No.376

Optiomal Authentication Systems and Combinatorial Designs

by
Masakazu Jimbo
and
Ryoh Fuji-Hara

July 1988

Optimal Authentication Systems and Combinatorial Designs

MASAKAZU JIMBO AND RYOH FUJI-HARA
INSTITUTE OF SOCIO-ECONOMIC PLANNING
THE UNIVERSITY OF TSUKUBA
TSUKUBA, IBARAKI, 305, JAPAN

Abstract

In 1982, G. J. Simmons introduced a mathematical model of authentication theory. Recently, Brickell(1984) and Stinson(1987) have shown some combinatorial constructions for optimal authentication systems. We propose here game theoretical models of authentication systems which has multi-level costs on sources, and obtain lower bounds of the game values. We show some constructions of the optimal authentication systems which attain the bounds.

1. Introduction

In 1982, G. J. Simmons proposed a game theoretical model of authentication theory. In this model, there are three participants: a transmitter, a receiver and an opponent. The transmitter wants to communicate to the receiver, whereas the opponent wants to deceive the receiver. There are two actions the opponent can take. First, the opponent can try to impersonate the transmitter and send a message to the receiver while, in fact, the transmitter has not sent a message. This is called *impersonation*. Second, he can intercept a message from the transmitter and substitute a different message, which will be sent to the receiver, called *substitution*. In both cases, the opponent will be successful if the receiver accept the message as authentic and is thus misled about the source state.

Let $\mathcal{S} = \{s_1, \cdots, s_k\}$ be a set of *source states*, $\mathcal{M} = \{m_1, \cdots, m_v\}$ be a set of *messages* and $\mathcal{E} = \{e_1, \cdots, e_b\}$ be a set of *keys*. A source state $s \in \mathcal{S}$ is the information that the transmitter wishes to communicate to the receiver. The transmitter/receiver will have secretly chosen a key $e \in \mathcal{E}$ beforehand. A source state $s \in \mathcal{S}$ is encoded to a message m according to a key e. Generally, the message space is assumed to be larger enough than the source space. In order for the receiver to be able to uniquely determine the source state from the sent message, there can be at most one source state which is encoded by any given message $m \in \mathcal{M}$. Hence each key e determines a mapping f_e from $\mathcal{M}$ onto $\mathcal{S} \cup \{\phi\}$. By a mapping f_e, a source state s is encoded to message m satisfying $f_e(m) = s$. We assume that $f_e(m) = \phi$ if there are no source states corresponding to a message m when a key e is used. Let $\mathcal{F} = \{f_e | e \in \mathcal{E}\}$. A quadruple $(\mathcal{S}, \mathcal{M}, \mathcal{E}, \mathcal{F})$ is called an *authentication system*. It is possible that more than one message correspond to a source state by a mapping f_e, which is called *splitting*. Except Section 2, we shall devote ourselves to the case of no splitting. In the case of no splitting, the inverse mapping $g_e : \mathcal{S} \to \mathcal{M}$ is well defined for each f_e. A $b \times k$ array $A = (a_{ij})$ with $a_{ij} = g_{e_i}(s_j)$ for $e_e \in \mathcal{E}$, $s_j \in \mathcal{S}$ is the *array representation* of an authentication system (with no splitting).

Let S, E, M be random variables representing a source state, a key, and a message

sent by transmitter, respectively. A probability distribution $P_r(S = s)$ is given on the set of source states $\mathcal{S}$. Given a probability distribution on $\mathcal{S}$, the transmitter/receiver will determine a probability distribution $r_e = P_r(E = e)$ on $\mathcal{E}$, called *encoding strategy*. If splitting occurs, then they will also determine a *splitting strategy* $\pi(m|e,s) = P_r(M = m|E = e, S = s)$. Then the probability distribution on $\mathcal{M}$ is determined by the conditional probability

$$P_r(M = m|E = e) = P_r(S = f_e(m))\pi(m|e, f_e(m)),$$

where we assume that $P_r\{S = \phi\} = 0$, for convenience.

Simmons(1982) defined two types of games, *impersonation game* and *substitution game*. In both games, transmitter/receiver will choose the encoding and splitting strategies to minimize the chance that the opponent can deceive them. Let N be a random variable representing a message sent by the opponent. In case of impersonation, the opponent will choose the probability $P(N = n), n \in \mathcal{M}$ to maximize the deceiving probability. In case of substitution, he can determine his strategy after catching a message m sent by transmitter. Here, he can choose a substitution strategy $q_{n|m} = P_r(N = n|M = m)$ for each $m \in \mathcal{M}$ in order to maximize the deceiving probability.

