On Self-healing Key Distribution Schemes*

Carlo Blundo, Paolo D'Arco, and Alfredo De Santis

Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
e-mail: {carblu, paodar, ads}@dia.unisa.it

August 6, 2004

Abstract

Self-healing key distribution schemes allow group managers to broadcast session keys to large and dynamic groups of users over unreliable channels. Roughly speaking, even if during a certain session some broadcast messages are lost due to network faults, the self-healing property of the scheme enables each group member to recover the key from the broadcast messages he/she has received before and after that session. Such schemes are quite suitable in supporting secure communication in wireless networks and mobile wireless ad-hoc networks. Recent papers have focused on self-healing key distribution, and have provided definitions, stated in terms of the entropy function, and some constructions. The contribution of this paper is the following:

- We analyse current definitions of self-healing key distribution and, for two of them, we show that no protocol can achieve the definition.
- We show that a lower bound on the size of the broadcast message, previously derived, does not hold.
- We propose a new definition of self-healing key distribution, and we show that it can be achieved by concrete schemes.
- We give some lower bounds on the resources required for implementing such schemes i.e., user memory storage and communication complexity. We prove that the bounds are tight.

Along the same lines of previous works on the subject, we use concepts and techniques from Information Theory in our analysis of existing models, in proving/confuting statements, and in stating our new definition.

Keywords: Self-healing, Key Distribution, Reliability, Group Communication, Information Theory.

1 Introduction

Self-healing key distribution. *Self-healing key distribution schemes*, recently introduced in [39], enable a dynamic group of users to establish a group key over an unreliable network. In such a scheme, a group manager, at the beginning of each session, in order to provide a key to each member of the group, sends packets over a broadcast channel. Every user, belonging to the group, computes the group key

*The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. An abstract of this paper appeared in the Proceedings of the 31-st International Colloquium on Automata, Languages, and Programming (ICALP 2004).

by using the packets and some private information. The group manager can start multiple sessions during a certain time-interval, by adding/removing users to/from the initial group. The main property of the scheme is that, if at the beginning of 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 at the beginning of a previous session and the packets they will receive at the beginning of a subsequent one, without requesting additional transmission from the group manager. Indeed, the only requirement that must be satisfied, in order for the user to recover the lost keys, is membership in the group both before and after the sessions in which the broadcast messages containing the keys are sent and lost. Self-healing key distribution schemes are *stateless* and *non-interactive*, i.e., users do not need to update the secret information they receive in the setup phase, and they do not need to send any key-request message to the group manager. Some benefits of such an approach basically are: reduction of network traffic, reduction of the work load on the group manager, and a lower risk of user exposure through traffic analysis.

Applications. The relevance of self-healing key distribution has been well motivated in [39] and, later on, in [32]. Self-healing key distribution schemes can be used to achieve efficiently secure communication in wireless networks and mobile wireless ad-hoc networks. International peace operations and rescue missions, where there is no network infrastructure support and the adversary may intercept, modify, and/or partially interrupt the communication, are important applicative examples of cases in which reliability, confidentiality and authenticity of the communication is a major concern. In the above settings, all techniques developed for secure group communication in traditional networks might be used. However, some unique features of mobile and ad-hoc networks identify a new scenario: nodes/devices in mobile networks may move in and out of range frequently. Devices are powered by batteries. Hence, expensive computations like the ones required by public key cryptography are not suitable. In a battle field there could be a need for a rapid revocation of devices caught by the enemy and so on. All these aspects pose new challenges and the idea of self-healing key distribution can be of great benefit. Applications for self-healing key distribution can be also found in broadcast communication over low-cost channels: live-event transmissions (e.g., concerts, formal ceremonies, soccer games, ...) for users who have subscribed to (and paid for) the service. Electronic services delivering sensitive content/information to authorized recipients can take advantage from self-healing key distribution schemes as well. Hence, the spectrum of applicability is quite large.

Previous Work. Self-healing key distribution was introduced in [39]. Definitions and lower bounds on the resources required for implementing such schemes, stated in terms of the entropy function, and some constructions were provided. Later on, in [32], the definition given in [39], was generalised and more efficient constructions were presented. Other constructions were given in [29]. Finally, in [5], a slightly different definition was used, some efficient constructions were presented, and it was pointed that some of the constructions given in [39] present flaws. The above papers have mainly considered unconditionally secure schemes.

Related Work. Broadcast Encryption is a closely related research area. Loosely speaking, in broadcast encryption a broadcaster delivers in a secure way to a privileged subset of recipients of a given universe a session key. Then, the recipients use this key for decrypting broadcast transmissions. Broadcast Encryption is *static*, i.e., the family of possible privileged subsets is specified during the setup phase of the scheme. Originated in [2], and formally defined in [17], it has been extensively studied (e.g., [4, 8, 20, 42, 27, 43]), and it has grown up in different directions: mainly, re-keying schemes for *dynamic* subsets of users (e.g., [48, 9, 10, 36, 15, 28]), i.e., schemes where the privileged subset changes, from session to session, by means of join and remove operations, and broadcast schemes with tracing capability for dishonest users (e.g., [12, 35, 16, 18, 44, 45, 46, 40, 19, 37, 22, 23]), i.e., users who illegally give away their private information for computing session keys or collude in order to enable illegal decryption of transmission to unauthorised users. Moreover, several papers have addressed the special case of *efficient users revocation* from the privileged subset (e.g., [24, 1, 31, 30, 21, 25]). Indeed, in certain applications it could be important to be able to remove users immediately from the subset. Such an issue has also been referred to as *the blacklisting problem.* Few years ago, the authors of [34] and [49] have considered a setting in which packets can get lost during transmission.

In the first case, error correction techniques have been employed. In the second, short hint messages have been appended to the packets. The schemes given in [24], by accurately choosing the values of the parameters, can provide resistance to packet loss as well. In [14] several known constructions for broadcast encryption have been generalised in order to gain resistance to packet loss. In [26] the issue of packet loss due to the presence of an unreliable network has been addressed, and a key recovery mechanism, quite similar to the one employed in the schemes provided in [39], was given. Recently, in [47], some existing constructions have been easily extended in order to provide the self-healing property [39]. Both unconditionally secure and computationally secure schemes have been provided in the above cited papers.

Our Contribution: In this paper we deal firstly with the *definitional task* of self-healing key distribution. We give some attention to the constructive task as well. We start by analysing the definition proposed in [39] and subsequently generalized in [32]. We discuss some issues related to such a formalization, and we show that no protocol can achieve some of the security requirements stated in [39, 32]. Then, we show that a lower bound on the size of the broadcast messages the group manager has to sent in order to establish session keys, proved in [39] and also used in [32], does not hold. After the analysis, we propose a new definition for self-healing key distribution, by extending and opportunely modifying the definition given in [39]. Subsequently, we give some lower bounds on the resources required for implementing such schemes, i.e., user memory storage and communication complexity, and we show that the bounds are tight. Along the same lines of previous works on the subject, we use concepts and techniques from Information Theory in our analysis of existing models, in proving/confuting statements, and in stating our new definition.

2 Background

In this section we briefly provide some basic elements of Information Theory, and some technical lemmas we use in proving our results. For a good introduction to Information Theory, the interested reader is referred to [13].

2.1 Information Theory Measures

A discrete random experiment is defined by a finite set, called *sample space*, consisting of all elementary events, and a *probability measure* assigning a non-negative real number to every elementary event, such that the sum of all these probabilities is equal to 1. An *event* of a discrete random experiment is a subset of the sample space, and the probability assigned to it is the sum of the probabilities of its elementary events.

A *discrete random variable* $\mathbf{X}$ is a mapping from a sample space to a certain range X, and is characterized by its probability distribution $\{P_{\mathbf{X}}(x)\}_{x\in X}$ that assigns to every $x \in X$ the probability $P_{\mathbf{X}}(x)$ of the event that $\mathbf{X}$ takes on the value x.

The *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is a real number that measures the uncertainty about the value of $\mathbf{X}$ when the underlying random experiment is carried out. It is defined by

$$H(\mathbf{X}) = -\sum_{x\epsilon X} P_{\mathbf{X}}(x)\log P_{\mathbf{X}}(x),$$

assuming that the terms of the form $0\log 0$ are excluded from the summation, and where the logarithm is relative to the base 2. The entropy satisfies $0 \le H(\mathbf{X}) \le \log|X|$, where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr(\mathbf{X} = x_0) = 1$; whereas, $H(\mathbf{X}) = \log|X|$ if and only if $Pr(\mathbf{X} = x) = 1/|X|$, for all $x \in X$. The deviation of the entropy $H(\mathbf{X})$ from its maximal value can be used as a measure of non-uniformity of the distribution $\{P_{\mathbf{X}}(x)\}_{x\in X}$.

Given two random variables $\mathbf{X}$ and $\mathbf{Y}$, taking values on sets X and Y, respectively, according to a probability distribution $\{P_{\mathbf{XY}}(x,y)\}_{x\in X, y\in Y}$ on their Cartesian product, the conditional uncertainty of $\mathbf{X}$, given the random variable $\mathbf{Y}$, called *conditional entropy* and denoted by $H(\mathbf{X}|\mathbf{Y})$, is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} P_{\mathbf{Y}}(y) P_{\mathbf{X}|\mathbf{Y}}(x|y) \log P_{\mathbf{X}|\mathbf{Y}}(x|y).$$

Notice that the conditional entropy is not the entropy of a probability distribution but the *average* over all entropy $H(\mathbf{X}|\mathbf{Y} = y)$. Simple algebra shows that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0 \tag{1}$$

with equality if and only if X is a function of Y.

The *mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ is a measure of the amount of information by which the uncertainty about $\mathbf{X}$ is reduced by learning $\mathbf{Y}$, and vice versa. It is given by

$$I(\mathbf{X}; \mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y}|\mathbf{X}).$$

Since,

$$I(\mathbf{X}; \mathbf{Y}) = I(\mathbf{Y}; \mathbf{X}) \text{ and } I(\mathbf{X}; \mathbf{Y}) \geq 0, \tag{2}$$

it is easy to see that

$$H(\mathbf{X}) \geq H(\mathbf{X}|\mathbf{Y}), \tag{3}$$

with equality if and only if $\mathbf{X}$ and $\mathbf{Y}$ are independent. Along the same lines, given three random variables, $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, the *conditional mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ can be written as

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}|\mathbf{Z}) &= H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Z}, \mathbf{Y}) \\ &= H(\mathbf{Y}|\mathbf{Z}) - H(\mathbf{Y}|\mathbf{Z}, \mathbf{X}) \\ &= I(\mathbf{Y}; \mathbf{X}|\mathbf{Z}). \end{aligned} \tag{4}$$

Since the conditional mutual information $I(\mathbf{X}; \mathbf{Y}|\mathbf{Z})$ is always non-negative, it holds that

$$H(\mathbf{X}|\mathbf{Z}) \geq H(\mathbf{X}|\mathbf{Z}, \mathbf{Y}). \tag{5}$$

A useful equality, widely applied in information-theoretic proofs, is given by the so-called *chain rule*. It is stated as follows: given $n+1$ random variables, $\mathbf{X}_1, \ldots, \mathbf{X}_n$ and $\mathbf{Z}$, the entropy of $\mathbf{X}_1 \ldots \mathbf{X}_n$, given $\mathbf{Z}$, can be written as

$$H(\mathbf{X}_1, \ldots, \mathbf{X}_n|\mathbf{Z}) = H(\mathbf{X}_1|\mathbf{Z}) + H(\mathbf{X}_2|\mathbf{X}_1, \mathbf{Z}) + \cdots + H(\mathbf{X}_n|\mathbf{X}_1, \ldots, \mathbf{X}_{n-1}, \mathbf{Z}). \tag{6}$$

2.2 Technical Lemmas

The following simple lemmas are used in the proofs of our results. The first one plays a key-role in proving all our impossibility results. Indeed, we will use the following relations to show that, if a set of assumptions hold, then we get a contradiction.

Lemma 2.1 *Let $\mathbf{X}, \mathbf{Y}$, and $\mathbf{Z}$ be three random variables such that $H(\mathbf{Z}|\mathbf{X}, \mathbf{Y}) = 0$ and $H(\mathbf{Z}|\mathbf{Y}) = H(\mathbf{Z})$. Then,*

1. $H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) = H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{Z})$.
2. $H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) = H(\mathbf{X})$ *if and only if* $H(\mathbf{Z}) = 0$ *and* $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X})$.

Proof. Notice that $I(\mathbf{X}; \mathbf{Z}|\mathbf{Y})$, according to (2), can be written as

$$H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}) = H(\mathbf{Z}|\mathbf{Y}) - H(\mathbf{Z}|\mathbf{X}, \mathbf{Y}).$$

It follows that,

$$\begin{aligned} H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) &= H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{Z}|\mathbf{Y}) + H(\mathbf{Z}|\mathbf{X},\mathbf{Y}) \\ &= H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{Z}|\mathbf{Y}) \quad (\text{since } H(\mathbf{Z}|\mathbf{X},\mathbf{Y}) = 0) \\ &= H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{Z}) \quad (\text{since } H(\mathbf{Z}|\mathbf{Y}) = H(\mathbf{Z})). \end{aligned}$$

Hence, statement *1.* is proved. In order to prove statement *2.* notice that, if $H(\mathbf{Z}) = 0$ and $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X})$, then, from *1.* we have that $H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) = H(\mathbf{X})$. On the other hand, if $H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) = H(\mathbf{X})$, then, from *1.*, it must be $H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{Z}) = H(\mathbf{X})$. Since the entropy of a random variable is non-negative, such an equality is satisfied only if $H(\mathbf{Z}) = 0$ and $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X})$. ■

Notice that point *2.* of Lemma 2.1 means that $H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) = H(\mathbf{X})$ if and only if the value of $\mathbf{Z}$ is univocally determined (i.e., $H(\mathbf{Z}) = 0$) and the random variables $\mathbf{X}$ and $\mathbf{Y}$ are independent (i.e., $H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X})$.)

