Information Processing Letters 113 (2013) 151–155

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A note on time-bound hierarchical key assignment schemes

Giuseppe Ateniese[a], Alfredo De Santis[b], Anna Lisa Ferrara[c], Barbara Masucci[b,*]

[a] *The Johns Hopkins University, Baltimore, MD 21218, USA*
[b] *Università di Salerno, 84084 Fisciano (SA), Italy*
[c] *Bristol University, Bristol, BS8 1UB, UK*

ARTICLE INFO

Article history:
Received 15 September 2010
Received in revised form 10 May 2012
Accepted 5 January 2013
Available online 10 January 2013
Communicated by A. Tarlecki

Keywords:
Cryptography
Distributed systems
Safety/security in digital systems
Access control

ABSTRACT

A *time-bound hierarchical key assignment scheme* is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that each class can compute the keys of all classes lower down in the hierarchy, according to temporal constraints.

In this paper we consider the *unconditionally secure* setting for time-bound hierarchical key assignment schemes and distinguish between two different goals: security with respect to *key indistinguishability* and against *key recovery*. We first present definitions of security with respect to both goals; then, we prove a tight lower bound on the size of the private information distributed to each class; finally, we show an optimal construction for time-bound hierarchical key assignment schemes.

1. Introduction

A *time-bound hierarchical key assignment scheme* is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that each class can compute the keys of all classes lower down in the hierarchy, according to temporal constraints. Specifically, we consider a scenario where the users of a computer system are organized in a certain number of disjoint classes, called security classes. The life-time of the system is divided into a sequence of time periods. Each user in a class is authorized to access the data of a class lower down in the hierarchy at a certain time period, provided that she has the credentials to compute the key corresponding to that class and for that time period.

There are several applications which may be implemented by using a time-bound hierarchical key assignment scheme. As an example, consider a web-based electronic newspaper company which offers several types of subscription packages, covering different topics. Each user may decide to subscribe to a package for a certain period of time (e.g., a week, a month, or a year). Subscription packages could be structured to form a partially ordered hierarchy where leaf nodes represent different topics and an internal node represents a package covering all topics associated to the leaf classes which can be reached by that node. For each time period, an encryption key is then assigned to each node in the hierarchy. The key corresponding to a leaf class can be computed by each user that subscribes to a package which includes the topic associated to that leaf class and for that period of time. A similar solution was employed by Bertino et al. [4], who showed how to control access to an XML document according to temporal constraints.

In this paper, we consider two different security goals: security with respect to *key indistinguishability* and security against *key recovery*. Security with respect to key indistinguishability formalizes the requirement that the adversary is not able *to learn any information* about a key that it should not have access to, i.e., it is not able to distinguish it from a random string having the same length. On the

[*] Corresponding author.
E-mail addresses: ateniese@cs.jhu.edu (G. Ateniese), ads@dia.unisa.it (A. De Santis), anna.lisa.ferrara@bristol.ac.uk (A.L. Ferrara), masucci@dia.unisa.it (B. Masucci).

0020-0190/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ipl.2013.01.006

other hand, security against key recovery corresponds to the requirement that an adversary is not able to *compute* a key that it should not have access to.

The most used approach to time-bound key assignment schemes is based on unproven specific assumptions (e.g., [1,2,9,5,7,16,11,15,14,12,13,3]). In this paper we focus on an information-theoretic approach which differs from the above computational approach since it does not depend on any unproven assumption. In [8] an information-theoretic approach to hierarchical key assignment schemes has been considered. A hierarchical key assignment scheme controls the accesses among the classes with respect to the structure of the hierarchy but does not consider time-dependent constraints.

In the information-theoretic setting, the key assigned to each class at a certain time period is *unconditionally secure*, with respect to one of the above security goals, against an adversary with unlimited computing power, controlling any coalition of classes not allowed to compute such a key. We present definitions of security with respect to each goal in the unconditionally secure setting and then we prove a tight lower bound on the size of the private information distributed to each class.

