Self-Healing Key Distribution Schemes with Sponsorization *

Germán Sáez

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034-Barcelona, Spain
german@ma4.upc.edu

Abstract. In a self-healing key distribution scheme a group manager enables a large and dynamic group of users to establish a group key over an unreliable network. The group manager broadcasts in every session some packet of information in order to provide a common key to members of the session group. The goal of self-healing key distribution schemes is that, even if the broadcast is lost in a certain session, the group member can recover the key from the broadcast packets received before and after the session. This approach to key distribution is quite suitable for wireless networks, mobile wireless ad-hoc networks and in several Internet-related settings, where high security requirements need to be satisfied.
In this work we provide a generalization of previous definitions in two aspects. The first one is to consider general structures instead of threshold ones to provide more flexible performance to the scheme. The second one is to consider the possibility that a coalition of users sponsor a user outside the group for one session: we give the formal definition of self-healing key distribution schemes with sponsorization, some bounds on the required amount of information. We also give a general construction of a family of self-healing key distribution schemes with sponsorization by means of a linear secret sharing scheme. Our construction differs from previous self-healing key distribution schemes in the fact that the length of the broadcast is almost constant. Finally we analyze the particular case of this general construction when Shamir's secret sharing scheme is used.

Keywords: group key, self-healing, dynamic groups, linear secret sharing schemes, broadcast.

1 Introduction

Self-healing key distribution schemes enable large and dynamic groups of users of an *unreliable* network to establish group keys for secure communication. In a

* This work was done while the author was in the *Dipartimento di Informatica ed Applicazioni* at the *Università di Salerno*, Italy. The author would like to thank people in the Crypto Research Group for their kind hospitality and useful comments. Research supported in part by Spanish *Ministerio de Ciencia y Tecnología* under project CICYT TIC 2003–00866.

self healing key distribution scheme, a group manager provides a common key to a group of users by using packets that he sends over a broadcast channel at the beginning of each session. Every user on the group computes the group key by means of this packet and some private information supplied by the group manager. Multiple groups can be established by the group manager for different sessions by joining or removing users from the initial group. The main goal of these schemes is the self-healing property: if during a certain session some broadcasted packet gets lost, then users are still capable of recovering the group key for that session simply by using the packets they have received during a previous session and the packets they will receive at the beginning of a subsequent one, without requesting additional transmission from the group manager.

This new approach to key distribution is very useful due to the self-healing property, supporting secure communications in wireless networks, mobile wireless ad-hoc networks, broadcast communications over low-cost channels (live-events transmissions, etc.) and in several Internet-related settings.

Self-healing key distribution schemes were introduced by Staddon et al. in [7] providing formal definitions, lower bounds to the resources required to such schemes as well as some constructions. In [6], Liu et al. generalised the above definition and gave some constructions. Blundo et al. in [1] modified the proposed definitions, gave new lower bounds, proposed some efficient constructions and showed some problems in previous constructions. Finally, Blundo et al. in [2] analysed previous definitions and showed that no protocol could exist for some of them; they proposed a new definition, gave some lower bounds for it and proposed some schemes. All of these papers mainly focused on unconditionally secure schemes.

The contributions of our paper are the following. First of all we formally define self-healing key distribution schemes with sponsorization in Section 2. This definition contains two main differences comparing with the one presented in [1]. The first one is to consider a monotone decreasing family of rejected subsets of users instead of a monotone decreasing threshold structure and the second one is to consider the feature that a coalition of users can sponsor a user outside the group for one session. The first modification allows us to consider more flexible self-healing key distribution schemes that can reach better properties. The motivation for the second modification is to give dynamism to the scheme allowing an authorized subset of users in the group to invite a new user without the help of the group manager. Of course the proposal considers the case in which certain majorities (the coalition of authorized subsets of users to sponsor) can perform this action. This feature has been considered in other distributed protocols as group key distribution schemes [5, 4]. In Section 3 some lower bounds on the resources required to such schemes are presented. We give lower bounds on the amount of information given to sponsor a user and on the personal key of a user with this capability. In Section 4 a family of self-healing key distribution schemes with sponsorization is presented. This construction follows in part the ideas of [1] but considering any possible linear secret sharing scheme instead of a threshold one and ideas of [5, 4] for sponsorization capability. At the end of the

section we comment the security and efficiency of the scheme. Finally we present in Section 5 the scheme obtained when Shamir's secret sharing scheme is used.

2 Self-Healing Key Distribution Schemes with Sponsorization

The models presented in [1] and [7] implement self-healing key distribution schemes with good properties. However these models do not consider the possibility that a coalition of users in the group can invite a new user to the group. This feature has been considered in other protocols to distribute keys as group key distribution schemes [5, 4]. In this section we propose a model for this feature.

