Modeling Costs of Access Control with Various Key Management Systems

Yamasaki, Tomomi
Graduate School of Information Science and Electrical Engineering, Kyushu University

Inenaga, Shunsuke
Graduate School of Information Science and Electrical Engineering, Kyushu University

Ikeda, Daisuke
Graduate School of Information Science and Electrical Engineering, Kyushu University

Yasuura, Hiroto
Graduate School of Information Science and Electrical Engineering, Kyushu University

出版情報：International Conference on Parallel and Distributed Processing Techniques and Applications. 2009, pp.676-682, 2009-07
バージョン：
権利関係：

Modeling Costs of Access Control with Various Key Management Systems

Tomomi Yamasaki, Shunsuke Inenaga, Daisuke Ikeda, and Hiroto Yasuura
Graduate School of Information Science and Electrical Engineering, Kyushu University,
744 Motooka, Fukuoka 819-0395, Japan

Abstract—*Access control, a task of managing permission or denial to the use of particular resources by particular entities, is achieved by credentials such as passwords and physical keys. Although security of access control has extensively been studied, researchers have not paid much attention to comparing costs of the systems with different credentials. This paper provides a general model of* door-key management systems *for access control, where a* door *represents a resource to control access and a* key *does a credential. We show door-key management systems based on smart cards, biometrics, metal keys, and passwords will well fit to our model. Then, we introduce management costs to the proposed model. Finding the best door-key management system in terms of minimum management cost is a hard task, since different systems have different restrictions. We present a general algorithm that computes the minimum cost of door-key management systems with different types of keys.*

Keywords: access control, door-key management system, deterministic finite state machine, cost evaluation

1. Introduction

Access control, a task of managing permission or denial to the use of a particular resource by a particular entity, has been critical in human society. Considered resources to control access are in a wide range from physical resources, such as secure rooms, to digital resources, such as computer files.

Access control is achieved with credentials, and in fact there exist many kinds of credentials we can use for access control. For instance a physical key is a classical, yet practical, credential for physical access control, and an electronic key has become popular as a credential. Using electronic credentials offers us more sophisticated physical access control, as well as it also improves security. We are at the stage where a variety of possible credentials are available for access control.

However, this fact poses a new challenging problem in access control: How can we select the most suitable type of credential for a particular measure such as access control management costs? Here we mean by the costs the burden of the administrator of the system to manage some changes in the security policy, e.g., making a particular person able to enter a secure room. Note that these kinds of costs are heavily dependent on the type of credentials and hence they are not negligible at all. In fact, it is reported that using some sorts of electronic credential has increased the costs of the administrators to maintain the access control policy [1].

However, to the best of our knowledge, there exist no researches considering to reduce or estimate the costs of access control, although we can find many researches on security of (digital) access control systems [2], [3] and many services of identity and access management, such as Microsoft Identity and Access Management, and that of physical access control systems with some fixed type of credentials, such as biometrics. In the existing researches, services, and systems, we do not need to consider the cost of access control management because every cost of changing the security policy is the same. For instance, in a digital access control system, the costs for making some person both able and disable to access some resource are the same, because they are completed by modifying entries of an access control database. Therefore, it is important to compare costs among access control with different types of credentials. But, we can find no general approaches to evaluate such costs.

In this paper, we first formalize a model of access control in which a *door* represents a resource to protect. The model is based on a deterministic finite state machine in which each state represents a binary relation between doors and users. We define two types of requests in the model, one of which enables users to open doors, and the other disables users from opening doors. Then, we propose a model of *door-key management systems* in which a *key* represents a credential. This model is based on another deterministic finite state machine, in which each state represents a pair of binary relations between doors and keys, and between keys and users. We define four unit operations in the model, to enable keys to unlock doors, to disable keys from unlocking doors, to issue keys to users, and to collect keys from users. We show that electronic door-key systems using smart cards, biometrics, metal keys, and passwords all well fit in our model.

The access control model we propose describes a policy of access control and a door-key management system model is an implementation of the policy using keys as credentials. The separation of the door-key management system from the access control policy enables us to uniformly evaluate the

costs of implementations with different types of keys.

We then consider how to evaluate the minimum cost for a given request when some changes occur in the access control policy. We emphasize this problem of computing the minimum cost is not as easy as it may sound, as the cost varies with the door-key management system. Section 3 will discuss it in more details. We present a general algorithm to solve the problem for any type of door-key management systems, by reduction to the single-source shortest path problem of a directed graph [4].