Each game has the value which is the deceiving probability for optimal strategies, denoted by P_I and P_S, respectively. Simmons(1982,1984,1985), Brickell(1984) and Stinson(1987) obtained lower bounds on the probabilities P_I and P_S. Further Brickell(1984) and Stinson(1987) gave constructions of authentication systems attaining the bounds.

In this paper, we introduce a notion of costs on sources, and generalize their results by considering mini-max expected loss.

Let $c(s), > 0$, is a *cost* for a source state $s \in \mathcal{S}$. In case of impersonation game, we define a payoff

$$\gamma(e,m) = \begin{cases} c(s) & \text{if } f_e(m) \in \mathcal{S}, \\ 0 & \text{if } f_e(m) = \phi. \end{cases}$$

That is, $\gamma(e,m)$ is the loss when the opponent sends a message m while transmitter/receiver are using key e and no message is transmitted. Then the expected loss

is

$$L_I = \sum_e \sum_{n \in M} r_e q_n \gamma(e, n).$$

The value of the impersonation game is

$$V_I = \max_{q_n} \min_{r_e} L_I = \min_{r_e} \max_{q_n} L_I.$$

Note that, in case of $c(s) = 1$ for any $s \in S$, V_I is identical with the optimal deceiving probability P_I.

In substitution game, let $\gamma(e, m, n)$ is the loss when the transmitter send message m using key e and the opponent substitute message n for the transmitted message m. Here, we assume that the loss occurs only when the receiver could not detect the substituted message. The amount of loss is assumed to be the sum of the loss $\gamma(e, m)$ and $\gamma(e, n)$, where $\gamma(e, m)$ is the loss when the receiver lost the message m sent by the transmitter and $\gamma(e, n)$ is the loss when the receiver accept the substituted message n as authentic, i.e.

$$\gamma(e, m, n) = \begin{cases} \gamma(e, m)\delta(e, n) + \gamma(e, n)\delta(e, m) & m \neq n, \\ 0 & \text{otherwise}, \end{cases}$$

where

$$\delta(e, m) = \begin{cases} 1 & \gamma(e, m) > 0\ , \\ 0 & \text{otherwise.} \end{cases}$$

The expected loss, in this case, is as follows:

$$L_S = \sum_e \sum_m \sum_n r_e \pi(m|e, s) P_r(S = f_e(m)) q_{n|m} \gamma(e, m, n).$$

The transmitter/receiver want to minimize the expected loss by choosing encoding strategy $\{r_e\}$ and splitting strategy $\pi(m|e, s)$. On the other hand, the opponent wants to maximize L_S by choosing conditional probabilities $q_{n|m}$. The existence of the value of the substitution game is proved in Appendix. Let V_S be the value of the game, then

$$V_S = \max_{q_{n|m}} \min_{r_e} L_S = \min_{r_e} \max_{q_{n|m}} L_S.$$

Here, we mention about the relation of the values between games introduced by Simmons and us. In Simmons' case, the loss function is defined by

$$\gamma(e,m,n) = \delta(e,m)\delta(e,n),$$

which is the half of our loss function with $c(s) = 1$ for $s \in S$.

In Section 2, we shall obtain bounds of V_I and V_S for a given authentication system. Some of them are based on entropies. In Section 3, conditions for authentication systems to attain the bounds will be discussed. Furthermore, we shall construct authentication systems attaining the bounds. In Section 4, we shall restrict ourselves to the sources with uniform distribution and discuss conditions for attaining the bounds. And a construction will be given. Finally, in Section 5, we shall mention about conditions to attain the bounds in the case of $c(s) = 1$ for any source state $s \in S$, which is just the case Simmons(1982,1984,1985), Brickell(1984) and Stinson(1987) treated.

2. Bounds for the game values

Firstly, we shall show in this section that, the values V_I and V_S are bounded from below by entropy functions depending on a given authentication system. Secondly, we shall obtain lower bounds for V_I and V_S which does not depend on a given authentication system.