Lemma 2.1 has an interesting interpretation in the theory of secret sharing schemes [3, 38]. Loosely speaking, a secret sharing scheme is a protocol divided in two phases, called *Share* and *Reconstruct*, by means of which a dealer shares a secret among a set of participants, in such a way that any *qualified* subset can reconstruct the secret while any *forbidden* subset does not get any information about it. The simplest secret sharing scheme consists of two participants. It works as follows: during *Share*, each of them receives a piece of information, called share. Let us assume that $\mathbf{Z}$ denotes the secret shared by the dealer among the two participants, and $\mathbf{X}$ and $\mathbf{Y}$ represent the shares received by the two participants. Later on, during *Reconstruct*, by pooling together their shares, the two participants recover the secret (i.e., $H(\mathbf{Z}|\mathbf{X},\mathbf{Y}) = 0$), while none of them alone has any information about it (i.e., $H(\mathbf{Z}|\mathbf{Y}) = H(\mathbf{Z})$ and $H(\mathbf{Z}|\mathbf{X}) = H(\mathbf{Z})$). Lemma 2.1 says that, unless there is no uncertainty on the secret, i.e., $H(\mathbf{Z}) = 0$, there exists no secret sharing scheme for two participants satisfying the following condition: the secret Z and one of the shares, say Y, do not give any information about the other share X, i.e., $H(\mathbf{X}|\mathbf{Y},\mathbf{Z}) = H(\mathbf{X})$.

Assume that we have access to the outcomes of some related random variables $\mathbf{X}, \mathbf{Y}$, and $\mathbf{W}$. The following simple lemma establishes that the amount of information we get on a certain random variable $\mathbf{X}$ from another one $\mathbf{W}$, *does not* grow if we consider also another random variable $\mathbf{Y}$, which is function of $\mathbf{W}$. In other words, *any* computation based on the value of $\mathbf{W}$ does not improve our knowledge on $\mathbf{X}$.

Lemma 2.2 *Let* $\mathbf{X}$, $\mathbf{Y}$, *and* $\mathbf{W}$ *be three random variables. If* $H(\mathbf{Y}|\mathbf{W}) = 0$ *then*

$$H(\mathbf{X}|\mathbf{Y},\mathbf{W}) = H(\mathbf{X}|\mathbf{W}).$$

Proof. Notice that $H(\mathbf{Y}|\mathbf{W}) = 0$ implies $H(\mathbf{Y}|\mathbf{X},\mathbf{W}) = 0$. Indeed, (1) and (5) yield

$$0 \leq H(\mathbf{Y}|\mathbf{X},\mathbf{W}) \leq H(\mathbf{Y}|\mathbf{W}) = 0.$$

The mutual information $I(\mathbf{X};\mathbf{Y}|\mathbf{W})$, according to (2), can be written either as

$$H(\mathbf{X}|\mathbf{W}) - H(\mathbf{X}|\mathbf{W},\mathbf{Y}) = H(\mathbf{Y}|\mathbf{W}) - H(\mathbf{Y}|\mathbf{X},\mathbf{W}).$$

Since $H(\mathbf{Y}|\mathbf{W}) - H(\mathbf{Y}|\mathbf{X},\mathbf{W}) = 0$, it holds that $H(\mathbf{X}|\mathbf{W}) = H(\mathbf{X}|\mathbf{Y},\mathbf{W})$. ■

In our proofs we will consider also a slightly different variant of the above lemma, which can be stated as follows:

Lemma 2.3 *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ *and* $\mathbf{W}$ *be four random variables. If* $H(\mathbf{Y}|\mathbf{Z},\mathbf{W}) = 0$ *then*

$$H(\mathbf{X}|\mathbf{Z},\mathbf{W}) \leq H(\mathbf{X}|\mathbf{Y},\mathbf{W}).$$

Proof. Denote by $\mathbf{T}$ the joint random variable $\mathbf{ZW}$. The random variables $\mathbf{X}, \mathbf{Y}$ and $\mathbf{T}$ satisfy the hypothesis of Lemma 2.2, i.e., $H(\mathbf{Y}|\mathbf{T}) = 0$. Therefore, it holds that

$$H(\mathbf{X}|\mathbf{Y}, \mathbf{Z}, \mathbf{W}) = H(\mathbf{X}|\mathbf{Z}, \mathbf{W}).$$

Then, from (5), it follows that

$$H(\mathbf{X}|\mathbf{Z}, \mathbf{W}) \leq H(\mathbf{X}|\mathbf{Y}, \mathbf{W}).$$

■

The following lemma, proved in [39], considers four random variables $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$, and $\mathbf{W}$. Assuming that a certain relation, stated by means of two conditions, holds among them, it yields a lower bound on the amount of information that $\mathbf{Y}$ still has, once given $\mathbf{Z}$.

Lemma 2.4 *[39] Let $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$, and $\mathbf{W}$ be four random variables. If $H(\mathbf{X}|\mathbf{Y}, \mathbf{W}) = 0$ and $H(\mathbf{X}|\mathbf{Z}, \mathbf{W}) = H(\mathbf{X})$, then*

$$H(\mathbf{Y}|\mathbf{Z}) \geq H(\mathbf{X}).$$

3 Self-healing Key Distribution: Previous Definitions

Self-healing key distribution was introduced by Staddon et al. in [39]. We start by describing the network setting we will consider hereafter and the definition therein given.

3.1 Network Setting

Let $\mathcal{U} = \{U_1, \ldots, U_n\}$ be the finite universe of users of a network. A broadcast unreliable channel is available, and time is defined by a global clock. Let GM be 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 $G_j \subseteq \mathcal{U}$ be the communication group established by GM in session j. Each user $U_i \in G_j$ holds a secret key S_i, received from GM when he/she joins, at time j, the communication group G_j. A secret key S_i can be seen as a sequence of elements from a finite set, and is valid until the user U_i is not removed by GM from the communication group. Individual secret keys can be related.

We denote the number of sessions, supported by the scheme, by m, the set of users revoked by GM in session j by Rev_j, and the set of users who join the group in session j by $Join_j$. Hence, $G_j = (G_{j-1} \cup Join_j) \setminus Rev_j$. We assume that GM can revoke at most t users during the lifetime of the scheme, and that once a user is revoked he/she is kept revoked. However, notice that a revoked user that needs to re-join the group can always be treated as a new one: he/she receives a new identity and a new secret key, and joins the communication group. Therefore, the model we consider does not yield loss of generality, as long as the number of re-joins of a certain user and the number of other revoked users does not exceeds t.

Moreover, for $j = 1, \ldots, m$, let K_j be the session key chosen by GM and communicated to the group members through a broadcast message, B_j. For each $U_i \in G_j$, the key K_j is determined by B_j and the secret key S_i.

Let $\mathbf{S}_i, \mathbf{B}_j, \mathbf{K}_j$ be the random variables representing the secret key of user U_i, the broadcast message B_j and the session key K_j for session j, respectively. Moreover, let $\mathbf{Z}_{i,j}$ be a random variable which represents the amount of information $Z_{i,j}$ that user U_i gets from the broadcast B_j and S_i.

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 GM. In particular, we assume that session keys K_j are chosen independently.

3.2 Analysis of the Definition given in [39]

Using the entropy function, the following definition was stated:

Definition 3.1 *[Self-Healing Key Distribution Scheme with Revocation][39]*
Let $t, i \in \{1, \ldots, n\}$ be indices denoting, respectively, the maximum number of users that can be revoked by GM during the lifetime of the scheme and a generic user, and let $j \in \{1, \ldots, m\}$ be an index representing a session.

1. *$\mathcal{D}$ is a session key distribution scheme if the following are true:*

   1.a) *For any member U_i, the key K_j is determined by $Z_{i,j}$.* Formally, it holds that:

   $$H(\mathbf{Z}_{i,j}|\mathbf{B}_j, \mathbf{S}_i) = 0 \quad and \quad H(\mathbf{K}_j|\mathbf{Z}_{i,j}) = 0.$$

   1.b) *For any subset $F \subseteq \{U_1, \ldots U_n\}$, such that $|F| \leq t$ and $U_i \notin F$, the users in F cannot determine anything about S_i.* Formally, it holds that:

   $$H(\mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'} \in F}, \mathbf{B}_1, \ldots, \mathbf{B}_m) = H(\mathbf{S}_i).$$

   1.c) *What members $U_1, \ldots, U_n$ learn from the broadcast B_j and the secret keys cannot be determined from the broadcast or secret keys alone.* Formally, it holds that:

   $$H(\mathbf{Z}_{i,j}|\mathbf{B}_1, \ldots, \mathbf{B}_m) = H(\mathbf{Z}_{i,j}|\mathbf{S}_1, \ldots, \mathbf{S}_n) = H(\mathbf{Z}_{i,j}).$$

2. *$\mathcal{D}$ has t-revocation capability if, given any set $R \subseteq \{U_1, \ldots, U_n\}$, where $|R| \leq t$, the group manager can generate a broadcast B_j such that, for all $U_i \notin R$, the user U_i can recover K_j but the revoked users cannot.* Formally, it holds that:

   $$H(\mathbf{K}_j|\mathbf{B}_j, \mathbf{S}_i) = 0, \quad while \quad H(\mathbf{K}_j|\mathbf{B}_j, \{\mathbf{S}_{i'}\}_{U_{i'} \in R}) = H(\mathbf{K}_j).$$

3. *$\mathcal{D}$ is self-healing if, for any $1 \leq j_1 < j < j_2 \leq m$, the following properties are satisfied:*

   3.a) *For any U_i who is member in session j_1 and j_2, the key K_j is determined by $\{Z_{i,j_1}, Z_{i,j_2}\}$.* Formally, it holds that:

   $$H(\mathbf{K}_j|\mathbf{Z}_{i,j_1}, \mathbf{Z}_{i,j_2}) = 0.$$

   3.b) *For any two disjoint subsets $F, G \subset \{U_1, \ldots, U_n\}$, where $|F \cup G| \leq t$, the set $\{Z_{i',r}\}_{\{U_{i'} \in F, 1 \leq r \leq j_1\}} \cup \{Z_{i',r}\}_{\{U_{i'} \in G, j_2 \leq r \leq m\}}$, contains no information on K_j.* Formally, it holds that:

   $$H(\mathbf{K}_j|\{\mathbf{Z}_{i',r}\}_{\{U_{i'} \in F, 1 \leq r \leq j_1\}}, \{\mathbf{Z}_{i',r}\}_{\{U_{i'} \in G, j_2 \leq r \leq m\}}) = H(\mathbf{K}_j).$$

The definition is divided in three parts: the first one states that each non revoked user computes the session key; moreover, it states that secret keys held by honest users are secure w.r.t. coalitions of at most t malicious users who put together their secret keys and possess the whole sequence of broadcast messages, and that both secret keys and broadcast messages are needed to compute session keys. The second part states that revoked users do not get any information about session keys. The third one states the self-healing property and a security requirement that must hold against collusion attacks performed by coalitions of revoked and new users, who join the system in a certain session $j > 1$. More precisely, item 3.a) establishes that a user recovers, from two broadcast messages B_{j_1} and B_{j_2}, all session keys K_j, for $j_1 \leq j \leq j_2$. Item 3.b) essentially requires that a group F of users, revoked in session j_1, and a group G of new users, who join the system in session j_2, by pooling together their secret keys and all broadcast messages, do not get any information about each key they are not entitled to receive.

The above definition presents some problems: namely, there is *no protocol* that can achieve all conditions unless there is no uncertainty about the session keys, i.e., for $j = 1, \ldots, m$, $H(\mathbf{K}_j) = 0$.

We start by showing that conditions *1.a*), *1.b*), and *2* cannot be satisfied simultaneously. It turns out that the problem lies in condition *1.b*). Indeed, condition *1.a*) and *2* are required in order to define a basic scheme where users of the group can compute the session key and revoked users cannot. We will show that:

- condition *1.a)* and *2* imply the relation established by point *1.* of Lemma 2.1 for the random variables $\mathbf{S}_i$, $\mathbf{B}_r$, and $\mathbf{K}_r$, i.e., $H(\mathbf{S}_i|\mathbf{B}_r,\mathbf{K}_r) = H(\mathbf{S}_i|\mathbf{B}_r) - H(\mathbf{K}_r)$;
- on the other hand, condition 1.*b*) implies a sort of a-posteriori security for the secret key, once given the broadcast message and the session key for a certain session i.e., $H(\mathbf{S}_i|\mathbf{B}_r,\mathbf{K}_r) = H(\mathbf{S}_i)$;
- it follows that $H(\mathbf{S}_i|\mathbf{B}_r) - H(\mathbf{K}_r) = H(\mathbf{S}_i)$, which holds if and only if $H(\mathbf{S}_i|\mathbf{B}_r) = H(\mathbf{S}_i)$ and $H(\mathbf{K}_r) = 0$.

Hence, condition *1.b)* has to be removed. More precisely, we show the following result:

Theorem 3.2 *If conditions 1.a), 1.b) and 2 of Definition 3.1 are satisfied then, for any* $1 \le r \le m$,

$$H(\mathbf{K}_r) = 0.$$

Proof. Let G_r be the communication group established in session r, for some $r \in \{1,\dots,m\}$. Let F be any subset of $\mathcal{U}$ such that $|F| \le t$, $F \cap G_r \neq \emptyset$, and $F \neq G_r$. Finally, let $U_i \in G_r \setminus F$. By using conditions *1.a)* and *2.*, and Lemmas 2.1 and 2.3, we show that

$$H(\mathbf{K}_r|\mathbf{S}_i,\mathbf{B}_r) = 0, \text{ and } H(\mathbf{K}_r|\mathbf{B}_r) = H(\mathbf{K}_r).$$

Setting $\mathbf{X} = \mathbf{S}_i$, $\mathbf{Y} = \mathbf{B}_r$, and $\mathbf{Z} = \mathbf{K}_r$, and applying point *1.* of Lemma 2.1, it follows that $H(\mathbf{S}_i|\mathbf{B}_r,\mathbf{K}_r) = H(\mathbf{S}_i|\mathbf{B}_r) - H(\mathbf{K}_r)$. Then, if condition *1.b)* holds, we show that $H(\mathbf{S}_i|\mathbf{B}_r,\mathbf{K}_r) = H(\mathbf{S}_i)$. Therefore, it must be $H(\mathbf{S}_i|\mathbf{B}_r) - H(\mathbf{K}_r) = H(\mathbf{S}_i)$ which holds if and only if $H(\mathbf{S}_i|\mathbf{B}_r) = H(\mathbf{S}_i)$ and $H(\mathbf{K}_r) = 0$.