2. Modeling Door Access Control and Door-Key Management

We firstly propose a model of door access control in Section 2.1, which represents the access control policy to doors. Then in Section 2.2, we introduce a model of door-key management systems that implement the door access control using keys as credentials of users to access doors. Section 2.3 shows that the above model is general enough to deal with different types of keys such as smart cards, biometrics, metal keys and passwords.

2.1 Door Access Control

In this section, we consider a model of door access control where the task is to maintain a binary relation between doors and users. Here the binary relation implies that the doors may be opened by the users. We model door access control based on a deterministic finite state machine where each state represents each binary relation.

Definition 1 (Door Access Control) *A* door access control *is a tuple* (D, U, M) *such that* D *is a finite set of* doors, U *is a finite set of* users, *and* M *is a deterministic finite state machine* (Q, Σ, δ, q_0) *where*

- $Q = 2^{D\times U}$ *is the set of states,*
- $\Sigma = \{\mathtt{gr}, \mathtt{re}\} \times 2^{D\times U}$ *is the input alphabet,*
- $\delta : Q \times \Sigma \to Q$ *is the transition function, and*
- $q_0 \in Q$ *is the initial state.*

Each state $q \in Q$ represents a policy of door access control. Let $d \in D$ and $u \in U$. If $(d, u) \in q$, then we say that the user u may *open* the door d in the state q. If $(d, u) \notin q$, then we say that user u must not open the door d in the state q.

Each element of the alphabet $\Sigma = \{\mathtt{gr}, \mathtt{re}\} \times 2^{D\times U}$ is called a *request* to change the policy of door access control, that is, to transit to another state. Namely, `gr` represents a request of enabling users to open doors. For instance, $(\mathtt{gr}, \{(u, d)\})$ is a request of enabling the user u to open the door d. On the other hand, `re` represents a request of disabling users from opening doors. For instance, $(\mathtt{re}, \{(u, d)\})$ is a request of disabling the user u from opening the door d.

The transition function δ is defined below:

Definition 2 (Transition Function δ) *For any states* $p, q \in Q$,

$$\delta(p, (\mathtt{gr}, q - p)) = q \quad \text{if } p \subset q \text{ and}$$
$$\delta(p, (\mathtt{re}, p - q)) = q \quad \text{if } p \supset q.$$

The above definition implies that we only consider a `gr` request which "newly" enables at least one user to open at least one door. Similarly, we only consider a `re` request which "newly" disables at least one user from opening at least one door.

Fig. 1 illustrates the finite state machine M of the door access control $(\{d\}, \{u_1, u_2\}, M)$, where $q_0 = \emptyset$.

In the sequel we assume D and U are fixed.

2.2 Door-Key Management System

Consider how to implement the door access control of Definition 1. A natural, yet practical, solution is to use *keys* as mediums of the right of users to open doors. We maintain a binary relation between doors and users using two binary relations between doors and keys, and between keys and users.

Definition 3 (Door-Key Management System) *A* door-key management system *is a quadruple* (D, K, U, M_K) *such that* D *is a finite set of* doors, K *is a finite set of* keys, U *is a finite set of* users, *and* M_K *is a deterministic finite state machine* $(Q_K, \Sigma_K, \delta_K, q_{K0})$ *where*

- $Q_K \subseteq 2^{D\times K} \times 2^{K\times U}$ *is the set of states,*
- $\Sigma_K \subseteq (\{\mathtt{ac}, \mathtt{in}\} \times 2^{D\times K}) \cup (\{\mathtt{is}, \mathtt{co}\} \times 2^{K\times U})$ *is the input alphabet,*
- $\delta_K : Q_K \times \Sigma_K \to Q_K$ *is the transition function, and*
- $q_{K0} \in Q_K$ *is the initial state.*

We call each element $q_K \in Q_K$ a *k-state*, to tell it from a state $q \in Q$ of the door access control.

Let $d \in D$, $k \in K$ and $u \in U$. Let $q_K \in Q_K$, and denote $q_K = (q_{K_a}, q_{K_b})$. Then $q_{K_a} \subseteq D \times K$ and $q_{K_b} \subseteq K \times U$. If $(d, k) \in q_{K_a}$, then we say that the key k can *unlock* the door d in the k-state q_K. If $(d, k) \notin q_{K_a}$, then we say that the key k cannot unlock the door d in the k-state q_K. If $(k, u) \in q_{K_b}$, then we say that the user u *has* the key k in the k-state q_K. If $(k, u) \notin q_{K_b}$, then we say that the user u does not have the key k in the k-state q_K.