For a random variable X with probability distribution $P_r(X = x)$, the *entropy* of X, $\mathrm{H}(X)$, is defined as follows:

$$\mathrm{H}(X) = -\sum_x P_r(X = x) \log P_r(X = x).$$

As well, the *conditional entropy* $\mathrm{H}(X|Y)$ is defined by

$$\mathrm{H}(X|Y) = -\sum_y \sum_x P_r(Y = y) P_r(X = x|Y = y) \log P_r(X = x|Y = y).$$

Theorem 2.1. *For a given authentication system, we have*

$$V_I \geq 2^{\mathrm{H}(M|E) - \mathrm{H}(M) + \mathrm{E}(\log c(S))},$$

where $E(X)$ is the expectation of a random variable X.

Proof. Let $W_m = \sum_e r_e^* \gamma(e, m)$ and $w_m(e) = r_e^* \gamma(e, m)/W_m$, where $\{r_e^*\}$ is an optimal encoding strategy of the impersonation game. Then we have

$$\begin{aligned} P_r(M = m) &= \sum_e r_e^* P_r(M = m|E = e) \\ &= \sum_e w_m(e) W_m u(e, m), \end{aligned}$$

where

$$u(e, m) = \begin{cases} \frac{P_r(M=m|E=e)}{\gamma(e,m)} & \text{if } \gamma(e, m) > 0, \\ 0 & \text{if } \gamma(e, m) = 0. \end{cases}$$

Hence, by the concavity of $-x\log x$, we have

$$\begin{aligned}
\mathrm{H}(M) &= -\sum_m P_r(M=m)\log P_r(M=m) \\
&\geq -\sum_m\sum_e w_m(e)W_m u(e,m)\log W_m u(e,m) \\
&= -\sum_m\sum_e P_r(M=m,E=e)\log W_m \\
&\quad -\sum_m\sum_e P_r(M=m,E=e)\log P_r(M=m|E=e) \\
&\quad +\sum_m\sum_e P_r(M=m,E=e)\log\gamma(e,m).
\end{aligned}$$

It is easy to see $W_m \leq V_I$ for any m by the well-known result for a two person matrix game and the last term equals to $\mathrm{E}(\log c(S))$. Therefore, we have

$$\mathrm{H}(M) \geq -\log V_I + \mathrm{H}(M|E) + \mathrm{E}(\log c(S)),$$

which prove the theorem. **Q.E.D.**

Corollary 2.1(Simmons). *We have*

$$P_I \geq 2^{\mathrm{H}(M|E)-\mathrm{H}(M)}.$$

Now, we shall obtain a bound for the substitution game. Let $\{r_e^*\}$ be an optimal encoding strategy. In the sequel, we use the notations $P_r^*(\cdot)$, $P_r^*(\cdot|\cdot)$ to represent probabilities corresponding to the optimal encoding strategy $\{r_e^*\}$. We take arbitrary probability distributions $\{p(n|m,e)\}$ satisfying the following conditions:

(1) $p(n|m,e) \geq 0.$

(2) If $\gamma(e,m,n) = 0$ then $p(n|m,e) = 0.$

(3) If $\gamma(e,m) > 0$ then $\sum_n p(n|m,e) = 1.$

Further, let

$$p^*(e,m,n) = p(n|m,e)r_e^* P_r(M=m|E=e),$$
$$p^*(n|m) = \sum_e p(n|m,e)P_r^*(E=e|M=m),$$
$$p^*(m,n) = P_r^*(M=m)p^*(n|m)$$

and

$$p^*(e|m,n) = \frac{p^*(e,m,n)}{p^*(m,n)}.$$

Then we have the following theorem for the substitution game:

Theorem 2.2. *Given an authentication system, we have*

$$V_S \geq 2^{H' - \mathrm{H}(E|M) + \mathrm{E}_p(\log \gamma(E,M,N))}$$

for any $\{p(n|m,e)\}$, *where* $\mathrm{E}_p(\cdot)$ *is the expectation with respect to a probability distribution* $\{p^*(e,m,n)\}$ *and* H' *is the following entropy:*

$$H' = -\sum_m \sum_n \sum_e p^*(e,m,n) \log p^*(e|m,n).$$

Proof. At first, define the following entropy functions:

$$\mathrm{H}(p(\cdot|m)) = -\sum_n p^*(n|m) \log p^*(n|m),$$
$$\mathrm{H}(p(\cdot|m,e)) = -\sum_n p(n|m,e) \log p(n|m,e),$$
$$\mathrm{H}(p(\cdot|m,E)) = -\sum_e P_r^*(E=e|M=m)\mathrm{H}(p(\cdot|m,e)),$$
$$\mathrm{H}(p(\cdot|M)) = -\sum_e P_r^*(M=m)\mathrm{H}(p(\cdot|m)),$$
$$\mathrm{H}(p(\cdot|M,E)) = -\sum_e \sum_m P_r^*(M=m,E=e)\mathrm{H}(p(\cdot|m,e)).$$