Let $\mathcal{U} = \{1, \ldots, n\}$ be the finite universe of users of a network. A broadcast unreliable channel is available, and time is defined by a global clock. Suppose that there is a group manager who sets up and manages, by means of join and revoke operations, a communication group, which is a dynamic subset of users of $\mathcal{U}$. Let $G_j \subset \mathcal{U}$ be the communication group established by the group manager in session j. Each user $i \in G_j$ holds a personal key S_i, received from the group manager before or when joining G_j. A personal key S_i can be seen as a sequence of elements from a finite set. A user $\ell \in G_j$ can sponsor a user $i \notin G_j$ for session j by giving to him some proof of sponsorization $P_{\ell i}^j$.

We denote the number of sessions supported by the scheme as m, the set of users revoked by the group manager in session j as R_j, and the set of users who join the group in session j as J_j. Hence, $G_j = (G_{j-1} \cup J_j) - R_j$ for $j \geq 2$ and by definition $R_1 = \emptyset$. Moreover, for $j = 1, \ldots, m$, let K_j be the session key chosen by the group manager and communicated to the group members through a broadcast message, B_j. For each $i \in G_j$, the key K_j is determined by B_j and the personal key S_i. This key can also be computed by a user $i \notin G_j$ sponsored by a subset of users $A \in \Gamma$, $A \subset G_j$ by means of B_j and $\{P_{\ell i}^j\}_{\ell \in A}$, for a certain family of subsets $\Gamma \subset 2^{\mathcal{U}}$. Then Γ is the family of authorized subsets to perform a sponsorization, that we suppose monotone increasing (if $A_1 \in \Gamma$ and $A_1 \subset A_2 \subset \mathcal{U}$, then $A_2 \in \Gamma$).

The family of subsets of users that can be revoked by the group manager is the monotone decreasing structure $\mathcal{R} \subset 2^{\mathcal{U}}$ (that is, if $A_2 \in \mathcal{R}$ and $A_1 \subset A_2 \subset \mathcal{U}$, then $A_1 \in \mathcal{R}$). In a natural way we assume that a subset of users which can be rejected cannot be authorized to sponsor a user. Then the monotone increasing access structure Γ satisfies $\Gamma \cap \mathcal{R} = \emptyset$. In order to define the security of the sponsorization capability we also consider the monotone decreasing structure $\mathcal{S} \subset 2^{\mathcal{U}}$ compound by the collection of tolerated coalition of users that can receive sponsorization by a unique sponsor.

Let $\mathbf{S}_i, \mathbf{P}_{\ell i}^j, \mathbf{B}_j, \mathbf{K}_j$ be random variables representing the personal key for user i, the proof used by user ℓ to sponsor user i in session j, the broadcast message B_j and the session key K_j for session j, respectively. The probability distributions according to whom the above random variables take values are determined by the key distribution scheme and the random bits used by the group manager.

In particular, we assume that session keys K_j are chosen independently and according to the uniform distribution.

We define a $(\mathcal{R}, \Gamma, \mathcal{S})$-*self-healing scheme with sponsorization* using the entropy function (see [3] for more details on Information Theory):

Definition 1 *Let $\mathcal{U}$ be the universe of users of a network, let m be the maximum number of sessions, and let $\mathcal{R} \subset 2^{\mathcal{U}}$ be a monotone decreasing access structure of subsets of users that can be revoked by the group manager. Assume that Γ is the family of authorized subsets of users to perform a sponsorization verifying $\Gamma \cap \mathcal{R} = \emptyset$. We also consider the monotone decreasing structure $\mathcal{S} \subset 2^{\mathcal{U}}$ of the tolerated coalition of users that can be sponsored by a unique sponsor. A $(\mathcal{R}, \Gamma, \mathcal{S})$-self-healing key distribution scheme with sponsorization is a protocol satisfying the following conditions:*