Each element of the alphabet $\Sigma_K \subseteq \{\mathtt{ac}, \mathtt{in}\} \times 2^{D\times K} \cup \{\mathtt{is}, \mathtt{co}\} \times 2^{K\times U}$ is called an *operation*. Here, `ac` represents an operation of enabling keys to unlock doors, `in` represents an operation of disabling keys from unlocking doors, `is` represents an operation of issuing keys to users, and `co` represents an operation of collecting keys from users.

We define the transition function δ_K in a somewhat similar way to the transition function δ of Definition 2.

Definition 4 (Transition Function δ_K) *For any k-states*

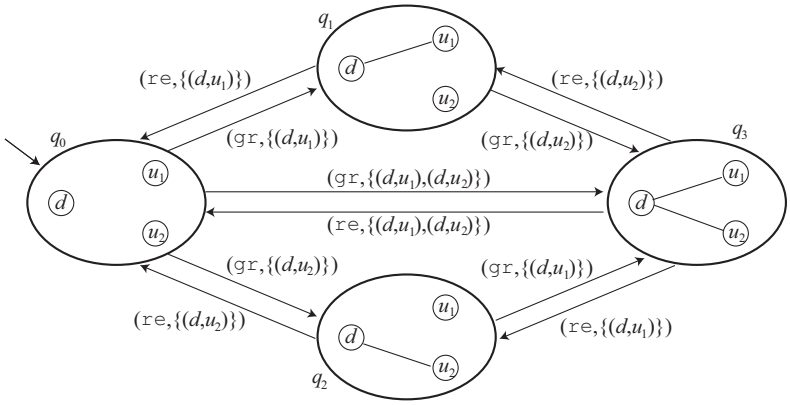

Fig. 1: The finite state machine M of the door access control $(\{d\}, \{u_1, u_2\}, M)$, where $q_0 = \emptyset$. Each state consisting of a binary relation between $\{d\}$ and $\{u_1, u_2\}$ is represented by a bipartite graph.

$p_K = (p_{K_a}, p_{K_b}), q_K = (q_{K_a}, q_{K_b}) \in Q_K$,

$\delta_K(p_K, (\mathtt{ac}, q_{K_a} - p_{K_a})) = q_K$ *if* $p_{K_a} \subset q_{K_a}, p_{K_b} = q_{K_b}$,
$\delta_K(p_K, (\mathtt{in}, p_{K_a} - q_{K_a})) = q_K$ *if* $p_{K_a} \supset q_{K_a}, p_{K_b} = q_{K_b}$,
$\delta_K(p_K, (\mathtt{is}, q_{K_b} - p_{K_b})) = q_K$ *if* $p_{K_b} \subset q_{K_b}, p_{K_a} = q_{K_a}$,
$\delta_K(p_K, (\mathtt{co}, p_{K_b} - q_{K_b})) = q_K$ *if* $p_{K_b} \supset q_{K_b}, p_{K_a} = q_{K_a}$.

See Fig. 2 which illustrates an example of the finite state machine M of the door access control $(\{d\}, \{k\}, \{u_1, u_2\}, M_K)$, where $q_{K0} = \emptyset$.

Now we consider the correspondence between a k-state of a door-key management system and a state of the door access control.

Definition 5 (Function ζ from K-States to States) *Let $q_K = (q_{K_a}, q_{K_b})$ be any k-state in Q_K and q any state in Q, respectively. Define a binary relation $R \subseteq D \times U$ such that $(d, u) \in R$ iff $(d, k) \in q_{K_a}$ and $(k, u) \in q_{K_b}$ for some $k \in K$. If $R = q$, then we denote $\zeta(q_K) = q$.*

If $\zeta(q_K) = q$, we say that the k-state q_K in a door-key management system (D, K, U, M_K) *corresponds* to the state q in the door access control (D, U, M). Note that ζ may be a many-to-one function, that is, more than one k-state in Q_K may correspond to a state in Q. For the door access control of Fig. 1 and the door-key management system of Fig. 2, we have that $\zeta(q_{K0}) = \zeta(q_{K1}) = \zeta(q_{K2}) = \zeta(q_{K3}) = \zeta(q_{K5}) = q_0$, $\zeta(q_{K4}) = q_1$, $\zeta(q_{K6}) = q_2$, and $\zeta(q_{K7}) = q_3$.

Consider to implement the door access control using a door-key management system. In so doing, the following extended version of the transition function δ_K is useful.

Definition 6 (Extended Transition Function δ_K) *For any k-state $q_K \in Q_K$,*

$\delta_K(q_K, \varepsilon) = q_k$ *for the empty sequence* ε,
$\delta_K(q_K, z\beta) = \delta_K(\delta_K(q_K, z), \beta)$ *for any* $z \in \Sigma_K$, $\beta \in \Sigma_K^*$.