Let

$$W_{mn} = \sum_e \gamma(e,m,n)P_r^*(E=e|M=m),$$

and let

$$w_{mn}(e) = \gamma(e,m,n)P_r^*(E=e|M=m)/W_{mn}.$$

Then, by Corollary A.2 in Appendix, $P_r^*(M=m)W_{mn} \leq v_m$ holds for any m and n. And we obtain

$$p(n|m) = \sum_e w_{mn}(e)W_{mn}u(e,m,n),$$

where

$$u(e,m,n) = \begin{cases} \frac{p(n|m,e)}{\gamma(e,m,n)} & \text{if } \gamma(e,m,n) > 0, \\ 0 & \text{if } \gamma(e,m,n) = 0. \end{cases}$$

Hence, similarly to the case of the impersonation game,

$$\begin{aligned} \mathrm{H}(p(\cdot|m)) &= -\sum_e p(n|m)\log p(n|m) \\ &\geq -\sum_n \sum_e w_{mn}(e)u(e,m,n)\log W_{mn}u(e,m,n) \\ &\geq -\log \frac{v_m}{P_r^*(M=m)} + \mathrm{H}(p(\cdot|m,E)) + K_m, \end{aligned} \tag{2.1}$$

where

$$K_m = \sum_n \sum_e p(n|e,m)P_r^*(E=e|M=m)\log\gamma(e,m,n).$$

Then $V_S = \sum_m v_m$. Hence, by multiplying $P_r^*(M=m)$ to the previous inequality(2.1) and by adding them with respect to m, we obtain

$$\begin{aligned} \mathrm{H}(p(\cdot|M)) &\geq -\sum_m P_r^*(M=m)\log\frac{v_m}{P_r^*(M=m)} + \mathrm{H}(p(\cdot|M,E)) + \mathrm{E}_p(\log\gamma(E,M,N)), \\ &\geq -\log V_S + \mathrm{H}(p(\cdot|M,E)) + \mathrm{E}_p(\log\gamma(E,M,N)), \end{aligned}$$

where $\mathrm{E}_p(\cdot)$ is the expected value with respect to the probability distribution $\{p^*(e,m,n)\}$, i.e.

$$\mathrm{E}_p(\log\gamma(E,M,N)) = \sum_e \sum_m \sum_n p^*(e,m,n)\log\gamma(e,m,n).$$

Finally,

$$\mathrm{H}(p(\cdot|M,E)) - \mathrm{H}(p(\cdot|M)) = H' - \mathrm{H}(E|M),$$

which complete the proof. **Q.E.D.**

Corollary 2.2. *When $c(s) = 1$ for any $s \in S$, we have*

$$P_S \geq 2^{H' - \mathrm{H}(E|M)}$$

for any $\{p(n|m,e)\}$.

The proof of the corollary is obvious. The bound given by Simmons(1982) is

$$P_S \geq 2^{-\mathrm{H}(E|M)}.$$

In case of no splitting, Stinson(1987) improved Simmons' bound as follows:

$$P_S \geq \delta \cdot 2^{-\mathrm{H}(E|M)},$$

where

$$\delta(e', m, n) = \frac{\sum_e \delta(e,m)\delta(e,n) r_e^* P_r(S = f_e(m))}{\delta(e',m)\delta(e',n) r_{e'}^* P_r(S = f_{e'}(m))}$$

and

$$\delta = \min \delta(e', m, n).$$

Choose the following $\{p(n|m,e)\}$:

$$p(n|m,e) = \frac{1}{k-1}\delta(e,m)\delta(e,n)$$

in Corollary 2.2. Then, because of no splitting,

$$p^*(e,m,n) = \frac{1}{k-1}\delta(e,m)\delta(e,n) r_e^* P_r(S = f_e(m)).$$

Hence

$$\begin{aligned} H' &= -\sum_e \sum_m \sum_n p^*(e,m,n) \log \frac{p^*(e,m,n)}{p^*(m,n)} \\ &= \sum_e \sum_m \sum_n p^*(e,m,n) \log \delta(e,m,n) \\ &\geq \log \delta. \end{aligned}$$

Thus the bound in Corollary 2.2 is sharper than that of Stinson(1987).