1. *The scheme is a session key distribution scheme, meaning that:*
   (a) *For each member $i \in G_j$, the key K_j is determined by B_j and S_i. Formally, it holds that: $H(\mathbf{K}_j|\mathbf{B}_j, \mathbf{S}_i) = 0$.*
   (b) *Keys $K_1, \ldots, K_n$ cannot be determined from the broadcast or personal keys alone. That is: $H(\mathbf{K}_1, \ldots, \mathbf{K}_m|\mathbf{B}_1, \ldots, \mathbf{B}_m) = H(\mathbf{K}_1, \ldots, \mathbf{K}_m|\mathbf{S}_{G_1 \cup \cdots \cup G_m}) = H(\mathbf{K}_1, \ldots, \mathbf{K}_m)$.*
2. *The scheme has $\mathcal{R}$-revocation capability. That is, for each session j, if $R = R_j \cup R_{j-1} \cup \cdots \cup R_2$ is such that $R \in \mathcal{R}$, then the group manager can generate a broadcast message B_j such that all revoked users in R cannot recover K_j (even knowing all the information broadcast in sessions $1, \ldots, j$). In other words: $H(\mathbf{K}_j|\mathbf{B}_j, \mathbf{B}_{j-1}, \ldots, \mathbf{B}_1, \mathbf{S}_R) = H(\mathbf{K}_j)$.*
3. *The scheme is $(\mathcal{R}, \Gamma)$-self-healing. This means that the two following properties are satisfied:*
   (a) *Every user $i \in G_r$ who has not been revoked before session s can recover all keys K_ℓ for $\ell = r, \ldots, s$, from broadcasts B_r and B_s, where $1 \leq r < s \leq m$. Formally, it holds that: $H(\mathbf{K}_r, \ldots, \mathbf{K}_s|\mathbf{S}_i, \mathbf{B}_r, \mathbf{B}_s) = 0$.*
   (b) *Let $B \subset R_r \cup R_{r-1} \cup \cdots \cup R_2$ be a coalition of users removed from the group before session r and let $C \subset J_s \cup J_{s+1} \cup \cdots \cup J_m$ be a coalition of users who join the group from session s with $r < s$. Suppose $B \cup C \in \mathcal{R}$. Then, such a coalition does not get any information about keys K_j, for any $r \leq j < s$. That is: $H(\mathbf{K}_r, \ldots, \mathbf{K}_{s-1}|\mathbf{B}_1, \ldots, \mathbf{B}_m, \mathbf{S}_B, \mathbf{S}_C) = H(\mathbf{K}_r, \ldots, \mathbf{K}_{s-1})$.*
4. *The scheme has $(\Gamma, \mathcal{S})$-sponsorization. This means that the three following properties are satisfied:*
   (a) *Every user $\ell \in G_j$ can generate a proof of sponsorization $P^j_{\ell i}$ to sponsor a user $i \notin G_j$ for session j using his personal key. In other words: $H(\mathbf{P}^j_{\ell i}|\mathbf{S}_\ell) = 0$.*
   (b) *A user $i \notin G_j$ that receives enough sponsorizations from a subset of users $A \subset G_j$ with $A \in \Gamma$ can compute the key K_j in the same conditions that users in G_j. That is: $H(\mathbf{K}_j|\mathbf{P}^j_{Ai}\mathbf{B}_r\mathbf{B}_s) = 0$ for $A \in \Gamma$, $A \subset G_j$, $i \notin G_j$ and $r \leq j \leq s$.*

(c) *Suppose that a coalition of users* $i_1, \ldots, i_u \notin G_j$*, not revoked before session* j*, have received sponsorization from subsets of users* $C_1, \ldots, C_u \notin \Gamma$ *respectively, with* $C_1 \cup \cdots \cup C_u = \{\ell_1, \ldots, \ell_v\} \subset G_j$*. This action is performed in such a way that users* $\ell_1, \ldots, \ell_v$ *sponsor subsets of users* $D_1, \ldots, D_v \in \mathcal{S}$ *respectively, with* $D_1 \cup \cdots \cup D_v = \{i_1, \ldots, i_u\} \subset \mathcal{U} - G_j$*; therefore* $P^j_{C_1 i_1} \ldots P^j_{C_u i_u} = P^j_{\ell_1 D_1} \ldots P^j_{\ell_v D_v}$*. In these conditions, such a coalition does not get any information about the value of key* K_j*. Formally, it holds that:* $H(\mathbf{K}_j | \mathbf{P}^j_{C_1 i_1} \ldots \mathbf{P}^j_{C_u i_u} \mathbf{B}_r \mathbf{B}_s) = H(\mathbf{K}_j)$ *for* $C_1, \ldots, C_u \notin \Gamma, D_1, \ldots, D_v \in \mathcal{S}$ *such that* $P^j_{C_1 i_1} \ldots P^j_{C_u i_u} = P^j_{\ell_1 D_1} \ldots P^j_{\ell_v D_v}$, $C_1 \cup \ldots \cup C_u = \{\ell_1, \ldots, \ell_v\} \subset G_j, D_1 \cup \ldots \cup D_v = \{i_1, \ldots, i_u\} \subset \mathcal{U} - G_j$ *and* $r \leq j \leq s$.