2. The model

Consider a set of users divided into a number of disjoint classes, called *security classes*. A security class can represent a person, a department, or a user group in an organization. A binary relation $\preccurlyeq$ that partially orders the set of classes V is defined in accordance with authority, position, or power of each class in V. The poset $(V, \preccurlyeq)$ is called a *partially ordered hierarchy*. For any two classes u and v, the notation $u \preccurlyeq v$ is used to indicate that the users in v can access u's data. We denote by A_v the set $\{u \in V\colon\ u \preccurlyeq v\}$, for any $v \in V$. The partially ordered hierarchy $(V, \preccurlyeq)$ can be represented by a directed graph where each class corresponds to a vertex in the graph and there is an edge from class v to class u if and only if $u \preccurlyeq v$. Further, this graph can be simplified by eliminating all self-loops and edges which can be implied by the property of the transitive closure. We denote by $G = (V, E)$ the resulting directed acyclic graph.

In this paper we consider the case where a user may be in a class for only a period of time. We consider a sequence $T = (t_1, \ldots, t_n)$ composed of n distinct time periods. Each user may belong to a class for a certain non-empty contiguous subsequence λ of T. Let $\mathcal{P} = \{(t_i, \ldots, t_j) | 1 \leqslant i \leqslant j \leqslant n\}$ be the set of all non-empty contiguous subsequences of T. Such a set is called the *interval-set* over T. In the following, given a time sequence $\lambda \in \mathcal{P}$, we denote by $t \in \lambda$ the fact that the time period t belongs to the sequence λ. Moreover, we abuse notation by using t to denote a time period $t \in T$ as well as the time sequence $(t) \in \mathcal{P}$.

A *time-bound hierarchical key assignment scheme* for a partially ordered hierarchy represented by a directed acyclic graph $G = (V, E)$ and a time sequence T is a method to assign a private information $s_{v,\lambda}$ to each class $v \in V$ for each time sequence $\lambda \in \mathcal{P}$ and an encryption key $k_{u,t}$ to each class $u \in V$ for each time period $t \in T$. The generation and distribution of the private information and keys is carried out by a trusted third party, the TA, which is connected to each class by means of a secure channel. The encryption key $k_{u,t}$ can be used by users belonging to class u in time period t to protect their sensitive data by means of a symmetric cryptosystem, whereas, the private information $s_{v,\lambda}$ can be used by users belonging to class v for the time sequence λ to compute the key $k_{u,t}$ for any class $u \in A_v$ and each time period $t \in \lambda$. For each class $u \in V$, each time sequence $\lambda \in \mathcal{P}$, and each time period $t \in T$, we denote by $S_{u,\lambda}$ and $K_{u,t}$ the sets of all possible values that $s_{u,\lambda}$ and $k_{u,t}$ can assume, respectively.

We formally define time-bound hierarchical key assignment schemes by using the entropy function (we refer the reader to the Appendix A for some proprieties of the entropy function and to [6] for a complete treatment of Information Theory), mainly because this leads to a compact and simple description of the schemes and because the entropy approach takes into account all probability distributions on the keys assigned to the classes. In the following, with a boldface capital letter, say $\mathbf{Y}$, we denote a random variable taking values on a set, denoted by the corresponding capital letter Y, according to some probability distribution $\{Pr_{\mathbf{Y}}(y)\}_{y \in Y}$. The values such a random variable can take are denoted by the corresponding lower case letter. Given a random variable $\mathbf{Y}$, we denote by $H(\mathbf{Y})$ the Shannon entropy of $\{Pr_{\mathbf{Y}}(y)\}_{y \in Y}$.

Now we are ready to describe the *correctness* and *security* requirements that a time-bound hierarchical key assignment scheme has to satisfy.

Correctness. *Each user can compute the key held by any class lower down in the hierarchy for each time period in which it belongs to its class.*
Formally, for each class $v \in V$, each class $u \in A_v$, each time sequence $\lambda \in \mathcal{P}$, and each time period $t \in \lambda$, it holds that $H(\mathbf{K}_{u,t} | \mathbf{S}_{v,\lambda}) = 0$.

Notice that the correctness requirement is equivalent to saying that the values of the private information $s_{v,\lambda}$ held by each user belonging to a class $v \in V$ for a time sequence $\lambda \in \mathcal{P}$ correspond to a unique value of the key $k_{u,t}$, for each class $u \in A_v$ and each time period $t \in \lambda$.