Now, we shall obtain bounds for the games, which may be weaker than the entropy bounds but not depending on authentication systems. In the sequel of this paper, we shall devote ourselves to the case of no splitting.

Firstly, we shall give a bound for the value of the impersonation game.

Theorem 2.3. *For any authentication system, we have*

$$V_I \geq \frac{K}{|\mathcal{M}|} = \frac{K}{v},$$

where $K = \sum_s c(s)$.

Proof. Let $\{r_e^*\}$, $\{q_n^*\}$ be optimal strategies for the transmitter/receiver and the opponent, respectively. Then we have

$$\begin{aligned} V_I &= \sum_e \sum_n r_e^* q_n^* \gamma(e,n), \\ &\geq \sum_e \sum_n r_e^* \frac{1}{|\mathcal{M}|} \gamma(e,n), \\ &= \sum_e r_e^* \frac{1}{|\mathcal{M}|} \sum_n \gamma(e,n), \\ &\geq \frac{1}{|\mathcal{M}|} K. \end{aligned}$$

Q.E.D.

By letting $c(s) = 1$ for any $s \in \mathcal{S}$, we obtain the following corollary:

Corollary 2.3(Simmons).

$$P_I \geq \frac{k}{v}$$

holds, where k is the number of source states.

Secondly, we shall give a lower bound for the value of the substitution game.

Theorem 2.4. *We have*

$$V_S \geq \frac{1}{v-1}\{(k-2)E(c(S)) + K\},$$

where $E(c(S))$ is the mean cost for the source states. Especially, when the source distribution is uniform,

$$V_S \geq \frac{1}{v-1}\{\frac{2(k-1)}{k}K\} \tag{2.2}$$

holds.

Proof. Let $\{r_e^*\}$ be an optimal strategy for the transmitter/receiver. In this case, the opponent can choose an optimal strategy $\{q_{n|m}^*\}$ for each message m. Clearly, we can assume that $q_{n|m}^* = 0$ since the payoff $\gamma(e,m,m) = 0$ for any e. We obtain

$$\begin{aligned} V_S &= \sum_e \sum_m \sum_n r_e^* P_r(M = m|E = e) q_{n|m}^* \gamma(e,m,n) \\ &\geq \sum_e \sum_m \sum_n r_e^* P_r(M = m|E = e) \frac{1}{v-1} \gamma(e,m,n). \end{aligned}$$

And

$$\begin{aligned} \sum_n \gamma(e,m,n) &= \sum_{n(\neq m)} \{\gamma(e,m)\delta(e,n) + \gamma(e,n)\delta(e,m)\} \\ &= (k-1)\gamma(e,m) + \delta(e,m)\{\sum_n \gamma(e,n) - \gamma(e,m)\} \\ &= (k-2)\gamma(e,m) + \delta(e,m)K. \end{aligned}$$

Hence

$$\begin{aligned} V_S &\geq \sum_e \sum_m r_e^* P_r(M = m|E = e) \frac{1}{v-1}\{(k-2)\gamma(e,m) + \delta(e,m)K\}, \\ &= \frac{k-2}{v-1}\mathrm{E}(c(S)) + \frac{1}{v-1}K. \end{aligned}$$

When source distribution is uniform, $\mathrm{E}(c(S)) = K/k$, thus the theorem is proved.

Q.E.D.

Corollary 2.4(Simmons). *We have*

$$P_S \geq \frac{k-1}{v-1}.$$

Proof. Let $c(s) = 1$ in Theorem 2.4 and note that $V_S = 2P_S$. **Q.E.D.**

The authentication systems attaining both bounds of Theorem 2.3 and 2.4 is called *optimal*.

3. Conditions for optimal authentication systems and their constructions

In this section we shall discuss conditions for an authentication system to be optimal. Further, we will show some constructions of optimal authentication systems. At first, a condition to attain the bound of the impersonation game is given as follows:

Theorem 3.1. *An authentication system with property*

$$\sum_e \gamma(e,n) = const. = R$$

attains the bound of Theorem 2.1.

Proof. We have

$$\begin{aligned} V_I &= \sum_e \sum_n r_e^* q_n^* \gamma(e,n) \\ &\leq \sum_e \sum_n \frac{1}{|\mathcal{E}|} q_n^* \gamma(e,n) \\ &= \frac{R}{|\mathcal{E}|} \\ &= \frac{R}{b}. \end{aligned}$$

Thus the theorem is proved by the fact that $Rv = Kb$. **Q.E.D.**

Now, we shall obtain a sufficient condition of an optimal authentication system.