Let us show the above statements. We start by proving that

$$H(\mathbf{K}_r|\mathbf{S}_i,\mathbf{B}_r) = 0, \ \textit{for any } U_i \in G_r. \tag{7}$$

From condition 1.*a*) of Definition 3.1, we have that $H(\mathbf{Z}_{i,j}|\mathbf{B}_r,\mathbf{S}_i) = 0$; hence, from Lemma 2.3, setting $\mathbf{X} = \mathbf{K}_r$, $\mathbf{Y} = \mathbf{Z}_{i,j}$, $\mathbf{Z} = \mathbf{B}_r,\mathbf{S}_i$, and $\mathbf{W}$ equals to the "empty" random variable, we get that $H(\mathbf{K}_r|\mathbf{B}_r,\mathbf{S}_i) \le H(\mathbf{K}_r|\mathbf{Z}_{i,j})$. Since from condition 1.*a*) of Definition 3.1 it also holds that $H(\mathbf{K}_r|\mathbf{Z}_{i,j}) = 0$, applying (1), we have that

$$0 \le H(\mathbf{K}_r|\mathbf{B}_r,\mathbf{S}_i) \le H(\mathbf{K}_r|\mathbf{Z}_{i,j}) = 0.$$

Therefore, equality (7) is satisfied. To prove that $H(\mathbf{K}_r|\mathbf{B}_r) = H(\mathbf{K}_r)$, consider the following chain of equalities/inequalities.

$$\begin{aligned} H(\mathbf{K}_r) &= H(\mathbf{K}_r|\{\mathbf{S}_{i'}\}_{U_{i'}\in F},\mathbf{B}_r) \text{ (from condition 2) of Definition 3.1)} \\ &\le H(\mathbf{K}_r|\mathbf{B}_r) \text{ (applying property (5))} \\ &\le H(\mathbf{K}_r) \text{ (applying property (3))}. \end{aligned}$$

Hence, $H(\mathbf{K}_r|\mathbf{B}_r) = H(\mathbf{K}_r)$. Finally, if condition 1.*b*) holds, then for $U_j \in F \cap G_r$ and $U_i \in G_r \setminus F$, it follows that that $H(\mathbf{S}_i|\mathbf{S}_j,\mathbf{B}_r) = H(\mathbf{S}_i)$. Indeed:

$$\begin{aligned} H(\mathbf{S}_i) &= H(\mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'}\in F},\mathbf{B}_1,\dots,\mathbf{B}_m) \text{ (from condition 1.}b\text{))} \\ &\le H(\mathbf{S}_i|\mathbf{S}_j,\mathbf{B}_r) \text{ (applying property (5))} \\ &\le H(\mathbf{S}_i) \text{ (applying property (3))}. \end{aligned}$$

At this point notice that, since (7) establishes that $H(\mathbf{K}_r|\mathbf{S}_j,\mathbf{B}_r) = 0$, from Lemma 2.3, setting $\mathbf{X} = \mathbf{S}_i$, $\mathbf{Y} = \mathbf{K}_r$, $\mathbf{Z} = \mathbf{S}_j$, and $\mathbf{W} = \mathbf{B}_r$, we get that $H(\mathbf{S}_i|\mathbf{S}_j,\mathbf{B}_r) \le H(\mathbf{S}_i|\mathbf{K}_r,\mathbf{B}_r)$. Hence, applying (3), it holds that

$$H(\mathbf{S}_i) = H(\mathbf{S}_i|\mathbf{S}_j,\mathbf{B}_r) \le H(\mathbf{S}_i|\mathbf{K}_r,\mathbf{B}_r) \le H(\mathbf{S}_i),$$

i.e., $H(\mathbf{S}_i|\mathbf{K}_r,\mathbf{B}_r) = H(\mathbf{S}_i)$, and the theorem is proved. ■

Notice that the authors of [32] changed condition *1.b*) of Definition 3.1. Indeed, as a side note, they pointed out that the schemes given in [39] do not meet such a condition, and a sketch of the reason was briefly provided. With Theorem 3.2 we have shown that *it is not* due to a design problem of those schemes. They relaxed condition *1.b*) and required:

> *For any subset $F \subseteq \mathcal{U}$, such that $|F| \leq t$, and for each $U_i \notin F$, the users in F have at least b bits of uncertainty about S_i.* Formally, it holds that:
>
> $$H(\mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'}\in F}, \mathbf{B}_1, \ldots, \mathbf{B}_m) \geq b. \tag{8}$$

In [32] a scheme satisfying condition (8) was presented. We notice that, given a scheme where the above condition is not satisfied, it is possible to construct a new scheme which does meet the condition still preserving all other conditions. Basically, for any b, the design strategy is that in the new scheme, to every $\mathbf{S}_i$ must be added b *random bits* chosen, for each $\mathbf{S}_i$, independently of all other variables. In such a case, it is easy to check that also condition (8) holds.

Definition 3.1 presents another problem: conditions *3.a*) and *3.b*) cannot be satisfied simultaneously. Consider the following situation. Let $F = \{U_s\}$ and $G = \{U_1, \ldots, U_{s-1}\}$ be two subsets of users, where $s \leq t$, and let $1 = j_1 < j < j_2 = m$. Condition *3.b*) of Definition 3.1 implies that:

$$H(\mathbf{K}_j|\mathbf{Z}_{1,m}, \ldots, \mathbf{Z}_{s-1,m}, \mathbf{Z}_{s,1}) = H(\mathbf{K}_j), \tag{9}$$

while, if U_s belongs to G_1 and is not revoked in session m, condition *3.a*) implies that

$$H(\mathbf{K}_j|\mathbf{Z}_{s,m}, \mathbf{Z}_{s,1}) = 0. \tag{10}$$

Since the random variable $\mathbf{Z}_{i,j}$ is defined as the information user U_i gets from S_i and B_j, we suppose the users do not perform any computation, i.e., they just look at the broadcast B_j and at S_i. Hence, the first members of equalities (9) and (10) can be rewritten as

$$H(\mathbf{K}_j|\mathbf{S}_1, \ldots, \mathbf{S}_{s-1}, \mathbf{S}_s, \mathbf{B}_m, \mathbf{B}_1) \text{ and } H(\mathbf{K}_j|\mathbf{S}_s, \mathbf{B}_1, \mathbf{B}_m).$$

Equation (10), property (5), and Lemma 2.2 imply that $H(\mathbf{K}_j|\mathbf{S}_s, \mathbf{B}_1, \mathbf{B}_m) = 0$. Indeed,

$$0 = H(\mathbf{K}_j|\mathbf{Z}_{i,1}, \mathbf{Z}_{i,m}) \geq H(\mathbf{K}_j|\mathbf{Z}_{i,1}, \mathbf{Z}_{i,m}, \mathbf{S}_s, \mathbf{B}_1, \mathbf{B}_m) = H(\mathbf{K}_j|\mathbf{S}_s, \mathbf{B}_1, \mathbf{B}_m) \geq 0.$$

Then, from (1) and (5), we get that

$$0 \leq H(\mathbf{K}_j|\mathbf{S}_1, \ldots, \mathbf{S}_{s-1}, \mathbf{S}_s, \mathbf{B}_m, \mathbf{B}_1) \leq H(\mathbf{K}_j|\mathbf{S}_s\mathbf{B}_1, \mathbf{B}_m) = 0.$$

Hence, conditions *3.a*) and *3.b*) hold simultaneously only if $H(\mathbf{K}_j) = 0$, for any $1 < j < m$.

To make conditions *3.a*) and *3.b*) working, Definition 3.1 *should specify* that F and G correspond to subsets of revoked and joining users. Notice that the authors of [39] informally gave such a meaning to F and G in motivating the definition, but the requirement was not formally stated (and not used).

By using conditions *3.a*) and *3.b*) with no constraint on F and G, a lower bound on the size of the broadcast message the group manager sends at the beginning of each session, was therein derived. Such a bound holds only if $H(\mathbf{K}_2) = \ldots = H(\mathbf{K}_{m-1}) = 0$. For completeness we report and discuss it below. Assuming the "corrected" version of conditions *3.a*) and *3.b*), i.e., where F and G correspond to subsets of revoked and joining users, the proof of the bound does not work, and the bound does not hold. Indeed, in the following sections we will give another bound and a protocol meeting it.

Theorem 3.3 *[39] In any self-healing key distribution scheme $H(\mathbf{B}_j)$ is $\Omega(mtH(\mathbf{K}))$.*

Proof [39]. Notice that conditions *1.a*) and *1.c*) of Definition 3.1 imply that

$$H(\mathbf{Z}_{1,j}, \ldots, \mathbf{Z}_{n,j}|\mathbf{B}_j, \mathbf{S}_1, \ldots, \mathbf{S}_n) = 0$$

and

$$H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{n,j}|\mathbf{S}_1,\dots,\mathbf{S}_n) = H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{n,j}).$$

Applying Lemma 2.4, it follows that $H(\mathbf{B}_j) \geq H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{n,j})$. Hence, a lower bound on $H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{n,j})$ yields a lower bound on $H(\mathbf{B}_j)$. From (5) and the chain rule, we get that:

$$H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{n,j}) \geq H(\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{t,j}) \quad = \quad \sum_{s=1}^{t} H(\mathbf{Z}_{s,j}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j}).$$

Using property 3.*a*) *and* 3.*b*) *of Definition 3.1, for* $1 \leq s \leq t$*, it holds that*

$$H(\mathbf{K}_2,\dots,\mathbf{K}_{j-1}|\mathbf{Z}_{s,j},\mathbf{Z}_{s,1}) = 0 \tag{11}$$

and

$$H(\mathbf{K}_2,\dots,\mathbf{K}_{j-1}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j},\mathbf{Z}_{s,1}) = H(\mathbf{K}_2,\dots,\mathbf{K}_{j-1}). \tag{12}$$

Applying Lemma 2.4 it holds that $H(\mathbf{Z}_{s,j}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j}) \geq (j-2)H(\mathbf{K})$. Similarly, from

$$H(\mathbf{K}_{j+1},\dots,\mathbf{K}_m|\mathbf{Z}_{s,j},\mathbf{Z}_{s,m}) = 0$$

and

$$H(\mathbf{K}_{j+1},\dots,\mathbf{K}_m|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j},\mathbf{Z}_{s,m}) = H(\mathbf{K}_{j+1},\dots,\mathbf{K}_m),$$

and applying Lemma 2.4, it follows that $H(\mathbf{Z}_{s,j}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j}) \geq (m-j-1)H(\mathbf{K})$. Combining the two lower bounds, for any $1 \leq s \leq t$, it holds that

$$H(\mathbf{Z}_{s,j}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j}) \geq (m/2-2)H(\mathbf{K}).$$

Hence, $H(\mathbf{B}_j) \geq t(m/2-2)H(\mathbf{K})$. ■

First of all, notice that there is a minor problem in the above proof. It is not clear how to derive (12) from Definition 3.1. Moreover, by looking at equalities (11) and (12) it is easy to see that they represent exactly the case we have discussed before, i.e., equations (10) and (9). Indeed, if U_s is member of the group in all sessions from 1 to j, equality (11) holds due to self-healing, but, equality (12) does not since, given B_1, B_j and S_s, all keys $K_2,\dots,K_{j-1}$ are uniquely determined i.e.,

$$H(\mathbf{K}_2,\dots,\mathbf{K}_{j-1}|\mathbf{Z}_{1,j},\dots,\mathbf{Z}_{s-1,j},\mathbf{Z}_{s,1}) = 0.$$

On the other hand, if U_s is revoked in session j, equality (12) holds but equality (11) does not, since the self-healing condition cannot be applied.

In conclusion, conditions *3.a*) and *3.b*) of Definition 3.1 should specify that F and G correspond to subsets of revoked and joining users. Indeed, if such a specification is not stated, the above lower bound on the size of the broadcast message holds but it can be achieved only by schemes where there is no uncertainty on the session keys. On the other hand, if the specification is given, the bound does not hold.

Notice that, in [29], a simplified version of the definition of self-healing key distribution given in [39, 32] was used. We do not go through details but the reader can easily check that condition 3.(b) of this simplified version of the definition corresponds to condition *1.b*) of Definition 3.1. Therefore, such a condition, along with conditions 1.(a) and 3.(c) of that definition, is impossible to achieve. It follows that the proof of security concerning with collusion resistance therein given in Subsection 5.1 for the construction the authors had presented before in Section 4, does not work.

4 Personal Key Distribution Schemes

In this section we analyse the definition of personal key distribution scheme. In all proposed self-healing key distribution schemes, every user has a secret key S_i, which stays the same for all the lifetime of the scheme. At the beginning of the j-th session, every user who has not been revoked, computes his/her own new key Pk_i, by using S_i and the first part of the broadcast message B_j. Then, by means of Pk_i and the second part of the broadcast message B_j, he/she computes the group session key K_j.

In Appendix C of [39] and in [32], this behaviour was formalised as an intermediate step towards the definition of a self-healing key distribution scheme, and it was simply referred to as key distribution in [39] (no specific term was used to designate such a sort of one-time keys used to compute the group session key), and as *Personal Key Distribution* in [32]. The definitions are equivalent. In the next subsection we will refer to S_i as to the secret (long-term) key, and to Pk_i as to the personal (one-time) key.