As regards as the security requirement, for each class $u \in V$ and each time period $t \in T$, the key $k_{u,t}$ should be protected against a coalition of users belonging to each class v such that $u \notin A_v$ in all time periods, and users belonging to each class w such that $u \in A_w$ in all time periods but t. We denote by $F_{u,t}$ the set of all pairs (class, time-sequence) whose credentials do not allow to compute the key $k_{u,t}$. Formally, $F_{u,t} = \{(v, \lambda) \in V \times \mathcal{P}\colon\ u \notin A_v$ or $t \notin \lambda\}$. Given a set $X = \{(v_1, \lambda_1), \ldots, (v_\ell, \lambda_\ell)\} \subseteq F_{u,t}$, we denote by S_X the set $S_{v_1,\lambda_1} \times \cdots \times S_{v_\ell,\lambda_\ell}$. We consider two different security goals: security with respect to *key indistinguishability* and security against *key recovery*. Security with respect to key indistinguishability formalizes the requirement that the adversary coalition is not able *to learn any information* about a key that it should not have access to, i.e., it is not able to distinguish it from a random string having the same length. On the other hand, security against key recovery corresponds to the requirement that an adversary coalition is not able to *compute* a key that it should not have access to. In order to capture both the above security requirements with a single formal definition having different meanings, we use a parameter α, where $0 \leqslant \alpha \leqslant 1$.

Security. *Each coalition of users* cannot compute/have absolutely no information about *each key the coalition is not entitled to obtain.*
Formally, for each class $u \in V$, each time period $t \in T$, and each coalition $X \subseteq F_{u,t}$, it holds that $H(\mathbf{K}_{u,t}|\mathbf{S}_X) \geqslant \alpha \cdot H(\mathbf{K}_{u,t})$.

Notice that when $\alpha = 1$, the above requirement formalizes security with respect to *key indistinguishability* and is equivalent to saying that the probability that the unauthorized key is equal to $k_{u,t}$, given the values of the private information s_X held by the users in the coalition, is the same as the a priori probability that the key is $k_{u,t}$, i.e., the random variables $\mathbf{K}_{u,t}$ and $\mathbf{S}_X$ are statistically independent. On the other hand, if $0 < \alpha < 1$, the requirement formalizes security against *key recovery* and is equivalent to saying that the coalition is not able to *compute* the unauthorized key $k_{u,t}$, but could obtain some *partial information* about it, for example, it could be able to compute part of the key. Clearly, if $\alpha = 0$, there is no security requirement, since the conditional entropy of $\mathbf{K}_{u,t}$ given $\mathbf{S}_X$ is always greater than or equal to zero.

A time-bound hierarchical key assignment scheme satisfying the above correctness and security requirements, for a parameter $0 \leqslant \alpha \leqslant 1$, is called an *$\alpha$-unconditionally secure scheme*. The case $\alpha = 1$ has been analyzed in [8,10] for key assignment schemes without time constraints.

3. A tight lower bound

In the following we show a tight lower bound on the size of the private information distributed to each user in any α-unconditionally secure time-bound hierarchical key assignment scheme. We will use the next definition.

Definition 1. Let $G = (V, E)$ be a directed acyclic graph representing a partially ordered hierarchy, let T be a sequence of distinct time periods, let $\mathcal{P}$ be the interval-set over T, and let $0 \leqslant \alpha \leqslant 1$. In any α-unconditionally secure time-bound hierarchical key assignment scheme for G and T, a sequence $((u_1, t_1), \ldots, (u_\ell, t_\ell))$ of pairs in $V \times T$ is called *well-ordered* if either $\ell = 1$, or $\ell > 1$ and for each $j = 2, \ldots, \ell$, it holds that $\{(u_i, t_i)\colon\ 1 \leqslant i \leqslant j-1\} \subseteq F_{u_j,t_j}$.

The next lemma will be a useful tool to prove our results.