Theorem 3.2. *An authentication system satisfying the following condition is optimal:*

For any distinct two sources s_1, s_2 and for any distinct two messages m, n, there exist exactly μ keys e satisfying $s_1 = f_e(m), s_2 = f_e(n)$.

Proof. The value of the substitution game is

$$\begin{aligned} V_S &= \sum_e \sum_m \sum_n r_e^* P_r(M=m|E=e) q_{n|m}^* \gamma(e,m,n) \\ &\leq \frac{1}{|\mathcal{E}|} \sum_m \sum_{n(\neq m)} q_{n|m}^* \sum_e P_r(M=m|E=e)\gamma(e,m,n). \end{aligned}$$

And

$$\begin{aligned} &\sum_e P_r(M=m|E=e)\gamma(e,m,n) \\ &\qquad = \sum_e P_r(M=m|E=e)\{\gamma(e,m)\delta(e,n)+\gamma(e,n)\delta(e,m)\} \\ &\qquad = \sum_e P_r(M=m|E=e)\gamma(e,m)\delta(e,n) + \sum_e P_r(M=m|E=e)\gamma(e,n). \end{aligned}$$

Let

$$B_{m,n} = \sum_e P_r(M=m|E=e)\gamma(e,m)\delta(e,n)$$

and

$$C_{m,n} = \sum_e P_r(M=m|E=e)\gamma(e,n),$$

then

$$\begin{aligned} B_{m,n} &= \sum_e P_r(S=f(e,m))c(f(e,m))\delta(e,n) \\ &= \mu \sum_{s_1} \sum_{s_2(\neq s_1)} P_r(S=s_1)c(s_1) \\ &= \mu(k-1)\sum_{s_1} P_r(S=s_1)c(s_1) \\ &= \mu(k-1)\mathrm{E}(c(S)) \end{aligned}$$

and

$$\begin{aligned}
C_{m,n} &= \sum_e P_r(M=m|E=e)\gamma(e,n) \\
&= \sum_e P_r(S=f_e(m))\gamma(e,n) \\
&= \mu \sum_{s_1} \sum_{s_2(\neq s_1)} P_r(S=s_1)c(s_2) \\
&= \mu \sum_{s_1}\sum_{s_2} P_r(S=s_1)c(s_2) - \mu \sum_{s_1} P_r(S=s_1)c(s_1) \\
&= \mu(K - \mathrm{E}(c(S))).
\end{aligned}$$

Therefore,

$$\begin{aligned}
V_S &\leq \frac{1}{|\mathcal{E}|}\sum_m \sum_{n(\neq m)} q^*_{n|m}\{(k-2)\mathrm{E}(c(S)) + \mu K\}, \\
&= \mu\frac{|\mathcal{M}|}{|\mathcal{E}|}\{(k-2)\mathrm{E}(c(S)) + K\}.
\end{aligned}$$

For any distinct two sources s_1, s_2, there exist exactly μ pairs of distinct messages m, n which are encoded from s_1, s_2, respectively. Therefore,

$$|\mathcal{E}| = \mu|\mathcal{M}|(|\mathcal{M}| - 1)$$

holds. It is easy to see that this system satisfy the condition of Theorem 3.1. Thus the proof is completed. **Q.E.D.**

We should note that if an authentication system satisfies the condition of Theorem 3.2, then it is optimal for any source distribution and for any costs $\{c(\cdots)\}$. This means that, even if we do not know exact source distribution or we can not determine the precise cost of sources, this system guarantees the optimality.

Now we consider a construction of authentication system satisfying the condition of Theorem 3.2.

A $\lambda v^2 \times k$ array $\Pi = (\pi_{ij})$ with entries from a set $\mathcal{M}$ of cardinality v is called *orthogonal array*, denoted by $\mathrm{OA}(v, k, ; \lambda)$, if every ordered pair of $\mathcal{M}$ occurs exactly λ times among each two columns of Π as row.

There are several constructions of orthogonal arrays (see, for example, Beth *et als*(1986)).