This definition has two differences with respect to the one presented in [1]. First the family of subsets that can be rejected in [1] is $\mathcal{R} = \{R \subset \mathcal{U} : |R| \leq t\}$ while in our definition we consider the general case of any possible monotone decreasing structure $\mathcal{R}$, not only threshold ones. This allows us to consider more general self-healing key distribution schemes, where, for instance, some users can be more revocable than others. And the second one is that the possibility of sponsorization is considered. The conditions to define this feature are the following. Condition 4.(a) expresses the mechanism of sponsorization: the information used to sponsor is computed from the personal key. The condition 4.(b) expresses the fact that the information obtained from enough sponsorizations with the correspondent broadcast allows to compute the personal key of the session. The last condition 4.(c) gives us the security condition: a coalition of users outside G_j sponsored by not enough users cannot obtain any information about the value of the key K_j. The key remains secure even if every user receives sponsorization of a coalitions in $\mathcal{S}$.

3 Lower Bounds

In this section we present some bounds for a $(\mathcal{R}, \Gamma, \mathcal{S})$-self-healing key distribution scheme with sponsorization. The first one is a lower bound on the size of proofs of sponsorization and the second one is a lower bound on the size of the personal key.

Proposition 1 *In any* $(\mathcal{R}, \Gamma, \mathcal{S})$*-self-healing key distribution scheme with sponsorization, for any user* $\ell \in G_j$ *and* $i \notin G_j$*, it holds that*

$$H(\mathbf{P}^j_{\ell i}) \geq H(\mathbf{K}_j).$$

Proof. Suppose that there exists a subset of users $C \subset G_j$ such that $C \notin \Gamma$ and $C \cup \{\ell\} \in \Gamma$. From conditions 4.(b) and (c) we have that:

$$H(\mathbf{K}_j | \mathbf{P}^j_{Ci} \mathbf{P}^j_{\ell i} \mathbf{B}_j) = 0 \text{ and } H(\mathbf{K}_j | \mathbf{P}^j_{\ell i} \mathbf{B}_j) = H(\mathbf{K}_j).$$

Then we can apply Lemma 5.1 in [1] finding $H(\mathbf{P}^j_{\ell i}) \geq H(\mathbf{K}_j)$.

□

If the secret keys are uniformly chosen in a finite field $GF(q)$ then $\log |P^j_{\ell i}| \geq \log q$ for any $\ell \in G_j$ and $i \notin G_j$ because $H(\mathbf{P}^j_{\ell i}) \leq \log |P^j_{\ell i}|$. That is: every proof of sponsorization must have at least $\log q$ bits. Moreover for a fixed session j and a user $i \notin G_j$, conditions 4.(b) and (c) determine a secret sharing scheme that distributes secrets K_j, with shares $P^j_{\ell i}$ for users $i \in \mathcal{U} - G_j$ realizing structure $\Gamma_j = \{A \subset \mathcal{U} - G_j \ : \ A \in \Gamma\}$. Then: $\max_{i \in \mathcal{U}-G_j} \log |P^j_{\ell i}| \geq \frac{\log q}{\rho^*(\Gamma_j)}$.

With regard to lower bounds for the size of the personal key it can be proved the following result. For any user i belonging to the group since session j and any subset of users $C \in \mathcal{S}$ with $C \cap G_j = C \cap G_{j+1} = \cdots = C \cap G_m = \emptyset$, it holds that $H(\mathbf{S}_i) \geq H(\mathbf{P}^j_{iC} \mathbf{P}^{j+1}_{iC} \ldots \mathbf{P}^m_{iC})$. Assuming that the proofs of sponsorization are statistically independent and secret keys are uniformly chosen in a finite field $GF(q)$ (using Proposition 1), then $H(\mathbf{S}_i) \geq (m - j + 1) \ |C| \ \log q$. So, in this situation every user added in session j must store a personal key of at least $(m - j + 1)|C| \log q$ bits because $\log |S_i| \geq (m - j + 1)|C| \log q$.

With respect to lower bounds on the broadcast information, the one found in [1] is valid for our model with the same proof.