Lemma 1. *Let $G = (V, E)$ be a directed acyclic graph representing a partially ordered hierarchy, let T be a sequence of distinct time periods, let $\mathcal{P}$ be the interval-set over T, and let $0 \leqslant \alpha \leqslant 1$. In any α-unconditionally secure time-bound hierarchical key assignment scheme for G and T, if $((u_1, t_1), \ldots, (u_\ell, t_\ell))$ is a well-ordered sequence of pairs in $V \times T$, then it holds that*

$$H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_\ell,t_\ell}) \geqslant H(\mathbf{K}_{u_1,t_1}) + \alpha \cdot \sum_{j=2}^{\ell} H(\mathbf{K}_{u_j,t_j}).$$

Proof. Let $X_j = \{(u_i, t_i)\colon\ 1 \leqslant i \leqslant j-1\}$, for any $j = 2, \ldots, \ell$. Since $((u_1, t_1), \ldots, (u_\ell, t_\ell))$ is a well-ordered sequence of pairs in $V \times T$, from Definition 1 we have that, $X_j \subseteq F_{u_j,t_j}$. Therefore, from the security requirement it holds that

$$H(\mathbf{K}_{u_j,t_j}|\mathbf{S}_{X_j}) \geqslant \alpha \cdot H(\mathbf{K}_{u_j,t_j}). \tag{1}$$

From the correctness requirement it holds that $H(\mathbf{K}_{u_i,t_i}|\mathbf{S}_{u_i,t_i}) = 0$ and from (11) of Appendix A we have that

$$H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{S}_{X_j}) \leqslant \sum_{i=1}^{j-1} H(\mathbf{K}_{u_i,t_i}|\mathbf{S}_{X_j}) \leqslant \sum_{i=1}^{j-1} H(\mathbf{K}_{u_i,t_i}|\mathbf{S}_{u_i,t_i}) = 0.$$

Hence, from (10) of Appendix A it follows that

$$H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{K}_{u_j,t_j}\mathbf{S}_{X_j}) \leqslant H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{S}_{X_j}) = 0. \tag{2}$$

Consider the mutual information $I(\mathbf{K}_{u_j,t_j}; \mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{S}_{X_j})$. From (9) of Appendix A it holds that

$$\begin{aligned} &H(\mathbf{K}_{u_j,t_j}|\mathbf{S}_{X_j}) - H(\mathbf{K}_{u_j,t_j}|\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}\mathbf{S}_{X_j}) \\ &\quad = H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{S}_{X_j}) \\ &\qquad - H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}|\mathbf{K}_{u_j,t_j}\mathbf{S}_{X_j}). \end{aligned} \tag{3}$$

Hence, from (2) and (3) it follows that

$$H(\mathbf{K}_{u_j,t_j}|\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}\mathbf{S}_{X_j}) = H(\mathbf{K}_{u_j,t_j}|\mathbf{S}_{X_j}). \tag{4}$$

Therefore, from (7) of Appendix A it holds that

$$\begin{aligned} &H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_\ell,t_\ell}) \\ &\quad = H(\mathbf{K}_{u_1,t_1}) + \sum_{j=2}^{\ell} H(\mathbf{K}_{u_j,t_j}|\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}) \\ &\quad \geqslant H(\mathbf{K}_{u_1,t_1}) + \sum_{j=2}^{\ell} H(\mathbf{K}_{u_j,t_j}|\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{j-1},t_{j-1}}\mathbf{S}_{X_j}) \\ &\qquad \big(\text{from (10) of Appendix A}\big) \\ &\quad = H(\mathbf{K}_{u_1,t_1}) + \sum_{j=2}^{\ell} H(\mathbf{K}_{u_j,t_j}|\mathbf{S}_{X_j}) \quad \big(\text{from (4)}\big) \\ &\quad \geqslant H(\mathbf{K}_{u_1,t_1}) + \alpha \cdot \sum_{j=2}^{\ell} H(\mathbf{K}_{u_j,t_j}) \quad \big(\text{from (1)}\big). \qquad \square \end{aligned}$$

The next theorem shows a lower bound on the size of the private information distributed to each user. Such a result applies to the general case of arbitrary entropies of keys, but, for the sake of simplicity, we consider the case when all entropies of keys are equal. We denote this common entropy by $H(\mathbf{K})$.

Theorem 1. *Let $G = (V, E)$ be a directed acyclic graph representing a partially ordered hierarchy, let T be a sequence of distinct time periods, let $\mathcal{P}$ be the interval-set over T, and let*

Let $G = (V, E)$ be a directed acyclic graph representing a partially ordered hierarchy, let T be a sequence of distinct time periods, let $\mathcal{P}$ be the interval-set over T, and let $0 \leqslant \alpha \leqslant 1$ be a rational number, say $\alpha = a/b$, with a and b integers and $b \neq 0$. Moreover, let $q \geqslant 1$.

