1, w_2 + 1, \ldots, w_u + 1)$-coalition can compromise *any* node.

If totally k nodes were compromised, then the probability that a node (and also all nodes) from ℓ-th group is compromised is $\frac{\binom{N_\ell}{w_\ell+1}\binom{N-N_\ell}{k-w_\ell-1}}{\binom{N}{k}}$. So the resilience of the network is falling gradually with the compromise of nodes and can be controlled by selecting an appropriate number of groups.

Group-bounded strategy. Since the columns of $\mathbf{H}_{ind}$ corresponding to different groups are linear independent, from corollary 1 we obtain the following property of the scheme. A node from group ℓ could only be compromised by at least $w_\ell + 1$ colluders from that group: *No* coalition including less than $w_\ell + 1$ colluders from group ℓ can compromise the node. Thus, if nodes are compromised only within certain groups, then the resiliency degradation is restricted

to the affected groups. So groups are securely isolated from each other. This justifies the term *independent groups* in the description of the scheme.

4.2 Hierarchical groups

The linear KPS for independent groups might by not enough secure against the group-bounded attacking strategy. To attack a particular group the adversary needs to compromise only $w_\ell + 1$ nodes, while the node's key block includes $n \sim uw_\ell$ keys. The original Blom's scheme offers for this storage n-security, however without secure isolation of groups.

In this section, we describe an "intermediate" solution. We assume that there is a *hierarchy* among groups of nodes, so that it must be more difficult to compromise a node from group i than from group j if $i < j$. Instead of the term *group* it is better to use the term *level*. Level 1 will be the highest level, level u — the lowest level.

Apart from obvious military applications, we can imagine a scenario of sensor networks for which hierarchy of groups seems suitable. On the lowest level there are sensors, which are scattered around some territory. On the next level there are some moving or portable information gathering agents. And on the top level there are stationary controllers collecting all the information and controlling the network. Obviously nodes from different levels are prone to compromise in a different degree, and the KPS must match this situation.

Now we describe a construction of a linear KPS which directly allows grouping nodes into levels, such that the higher the level the node belongs to, the more powerful must be a colluders' coalition to compromise its keys.

Let $\mathbf{H}_0$ be a parity check matrix of a generalized Reed-Solomon code, say $\mathbf{H}_0 = [z_j h_j^{i-1}]$, for different non-zero $h_j \in GF(Q)$ and non-zero $z_j \in GF(Q)$.

Consider the lower-triangular block matrix

$$\mathbf{H}_{hrc} = \begin{pmatrix} \mathbf{H}_{11} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H}_{21} & \mathbf{H}_{22} & \dots & \mathbf{0} \\ & & \ddots & \\ \mathbf{H}_{u1} & \mathbf{H}_{u2} & & \mathbf{H}_{uu} \end{pmatrix}, \tag{4}$$

which is obtained from $\mathbf{H}_0$ by zeroing blocks over the main diagonal. Here $\mathbf{H}_{\ell\ell}$ is a $(w_\ell + 1) \times N_\ell$ matrix. The matrix $(\mathbf{H}_{\ell\ell}^T, \mathbf{H}_{\ell+1,\ell}^T, \dots, \mathbf{H}_{u\ell}^T)^T$ is a parity check matrix of a GRS-code over $GF(Q)$ of length N_ℓ and distance $D_\ell = 1 + \sum_{i=\ell}^{u}(w_i + 1)$.

The nodes corresponding to the columns of $\mathbf{H}_{\ell\ell}$ will belong to level ℓ.

4.2.1 Security analysis

Whole network strategy. Take from $\mathbf{H}_{hrc}$ any $w_1 + 1$ columns at level 1, $w_2 + 1$ columns at level 2, $w_3 + 1$ columns at level 3 and so on. They

altogether form a non-singular matrix. Then immediately from corollary 1, we see that *any* $(w_1+1, w_2+1, \ldots, w_u+1)$-coalition can compromise *any* node. However, *no* $(w_1+1, \ldots, w_{\ell-1}+1, w_\ell, w_{\ell+1}+1, \ldots, w_u+1)$-coalition or smaller can compromise a node from level ℓ.

Group-bounded strategy. Consider the situation, when all the colluders are from level ℓ only. Since the matrix $(\mathbf{H}_{\ell\ell}^T, \mathbf{H}_{\ell+1,\ell}^T, \ldots, \mathbf{H}_{u\ell}^T)^T$ is a parity check matrix of a GRS-code with distance D_ℓ, then to compromise a node at level ℓ it is required a coalition of size $D_\ell - 1 = \sum_{i=\ell}^{u}(w_i+1)$. So for higher levels the coalition will be larger than for lower ones.

If the colluders are from level ℓ and lower, then a coalition compromising a node at level ℓ must include at least $w_\ell + 1$ colluders from level ℓ independently on how many colluders there are from levels lower than ℓ. This trivially follows from the fact, that $\mathbf{H}_{\ell\ell}$ is a parity check matrix of a GRS-code with distance $w_\ell + 2$.

Both facts justify the use of the term *hierarchy* among groups.

5 Conclusion

We described simple group-based constructions for linear key-predistribution schemes. These constructions are useful for deployment of nodes in independent and hierarchical groups. They guarantee that two nodes possess a common pairwise key. However, unlike the basic Blom's scheme the new constructions do not reveal "all-or-nothing" behavior and do allow secure isolation of some groups of nodes from others.

References

[1] K. Martin, M. Paterson, D. Stinson, Key Predistribution for Homogeneous Wireless Sensor Networks with Group Deployment of Nodes, *ACM Trans. Sensor Netw.,* **7**(2), Article 11, 2010.

[2] S. Camtepe, B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: A Survey, *Technical Report,* **TR-05-07**, Rensselaer Polytechnic Institute, Computer Science Department, 2005.

[3] R. Blom, An optimal class of symmetric key generation systems, in *Proc. of EUROCRYPT'84,* LNCS **209**, 335–338 (1985).

[4] V. M. Sidel'nikov, *Coding Theory,* Fizmatlit, Moscow, 2008, (in Russian).

[5] C. Padro, I. Gracia, S. M. Mollevi, P. Morillo, Linear Key Predistribution Schemes. *Designs, Codes and Cryptography,* **25** (3), 281–298, 2002.