4 A Family of Self-Healing Key Distribution Schemes with Sponsorization

To construct this family of self-healing key distribution schemes with sponsorization we follow in part ideas of Scheme 2 in [1] and sponsorization mechanism in [5, 4]. Our construction has three main differences with Scheme 2 in [1]. The first one is that we use linear secret sharing schemes instead of Shamir secret sharing scheme as Scheme 2 in [1] does, supporting in this way new properties and features. See [8] for more details on secret sharing schemes. The second one is to increase the information given to users on the personal key. This operation allows a subset of users in a group to sponsor new users in such a way that they obtain the key of the session without the help of the group manager. A secure unicast channel between the sponsors and the sponsored user is necessary. And the third one is that this construction uses a different broadcast than the one in [1]. In fact the broadcast in [1] can also be used in our construction, but ours gives us an almost constant length broadcast. In this section we present this construction, prove the security and analyze the efficiency.

Let q be a prime power and denote by $K_j \in GF(q)$ the session key for group G_j. Let Γ be a monotone increasing access structure. We suppose for simplicity that there exists a public map

$$\psi : \mathcal{U} \cup \{D\} \longrightarrow GF(q)^t$$

which defines Γ as a vector space access structure, with D a special user outside $\mathcal{U}$ (see [8] for definitions). But the construction that we present here can be extended in a natural way to work with any access structure Γ by means of a linear

secret sharing scheme realizing it. The use of a specific ψ fixes the properties of the scheme. Let $\mathcal{R} = 2^{\mathcal{U}} - \Gamma$ be a monotone decreasing access structure and $\mathcal{S} = 2^{\mathcal{U}} - \Gamma'$ where Γ' is defined as $\Gamma' = \{A \subset \mathcal{U} \ : \ GF(q)^t = \langle \psi(A) \rangle\}$. Note that $\Gamma' \subset \Gamma$ is a monotone increasing access structure that depends on the function ψ chosen to represent Γ.

We are going to present a self-healing key distribution scheme with sponsorization in which Γ is the family of subsets of users that can perform a sponsorization, $\mathcal{R} = 2^{\mathcal{U}} - \Gamma$ is the family of subsets of users that can be revoked by the group manager and $\mathcal{S} = 2^{\mathcal{U}} - \Gamma'$ is the family of tolerated coalition of users that can be sponsored by a unique sponsor. In order to construct the scheme we need to prove the following lemma:

Lemma 1 *Let $v_1, \ldots, v_n$ be non null vectors in $GF(q)^t$, for q a prime power. If $q \geq n$ then there exists at least one vector $v \in GF(q)^t$ such that $v \cdot v_i \neq 0$ for all $i = 1, \ldots, n$.*

Proof. Let $A_i = \{v \in GF(q)^t : v \cdot v_i \neq 0\}$. First we will prove that for any positive integer $k = 1, \ldots, n$ we have that $|A_1 \cap \cdots \cap A_k| \geq q^t - kq^{t-1} + (k-1)$. The proof is by induction on k.

For $k = 1$ we can take into account that $A_1 = GF(q)^t - \langle v_1 \rangle^{\perp}$ where $\langle v_1 \rangle^{\perp}$ is the $(t-1)$-dimensional orthogonal subspace of $\langle v_1 \rangle$ in $GF(q)^t$. Then $|A_1| = q^t - q^{t-1}$ and, in fact, $|A_i| = q^t - q^{t-1}$ for any i.

If this result is true for k then

$$|A_1 \cap \cdots \cap A_k \cap A_{k+1}| = |A_1 \cap \cdots \cap A_k| + |A_{k+1}| - |(A_1 \cap \cdots \cap A_k) \cup A_{k+1}| \geq$$

$$\geq q^t - kq^{t-1} + (k-1) + q^t - q^{t-1} - (q^t - 1) = q^t - (k+1)q^{t-1} + k$$

because $(A_1 \cap \cdots \cap A_k) \cup A_{k+1}$ is a subset of $GF(q)^t$ that does not contain the null element.

The proof of the lemma ends observing that for $n = 1$ the result is true because $|A_1| = q^t - q^{t-1} > 0$ and for $n \geq 2$ we have $|A_1 \cap \cdots \cap A_n| \geq q^t - nq^{t-1} + (n-1) \geq q^{t-1}(q-n) + 1 \geq 1$ if $q \geq n$.

□

Now we describe the different phases of our proposal of self-healing key distribution scheme. In order to design the scheme we need a vector $v \in GF(q)^t$ such that $v \cdot \psi(i) \neq 0$ for all $i \in \mathcal{U}$. Suppose $q \geq n$, then vector v exists applying Lemma 1. For instance, for vectors defining Shamir secret sharing scheme (see [8]) we have that an appropriate vector is $v = (1, 0, \ldots, 0)$.