We say that a door-key management system *implements* the door access control if

(1) ζ is a surjection, and
(2) for any $p, q \in Q$ such that $\delta(p, r) = q$ with some $r \in \Sigma$, there exists $(p_K, q_K) \in Q_K$ such that $\zeta(p_K) = p$, $\zeta(q_K) = q$, and $\delta_K(p_K, s) = q_K$ with some $s \in \Sigma_K^*$.

Note the door-key management system of Fig. 2 implements the door access control of Fig. 1.

The following proposition gives the lower bound for the number of keys for a door-key management system to implement the door access control.

Proposition 1 *Any door-key management system (D, K, U, M_K) implements the door access control (D, U, M) only if $|K| \geq \min\{|D|, |U|\}$.*

Proof. Assume $|D| \leq |U|$. Consider state $q = \{(d_i, u_i) \mid 1 \leq i \leq |D|, d_i \neq d_{i+1}\} \cup \{(d_{|D|}, u_\ell) \mid |D| + 1 \leq \ell \leq |U|, u_\ell \neq u_{\ell+1}\}$. If $|K| < |U|$, due to the pigeonhole principle (refer to e.g. [5]), no k-states in Q_K correspond to q. The case $|D| > |U|$ can be shown similarly. □

By Proposition 1 we will only consider door-key management systems with $|K| \geq \min\{|D|, |U|\}$.

2.3 Modeling Real-World Door-Key Management Systems

In this section we describe real-world door-key management systems based on our general door-key management system model of Definition 3.

Definition 7 *A* smart-card-based door-key management system *is a door-key management system of Definition 3 with the following restrictions:*

1) For any $q_K = (q_{K_a}, q_{K_b}) \in Q_K$, let $(k, u) \in q_{K_b}$. Then for any $u' \neq u$ it holds that $(k, u') \notin q_{K_b}$.
2) $\Sigma_K = (\{\mathtt{ac}, \mathtt{in}\} \times D \times K) \cup (\{\mathtt{is}, \mathtt{co}\} \times K \times U)$.

Condition 1 implies that at every k-state each key is not shared by two or more users. That is, for each smart card