Initialization

1. If $a \neq b$, the TA randomly chooses a string $\eta \in \{0,1\}^{(b-a)\cdot q}$; if $a = b$, let η be the empty string;
2. Afterwards, if $a \neq 0$, for any class $u \in V$ and any time period $t \in T$, the TA randomly chooses a string $k'_{u,t} \in \{0,1\}^{a\cdot q}$; if $a = 0$, let $k'_{u,t}$ be the empty string;
3. Then, the TA computes the key $k_{u,t} = \eta \| k'_{u,t}$, where $\|$ denotes string concatenation;
4. When a user is assigned to a class $u \in V$ for a time sequence $\lambda \in \mathcal{P}$, the TA delivers to the user, by means of a secure channel, the private information $s_{u,\lambda}$, containing the string η, as well as the string $k'_{v,t}$, for any class $v \in A_u$ and any time period $t \in \lambda$.

Key derivation

Each user belonging to a class $u \in V$ for a time sequence $\lambda \in \mathcal{P}$ can use its private information $s_{u,\lambda}$ to compute the key $k_{v,t} = \eta \| k'_{v,t}$ for any class $v \in A_u$ and any time period $t \in \lambda$, since both strings η and $k'_{v,t}$ are contained in $s_{u,\lambda}$.

Fig. 1. An α-unconditionally secure key assignment scheme.

$0 \leqslant \alpha \leqslant 1$. *In any α-unconditionally secure time-bound hierarchical key assignment scheme for G and T, for any pair $(u, \lambda) \in V \times \mathcal{P}$, it holds that*

$$H(\mathbf{S}_{u,\lambda}) \geqslant \bigl(1 - \alpha + \alpha \cdot |A_u| \cdot |\lambda|\bigr) \cdot H(\mathbf{K}),$$

where $|\lambda|$ denotes the number of time periods in the time sequence λ.

Proof. Let u be a class and consider the directed acyclic graph $G' = (V', E')$ induced by G and involving all the classes in $A_u = V'$. Moreover, let $(u_{|A_u|}, \ldots, u_1)$ be the sequence of classes output by the topological sorting on G'. This sequence has the property that for each pair of classes u_i, $u_j \in A_u$ such that $(u_j, u_i) \in E'$, the class u_j appears before that u_i in the ordering. Notice that class $u_{|A_u|}$ corresponds to class u. Let $\lambda = (t_1, \ldots, t_{|\lambda|})$ be a time sequence. It is easy to see that the sequence of pairs $((u_1, t_1), \ldots, (u_1, t_{|\lambda|}), \ldots, (u_{|A_u|}, t_1), \ldots, (u_{|A_u|}, t_{|\lambda|}))$ is well-ordered. Therefore, from (11) of Appendix A and from the correctness requirement, we have that

$$\begin{aligned} H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}} | \mathbf{S}_{u,\lambda}) &\leqslant \sum_{i=1}^{|A_u|} \sum_{j=1}^{|\lambda|} H(\mathbf{K}_{u_i,t_j} | \mathbf{S}_{u,\lambda}) \\ &\leqslant \sum_{i=1}^{|A_u|} \sum_{j=1}^{|\lambda|} H(\mathbf{K}_{u_i,t_j} | \mathbf{S}_{u_i,t_j}) \\ &= 0. \end{aligned} \tag{5}$$

Consider the mutual information $I(\mathbf{S}_{u,\lambda}; \mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}})$. From (8) of Appendix A we have that

$$\begin{aligned} &H(\mathbf{S}_{u,\lambda}) - H(\mathbf{S}_{u,\lambda} | \mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}}) \\ &\quad = H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}}) - H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}} | \mathbf{S}_{u,\lambda}). \end{aligned} \tag{6}$$

Since $H(\mathbf{S}_{u,\lambda} | \mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}}) \geqslant 0$, from (5) and (6) it follows that

$$H(\mathbf{S}_{u,\lambda}) \geqslant H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}}).$$

From Lemma 1 we get

$$\begin{aligned} H(\mathbf{K}_{u_1,t_1} \ldots \mathbf{K}_{u_{|A_u|},t_{|\lambda|}}) &\geqslant H(\mathbf{K}) + \alpha \cdot \bigl(|A_u| \cdot |\lambda| - 1\bigr) \cdot H(\mathbf{K}) \\ &= (1 - \alpha + \alpha \cdot |A_u| \cdot |\lambda|) \cdot H(\mathbf{K}). \end{aligned}$$

Hence, the theorem follows. □

4. An optimal protocol

The bound of Theorem 1 is tight. Indeed, in Fig. 1 we describe an α-unconditionally secure key assignment scheme which meets it with equality.