Set-up. Let $G_1 \subset \mathcal{U}$. The group manager randomly chooses $t \times t$ matrices $P_1, \ldots, P_m$ and session keys $K_1, \ldots, K_m \in GF(q)$. For each $j = 1, \ldots, m$ the group manager computes the vector $z_j = K_j v + \psi(D)^{\top} P_j \in GF(q)^t$. The group manager sends privately to user $i \in G_1$ the personal key $S_i = (\psi(i)^{\top} P_1, \ldots, \psi(i)^{\top} P_m) \in GF(q)^{tm}$. Note that if we use a linear secret sharing scheme in which a user i is associated with $m_i \geq 1$ vectors, then his secret information S_i consists of m_i vectors of tm components.

Full addition. In order to add users $J_j \subset \mathcal{U}$ in session j, the group manager sends privately $S_i = (\psi(i)^\top P_j, \psi(i)^\top P_{j+1}, \ldots, \psi(i)^\top P_m) \in GF(q)^{t(m-j+1)}$ to every user $i \in J_j$ as his personal key.

Broadcast. Suppose $R_j \subset G_{j-1}$ with $R_1 \cup R_2 \cup \cdots \cup R_j \in \mathcal{R}$ if $j \geq 2$. By definition we have $R_1 = \emptyset$. The group manager chooses a maximal non-authorized subset of users $W_j \in \mathcal{R}_0 = \overline{\Gamma}_0$ such that $R_1 \cup R_2 \cup \cdots \cup R_j \subset W_j$ and $W_j \cap G_j = \emptyset$ with minimum cardinality. The broadcast B_j in session $j = 1, \ldots, m$ is given by $B_j = B_j^1 \cup B_j^2$. The first part of the broadcast is defined as follows: let us suppose that vectors z_j are divided in two parts $z_j = (x_j, y_j)$ where the x_j is the first part of the binary representation of every component of z_j and y_j is the second part. So x_j and y_j are $\frac{1}{2}t \log q$ bits long. Then $B_j^1 = (X_j, Y_j)$, where:

$$X_j = \begin{cases} x_j & \text{if } j = 1, 2 \\ x_1 + x_2, x_1 + x_3, \ldots, x_1 + x_{j-1}, x_j & \text{if } j = 3, \ldots, m \end{cases},$$

$$Y_j = \begin{cases} y_j, y_m + y_{j+1}, y_m + y_{j+2}, \ldots, y_m + y_{m-1} & \text{if } j = 1, \ldots, m-2 \\ y_j & \text{if } j = m-1, m \end{cases}.$$

The second part of the broadcast is defined as follows: for $j = 1, 2$

$$B_j^2 = \{(k, \psi(k)^\top P_j)\}_{k \in W_j} \text{ and for } j \geq 3,\ B_j^2 = B_{j-1}^2 \cup \{(k, \psi(k)^\top P_j)\}_{k \in W_j}.$$

Sponsored addition of users. If a user $\ell \in G_j$ wants to sponsor a user $i \notin G_j$ for session j, then he sends $(\ell, \psi(\ell)^\top P_j \psi(i))$ privately to i (computed from its personal key: $(\ell, \psi(\ell)^\top P_j)$).

For lack of space we do not include the proof of the following result: *the proposed scheme is a $(\mathcal{R}, \Gamma, \mathcal{S})$-self-healing key distribution scheme with sponsorization for $\mathcal{R} = 2^{\mathcal{U}} - \Gamma$ and $\mathcal{S} = 2^{\mathcal{U}} - \Gamma'$*. Observe that the assert $\mathcal{S} = 2^{\mathcal{U}} - \Gamma'$ is strict to ensure condition 4.(c) in the sense that if some $D_i \in \Gamma'$ then sponsored users in D_i by $i \in G_j$ can obtain the key K_j. This happens because $\{(\psi(i)^\top P_j \psi(d))\}_{d \in D_i}$ determines $\psi(i)^\top P_j$: suppose that $e_1, \ldots, e_t$ is the canonical basis of $GF(q)^t$, then they can find scalars λ_{kd} such that $e_k = \sum_{d \in D_i} \lambda_{kd} \psi(d)$, so $\psi(i)^\top P_j e_k = \sum_{d \in D_i} \lambda_{kd} \psi(i)^\top P_j \psi(d)$ and we know that $\psi(i)^\top P_j = (\psi(i)^\top P_j e_1, \ldots, \psi(i)^\top P_j e_t)$; from $\psi(i)^\top P_j$ and the correspondent broadcast, the key K_j can be determined.