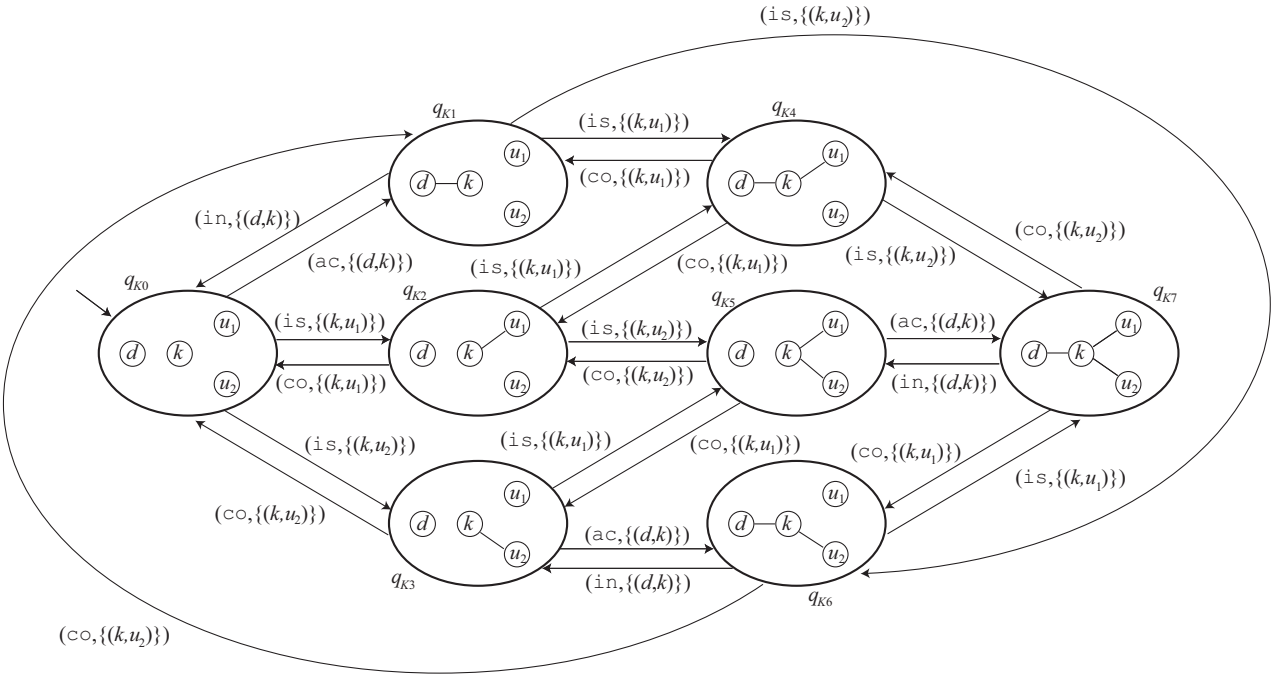

Fig. 2: The finite state machine M_K of the door access control $(\{d\}, \{k\}, \{u_1, u_2\}, M_K)$, where $Q_K = 2^{\{d\}\times\{k\}} \cup 2^{\{k\}\times\{u_1,u_2\}}$, $\Sigma_K = \{\mathtt{ac}, \mathtt{in}\} \times (\{d\} \times \{k\}) \cup \{\mathtt{is}, \mathtt{co}\} \times (\{k\} \times \{u_1, u_2\})$ and $q_{K0} = \emptyset$. Each k-state consisting of a pair of binary relations between $\{d\}$ and $\{k\}$, and between $\{k\}$ and $\{u_1, u_2\}$ is represented by a tripartite graph.

there is a unique user who has it. This describes a smart card often contains personal information of the user which is not shared by other users. Condition 2 implies that at a single step of the system we can make an operation to a single pair of a door and a key, or of a key and a user.

Definition 8 *A* biometrics-based door-key management system *is a door-key management system of Definition 3 with the following restrictions:*

1) *For any $q_K = (q_{K_a}, q_{K_b}) \in Q_K$ and any $u \in U$, there exists $k \in K$ such that $(k, u) \in q_{K_b}$.*
2) *For any $q_K = (q_{K_a}, q_{K_b}) \in Q_K$ and for any $(k, u), (k', u') \in q_{K_b}$ with $u \neq u'$, it holds that $k \neq k'$.*
3) *For any $p_K = (p_{K_a}, p_{K_b}), q_K = (q_{K_a}, q_{K_b}) \in Q_K$, it holds that $p_{K_b} = q_{K_b}$.*
4) *$\Sigma_K = \{\mathtt{ac}, \mathtt{in}\} \times D \times K$.*

Condition 1 implies that at any k-state, every user has at least one key. This describes that each user has at least one biometric key such as fingerprints, iris, and hand vein patterns. Condition 2 implies that at any k-state, no key is shared by two or more users. This describes the uniqueness of biometric keys. Condition 3 implies that at any k-states, the binary relation between keys and users is identical. This describes the permanency of biometric keys. Condition 4 implies that a single operation either enables or disables a key from unlocking a door. From the other conditions it is clear that there is no transition with `is` or `co` operations. This assumes that biometric keys cannot be given to or taken from a user afterwards.

Definition 9 *A* metal door-key management system *is a door-key management system of Definition 3 with the following restriction:*

1) *$\Sigma_K = (\{\mathtt{ac}\} \times D \times K) \cup (\{\mathtt{is}, \mathtt{co}\} \times K \times U) \cup \big(\bigcup_{q_K \in Q_K, d \in D}(\{\mathtt{in}\} \times \{(d, k) \in q_{K_a}\})\big)$.*

Condition 1 implies that a single operation enables a key to unlock a door, issues a key to a user, or collects a key from a user. A special `in` operation implies that at any k-state all keys which can unlock the same door are disabled at once. This describes that if a key hole of a door is changed, then all metal keys associated with the old key hole become unable to unlock the door.

Definition 10 *A* password-based door-key management system *is a door-key management system of Definition 3 with the following restrictions:*

1) *For any $q_K = (q_{K_a}, q_{K_b}) \in Q_K$, let $(d, k) \in q_{K_a}$. Then for any $k' \neq k$, it holds that $(d, k') \notin q_{K_a}$.*
2) *Let $p_K = (p_{K_a}, p_{K_b}), q_K = (q_{K_a}, q_{K_b}) \in Q_K$ be any k-states such that $\delta_K(p_K, (\mathtt{in}, \{(d, k)\})) = q_K$ for some d and k. Then q_K has exactly one transition $\delta_K(q_K, (\mathtt{co}, \{(k, u) \in q_{K_b}\}))$.*
3) *$\Sigma_K = (\{\mathtt{ac}, \mathtt{in}\} \times D \times K) \cup (\{\mathtt{is}\} \times K \times U) \cup \big(\bigcup_{q_K \in Q_K}\{\mathtt{co}, \{(k, u) \in q_{K_b}\}\}\big)$, where $\{\mathtt{co}, \{(k, u) \in$*