Theorem 3.3. *If there exists an orthogonal array* $OA(v^2, k+1, 1)$ *then there exists an optimal authentication system with* v *messages,* k $(k \leq v)$ *sources and* $v(v-1)$ *keys.*

Proof. Let $\Pi = (\pi_{ij})$ $(i = 1, \cdots, v^2, j = 1, \cdots, k)$ is an orthogonal array. Without loss of generality, we can assume $\pi_{t+i,1} = i$ for $0 \leq i \leq v-1$ and $\pi_{t+i,k+1} = 0$, where $t = v(v-1)+1$. Now for each column j $(1 \leq j \leq k)$, we apply the following permutation on the symbols of the column

$$\begin{pmatrix} \pi_{t+1,j}, & \pi_{t+2,j}, & \cdots & ,\pi_{t+v,j} \\ 0, & 1, & \ldots & ,v-1 \end{pmatrix}.$$

The array Π_1 whose symbols are replaced by the above permutations is also an orthogonal array. It has a property that no same symbol appears twice in the i-th row $(1 \leq i \leq v(v-1))$. Let Π_2 be $(v^2 - v) \times k$ subarray obtained by taking off the last column and the last v rows from Π_1. Then Π_2 is the desired authentication system. **Q.E.D.**

4. Optimal authentication system for uniformly distributed sources

The condition of Section 3 is considered for the case of general source distribution and also of general source costs $c(s)$. But in some cases, we may assume that each source state occurs equally often. By restricting the source distribution to be uniform, the condition to attain the bound of substitution game can be weakened. To show this, we need the following lemma.

Lemma 4.1. *Assume that an authentication system satisfies the following conditions:*

$$\sum_e \gamma(e,m) = \ const. \ = R(= \frac{bK}{v}), \tag{4.1}$$

$$\sum_e \gamma(e,m,n) = \ const. \ = \Lambda. \tag{4.2}$$

Then

$$\sum_e \delta(e,m) = \ const. \ (= r = \frac{bk}{v})$$

and

$$\Lambda(v-1) = 2R(k-1) \tag{4.3}$$

hold.

Proof. Let $r_m = \sum_e \gamma(e,m)$ for a message $m \in \mathcal{M}$. We evaluate $\sum_e \sum_{n(\neq m)} \gamma(e,n)\delta(e,m)$ in two ways. First,

$$\begin{aligned}\sum_{n(\neq m)} \sum_e \gamma(e,n)\delta(e,m) &= \sum_{n(\neq m)} \{\sum_e \gamma(e,m,n)\} - \sum_{n(\neq m)} \sum_e \delta(e,n)\gamma(e,m) \\ &= \Lambda(v-1) - \sum_e \gamma(e,m)(k-1) = \Lambda(v-1) - R(k-1).\end{aligned}$$

Second,

$$\begin{aligned}\sum_e \sum_{n(\neq m)} \gamma(e,n)\delta(e,m) &= \sum_e \delta(e,m)\{\sum_n \gamma(e,n) - \gamma(e,m)\} \\ &= \sum_e \delta(e,m)\{K - \gamma(e,m)\} \\ &= K\sum_e \delta(e,m) - \sum_e \gamma(e,m) \\ &= Kr_m - R.\end{aligned}$$

Hence we have

$$\Lambda(v-1) - R(k-2) = Kr_m,$$

which means that r_m is a constant$(= r)$. Therefore, $\Lambda(v-1) - R(k-2) = Kr$. By the way, since $vr = bk$ and $vR = bK$, $rK = Rk$ holds. Thus we have the lemma. **Q.E.D.**

Theorem 4.1. *In the case that the source distribution is uniform, an authentication system satisfying the conditions (4.1) and (4.2) is optimal.*

Proof. By the condition (4.1) we have

$$\begin{aligned}V_S &= \sum_e \sum_m \sum_n r_e^* P_r(M=m|E=e) q^*_{n|m} \gamma(e,m,n) \\ &\leq \frac{1}{|\mathcal{E}|} \sum_m \sum_{n(\neq m)} q^*_{n|m} \sum_e P_r(M=m|E=e)\gamma(e,m,n) \\ &= \frac{1}{|\mathcal{E}|}\frac{1}{|\mathcal{S}|} \sum_m \sum_{n(\neq m)} q^*_{n|m} \sum_e \gamma(e,m,n) \\ &= \frac{v}{bk}\Lambda.\end{aligned}$$

By the equation (4.3) of Lemma 4.1 and by the fact that $vR = bK$, we have

$$V_S = \frac{2K(k-1)}{(v-1)k}.$$

Finally, from Theorem 3.1, this system attains the bound of Theorem 2.3. **Q.E.D.**

We shall show examples of authentication system satisfying Conditions (4.1) and (4.2).