4.1 Formal Definition

Let us consider a generic session, and let $\mathbf{S}_i, \mathbf{Pk}_i$, and $\mathbf{B}$ represent the secret key (which can be used by user U_i as long as he/she is not revoked), the personal key computed by user U_i in the session, and the broadcast message sent by GM at the beginning of the session, respectively. The definition of personal key distribution can be stated as follows:

Definition 4.1 *[39, 32] Let $t, i \in \{1, \ldots, n\}$. In a* personal key distribution scheme *$\mathcal{D}$, the group manager seeks to establish a new key Pk_i with each group member U_i through a broadcast message B. $\mathcal{D}$ is a personal key distribution scheme if*

a) For any group member U_i, the key Pk_i is determined by S_i and B, i.e.,

$$H(\mathbf{Pk}_i|\mathbf{B}, \mathbf{S}_i) = 0.$$

b) For any set $F \subseteq \{U_1, \ldots, U_n\}$ such that $|F| \leq t$, and any $U_i \notin F$, the members in F are not able to learn anything about S_i, i.e.,

$$H(\mathbf{Pk}_i, \mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'} \in F}, \mathbf{B}) = H(\mathbf{Pk}_i, \mathbf{S}_i).$$

c) No information on $Pk_1, \ldots, Pk_n$ is learned from either the broadcast or the secret keys alone, i.e.,

$$H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n|\mathbf{B}) = H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n|\mathbf{S}_1, \ldots, \mathbf{S}_n) = H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n).$$

The concept of the distribution of a (different) personal key to every user could be of independent interest. But we show that there is *no protocol* achieving Definition 4.1 unless there is no uncertainty on the personal keys, i.e., for any $i \in \{1, \ldots, n\}$, $H(\mathbf{Pk}_i) = 0$.

Along the same lines of the proof of Theorem 3.2, we show that the problem lies in condition b). Indeed:

- conditions a) and c imply the relation established by point *1.* of Lemma 2.1 for the random variables $\mathbf{S}_j, \mathbf{S}_i$, $\mathbf{B}$, and $\mathbf{Pk}_i$, i.e., $H(\mathbf{S}_j, \mathbf{B}|\mathbf{Pk}_i, \mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) - H(\mathbf{Pk}_i)$;
- on the other hand, condition b) implies $H(\mathbf{S}_j, \mathbf{B}|\mathbf{Pk}_i, \mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B})$;
- it follows that $H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) - H(\mathbf{Pk}_i) = H(\mathbf{S}_j, \mathbf{B})$, which holds if and only if $H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B})$ and $H(\mathbf{PK}_i) = 0$.

More precisely, we show the following result:

Theorem 4.2 *If conditions* $a), b)$ *and* $c)$ *of Definition 4.1 are satisfied then, for any* $i \in \{1, \ldots, n\}$,

$$H(\mathbf{Pk}_i) = 0.$$

Proof. Let $G \subset \mathcal{U}$ be the communication group, and let $F \subset \mathcal{U}$ be such that $|F| \leq t$ and $F \cap G \neq \emptyset$. Choose $U_i \in G \setminus F$ and $U_j \in G \cap F$. By using conditions $a)$ and $c)$ and some of the technical lemmas, we show that

$$H(\mathbf{Pk}_i|\mathbf{S}_j, \mathbf{B}, \mathbf{S}_i) = 0 \text{ and } H(\mathbf{Pk}_i|\mathbf{S}_i) = H(\mathbf{Pk}_i). \tag{13}$$

Setting $\mathbf{Z} = \mathbf{Pk}_i, \mathbf{X} = (\mathbf{S}_j, \mathbf{B})$, and $\mathbf{Y} = \mathbf{S}_i$, and applying point *1*. of Lemma 2.1, it holds that

$$H(\mathbf{S}_j, \mathbf{B}|\mathbf{Pk}_i, \mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) - H(\mathbf{Pk}_i). \tag{14}$$

We also show that, if condition $b)$ holds, then

$$H(\mathbf{S}_j, \mathbf{B}|\mathbf{Pk}_i, \mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B}). \tag{15}$$

Therefore, it must be $H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) - H(\mathbf{Pk}_i) = H(\mathbf{S}_j, \mathbf{B})$, which holds if and only if $H(\mathbf{S}_j, \mathbf{B}|\mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B})$ and $H(\mathbf{Pk}_i) = 0$.

Let us prove our statements. It is easy to see that (1), (5), and condition $a)$ imply that

$$0 \leq H(\mathbf{Pk}_i|\mathbf{S}_j, \mathbf{B}, \mathbf{S}_i) \leq H(\mathbf{Pk}_i|\mathbf{B}, \mathbf{S}_i) = 0.$$

On the other hand, from condition $c)$ of Definition 4.1, it follows that $H(\mathbf{Pk}_i|\mathbf{S}_i) = H(\mathbf{Pk}_i)$. Indeed, from (3) we get that $H(\mathbf{Pk}_i|\mathbf{S}_i) \leq H(\mathbf{Pk}_i)$; while, setting $\mathbf{X}_1 = \mathbf{Pk}_i$, $\mathbf{X}_2 = \mathbf{Pk}_1, \ldots, \mathbf{Pk}_{i-1}, \mathbf{Pk}_{i+1}, \ldots, \mathbf{Pk}_n$, and $\mathbf{Z} = \mathbf{S}_1, \ldots, \mathbf{S}_n$, a simple chain of equalities/inequalities shows that:

$$\begin{aligned}
H(\mathbf{Pk}_i|\mathbf{S}_i) \quad &\geq \quad H(\mathbf{Pk}_i|\mathbf{S}_1, \ldots, \mathbf{S}_n) \text{ (due to (5))} \\
&= \quad H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n|\mathbf{S}_1, \ldots, \mathbf{S}_n) - H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_{i-1}, \mathbf{Pk}_{i+1}, \ldots, \mathbf{Pk}_n|\mathbf{S}_1, \ldots, \mathbf{S}_n, \mathbf{Pk}_i) \\
&\qquad \text{(applying (6))} \\
&= \quad H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n) - H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_{i-1}, \mathbf{Pk}_{i+1}, \ldots, \mathbf{Pk}_n|\mathbf{S}_1, \ldots, \mathbf{S}_n, \mathbf{Pk}_i) \\
&\qquad \text{(due to condition } c) \text{ of Definition 4.1)} \\
&\geq \quad H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_n) - H(\mathbf{Pk}_1, \ldots, \mathbf{Pk}_{i-1}, \mathbf{Pk}_{i+1}, \ldots, \mathbf{Pk}_n|\mathbf{Pk}_i) \text{ (due to (5))} \\
&= \quad H(\mathbf{Pk}_i) \text{ (applying (6))}.
\end{aligned}$$

Hence, the equalities assumed in (13) hold, and we are left with proving (14). To this aim, notice that $H(\mathbf{Pk}_i, \mathbf{S}_i|\mathbf{S}_j, \mathbf{B}) = H(\mathbf{Pk}_i, \mathbf{S}_i)$. Indeed,

$$\begin{aligned}
H(\mathbf{Pk}_i, \mathbf{S}_i) \quad &= \quad H(\mathbf{Pk}_i, \mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'} \in F}, \mathbf{B}) \text{ (from condition } b)) \\
&\leq \quad H(\mathbf{Pk}_i, \mathbf{S}_i|\mathbf{S}_j, \mathbf{B}) \text{ (applying (5))} \\
&\leq \quad H(\mathbf{Pk}_i, \mathbf{S}_i) \text{ (applying (3))}.
\end{aligned}$$

However, the above equality, due to (2), is equivalent to say that

$$H(\mathbf{S}_j, \mathbf{B}|\mathbf{Pk}_i, \mathbf{S}_i) = H(\mathbf{S}_j, \mathbf{B}),$$

which proves our claim. Hence, the theorem holds. ■

Notice that in both [39, 32] constructions for personal key distribution schemes were provided. We identify in the following subsection where the proofs for such constructions fail.

4.2 Personal Key Distribution Protocols

We show that the protocols for personal key distribution given in [39, 32] do not meet condition b) of Definition 4.1. Let us start by considering the scheme given in [39]. Let q be a prime number, and let F_q be the corresponding finite field. Moreover, let $F_q[x]$ ($F_q[x, y]$) be the set of all univariate (bivariate) polynomials with coefficients and values in F_q.

Personal Key Distribution Scheme [39].

- Setup. Let $G = \{U_1, \ldots, U_n\}$ be the group of users. Let t be a positive integer, and let $N \in F_q$ be an element different from any user's index. The group manager chooses at random from $F_q[x, y]$ a polynomial $s(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + \ldots + a_{t,t}x^t y^t$. For $i = 1, \ldots, n$, user U_i receives and stores the secret key $s(i, i)$.
- Broadcast. The group manager chooses at random a polynomial $f(x)$ of degree t in $F_q[x]$. Let $W_1 \subseteq \{1, \ldots, n\}$, such that $|W_1| = r < t$, consist of the indices of the users that should not be allowed to recover a new key from the broadcast, and let $W_2 \subset F_q \setminus \{1, \ldots, n\}$ such that $|W_2| = t - r$. The broadcast consists of the following polynomials
$$\{f(x) + s(N, x)\} \cup \{(\omega, s(\omega, x)) : \omega \in W_1 \cup W_2\}.$$
- Personal Key Recovery. A user U_i such that $i \notin W_1$, can evaluate each polynomial $s(\omega, x)$ at $x = i$ to get the t points on the polynomial $s(x, i)$. Coupling these with his/her secret key $s(i, i)$, user U_i has $t+1$ points on $s(x, i)$ and so is able to recover that polynomial and evaluate it at $x = N$ to recover $s(N, i)$. Then, he/she may evaluate $f(x) + s(N, x)$ at $x = i$, subtract off $s(N, i)$, and recover the personal key $f(i)$.

The security of the above construction is claimed by means of Lemma 4 of [39], whose proof is given in Appendix C of [39]. However, the proof does not show that condition b) of Definition 4.1 is satisfied. Indeed, it is easy to see that such a condition does not hold since, given $f(i)$, the value of $s(i, i)$ is uniquely determined by $\{(\omega, s(\omega, i)) : \omega \in W_1 \cup W_2\} \cup \{(N, s(N, i))\}$, where $s(N, i)$ can be computed by evaluating $f(x) + s(N, x)$ at $x = i$, and by subtracting $f(i)$. Once obtained the $t + 1$ pairs $\{(\omega, s(\omega, i)) : \omega \in W_1 \cup W_2\} \cup \{(N, s(N, i))\}$, it is possible to interpolate $s(x, i)$ and compute the secret key $s(i, i)$. For example, assume that $s(x, y)$ and $f(x)$ are chosen uniformly at random in setup phase. By construction $f(x)$ and $s(x, y)$ are each other independent. Therefore, the pair $(f(i), s(i, i))$ can be a-priori any pair of values in F_q^2. However, in the protocol the two values are related via the broadcast message $f(x) + s(N, x)$. Hence, $\log q = H(\mathbf{Pk}_i, \mathbf{S}_i|\mathbf{B}) = H(\mathbf{Pk_i}) < H(\mathbf{Pk}_i, \mathbf{S}_i) = 2 \cdot \log q$.

Similarly, a construction for a personal key distribution scheme was given in Section 3.1 of [32]. The scheme distributes distinct shares of a target t-degree polynomial $f(x)$ to non-revoked group members. It works as follows:

> Personal Key Distribution Scheme [32].
>
> - Setup. The group manager randomly picks a $2t$-degree masking polynomial, $h(x) = h_0 + h_1x + \ldots + h_{2t}x^{2t}$, from $F_q[x]$. Each group member U_i gets the secret key $S_i = h(i)$, from the group manager via a secure communication channel between them.
>
> - Broadcast. Given a set of revoked group members, $R = \{r_1, \ldots, r_\omega\}$, where $|R| \leq t$, the group manager distributes the shares of a t-degree polynomial $f(x)$ to non-revoked group members via the following broadcast message:
>
> $$B = \{R\} \cup \{\omega(x) = g(x)f(x) + h(x)\}$$
>
> where the polynomial $g(x)$ is constructed as $g(x) = (x - r_1)(x - r_2)\ldots(x - r_\omega)$.
>
> - Personal Key Recovery. If any non-revoked group member U_i receives such a broadcast message, it evaluates the polynomial $\omega(x)$ at point i and gets $\omega(i) = g(i)f(i) + h(i)$. Because U_i knows $h(i)$ and $g(i) \neq 0$, it can compute the personal key $f(i) = (\omega(i) - h(i))/g(i)$.

The above construction was claimed to satisfy Definition 4.1 by means of Theorem 1 in [32] without proof. A proof of Theorem 1 was provided in [33]. However, the proof fails in proving condition *b)* of Definition 4.1 since the value of $f(i)$ and the broadcast message $\omega(i) = g(i)f(i) + h(i)$, uniquely determine the value of $h(i)$. Indeed, $g(i)$ can be easily computed by using the identities of the revoked users, which are part of the broadcast, and knowing that $g(x) = (x-r_1)(x-r_2)\ldots(x-r_\omega)$. Therefore, given $\omega(i)$, $g(i)$ and $f(i)$, it is easy to compute also $h(i) = \omega(i) - g(i)f(i)$. Hence, $h(i)$ and $f(i)$, if considered alone, are independent by construction and, if $h(x)$ and $f(x)$ are chosen uniformly at random, the pair $(h(i), f(i))$ can be a-priori any pair of values in F_q^2. However, they are related via the broadcast message $\omega(i) = g(i)f(i) + h(i)$. For any given value of $f(i)$, the value of $h(i)$ is uniquely determined from the broadcast message. Therefore, $\log q = H(\mathbf{Pk}_i, \mathbf{S}_i|\mathbf{B}) = H(\mathbf{Pk_i}) < H(\mathbf{Pk}_i, \mathbf{S}_i) = 2 \cdot \log q$.

5 A new Definition of Self-healing Key Distribution

In this section we propose a new definition of self-healing key distribution. It is compact and it extends and opportunely modifies the definition given in [39].