$q_{K_b}\}\}$ *is as defined in Condition 2.*

Condition 1 implies that for each door there is a unique key that can unlock the door. This assumes only one password is associated with each door. Condition 2 implies that once the key k gets disable from unlocking the door d, then the key k is immediately collected from all the users who have the key k. By "a user has a password", we mean that the user can open the door at the first trial of typing a password. Once the password is changed to a new one, then since the user does not know the new one, the user can open the door only with a negligible (very small) probability. This suggests the key has been collected from the user. Condition 3 implies a single operation enables a key to unlock a door, disables a key from unlocking a door, or issues a key to a user. A special co operation takes place at a single step as defined in Condition 2.

It is not difficult to prove the following theorem.

Theorem 1 *Every door-key management system of Definition 7, Definition 8, Definition 9 and Definition 10 implements the door access control of Definition 1.*

3. Evaluating Costs of Door-Key Management Systems

In this section we consider how to evaluate the minimum costs of gr and re requests of the door access control. We remark that the minimum cost may vary with the door-key management system that implements the door access control, as real-world systems often have some restrictions such as those introduced in Section 2.3. Hence general measures of the costs of requests, and an efficient method to compute them, are significantly important to evaluate door-key management systems.

Let $\mathcal{N}$ be the set of non-negative integers. We define the cost of each single operation of a door-key management system as follows.

Definition 11 (Cost Function $cost$**)** *Function* $cost : \Sigma_K^+ \to \mathcal{N}$ *is defined as follows.*

$$cost(\sigma) = \begin{cases} \mathtt{C_{ac}} \in \mathcal{N} & \text{if } \sigma = (\mathtt{ac}, A) \in \Sigma_K, \\ \mathtt{C_{in}} \in \mathcal{N} & \text{if } \sigma = (\mathtt{in}, A) \in \Sigma_K, \\ \mathtt{C_{is}} \in \mathcal{N} & \text{if } \sigma = (\mathtt{is}, B) \in \Sigma_K, \\ \mathtt{C_{co}} \in \mathcal{N} & \text{if } \sigma = (\mathtt{co}, B) \in \Sigma_K, \text{ and} \end{cases}$$

$$cost(s) = \sum_{i=1}^{|s|} cost(s[i]) \quad \text{if } |s| \geq 2,$$

where $A \subseteq 2^{D \times K}$, $B \subseteq 2^{K \times U}$, *and* $s[i]$ *is the* i*-th element of the sequence* $s \in \Sigma_K^+$ *of operations.*

The actual values of $\mathtt{C_{ac}}$, $\mathtt{C_{in}}$, $\mathtt{C_{is}}$, and $\mathtt{C_{co}}$ may vary with the door-key management system. Hence, we need a general framework where we can deal with arbitrary costs to evaluate various types of door-key management systems. Computing the minimum cost of a given request is formalized as the following problem.

Problem 1 *The* minimum cost problem *of a request of the door access control* (D, U, M) *w.r.t. a door-key management system* (D, K, U, M_K) *is as follows.*

- *Input: A k-state* $p_K \in Q_K$ *and a request* $r \in \Sigma$.
- *Output: A positive integer* $c \in \mathcal{N}$ *and a k-state* $q_K \in Q_K$ *such that*

$$c = \min\{cost(\beta) \mid \zeta(\delta_K(p_K, \beta)) = \delta(\zeta(p_K), r)\},$$
$$q_K = \delta_K(p_K, s),$$

where s *is a sequence of operations such that* $s \in \mathrm{argmin}\{cost(\beta) \mid \zeta(\delta_K(p_K, \beta)) = \delta(\zeta(p_K), r)\}$.

Namely, the problem is: given a k-state $p_K \in Q_K$ and a request $r \in \Sigma$, find a sequence of operations of minimum cost which leads to a k-state corresponding to the target state $\delta(\zeta(p_K), r) \in Q$.

See Figure 1 and Figure 2. Assume that the inputs of Problem 1 are k-state q_{K_7} and request $(\mathtt{re}, \{(d, u_1), (d, u_2)\})$. If $\mathtt{C_{in}} = 3$ and $\mathtt{C_{co}} = 1$, then the solution is minimum cost $c = 2$ $(= 2 \times \mathtt{C_{co}})$ and k-state q_{K_1} which corresponds to state $q_0 = \emptyset$. However, if $\mathtt{C_{in}} = 3$ and $\mathtt{C_{co}} = 2$, then the solution is minimum cost $c = 3$ $(= \mathtt{C_{in}})$ and k-state q_{K_5} which also corresponds to state $q_0 = \emptyset$.