We analyze the efficiency of the family of the proposed self-healing key distribution schemes with sponsorization in terms of memory storage and communication complexity. In our construction every user i has to store a personal key of size $|S_i| = t(m - j + 1) \log q$ when the structure Γ is a vector space access structure. The length of the proofs of sponsorization achieve the bound presented in Proposition 1. In our construction, the broadcast length depends on the particular function ψ used. The second part of the broadcast has the same form as the proposed in [1] and its purpose is to perform the rejection capability as well as the computation of the key. Its length depends on the history of rejected subsets $R_2, R_3, etc.$. The first part of the broadcast has almost constant length in every

session (in contrast with the length in other proposals, for instance in [1]): B_1^1 and B_m^1 have $\frac{1}{2}tm\log q$ bits and B_j^1 for $j \neq 1, m$ has $\frac{1}{2}t(m-1)\log q$ bits. Then the total number of broadcast bits is $\frac{1}{2}t(m^2-m+2)\log q$.

5 A Particular Example Based in Shamir's Secret Sharing Scheme

We will present the particular self-healing key distribution scheme that we obtain using the polynomial Shamir's secret sharing scheme [8] in our general construction. This $(t,n)-$threshold scheme can be defined with the assignment of vectors $\psi(D) = (1,0,\ldots,0) \in GF(q)^t$ and $\psi(i) = (1,i,\ldots,i^{t-1}) \in GF(q)^t$ for $i \in \mathcal{U}$, and vector $v = (1,0,\ldots,0)$ that verifies conditions of Lemma 1. We should point out that the product of vector $\psi(i)$ by a vector of coefficients can be seen as the image of a polynomial, that is, $\psi(i)w = p(i)$ where $w = (a_0, a_1, \ldots, a_{t-1})$ and $p(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$. In a similar way the product of a vector $\psi(i)$ by a matrix can be seen as a polynomial in two variables. With this map ψ we find the following particular self-healing key distribution scheme:

Set-up. Let $G_1 \subset \mathcal{U}$. The group manager chooses randomly polynomials $P_1(x,y),\ldots,P_m(x,y)$ of degree $t-1$ in both variables and session keys $K_1,\ldots,K_m \in GF(q)$. For each $j = 1,\ldots,m$ the group manager computes the polynomial $z_j(y) = K_j + P_j(0,y) \in GF(q)[y]$. The group manager sends privately to user $i \in G_1$ the personal key $S_i = (P_1(i,y),\ldots,P_m(i,y)) \in (GF(q)[y])^m$.

Full addition. In order to add users $J_j \subset \mathcal{U}$ in session j, the group manager sends privately $S_i = (P_j(i,y), P_{j+1}(i,y),\ldots,P_m(i,y)) \in (GF(q)[y])^{m-j+1}$ to every user $i \in J_j$ as his personal key.

Broadcast. Let $R_j \subset G_{j-1}$ with $|R_2 \cup \cdots \cup R_j| < t$ if $j \geq 2$ and by definition $R_1 = \emptyset$. The group manager chooses a subset of users W_j with $|W_j| = t-1$ such that $R_1 \cup R_2 \cup \cdots \cup R_j \subset W_j$ and $W_j \cap G_j = \emptyset$. The broadcast B_j in session $j = 1,\ldots,m$ is given by $B_j = B_j^1 \cup B_j^2$. The first part of the broadcast is defined as follows: let us suppose that polynomials $z_j(y)$ are divided in two parts $z_j = (x_j, y_j)$ where x_j is the first part of the binary representation of every coefficient of $z_j(y)$ and y_j is the second part. So x_j and y_j are $\frac{1}{2}t\log q$ bits long. The rest of the definition of the broadcast follows the lines presented in Section 4. For instance for $j \geq 3$, $B_j^2 = B_{j-1}^2 \cup \{(k, P_j(k,y))\}_{k\in W_j}$.

Sponsored addition of users. If a user $\ell \in G_j$ wants to sponsor a user $i \notin G_j$ for session j, then he sends $(\ell, P_j(\ell,i))$ privately to i (computed from a part of its personal key: $(\ell, P_j(\ell,y))$).

Let us show how the session key computation is performed in this particular case. User $i \in G_j$ has $\{(k, P_j(k,y))\}_{k\in W_j}$ and computes $\{(k, P_j(k,i))\}_{k\in W_j}$. By means of $P_j(i,y)$ of its personal key, he computes $P_j(i,i)$. Then he computes $P_j(0,i)$ using $\{(k, P_j(k,i))\}_{k\in W_j\cup\{i\}}$ where $|W_j \cup \{i\}| = t$. In effect: interpolating these t points he can compute $P_j(0,i) = \sum_{k\in W_j\cup\{i\}} \lambda_k P_j(k,i)$ for some $\lambda_k \in$

$GF(q)$ (again the Lagrange coefficients of interpolation). From the broadcast information the user can compute the key because $z_j(i) = K_j + P_j(0,i)$. For the case of a user i sponsored by a subset of users $A \subset G_j$ with $|A| = t$ he proceeds as follows. User i can compute $P_j(0,i)$ because he has $\{(k, P_j(k,i))\}_{k\in A}$. In effect: since $|A| = t$, then $P_j(0,i) = \sum_{k\in A} \lambda_k P_j(k,i)$ for some $\lambda_k \in GF(q)$ (the Lagrange coefficients of interpolation). Then the key is easy to compute using the broadcast information: $z_j(i) = K_j + P_j(0,i)$.