The setting we consider is the same given at the beginning of Section 2, but we slightly change some notation. We do not use, in our formalization, the intermediate random variable $Z_{i,j}$, used in Definition 3.1. Then, in order to simplify the presentation, for any subset of users $Y = \{U_{i_1}, \ldots, U_{i_g}\} \subseteq \mathcal{U}$, where $i_1 < i_2 < \ldots < i_g$, we will denote the random variables $\mathbf{X}_{i_1} \ldots \mathbf{X}_{i_g}$ by means of $\mathbf{X}_Y$. Finally, we denote with G_0 the initial subset of users $U_i \in \mathcal{U}$ who receive, during the set-up phase, secret keys S_i.

We start by formally stating the properties that the possible strategies, for revoking and adding users from/to the communication group, have to satisfy.

Definition 5.1 *Let $\mathcal{U}$ be the universe of users of the network and, for $i = 0, \ldots, m$, let $G_i \subseteq \mathcal{U}$. The triple $\mathcal{H} = (\mathcal{R}, \mathcal{J}, G_0)$, where $\mathcal{R}$=$(Rev_1, \ldots, Rev_m)$ and $\mathcal{J}$=$(Join_1, \ldots, Join_m)$, is an m-long* t-revocation-joining strategy *if:*

- *$Rev_i \cap Join_j = \emptyset$, for $1 \leq i \leq j \leq m$.*
- *For $i = 1, \ldots, m$, $Rev_i \subseteq G_{i-1} \cup \ldots \cup G_0$ and $Rev_{i-1} \subseteq Rev_i$.*

- $|Rev_m| \leq t$.

The above definition states that the subsets of revoked users and of joining ones must be disjoint, and that revoked users in session i have been active users before. Moreover, the definition specifies that, once a user is revoked from the group, he/she is kept revoked in the subsequent sessions, and that the group manager can revoke up to t users.

In the following we assume that the m-long t-revocation-joining strategy, defined by the join/revoke operations performed at the beginning of each session by the group manager, belong to a family $\mathcal{F}$. Such a family might be the set of *all* possible strategies, as well as a smaller subset of it. Indeed, if the group manager already knows that some strategies will never occur, due to the properties of the application for which the scheme is designed, these strategies do not need to be considered. However, we stress that the group manager *does not* know a-priori which strategy in $\mathcal{F}$ will be realized: joining and revoking operations are event-driven. The group manager might only know that some events do not happen and, hence, that some strategies might be excluded from $\mathcal{F}$.

We denote by $\mathcal{H}_s$ the triple $(\mathcal{R}_s, \mathcal{J}_s, G_0)$, where $\mathcal{R}_s{=}(Rev_1, \ldots, Rev_s)$ and $\mathcal{J}_s{=}(Join_1, \ldots, Join_s)$, for any $0 \leq s \leq m$. It represents the *truncation* of the revocation-joining strategy $\mathcal{H}$ to session s. Notice that $\mathcal{H}_0$ is an empty strategy, while $\mathcal{H}_m = \mathcal{H}$. Moreover, we denote by $B_j^{\mathcal{H}_j}$ the broadcast message sent by GM in session j according to $\mathcal{H}_j$, and by $\mathbf{B}_j^{\mathcal{H}_j}$ the corresponding random variable.

Definition 5.2 *Let $\mathcal{U}$ be the universe of users of a network, let m and t be two integers, and let $\mathcal{F}$ be a family of m-long t-revocation-joining strategy. $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$ is a self-healing m-session key distribution scheme for $\mathcal{U}$ with t-revocation capability for the family $\mathcal{F}$ if, for any $\mathcal{H}$ in $\mathcal{F}$, the following conditions are satisfied:*

1. Key Computation. *Every $U_i \in G_j$ computes K_j from $B_j^{\mathcal{H}_j}$ and S_i.* Formally, it holds that:
$$H(\mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) = 0.$$
2. Self-Healing. *Let r and s be integers such that $1 \leq r < s \leq m$. Each $U_i \in G_r \cap G_s$, from the broadcast messages $B_r^{\mathcal{H}_r}$ and $B_s^{\mathcal{H}_s}$ recovers all keys $K_s, \ldots, K_r$.* Formally, it holds that:
$$H(\mathbf{K}_r, \ldots, \mathbf{K}_s | \mathbf{S}_i, \mathbf{B}_r^{\mathcal{H}_r}, \mathbf{B}_s^{\mathcal{H}_s}) = 0.$$
3. Security of future keys. *Let s be an integer such that $1 \leq s \leq m$. Users in G_s, by pooling together their own personal keys and broadcast messages $B_1^{\mathcal{H}_1}, \ldots, B_{s-1}^{\mathcal{H}_{s-1}}$, do not get any information about keys $K_s, \ldots, K_m$.* Formally, it holds that:
$$H(\mathbf{K}_s, \ldots, \mathbf{K}_m | \mathbf{S}_{G_s} \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_{s-1}^{\mathcal{H}_{s-1}}) = H(\mathbf{K}_s, \ldots, \mathbf{K}_m).$$
4. Security w.r.t. collusion attacks. *Let r and s be integers such that $1 \leq r \leq s \leq m$, and let*[1] *$J_s = \cup_{\ell=s+1}^{m} Join_\ell$. Any subset of users $Adv \subseteq Rev_r \cup J_s$, such that $|Adv| \leq t$, given the sequence of broadcast messages, does not get any information about keys $K_r, \ldots, K_s$.* Formally, it holds that:
$$H(\mathbf{K}_r, \ldots, \mathbf{K}_s | \mathbf{S}_{Adv}, \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_r, \ldots, \mathbf{K}_s).$$

The definition is divided in four parts: the first states that users in the group can compute the session key and the second one states the self-healing property. The third and fourth parts state the security requirements. Roughly speaking, point *3.* means that future keys are secure: even if a group of users tries to get information about new session keys by using only their own personal keys and the transcript of previous communication, they do not get anything. On the other hand, point *4.* means

[1] We define $J_m = \emptyset$.

that a coalition of revoked and new users of size at most t does not get any information about keys such users are not entitled to compute.

Notice that, setting $s = 1$ and assuming $G_1 = \{U_1, \ldots, U_n\}$, a particular case of point *3.*, implies that

$$H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_1, \ldots, \mathbf{S}_n) = H(\mathbf{K}_1, \ldots, \mathbf{K}_m). \tag{16}$$

On the other hand, point *4.*, has several implications. Briefly:

- revoked users at session j, for $j = 1, \ldots, m$, have no information on K_j: if $r = s = j$ and $Adv = Rev_j$, then
$$H(\mathbf{K}_j | \mathbf{S}_{Rev_j}, \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_j); \tag{17}$$
- revoked users at session j, for $j = 1, \ldots, m$, have no information on future keys: if $r = j$, $s = m$, and $Adv = Rev_j$, then
$$H(\mathbf{K}_j, \ldots, \mathbf{K}_m | \mathbf{S}_{Rev_j}, \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_j, \ldots, \mathbf{K}_m); \tag{18}$$
- joining users in session s, for $s = 1, \ldots, m$, have no information on previous keys: if $r = 1$ and $Adv \subseteq J_s$, then
$$H(\mathbf{K}_1, \ldots, \mathbf{K}_{s-1} | \mathbf{S}_{Adv}, \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_1, \ldots, \mathbf{K}_{s-1}); \tag{19}$$
- keys are independent from the broadcast messages: if $r = 1, s = m$, and $Adv = \emptyset$, then
$$H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_1, \ldots, \mathbf{K}_m). \tag{20}$$

The above equalities can be easily shown by applying some of the properties of the entropy function stated in Section 2.

Definition 3.1 and ours cannot be immediately compared. Indeed, in Definition 3.1, a random variable $\mathbf{Z}_{i,j}$ is used for representing the total amount of information that user $U_i \in G_j$ gets from a broadcast message B_j and his own personal key S_i. By using such a variable, point 1.a) of our definition, for example, is therein stated by saying that $H(\mathbf{Z}_{i,j} | \mathbf{B}_j, \mathbf{S}_i) = 0$, and $H(\mathbf{K}_j | \mathbf{Z}_{i,j}) = 0$. We have preferred to give a simplified formalization of the conditions by focusing directly on the secret keys. However, in order to compare the two definitions, if $\mathbf{Z}_{i,j} = f(\mathbf{S}_i, \mathbf{B}_j) = \mathbf{K}_j$, then

- condition *1.a*) of Definition 3.1 coincides with point *1.* of our definition;
- equations (16) and (20) jointly imply condition 1.c) of Definition 3.1.

On the other hand, if $\mathbf{Z}_{i,j} = f(\mathbf{S}_i, \mathbf{B}_j) = (\mathbf{S}_i, \mathbf{B}_j)$, then

- condition *2.* of Definition 3.1 can be derived from conditions *1.* and *4.* of our definition, by means of equations (18);
- conditions *3.a*) and *3.b*) (if F and G are considered the sets of revoked and joining users) can be derived from conditions *2.* and *4.* of our definition.

Actually, under such assumptions on the random variable $\mathbf{Z}_{i,j}$, our definition is slightly stronger than Definition 3.1. Indeed, we have expressed conditions *1.c*), *3.a*) and *3.b*), in terms of the *joint* entropy of the keys instead of considering a single key e.g.,

$$H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_1, \ldots, \mathbf{K}_m)$$

instead of $H(\mathbf{K}_i | \mathbf{B}_1^{\mathcal{H}_1}, \ldots, \mathbf{B}_m^{\mathcal{H}_m}) = H(\mathbf{K}_i)$, for $i = 1, \ldots, m$; while, for condition *2.* of Definition 3.1, we have required that revoked users do not get any information on a new key *even if* they pool together their secret keys *and* the broadcast messages. In condition *2.* of Definition 3.1 broadcast messages are not considered.

Notice that the above assumptions do not get any loss in generality. The assumption $\mathbf{Z}_{i,j} = f(\mathbf{S}_i, \mathbf{B}_j) = \mathbf{K}_j$ enables us to consider the security properties Definition 3.1 requires for the session keys, which can be seen as *some* of the private information that users belonging to the group should be able to compute from the broadcast message and their own secret keys. On the other hand, in considering the self-healing and the collusion resistance properties, the assumption $\mathbf{Z}_{i,j} = f(\mathbf{S}_i, \mathbf{B}_j) = (\mathbf{S}_i, \mathbf{B}_j)$, is the strongest possible: once given the values S_i and B_j any related value (i.e., function of them) can be computed.

In conclusion, Definition 5.2 basically captures all requirements but *1.b)* stated by Definition 3.1 via a different formalisation.

6 Lower Bounds and Constructions

Using Information Theory tools we prove lower bounds on the size of the secret key, each user has to store, and on the size of the broadcast messages the group manager has to send at the beginning of every session, in order to establish a new group key.

6.1 Lower Bounds

The two bounds reported in [5] can also be derived from Definition 5.2. Moreover, using similar techniques, we get lower bounds also on the joint entropies of the secret keys and the broadcast messages.

Let us start by setting up our notation. Our goal is to lower bound the size of the secret key each user receives when he/she joins the communication group. We need to know how long the user stays in the group. Therefore, for any family of strategies $\mathcal{F}$, let us define $\mathcal{F}_j$ to be the family of truncations $\mathcal{H}_j$ of the strategies $\mathcal{H}$ in $\mathcal{F}$ to session j. Moreover, for any truncation $\mathcal{H}_j$, let $\mathcal{F}^{\mathcal{H}_j} \subseteq \mathcal{F}$ be the subset of strategies of $\mathcal{F}$ such that, the truncation of each of them to session j is $\mathcal{H}_j$. In other words, $\mathcal{F}^{\mathcal{H}_j}$ represents the possible completions, with respect to family $\mathcal{F}$, of the truncated strategy $\mathcal{H}_j$. Then, for any $0 \leq j \leq m$, for any $\mathcal{H}_j$, and for any $U_i \in G_j$, we will denote by $q_{j,i}^{\mathcal{H}_j} = \max_{\mathcal{F}^{\mathcal{H}_j}} \{q \,|\, j \leq q \leq m \text{ and } U_i \in G_j \cap G_q\}$, i.e., the maximum value of q such that $U_i \in G_j \cap G_q$. Such a maximum value will be used to quantify the largest interval of sessions U_i *might* belong to the communication group, according to one of the strategies in $\mathcal{F}^{\mathcal{H}_j}$. When the meaning is clear from the context, we will simply denote $q_{j,i}^{\mathcal{H}_j}$ by q_j. We show the following result:

Theorem 6.1 *In any $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$, for any $j = 1, \ldots, m$, for any $\mathcal{H}_j \in \mathcal{F}_j$, and for any $U_i \in Join_j$, it holds that*

$$H(\mathbf{S}_i) \geq H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_{q_j});$$

moreover, for any $U_i \in G_0$, if $q_0 \neq 0$, then $H(\mathbf{S}_i) \geq H(\mathbf{K}_1) + \ldots + H(\mathbf{K}_{q_0})$.