It is also noteworthy that, even in the simplest unit cost model where $\mathtt{C_{ac}} = \mathtt{C_{in}} = \mathtt{C_{is}} = \mathtt{C_{co}} = 1$, the minimum cost varies with the type of door-key management system. Remark that in the unit cost model, the minimum cost equals the minimum number of operations. See Figure 3. In each system, the input is a pair of a k-state corresponding to a state $\{(d_1, u_1), (d_1, u_2), (d_2, u_1), (d_2, u_2)\}$ and a request $(\mathtt{re}, \{(d_1, u_1), (d_2, u_1)\})$. Hence the target state is $\{(d_1, u_2), (d_2, u_2)\}$ in which only the user u_2 can open the doors d_1 and d_2. In the smart card based system of Definition 7, the minimum cost is $cost((\mathtt{co}, \{(k_1, u_1)\})) = 1$. In the biometrics based system of Definition 8, the minimum cost is $cost((\mathtt{in}, \{(d_1, k_1)\}), (\mathtt{in}, \{(d_2, k_1)\})) = 2$. In the metal key based system of Definition 9, the minimum cost is $cost((\mathtt{in}, \{(d_1, k_1), (d_1, k_2)\}), (\mathtt{in}, \{(d_2, k_1), (d_2, k_2)\}), (\mathtt{ac}, \{(d_1, k_3)\}), (\mathtt{ac}, \{(d_2, k_3)\}), (\mathtt{is}, \{(k_3, u_2)\})) = 5$. In the password based system of Definition 10, the minimum cost is $cost((\mathtt{in}, \{(d_1, k_1)\}), (\mathtt{co}, \{(k_1, u_1), (k_1, u_2)\}), (\mathtt{in}, \{(d_2, k_2)\}), (\mathtt{co}, \{(k_2, u_1), (k_2, u_2)\}), (\mathtt{ac}, \{(d_1, k_3)\}), (\mathtt{ac}, \{(d_2, k_4)\}), (\mathtt{is}, \{(k_3, u_2)\}), (\mathtt{is}, \{(k_4, u_2)\})) = 8$.

As observed above, the solution to Problem 1 varies with the cost function and the door-key management system, and therefore a general algorithm to solve the problem with arbitrary costs is of significant importance. The following theorem shows that we indeed have such an algorithm.

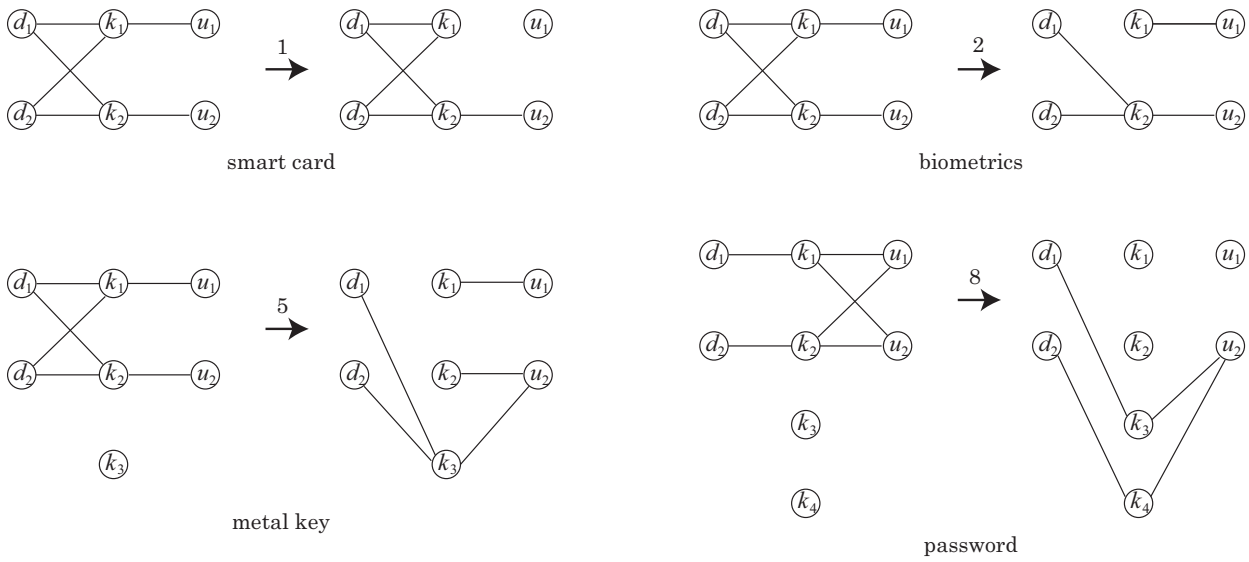

Fig. 3: The minimum cost for the same request may vary with the door-key management system.