In the following we show that the scheme of Fig. 1 satisfies the security requirement. Indeed, let $u \in V$ be a class, $t \in T$ be a time period, and $X \subseteq F_{u,t}$ be a coalition of corrupted users trying to compute the key $k_{u,t}$. We distinguish two cases:

1. Case $\alpha = 1$.
   The key $k_{u,t}$ is independent from the private information s_X held by the coalition, hence, the corrupted users have absolutely no information about $k_{u,t}$.
2. Case $0 < \alpha < 1$.
   The key $k_{u,t}$ is equal to $\eta \| k'_{u,t}$. Since the string η is part of the private information s_X and the string $k'_{u,t}$ is randomly chosen by the TA, the uncertainty on $\mathbf{K}_{u,t}$, given $\mathbf{S}_X$, is equal to the uncertainty on $\mathbf{K}'_{u,t}$. Since $H(\mathbf{K}'_{u,t}) = a \cdot q$ and $H(\mathbf{K}_{u,t}) = b \cdot q$, it follows that $H(\mathbf{K}_{u,t} | \mathbf{S}_X) = \alpha \cdot H(\mathbf{K}_{u,t})$.

It is easy to see that the scheme of Fig. 1 meets the bound of Theorem 1 with equality. Consider a user belonging to a class $u \in V$ for a time sequence $\lambda \in \mathcal{P}$. If $\alpha = 1$, the size of the private information $s_{u,\lambda}$ is equal to $|A_u| \cdot |\lambda| \cdot a \cdot q$ bits, whereas, the size of each key is equal to $a \cdot q$ bits. On the other hand, when $\alpha = 0$, $s_{u,\lambda}$ contains a key, having size $b \cdot q$ bits, which is the same for each class and each time period. Finally, if $0 < \alpha < 1$, $s_{u,\lambda}$ consists of $(b - a + a \cdot |A_u| \cdot |\lambda|) \cdot q$ bits, whereas, the size of each key is equal to $b \cdot q$ bits.

Appendix A

In this appendix we review the basic concepts of Information Theory used in our definitions and proofs. For a complete treatment of the subject the reader is advised to consult [6].

Given a probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x\in X}$ on a set X, we define the *entropy*[1] of $\mathbf{X}$, $H(\mathbf{X})$, as

$$H(\mathbf{X}) = -\sum_{x\in X} Pr_{\mathbf{X}}(x)\log Pr_{\mathbf{X}}(x).$$

The entropy satisfies the following property

$$0 \leqslant H(\mathbf{X}) \leqslant \log|X|,$$

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 $x \in X$.

Given two sets X and Y and a joint probability distribution on their Cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$, is defined as

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

From the definition of conditional entropy it is easy to see that

$$H(\mathbf{X}|\mathbf{Y}) \geqslant 0.$$

Given n sets $X_1,\ldots,X_n$ and a joint probability distribution on their Cartesian product, the entropy of $\mathbf{X}_1\ldots\mathbf{X}_n$ can be expressed as

$$H(\mathbf{X}_1\ldots\mathbf{X}_n) = H(\mathbf{X}_1) + \sum_{i=2}^{n} H(\mathbf{X}_i|\mathbf{X}_1\ldots\mathbf{X}_{i-1}).$$

Given $n+1$ sets $X_1,\ldots,X_n,Y$ and a joint probability distribution on their Cartesian product, the entropy of $\mathbf{X}_1\ldots\mathbf{X}_n$ given $\mathbf{Y}$ can be expressed as

$$H(\mathbf{X}_1\ldots\mathbf{X}_n|\mathbf{Y}) = H(\mathbf{X}_1|\mathbf{Y}) + \sum_{i=2}^{n} H(\mathbf{X}_i|\mathbf{X}_1\ldots\mathbf{X}_{i-1}\mathbf{Y}). \quad (7)$$