Proof. Let $j \in \{1, \ldots, m\}$, and let $U_i \in G_j \cap G_{q_j}$. Condition *2.* of Definition 5.2 implies that $H(\mathbf{K}_j, \ldots, \mathbf{K}_{q_j} | \mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_{q_j}^{\mathcal{H}_{q_j}}) = 0$; while, from condition *4.* of Definition 5.2, we get that $H(\mathbf{K}_j, \ldots, \mathbf{K}_{q_j} | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_{q_j}^{\mathcal{H}_{q_j}}) = H(\mathbf{K}_j, \ldots, \mathbf{K}_{q_j})$. Then, setting $\mathbf{X} = (\mathbf{K}_j, \ldots, \mathbf{K}_{q_j})$, $\mathbf{Y} = \mathbf{S}_i$, $\mathbf{W} = (\mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_{q_j}^{\mathcal{H}_{q_j}})$, and $\mathbf{Z} = \emptyset$, and applying Lemma 2.4, it holds that $H(\mathbf{S}_i) \geq H(\mathbf{K}_j, \ldots, \mathbf{K}_{q_j})$. From the independence of $\mathbf{K}_j, \ldots, \mathbf{K}_{q_j}$, it results

$$H(\mathbf{K}_j, \ldots, \mathbf{K}_{q_j}) \quad = \quad H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_{q_j}).$$

If $U_i \in G_0$ and $q_0 \neq 0$, then $U_i \in G_1$ as well. Therefore, we apply the above proof. ■

The above result basically says that a user has to store a secret key which is, in terms of bits, greater than or equal to the sum of the bits of the maximum number of session keys he/she might compute as member of the communication group. Moreover, notice that it implies that, for any $\ell = j, \ldots, q_j$, if $U_i \in G_\ell$, then $H(\mathbf{S}_i) \geq H(\mathbf{K}_\ell) + \ldots + H(\mathbf{K}_{q_j})$.

Now, we show a lower bound on the size of the broadcast message. In order to enable all entitled users to recover through self-healing lost session keys, we need to know the largest interval of sessions in which a user has been member of the communication group. Therefore, for any family of strategies $\mathcal{F}$, for any $2 \leq j \leq m$, and for any $\mathcal{H}_j \in \mathcal{F}_j$, we will denote by $r_j^{\mathcal{H}_j} = \min\{r \,|1 \leq r \leq j \text{ and } G_r \cap G_j \neq \emptyset\}$, i.e., the minimum value of r such that $G_r \cap G_j \neq \emptyset$. The following result holds:

Theorem 6.2 *In any $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$, for any $j = 2, \ldots, m$, and for any $\mathcal{H}_j$ in $\mathcal{F}_j$, if $G_j \neq \emptyset$,*

1. *if $r_j < j$, then $H(\mathbf{B}_j^{\mathcal{H}_j}) \geq H(\mathbf{K}_{r_j+1}) + \ldots + H(\mathbf{K}_j)$;*
2. *if $r_j = j$, then $H(\mathbf{B}_j^{\mathcal{H}_j}) \geq H(\mathbf{K}_j)$;*

moreover, if $G_1 \neq \emptyset$, then $H(\mathbf{B}_1^{\mathcal{H}_1}) \geq H(\mathbf{K}_1)$.

Proof. Let $r_j < j$, and let U_i be one of the users in $G_{r_j} \cap G_j$. Notice that $I(\mathbf{B}_j^{\mathcal{H}_j}; \mathbf{K}_{r_j}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}})$, according to (2), can be written either as

$$H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) - H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{K}_{r_j}, \ldots, \mathbf{K}_j)$$

or

$$H(\mathbf{K}_{r_j}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) - H(\mathbf{K}_{r_j}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{B}_j^{\mathcal{H}_j}).$$

Applying the chain rule (6), we have that

$$H(\mathbf{K}_{r_j}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) = H(\mathbf{K}_{r_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) + H(\mathbf{K}_{r_j+1}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{K}_{r_j}).$$

Then, condition *1*. of Definition 5.2 implies that $H(\mathbf{K}_{r_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) = 0$; while, Lemma 2.2 and condition *3*. of Definition 5.2 yield

$$H(\mathbf{K}_{r_j+1}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{K}_{r_j}) = H(\mathbf{K}_{r_j+1}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) = H(\mathbf{K}_{r_j+1}, \ldots, \mathbf{K}_j).$$

Moreover, due to condition *2*. of Definition 5.2, it holds that

$$H(\mathbf{K}_{r_j}, \ldots, \mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{B}_j^{\mathcal{H}_j}) = 0.$$

Hence,

$$\begin{aligned} H(\mathbf{B}_j^{\mathcal{H}_j}) &\geq H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}) - H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{B}_{r_j}^{\mathcal{H}_{r_j}}, \mathbf{K}_{r_j}, \ldots, \mathbf{K}_j) \\ &\geq H(\mathbf{K}_{r_j+1}, \ldots, \mathbf{K}_j) \\ &= H(\mathbf{K}_{r_j+1}) + \ldots + H(\mathbf{K}_j). \end{aligned}$$

Now, let $r_j = j$, and let $U_i \in G_j$. We show that $H(\mathbf{B}_j^{\mathcal{H}_j}) \geq H(\mathbf{K}_j)$. Indeed, $I(\mathbf{B}_j^{\mathcal{H}_j}; \mathbf{K}_j | \mathbf{S}_i)$ can be written either as

$$H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i) - H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{K}_j) \quad \text{or as} \quad H(\mathbf{K}_j | \mathbf{S}_i) - H(\mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}).$$

Condition *1*. of Definition 5.2 implies that $H(\mathbf{K}_j | \mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) = 0$, while condition *3*. implies that $H(\mathbf{K}_j | \mathbf{S}_i) = H(\mathbf{K}_j)$. Moreover, due to property (1), $H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{K}_j) \geq 0$. Therefore, it holds that

$$H(\mathbf{B}_j^{\mathcal{H}_j}) \geq H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i) = H(\mathbf{K}_j) + H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{K}_j) \geq H(\mathbf{K}_j).$$

By applying the same argument, we show that, if $G_1 \neq \emptyset$, then $H(\mathbf{B}_1^{\mathcal{H}_1}) \geq H(\mathbf{K}_1)$. ■

The above result basically says that broadcast message B_j must be, in terms of bits, greater than or equal to the sum of the bits of the maximum number of session keys a user in G_j might recover through self-healing as member of the communication group.

In order to prove a lower bound on the joint entropy of the secret keys of a subset of users, we need to characterize the structure of the family of strategies $\mathcal{F}$. Let j and s be two integers such that $1 \leq j \leq s \leq m$, and let $\{U_{i_1}, \ldots, U_{i_{t+1}}\} \subseteq \mathcal{U}$ be a subset of users. Moreover, let $\mathcal{F}$ contain at least $t+1$ m-long t-revocation-joining strategies for which *one of the users* in $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$ keeps his/her membership until session s, while *the others* are revoked in session j, i.e., $\mathcal{F}$ contains $t+1$ strategies $\mathcal{H}$, such that $\{U_{i_1}, \ldots, U_{i_{t+1}}\} \subseteq G_{j-1}$ and, for any $\ell = 1, \ldots, t+1$, user $U_{i_\ell} \in G_j \cap G_s$ while $\{U_{i_1}, \ldots, U_{i_{t+1}}\} \setminus \{U_{i_\ell}\} = Rev_j$. We will say that the family $\mathcal{F}$ has the *one-shoot t-revocation property* with respect to sessions j and s for $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$.

The following theorem states a lower bound on the joint entropy of the secret keys of $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$, when the family $\mathcal{F}$ has such a property.

Theorem 6.3 *Let j and s be two integers such that $1 \leq j \leq s \leq m$, and let $\{U_{i_1}, \ldots, U_{i_{t+1}}\} \subseteq \mathcal{U}$. In any $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$ in which $\mathcal{F}$ has the* one-shoot t-revocation property *with respect to sessions j and s for $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$, it holds that*

$$H(\mathbf{S}_{i_1}, \ldots, \mathbf{S}_{i_{t+1}}) \geq (t+1) \cdot (H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_s)).$$

Proof. For $\ell = 1, \ldots, t+1$, let $T_\ell = \{U_{i_1}, \ldots, U_{i_{\ell-1}}\}$. By using the chain rule, it holds that

$$H(\mathbf{S}_{i_1}, \ldots, \mathbf{S}_{i_t+1}) = \sum_{\ell=1}^{t+1} H(\mathbf{S}_{i_\ell} | \mathbf{S}_{T_\ell}).$$

Since we show that, for any $\ell = 1, \ldots, t+1$,

$$H(\mathbf{S}_{i_\ell} | \mathbf{S}_{T_\ell}) = H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_s), \tag{21}$$

we have that

$$\sum_{j=1}^{t+1} H(\mathbf{S}_{i_\ell} | \mathbf{S}_{T_\ell}) \geq (t+1) \cdot (H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_s)).$$

Thus, the theorem holds. In order to prove equality (21) we proceed as follows: by hypothesis $\mathcal{F}$ has the *one-shoot t-revocation property* with respect to sessions j and s for $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$. Hence, for any $\ell = 1, \ldots, t+1$, there exists an $\mathcal{H}_s \in \mathcal{F}_s$ such that U_{i_ℓ} belongs to $G_j \cap G_s$, while T_ℓ is a subset of Rev_j. Then, properties (1) and (5), and condition *2.* of Definition 5.2, imply that

$$H(\mathbf{K}_j, \ldots, \mathbf{K}_s | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{i_\ell}, \mathbf{S}_{T_\ell}) = H(\mathbf{K}_j, \ldots, \mathbf{K}_s | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{i_\ell}) = 0,$$

and condition *4.* of Definition 5.2 that

$$H(\mathbf{K}_j, \ldots, \mathbf{K}_s | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{T_\ell}) = H(\mathbf{K}_j, \ldots, \mathbf{K}_s).$$

Therefore, from Lemma 2.4, setting $\mathbf{X} = (\mathbf{K}_j, \ldots, \mathbf{K}_s)$, $\mathbf{W} = (\mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{T_\ell})$, $\mathbf{Y} = \mathbf{S}_{i_\ell}$, and $\mathbf{Z} = \emptyset$, we get that $H(\mathbf{S}_{i_\ell} | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{T_\ell}) \geq H(\mathbf{K}_j, \ldots, \mathbf{K}_s)$. Hence, applying property (5) and the independence of the keys, it holds that

$$H(\mathbf{S}_{i_\ell} | \mathbf{S}_{T_\ell}) \geq H(\mathbf{S}_{i_\ell} | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_s^{\mathcal{H}_s}, \mathbf{S}_{T_\ell}) \geq H(\mathbf{K}_j, \ldots, \mathbf{K}_s) = H(\mathbf{K}_j) + \ldots + H(\mathbf{K}_s).$$

■

The next theorem shows a lower bound on the size of the first and last broadcast messages. It basically states that, in terms of bits, these two messages must be at least as long as the sum of the lengths in bits of the m session keys.

Theorem 6.4 *Let $\mathcal{F}$ contain at least a strategy ($\mathcal{R}$, $\mathcal{J}$, G_0) for which $G_1 \cap G_m \neq \emptyset$. Then, in any $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$, it holds that*

$$H(\mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}) \geq H(\mathbf{K}_1) + \ldots + H(\mathbf{K}_m).$$

Proof. Let $U_i \in G_1 \cap G_m$. Notice that $I(\mathbf{B}_m^{\mathcal{H}_m}; \mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1})$, according to (2), can be written either as

$$H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) - H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{K}_1, \ldots, \mathbf{K}_m)$$

or as

$$H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) - H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}).$$

Condition *3.* of Definition 3.1 implies that $H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}) = 0$. Moreover, applying the chain rule (6), we have that

$$H(\mathbf{K}_1, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) = H(\mathbf{K}_1 | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) + H(\mathbf{K}_2, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{K}_1).$$

Notice that condition *1.* of Definition 5.2 implies that,

$$H(\mathbf{K}_1 | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) = 0;$$

while, Lemma 2.2 and condition *3.* of Definition 5.2 yield

$$H(\mathbf{K}_2, \ldots, \mathbf{K}_m | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{K}_1) = H(\mathbf{K}_2, \ldots, \mathbf{K}_m).$$

Moreover, due to property (1), we have that $H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{K}_1, \ldots, \mathbf{K}_m) \geq 0$. Therefore,

$$\begin{aligned} H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) &= H(\mathbf{K}_2, \ldots, \mathbf{K}_m) + H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}, \mathbf{K}_1, \ldots, \mathbf{K}_m) \\ &\geq H(\mathbf{K}_2, \ldots, \mathbf{K}_m). \end{aligned}$$

Applying property (5), it follows that

$$H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{B}_1^{\mathcal{H}_1}) \geq H(\mathbf{B}_j^{\mathcal{H}_j} | \mathbf{S}_i, \mathbf{B}_1^{\mathcal{H}_1}) \geq H(\mathbf{K}_2, \ldots, \mathbf{K}_m).$$

Hence, applying the chain rule (3), Theorem 6.2 and the above inequality, it holds that

$$\begin{aligned} H(\mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}) &= H(\mathbf{B}_1^{\mathcal{H}_1}) + H(\mathbf{B}_m^{\mathcal{H}_m} | \mathbf{B}_1^{\mathcal{H}_1}) \\ &\geq H(\mathbf{K}_1) + H(\mathbf{K}_2, \ldots, \mathbf{K}_m). \end{aligned}$$

Since the m session keys are independent each other, we get that

$$H(\mathbf{K}_1) + H(\mathbf{K}_2, \ldots, \mathbf{K}_m) = H(\mathbf{K}_1) + \ldots + H(\mathbf{K}_m).$$

Thus, the theorem holds. ■

Theorem 6.1 establishes a lower bound on the size of the secret information each user has to store, while Theorem 6.2 states a lower bound on the size of the broadcast message. In the following section we will show that these lower bounds are tight. However, they cannot be attained simultaneously. More precisely, we show a trade-off between user memory storage S_i and the size of the broadcast message B_j. In our proof we use the following theorem, proved in the context of secret sharing schemes [11].

Theorem 6.5 *[11] Let $\mathbf{K}$, $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{W}$, and $\mathbf{Z}$ be five random variables such that*

$$H(\mathbf{K}|\mathbf{X}) = H(\mathbf{K}|\mathbf{Y}) = H(\mathbf{K}|\mathbf{W}) = H(\mathbf{K}|\mathbf{Z}) = H(\mathbf{K}|\mathbf{X}, \mathbf{W}) = H(\mathbf{K}|\mathbf{X}, \mathbf{Z}) = H(\mathbf{K}|\mathbf{Y}, \mathbf{Z}) = H(\mathbf{K})$$

and

$$H(\mathbf{K}|\mathbf{X}, \mathbf{Y}) = H(\mathbf{K}|\mathbf{Y}, \mathbf{W}) = H(\mathbf{K}|\mathbf{W}, \mathbf{Z}) = 0.$$

Then, it follows that $H(\mathbf{X}, \mathbf{Y}) \geq 3H(\mathbf{K})$.