Theorem 2 *Problem 1 is solvable in $O(|Q_K|^2)$ time.*

Proof. Consider an edge-weighted directed graph $G = (V, E)$ s.t. $V = Q_K$ and $E = \{(p_K, q_K, cost(\alpha)) \mid \delta_K(p_K, \alpha) = q_K\} \subseteq V \times V \times \mathcal{N}$. It follows from Definition 3 and Definition 11 that a solution to the single source shortest path problem based on $cost(\cdot)$ from the input vertex p_K to each vertex $q_K \in Q_K$ is equal to $\min\{cost(\alpha) \mid \delta_K(p_K, \alpha) = q_K\}$. For each vertex $q_K \in Q_K$, check if $\zeta(q_K) = \delta(\zeta(p_K), r)$, where r is a given request $r \in \Sigma$, and keep the solution of the shortest path problem from p_K if it is smaller than the previously kept solution for some vertex already checked. This checking can be done in $O(|D| \times |K| \times |U|)$ time for each vertex by e.g. implementing the binary relations between D and K, and between K and U, with matrices of size $|D| \times |K|$ and $|K| \times |U|$, respectively. It is well know that the single source shortest path problem can be solved in $O(|V|^2 + |E|)$ time, e.g. see [4]. Note that $|V| = |Q_K|$ and $|E| = O(|V|^2)$. Hence the overall time cost is $O(|Q_K|^2)$. □

4. Conclusions and Future Work

In this paper we considered door-key management systems for door access control. We model them based on deterministic finite state machines. Our model is general enough to describe various door-key management systems based on smart cards, biometrics, metal keys, and passwords. We gave an algorithm to compute the minimum cost of a door-key management systems to realize a given request on the door access control. The proposed algorithm is based on Dijkstra's algorithm [4] that solves the single-source shortest path problem on a directed graph.

Our future work includes the following.

1) In the proposed model, we did not consider that a user may take some operations. For instance, in the real world, a user might tell a password to another user who did not know it, independently of the administrator of the system. Yamasaki et al. [6] presented a mobile phone based door-key management system in which a user can copy his/her electronic door-key and can delegate it to another user's mobile phone in an "offline" manner (without communicating the administrator). Our model needs to be extended to dealing with such operations by users too.
2) To quickly evaluate large-scaled systems, it is necessary to speed up the algorithm to solve Problem 1. Our algorithm is inefficient when only a few k-states correspond to the target state of the door access control, as Dijkstra's algorithm preprocesses all vertices (k-states) and the total number of vertices is $|Q_K| = O(2^{|D|\times|K|+|K|\times|U|})$. Hence, if we can efficiently enumerate every and only k-state corresponding to the target state and compute the edit distance between the input k-state and each enumerated k-state, we can save considerable computational time and space. The edit operations we consider are insertion and deletion of edges of the tripartite graphs representing k-states. An efficient enumeration algorithm of pattern trees matching a given data tree has been studied [7]. It may be possible to modify the above algorithm to enumerating all tripartite graphs (k-states) which correspond to a given bipartite graph (target state).

References

[1] Art Japan Co., LTD, "Research result on door access control (in Japanese)," https://ssl.alpha-mail.ne.jp/art-japan.co.jp/research/index.html, 2007.

[2] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
[3] R. S. Sandhu and P. Samarati, "Authentication, access control, and intrusion detection," *The Computer Science and Engineering Handbook*, pp. 1929–1948, 1997.
[4] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Num. Math.*, vol. 1, no. 1, pp. 269–271, 1959.
[5] M. Bona, *A Walk through Combinatorics : An Introduction to Enumeration and Graph Theory*. World Scientific, 2006.
[6] T. Yamasaki, T. Nakamura, K. Baba, and H. Yasuura, "A door access control system with mobile phones," in *Proc. 12th IFIP International Conference on Personal Wireless Communications (PWC'07)*, ser. IFIP, no. 245. Springer, 2007, pp. 230–240.
[7] T. Asai, K. Abe, S. Kawasoe, H. Arimura, H. Sakamoto, and S. Arikawa, "Efficient substructure discovery from large semi-structured data," in *Proc. 2nd SIAM Int. Conf. on Data Mining*, 2002, pp. 158–174.