In this particular construction, a subset of at most $t-1$ users can be revoked, that is $|R| = |R_2 \cup \cdots \cup R_j| \leq t-1$. Then $\mathcal{R} = \{A \subset \mathcal{U} : |A| \leq t-1\}$. We also have that $\Gamma = \{A \subset \mathcal{U} : |A| \geq t\}$ and $\mathcal{S} = \{A \subset \mathcal{U} : |A| \leq t-1\}$ because $\Gamma' = \Gamma$. The bounds presented in Section 3 are achieved.

In this scheme a part of the broadcast is proportional to $t-1$, the cardinality of subset W_j. The almost constant length for every session of the first part of the broadcast can be observed in the following broadcasts for $m = 9$:

$$
\begin{aligned}
B_1^1 &= (x_1, y_9 + y_8, y_9 + y_7, y_9 + y_6, y_9 + y_5, y_9 + y_4, y_9 + y_3, y_9 + y_2, y_1)\\
B_2^1 &= (x_2, y_9 + y_8, y_9 + y_7, y_9 + y_6, y_9 + y_5, y_9 + y_4, y_9 + y_3, y_2)\\
B_3^1 &= (x_1 + x_2, x_3, y_9 + y_8, y_9 + y_7, y_9 + y_6, y_9 + y_5, y_9 + y_4, y_3)\\
B_4^1 &= (x_1 + x_2, x_1 + x_3, x_4, y_9 + y_8, y_9 + y_7, y_9 + y_6, y_9 + y_5, y_4)\\
B_5^1 &= (x_1 + x_2, x_1 + x_3, x_1 + x_4, x_5, y_9 + y_8, y_9 + y_7, y_9 + y_6, y_5)\\
B_6^1 &= (x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_5, x_6, y_9 + y_8, y_9 + y_7, y_6)\\
B_7^1 &= (x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_5, x_1 + x_6, x_7, y_9 + y_8, y_7)\\
B_8^1 &= (x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_5, x_1 + x_6, x_1 + x_7, x_8, y_8)\\
B_9^1 &= (x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_5, x_1 + x_6, x_1 + x_7, x_1 + x_8, x_9, y_9)
\end{aligned}
$$

Other schemes can be proposed using our construction with particular linear secret sharing schemes instead of Shamir's secret sharing scheme. For instance, a particular construction in which we have a short broadcast for small revocations of users can be proposed following the same idea presented in [4].

References

1. C. Blundo, P. D'Arco, A. De Santis and M. Listo. Design of Self-Healing Key Distribution Schemes. *Designs, Codes and Cryptography*, Vol. 32, pp. 15–44 (2004).
2. C. Blundo, P. D'Arco, A. De Santis and M. Listo. Definitions and Bounds for Self-Healing Key Distribution. In *ICALP'04*. LNCS, **3142** (2004) 234–245.
3. T.M. Cover and J.A. Thomas. Elements of Inform. Theory. *J. Wiley & Sons*, 1991.
4. V. Daza, J. Herranz and G. Sáez. Constructing General Dynamic Group Key Distribution Schemes with Decentralized User Join. In *8th Australasian Conference on Information Security and Privacy (ACISP '03)*. LNCS, **2727** (2003) 464–475.
5. H. Kurnio, R. Safavi-Naini and H. Wang. A Group Key Distribution Scheme with Decentralised User Join. *Security in Communication Networks, Third International Conference, SCN'02*. LNCS, **2576** (2002) 146–163.
6. D. Liu, P. Ning and K. Sun. Efficient Self-Healing Key Distribution with Revocation Capability. In *10th ACM Conf. on Computer and Com. Security* (2003).
7. J.Staddon, S.Miner, M.Franklin, D.Balfanz, M.Malkin and D.Dean. Self-Healing Key Distribution with Revocation. *IEEE Symp. on Security and Privacy*, (2002).
8. D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, Vol. **2**, pp. 357–390 (1992).