Using the above result, we show the following:

Theorem 6.6 *Let $\mathcal{F}$ contain two strategies, $\mathcal{H}$ and $\mathcal{H}^*$, and let $\mathcal{H}_j$ and $\mathcal{H}^*{}_j$ be the corresponding truncations to session j. If $\mathcal{H}_j$ enables users U_i and U_ℓ to recover the session key, i.e., $\{U_i, U_\ell\} \subseteq G_j$, while $\mathcal{H}^*{}_j$ enables only U_ℓ to recover the session key i.e., $\{U_i\} \subseteq Rev_j^*$ and $\{U_\ell\} \subseteq G_j$ then, it holds that*

$$H(\mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) \geq 3H(\mathbf{K}_j). \tag{22}$$

Proof. We prove the result by applying Theorem 6.5. Assume that $\mathbf{K} = \mathbf{K}_j$ represents the key the group manager chooses for session j. Let $\mathbf{X} = \mathbf{S}_i$ and $\mathbf{W} = \mathbf{S}_\ell$ represent the secret keys of users U_i, U_ℓ. Denote by $\mathbf{Y} = \mathbf{B}_j^{\mathcal{H}_j}$ and $\mathbf{Z} = \mathbf{B}_j^{\mathcal{H}_j^*}$ the two random variables associated to the broadcast messages defined by $\mathcal{H}_j$ and $\mathcal{H}^*{}_j$, respectively. Applying Definition 5.2, the assumptions of Theorem 6.5 are satisfied. More precisely:

- $H(\mathbf{K}_j|\mathbf{S}_i) = H(\mathbf{K}_j|\mathbf{S}_\ell) = H(\mathbf{K}_j|\mathbf{S}_i, \mathbf{S}_\ell) = H(\mathbf{K}_j)$, due to point *3.* of Definition 5.2.
- $H(\mathbf{K}_j|\mathbf{B}_j^{\mathcal{H}_j}) = H(\mathbf{K}_j|\mathbf{B}_j^{\mathcal{H}_j^*}) = H(\mathbf{K}_j|\mathbf{B}_j^{\mathcal{H}_j}, \mathbf{B}_j^{\mathcal{H}_j^*}) = H(\mathbf{K}_j|\mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j^*}) = H(\mathbf{K}_j|\mathbf{S}_\ell, \mathbf{B}_j^{\mathcal{H}_j^*}) = H(\mathbf{K}_j)$, due to point *4.* of Definition 5.2.
- $H(\mathbf{K}_j|\mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) = H(\mathbf{K}_j|\mathbf{S}_\ell, \mathbf{B}_j^{\mathcal{H}_j}) = H(\mathbf{K}_j|\mathbf{S}_\ell, \mathbf{B}_j^{\mathcal{H}_j^*}) = 0$, due to point *1.* of Definition 5.2.

Therefore,

$$H(\mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) \geq 3H(\mathbf{K}_j).$$

■

Hence, in any self-healing key distribution scheme for a non-trivial family of strategies $\mathcal{F}$, the lower bounds stated by Theorems 6.1 and 6.2 on user memory storage and communication complexity cannot be achieved simultaneously.

Strengthening the lower bounds. Notice that Theorems 6.1, 6.2, 6.3, 6.4, and Theorem 6.6 can be strengthened by using previous results obtained in the analysis of secret sharing schemes. First of all, notice that, given a random variable $\mathbf{W}$, there could be some value $\omega \in W$ such that $Pr(\mathbf{W} = \omega) = 0$. Therefore, let

$$\text{Support}(\mathbf{W}) = \{\omega \in W | Pr(\mathbf{W} = \omega) > 0\}$$

be the set of values assumed by $\mathbf{W}$ with positive probability. To simplify the discussion, assume that all session keys are chosen from the same fixed set K. Since Theorems 6.1, 6.2, 6.3, and 6.4 should intuitively hold *for any* probability distribution on the set of keys K, then they should hold also for the special case of the *uniform* one. In such a case $H(\mathbf{K}) = \log(|Support(\mathbf{K})|)$. The above intuition can be formalized applying the same techniques employed in [7], and we can prove the following results:

Theorem 6.7 *In any $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$, for any $j = 1, \ldots, m$, for any $\mathcal{H}_j \in \mathcal{F}_j$, and for any $U_i \in Join_j$, it holds that*

$$H(\mathbf{S}_i) \geq (q_j - j + 1) \cdot \log(|Support(\mathbf{K})|);$$

moreover, for any $U_i \in G_0$, if $q_0 \neq 0$, then

$$H(\mathbf{S}_i) \geq q_1 \cdot \log(|Support(\mathbf{K})|).$$

Theorem 6.8 *In any $\mathcal{D}(m, t, \mathcal{U}, \mathcal{F})$, for any $j = 2, \ldots, m$, and for any $\mathcal{H}_j$ in $\mathcal{F}_j$, if $G_j \neq \emptyset$,*

1. *if $r_j < j$, then $H(\mathbf{B}_j^{\mathcal{H}_j}) \geq (j - r_j) \cdot \log(|Support(\mathbf{K})|)$;*
2. *if $r_j = j$, then $H(\mathbf{B}_j^{\mathcal{H}_j}) \geq \log(|Support(\mathbf{K})|)$;*

moreover, if $G_1 \neq \emptyset$, then $H(\mathbf{B}_1^{\mathcal{H}_1}) \geq \log(|Support(\mathbf{K})|)$.

Theorem 6.9 *Let j and s be two integers such that $1 \leq j \leq s \leq m$, and let $\{U_{i_1}, \ldots, U_{i_{t+1}}\} \subseteq \mathcal{U}$. In any $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$ in which $\mathcal{F}$ has the* one-shoot t-revocation property *with respect to sessions j and s for $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$, it holds that*

$$H(\mathbf{S}_{i_1}, \ldots, \mathbf{S}_{i_{t+1}}) \geq (t+1) \cdot (s-j+1) \cdot \log(|Support(\mathbf{K})|).$$

Theorem 6.10 *Let $\mathcal{F}$ contain at least a strategy ($\mathcal{R}$, $\mathcal{J}$, G_0) for which $G_1 \cap G_m \neq \emptyset$. Then, in any $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$, it holds that*

$$H(\mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}) \geq m \cdot \log(|Support(\mathbf{K})|).$$

Theorem 6.11 *Let $\mathcal{F}$ contain two strategies, $\mathcal{H}$ and $\mathcal{H}^*$, and let $\mathcal{H}_j$ and ${\mathcal{H}^*}_j$ be the corresponding truncations to session j. If $\mathcal{H}_j$ enables users U_i and U_ℓ to recover the session key, i.e., $\{U_i, U_\ell\} \subseteq G_j$, while ${\mathcal{H}^*}_j$ enables only U_ℓ to recover the session key i.e., $\{U_i\} \subseteq Rev_j^*$ and $\{U_\ell\} \subseteq G_j$ then, it holds that*

$$H(\mathbf{S}_i, \mathbf{B}_j^{\mathcal{H}_j}) \geq 3 \cdot \log(|Support(\mathbf{K})|).$$

6.2 Constructions

We show that Theorems 6.7, 6.8, 6.9 and 6.10 are tight and, hence, also Theorems 6.1, 6.2, 6.3 and 6.4, by describing a meta-construction for $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$ self-healing key distribution schemes. Such a meta-construction uses, as a building block, two $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ constructions, which resemble the basic schemes given in [17]. The first $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ construction, referred to as Optimal User Memory Storage $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$, minimizes the size of the secret key each user has to store. The second one, referred to as Protocol $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ with Optimal Broadcast for Rev^*, requires a broadcast message B_j of short size. We start by describing such one-time constructions. Later on, we will show how they can be composed in order to set up a $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$.

Let $\mathcal{U} = \{U_1, \ldots, U_n\}$ be the universe of users, let t be an integer, and let F_q, where $q > n$, be a finite prime field. Moreover, let $G_0 \subset \mathcal{U}$ be an initial set of users.

The following $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ scheme shows that Theorem 6.7 is tight in the special case of 1-session schemes.

Optimal User Memory Storage $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$.

- Setup. The group manager chooses uniformly at random $t+1$ values, say $a_0, \ldots, a_t \in F_q$, and computes the polynomial $P(x) = \sum_{i=0}^{t} a_i x^i$ of degree t. Then, for each user $U_i \in G_0$, he computes the value $y_i = P(i) \bmod q$. Finally, he gives in a secure way to $U_i \in G_0$ as secret key the value $S_i = y_i$.
- Join. The group manager, for each user $U_i \in Join_1$, computes the value $y_i = P(i) \bmod q$. Then, he gives to U_i as secret key the value $S_i = y_i$.
- Broadcast. Let Rev_1 be the subset of revoked users. The group manager chooses uniformly at random a key K in F_q, computes the sequence of pairs of values $B_1^{\mathcal{H}_1} =< (K - y_i, i) >_{U_i \in G_1}$, and broadcasts $B_1^{\mathcal{H}_1}$.
- Session Key Computation. Every non-revoked user U_i computes $K = B_1^{\mathcal{H}_1} + y_i$.

It is easy to check that, in the above construction, $H(\mathbf{S}_i) = \log(|Support(\mathbf{K})|)$. On the other hand, the following $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ shows that Theorem 6.8 is tight in the special case of 1-session schemes.

Protocol $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ with Optimal Broadcast for Rev^*

- **Setup.** The group manager, for each possible subset $Rev \subset \mathcal{U}$ of size at most t, chooses, uniformly at random, a value $x^{Rev} \in F_q$. We assume that the subsets Rev are listed according to a lexicographic order. Then, the group manager gives to every user $U_i \in G_0$ as secret key the sequence of pairs $S_i =< (x^{Rev}, Rev) >_{U_i \notin Rev, Rev \subset \mathcal{U}}$.

- **Join.** The group manager gives to every user $U_i \in Join_1$ as secret key the sequence of pairs $S_i =< (x^{Rev}, Rev) >_{U_i \notin Rev, Rev \subset \mathcal{U}}$.

- **Broadcast.** Let Rev_1 be the subset of revoked users in the unique session. The group manager, at the beginning of the session, chooses uniformly at random a key K in F_q. Then, if Rev_1 is different from the subset Rev^*, it computes $B_1^{\mathcal{H}_1} = (K - x^{Rev_1}, Rev_1)$, and broadcasts $B_1^{\mathcal{H}_1}$. Otherwise, it simply computes and broadcasts $B_1^{\mathcal{H}_1} = K - x^{Rev^*}$.

- **Session Key Computation.** Every non-revoked user U_i computes $K = B_1^{\mathcal{H}_1} + x^{Rev_1}$.

When the set of revoked users is the set Rev^*, then $H(\mathbf{B}_1^{\mathcal{H}_1}) = \log(|Support(\mathbf{K})|)$. Therefore, Theorem 6.8 is tight in the special case of 1-session schemes.

In order to set up a $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$ scheme, the group manager operates as follows:

Meta-Construction for $\mathcal{D}(m,t,\mathcal{U},\mathcal{F})$ schemes.

- **Setup.** The group manager chooses one of the two $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ schemes described before, and generates m *independent* copies $\Sigma_1,\ldots,\Sigma_m$ of it. Then, he gives to user $U_i \in G_0$ a secret key S_i comprising the sequence of secret keys he/she would receive from $\Sigma_1,\ldots,\Sigma_{q_j}$.

- **Join.** The group manager gives to user $U_i \in Join_j$ a secret key S_i comprising the sequence of j secret keys he/she would receive from $\Sigma_j,\ldots,\Sigma_{q_j}$.

- **Broadcast.** Let $G_j \neq \emptyset$. In session $j = 1,2$, it broadcasts $B_j^{\mathcal{H}_j}$, according to scheme Σ_j. In session $j \geq 3$, it broadcasts the sequence of messages $< B_j^{\mathcal{H}_j}, B_{j-1}^{\mathcal{H}_{j-1}}, \ldots, B_{r_j}^{\mathcal{H}_{r_j}} >$, i.e., the broadcast messages associated to schemes $\Sigma_j,\ldots,\Sigma_{r_j}$, respectively. If $G_j = \emptyset$, then no broadcast is needed.

- **Session Key Computation.** Every non-revoked user computes the session keys he/she is entitled to by using the session key computation rules associated to scheme Σ_j.

Notice that, we are taking into account with every broadcast message $B_j^{\mathcal{H}_j}$, the largest possible self-healing interval at that time.

Conditions *1.*, *2.*, *3.*, and *4.* of Definition 5.2 are satisfied. Indeed, it is straightforward to check that:

- condition *1.* holds because every user $U_i \in G_j$ computes the session key K_j from $B_j^{\mathcal{H}_j}$ and S_i;

- condition *2.* holds because, if $U_i \in G_r \cap G_s$, from $B_r^{\mathcal{H}_r}$, $B_s^{\mathcal{H}_s}$, and his secret key S_i, he/she recovers all session keys $K_r,\ldots,K_s$.

- condition *3*. holds because the session key K_j is "contained" in $B_j^{\mathcal{H}_j}$. Hence, previous broadcast messages and users' secret keys do not give any information about the new key.
- condition *4*. is satisfied because, users revoked in session r and users joining the group after session s, do not possess the values necessary for recovering from $B_r^{\mathcal{H}_r}, \ldots, B_s^{\mathcal{H}_s}$ the session keys. Indeed, revoked users do not possess the values $x^{Rev_r}, \ldots, x^{Rev_s}$ (if the first $\mathcal{D}(1,t,\mathcal{U})$ scheme is used in the meta-construction) or the sequence of values $< y_i >_{U_i \in G_p}$, for $p = r, \ldots, s$ (if the second $\mathcal{D}(1,t,\mathcal{U})$ is used). While, users who join the group after session s get only values useful in the current and in future sessions.