The *mutual information* $I(\mathbf{X};\mathbf{Y})$ between $\mathbf{X}$ and $\mathbf{Y}$ is defined by

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) \quad (8)$$

and satisfies the following properties:

$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{Y};\mathbf{X})$$

and $I(\mathbf{X};\mathbf{Y}) \geqslant 0$, from which one gets

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

Given three sets X, Y, Z and a joint probability distribution on their Cartesian product, the *conditional mutual information* $I(\mathbf{X};\mathbf{Y}|\mathbf{Z})$ between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ is

$$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Z}\mathbf{Y}) \quad (9)$$

and satisfies the following properties:

$$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = I(\mathbf{Y};\mathbf{X}|\mathbf{Z})$$

and $I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) \geqslant 0$. Since the conditional mutual information is always non-negative we get

$$H(\mathbf{X}|\mathbf{Z}) \geqslant H(\mathbf{X}|\mathbf{Z}\mathbf{Y}). \quad (10)$$

From (7) and (10) one easily gets that for any sets $Y, X_1,\ldots,X_n$ and a joint probability distribution on their Cartesian product it holds that

$$\sum_{i=1}^{n} H(\mathbf{X}_i|\mathbf{Y}) \geqslant H(\mathbf{X}_1\mathbf{X}_2\ldots\mathbf{X}_n|\mathbf{Y}). \quad (11)$$

References

[1] Mikhail J. Atallah, Marina Blanton, Keith B. Frikken, Incorporating temporal capabilities in existing key management schemes, in: ESORICS, 2007, pp. 515–530.

[2] G. Ateniese, A. De Santis, A.L. Ferrara, B. Masucci, Provably-secure time-bound hierarchical key assignment schemes, in: Proc. of the ACM Conference on Computer and Communications Security, 2006, pp. 288–297.

[3] Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, Provably-secure time-bound hierarchical key assignment schemes, J. Cryptology 25 (2) (2012) 243–270.

[4] Elisa Bertino, Barbara Carminati, Elena Ferrari, A temporal key management scheme for secure broadcasting of XML documents, in: Proc. of the ACM Conference on Computer and Communications Security, 2002, pp. 31–40.

[5] Hung-Yu Chien, Efficient time-bound hierarchical key assignment scheme, IEEE Transaction on Knowledge and Data Engineering 16 (10) (2004) 1301–1304.

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

[7] Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, Enforcing the security of a time-bound hierarchical key assignment scheme, Information Sciences 176 (12) (2006) 1684–1694.

[8] Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, Unconditionally secure key assignment schemes, Discrete Applied Mathematics 154 (2) (2006) 234–252.

[9] Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, New constructions for provably-secure time-bound hierarchical key assignment schemes, Theoretical Computer Science 407 (1–3) (2008) 213–230.

[10] Anna Lisa Ferrara, Barbara Masucci, An information-theoretic-approach to the access control problem, in: Carlo Blundo, Cosimo Laneve (Eds.), ICTCS, in: Lecture Notes in Computer Science, vol. 2841, Springer, 2003, pp. 342–354.

[11] H.F. Huang, C.C. Chang, A new cryptographic key assignment scheme with time-constraint access control in a hierarchy, Computer Standards & Interfaces 26 (2004) 159–166.

[12] W.-G. Tzeng, A time-bound cryptographic key assignment scheme for access control in a hierarchy, IEEE Transactions on Knowledge and Data Engineering 14 (1) (2002) 182–188.

[13] W.-G. Tzeng, A secure system for data access based on anonymous and time-dependent hierarchical keys, in: Proc. of the ACM Symposium on Information, Computer and Communications Security, 2006, pp. 223–230.

[14] S.-Y. Wang, C. Laih, Merging: An efficient solution for a time-bound hierarchical key assignment scheme, IEEE Transactions on Dependable and Secure Computing 3 (1) (2006) 91–100.

[15] J. Yeh, An RSA-based time-bound hierarchical key assignment scheme for electronic article subscription, in: Proc. of the ACM CIKM International Conference on Information and Knowledge Management, 2005, pp. 285–286.

[16] X. Yi, Security of chien's efficient time-bound hierarchical key assignment scheme, IEEE Transactions on Knowledge and Data Engineering 17 (9) (2005) 1298–1299.

[1] All log's in this paper denote basis 2 logarithms.