The above meta-construction, instantiated with the OPTIMAL USER MEMORY STORAGE $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ scheme, shows that the bounds given by Theorems 6.7 and 6.9 are tight. Indeed, for any $U_i \in Join_j$, it holds that $H(\mathbf{S}_i) = (q_j - j + 1) \cdot \log q$. Similarly, for any $U_i \in G_0$ such that $q_0 \neq 0$, it holds that $H(\mathbf{S}_i) = q_0 \cdot \log q$. Moreover, if the family $\mathcal{F}$ has the *one-shoot t-revocation property* with respect to sessions j and s for $\{U_{i_1}, \ldots, U_{i_{t+1}}\}$, then $H(\mathbf{S}_{i_1}, \ldots, \mathbf{S}_{i_{t+1}}) = (t+1) \cdot (s-j+1) \cdot \log q$. Then, let $\mathcal{H} = (\mathcal{R}, \mathcal{J}, G_0) \in \mathcal{F}$, where $\mathcal{R}$=$(Rev_1, \ldots, Rev_m)$, be an m-long t-revocation joining strategy. The meta-construction, instantiated with m copies of the PROTOCOL $\mathcal{D}(1,t,\mathcal{U},\mathcal{F})$ WITH OPTIMAL BROADCAST FOR STRATEGY Rev^*, where, for $j = 1, \ldots, m$, $Rev^* = Rev_j$, shows that Theorems 6.8 and 6.10 are tight as well, i.e., $H(\mathbf{B}_j^{\mathcal{H}_j}) = (j - r_j) \cdot \log q$ and $H(\mathbf{B}_1^{\mathcal{H}_1}, \mathbf{B}_m^{\mathcal{H}_m}) = m \cdot \log q$.

7 Some Notes

Secret Sharing Schemes. Self-healing key distribution schemes and secret sharing schemes are strongly related. Indeed, from a formal point of view, notice that condition *1*. of Definition 5.2 is exactly the reconstruction property of a secret sharing scheme, i.e.,

$$H(\mathbf{K}_j | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{S}_i) = 0,$$

which means that the secret K_j is reconstructed once given the shares $B_j^{\mathcal{H}_j}$ and S_i, for each non-revoked user U_i. On the other hand, from (17) and (5) it follows that

$$H(\mathbf{K}_j | \mathbf{B}_j^{\mathcal{H}_j}, \mathbf{S}_{Rev_j}) = H(\mathbf{K}_j),$$

which is the security property of a secret sharing scheme, i.e., the set of shares composed of the secret keys of revoked users and the broadcast message does not give any information about the secret K_j. However, compared to secret sharing schemes, we have also some set of shares for which nothing is stated/required. Actually, by using conditions *2*. and *4*. of Definition 5.2 we can also point out that self-healing key distribution schemes are related to multi-secret sharing schemes. Such connections might be further investigated.

Impossibility Results: Practical Implications. The impossibility of achieving conditions 1.*b*) of Definition 3.1 and *b*) of Definition 5.2 has some important consequences. Applying the same techniques developed in [16], the authors of [29] suggested, in designing self-healing key distribution schemes, to introduce some valuable information, like the social security number of the user or any other information the member would want to keep secret, inside the secret key. The link between private keys and personal information is intended to serve as a deterrent to key sharing: many users will take extra care to keep their secret keys secret so that their personal information remains secret as well. On the other hand, dishonest users should be discouraged to disclose their own secret keys, in order to enable other users to illegally decrypt broadcast messages. The analysis we have done implies that it is *impossible to unconditionally protect* such a valuable information inside the secret key of a self-healing key distribution scheme. Information leakage is unavoidable.

8 Conclusions

We have considered mainly the definitional task of self-healing key distribution. We have discussed some issues related to the formalization of such a concept given in [39, 32], and we have shown that no protocol can achieve some of the security requirements therein stated. We have also analysed the notion of personal key distribution scheme [39, 32], showing that no protocol can achieve the security requirements and identifying where the proposed schemes fail. Then, we have shown that a lower bound on the size of the broadcast messages the group manager has to sent in order to establish session keys, proved in [39] and also used in [32], does not hold. After the analysis, we have proposed a new definition for self-healing key distribution, by extending and opportunely modifying the definition given in [39], and we have given some lower bounds on the resources required for implementing such schemes, i.e., user memory storage and communication complexity, and we have shown that they are tight. Moreover, we have shown that some of them cannot be attained at the same time.

An interesting open problem is to find constructions which exhibit a good trade-off between user memory storage and broadcast size.

References

[1] J. Anzai, N. Matsuzaki, and T. Matsumoto, *A Quick Group Key Distribution Scheme with Entity Revocation*, Advances in Cryptology - Asiacrypt '99, Lecture Notes in Computer Science, Vol. 1716, pp. 333-347, 1999.

[2] S. Berkovits, *How to Broadcast a Secret*, Advances in Cryptology - Eurocrypt '91, Lecture Notes in Computer Science, Vol. 547, pp. 536–541, 1991.

[3] G. R. Blakley, *Safeguarding Cryptographic keys*, Proceedings of AFIPS Conference, Vol. 48, pp. 313-317, 1979.

[4] C. Blundo and A. Cresti, *Space Requirements for Broadcast Encryption*, Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science, Vol. 950, pp. 287–298, 1995.

[5] C. Blundo, P. D'Arco, A. De Santis, and M. Listo. *Design of Self-healing Key Distribution Schemes*, Designs, Codes and Cryptography, N. 32, pp. 15–44, 2004.

[6] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, *Perfectly-Secure Key Distribution for Dynamic Conferences*, Information and Computation, Vol. 146, N. 1, pp. 1-23, 1998 .

[7] C. Blundo, A. De Santis, and U. Vaccaro, *On Secret Sharing Schemes*, Information Processing Letters, N. 65, pp. 25–32, 1998.

[8] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson, *Generalised Beimel-Chor Schemes for Broadcast Encryption and Interactive Key Distribution*, Theoretical Computer Science, Vol. 200, pp. 313–334, 1998.

[9] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Issue in Multicast Security: A Taxonomy and Efficient Constructions*, Proceedings of Infocom '99, pp. 708–716, 1999.

[10] R. Canetti, T. Malkin, and K. Nissim, *Efficient Communication-Storage Tradeoffs for Multicast Encryption*, Advances in Cryptology - Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, pp. 459–474, 1999.

[11] R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the Size of the Shares in Secret Sharing Schemes. Advances in Cryptology - Crypto '91, Lecture Notes in Computer Science, Vol. 576, pp. 101–113, 1992.

[12] B. Chor, A. Fiat, M. Naor and B. Pinkas, *Traitor Tracing*, IEEE Transactions on Information Theory, Vol. 46, N. 3, pp. 893–910, 2000.

[13] T. M. Cover and J. A. Thomas, **Elements of Information Theory**, John Wiley & Sons, 1991.

[14] P. D'Arco and D. R. Stinson, *Fault Tolerant and Distributed Broadcast Encryption*, Cryptographers' Track RSA Conference 2003 (CT-RSA 2003), Lecture Notes in Computer Science, Vol. 2612, pp. 262–279, 2003.

[15] G. Di Crescenzo and O. Kornievskaia, *Efficient Multicast Encryption Schemes*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, Vol. 2576, pp. 119–132, 2003.

[16] C. Dwork, J. Lotspiech, and M. Naor, *Digital Signets: Self-Enforcing Protection of Digital Information*, Proceedings of the 28-th Symposium on the Theory of Computation, pp. 489–498, 1996.

[17] A. Fiat and M. Naor, *Broadcast Encryption*, Advances in Cryptology - Crypto '93, Lecture Notes in Computer Science, Vol. 773, pp. 480–491, 1994.

[18] A. Fiat and T. Tessa, *Dynamic Traitor Tracing*, Journal of Cryptology, Vol. 14, pp. 211–223, 2001.

[19] E. Gafni, J. Staddon, and Y. L. Yin, *Efficient Methods for Integrating Traceability and Broadcast Encryption*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Vol. 1666, pp. 372–387, 1999.

[20] J. Garay, J. Staddon, and A. Wool, *Long-Lived Broadcast Encryption*, Advances in Cryptology - Crypto '00, Lecture Notes in Computer Science, Vol. 1880, pp. 333–352, 2000.

[21] D. Halevy and A. Shamir, *The LSD Broadcast Encryption Scheme*, Advances in Cryptology - Crypto '02, Lecture Notes in Computer Science, Vol. 2442, pp. 47-60, 2002.

[22] A. Kiayias and M. Yung, *Traitor Tracing with Constant Transmission Rate*, Advances in Cryptology - Eurocrypt '02, Lecture Notes in Computer Science, Vol. 2332, pp. 450-465, 2002.

[23] A. Kiayias and M. Yung, *Self Protecting Pirates and Black-Box Traitor Tracing*, Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, Vol.2139, pp. 63-79, 2001.

[24] R. Kumar, S. Rajagopalan, and A. Sahai, *Coding Constructions for Blacklisting Problems without Computational Assumptions*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Vol. 1666, pp. 609–623, 1999.

[25] H. Kurnio, R. Safani-Naini, and H. Wang, *A Group Key Distribution Scheme with Decentralised User Join*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, Vol. 2576, pp. 146–163, 2003.

[26] H. Kurnio, R. Safani-Naini, and H. Wang, *A Secure Re-keying Scheme with Key Recovery Property*, ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, pp. 40–55, 2002.

[27] M. Luby and J. Staddon, *Combinatorial Bounds for Broadcast Encryption*, Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science, Vol. 1403, pp. 512–526, 1998.

[28] M. Mihaljević, *Key Management Schemes for Stateless Receivers Based on Time Varying Heterogeneous Logical Key Hierarchy*, Advances in Cryptology - Asyacrypt '03, Lecture Notes in Computer Science, Vol. 2894, pp. 137–154, 2003.

[29] S. Miner, M. Malkin, J. Staddon, and D. Balfanz, *Sliding-Window Self-Healing Key Distribution*, Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems (SSRS '03), October 31, 2003, Fairfax, Virginia, USA.

[30] D. Naor, M. Naor, and J. Lotspiech, *Revocation and Tracing Schemes for Stateless Receivers* Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, Vol. 2139, pp. 41–62, 2001.

[31] M. Naor and B. Pinkas, *Efficient Trace and Revoke Schemes*, Financial Cryptography 2000, Lecture Notes in Computer Science, Vol. 1962, pp. 1–21, 2000.

[32] D. Liu, P. Ning, and K. Sun, *Efficient Self-Healing Key Distribution with Revocation Capability*, Proceedings of the 10-th ACM Conference on Computer and Communications Security, October 27-31, 2003, Washington, DC, USA.

[33] D. Liu, P. Ning, and K. Sun, *Efficient Self-Healing Key Distribution with Revocation Capability*, (full version of the conference paper) available at http://discovery.csc.ncsu.edu/ pning/pubs/ccs03-GKD-full.pdf

[34] A. Perrig, D. Song, and J. D. Tygar, *ELK, a new Protocol for Efficient Large-Group Key Distribution*, Proceedings of the IEEE Symposium on Security and Privacy, 2000.

[35] B. Pfitzmann, *Trials of Traced Traitors*, Information Hiding, Lecture Notes in Computer Science, Vol. 1174, pp. 49-64, 1996.

[36] R. Safavi-Naini and H. Wang, *New Constructions for Multicast Re-Keying Schemes Using Perfect Hash Families*, 7th ACM Conference on Computer and Communication Security, ACM Press, pp. 228–234, 2000.

[37] R. Safavi-Naini and Y. Wang, *Sequential Traitor Tracing*, Advances in Cryptology - Crypto '00, Lecture Notes in Computer Science, Vol. 1880, p. 316–332, 2000.

[38] A. Shamir, *How to Share a Secret*, Communications of ACM, Vol. 22, N. 11, pp. 612–613, 1979.

[39] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, *Self-Healing Key Distribution with Revocation*, IEEE Symposium on Security and Privacy, May 12-15, 2002, Berkeley, California.

[40] J. N. Staddon, D.R. Stinson and R. Wei, *Combinatorial Properties of Frameproof and Traceability Codes*, IEEE Transactions on Information Theory, Vol. 47, pp. 1042-1049, 2001.

[41] D.R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes, and Cryptography, Vol. 2, pp. 357–390, 1992.

[42] D. R. Stinson, *On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption*, Designs, Codes and Cryptography, Vol. 12, pp. 215–243, 1997.

[43] D. R. Stinson and T. van Trung, *Some New Results on Key Distribution Patterns and Broadcast Encryption*, Designs, Codes and Cryptography, Vol. 15, pp. 261–279, 1998.

[44] D. R. Stinson and R. Wei, *Key Preassigned Traceability Schemes for Broadcast Encryption*, Proceedings of SAC'98, Lecture Notes in Computer Science, Vol. 1556, pp. 144–156, 1999.

[45] D. R. Stinson and R. Wei, *Combinatorial Properties and Constructions of Traceability Schemes and Frameproof Codes*, SIAM Journal on Discrete Mathematics, Vol. 11, pp. 41–53, 1998.

[46] D. R. Stinson and R. Wei, *An Application of Ramp Schemes to Broadcast Encryption*, Information Processing Letters, Vol. 69, pp. 131–135, 1999.

[47] S. Zhu, S. Setia, and S. Jajodia, *Adding Reliable and Self-healing Key Distribution to the Subset Difference Group Rekeying Method for Secure Multicast*, Proceedings of the Fifth International Workshop on Networked Group Communication, NGC 2003.

[48] D. M. Wallner, E. J. Harder, and R. C. Agee, *Key Management for Multicast: Issues and Architectures*, Internet Draft (draft-wallner-key-arch-01.txt), ftp://ftp.ieft.org/internet-drafts/draft-wallner-key-arch-01.txt.

[49] C. Wong and S. Lam, *Keystone: A Group Key Management System*, in International Conference on Telecommunications, ICT 2000.