Example 4.1.

Let $v = |\mathcal{M}| = 5$, $k = |\mathcal{S}| = 3$, $\mathcal{S} = \{s_1, s_2, s_3\}$, $c(s_1) = 1$ and $c(s_2) = c(s_3) = 2$. Then the following authentication system A satisfies Conditions (4.1) and (4.2):

$$A = \begin{bmatrix} m_1 & m_0 & m_3 \\ m_2 & m_1 & m_4 \\ m_3 & m_2 & m_0 \\ m_4 & m_3 & m_1 \\ m_0 & m_4 & m_2 \\ m_4 & m_1 & m_0 \\ m_0 & m_2 & m_1 \\ m_1 & m_3 & m_2 \\ m_2 & m_4 & m_3 \\ m_3 & m_0 & m_4 \end{bmatrix}$$

and the payoff matrix $\Gamma = (\gamma(e, m))$ is as follows:

$$\Gamma = \begin{bmatrix} 2 & 1 & 0 & 2 & 0 \\ 0 & 2 & 1 & 0 & 2 \\ 2 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 2 & 1 \\ 1 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 0 & 1 \\ 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 1 & 2 & 2 \\ 2 & 0 & 0 & 1 & 2 \end{bmatrix}.$$

In this case $K = 5$, $R = 10$, $r = 6$, $b = |\mathcal{E}| = 10$, $\Lambda = 10$ and $V_I = 3/5$, $V_S = 1/2$.

Example 4.2.

Let $v = 7$, $k = 4$, $\mathcal{S} = \{s_1, s_2, s_3, s_4\}$, $c(s_1) = c(s_2) = 1$, $c(s_3) = c(s_4) = 2$. Then

the following authentication system A satisfies Conditions (4.1) and (4.2).

$$A = \begin{bmatrix} m_2 & m_4 & m_5 & m_6 \\ m_3 & m_5 & m_6 & m_0 \\ m_4 & m_6 & m_0 & m_1 \\ m_5 & m_0 & m_1 & m_2 \\ m_6 & m_1 & m_2 & m_3 \\ m_0 & m_2 & m_3 & m_4 \\ m_1 & m_3 & m_4 & m_5 \\ m_6 & m_5 & m_4 & m_2 \\ m_0 & m_6 & m_5 & m_3 \\ m_1 & m_0 & m_6 & m_4 \\ m_2 & m_1 & m_0 & m_5 \\ m_3 & m_2 & m_1 & m_6 \\ m_4 & m_3 & m_2 & m_0 \\ m_5 & m_4 & m_3 & m_1 \end{bmatrix}.$$

In this case, $K = 6$, $R = 12$, $r = 8$, $b = 4$,$\Lambda = 12$ and $V_I = 4/7$, $V_S = 1/2$.

Here, we shall obtain constructions of optimal authentication systems of Theorem 4.1 for some cases. The constructions are based on combinatorial designs.

Let X be a set with v elements and $\mathcal{B}$ a collection of k-subsets, called *blocks*, of X. A pair $(X, \mathcal{B})$ is called *BIBD* (*balanced incomplete block design)*, denoted by (v, k, λ)-*BIBD*, if any pair of distinct elements of X occurs in exactly λ blocks. For a (v, k, λ)-BIBD, it is well known that the number of blocks containing an element is constant$(= r)$ independent of the choice of the element. Let b be the number of blocks, then

$$vr = bk \qquad \text{and} \qquad \lambda(v-1) = r(k-1)$$

holds (see, for example, Beth *et als* (1986)). In this case, when $c(s) = 1$ for any $s \in S$, Stinson(1987) showed that, by arranging block of a (v, k, λ)-BIBD for rows(keys) of an authentication system, we can construct an optimal authentication system with k sources, v messages and $b = \lambda v(v-1)/k(k-1)$ keys. Now we can show the following theorem.

Theorem 4.2. *Assume that source distribution is uniform and* $c(s_1) = \cdots = c(s_{k'}) = a$ *and* $c(s_{k'+1}) = \cdots = c(s_k) = b$, *where* $k = 2k'$. *In this case, if there exists a* (v, k, λ)-*BIBD* (k *is even*) D, *then there exists an optimal authentication system with two level*

costs on sources, which has parameters

$$|\mathcal{S}| = k, \qquad |\mathcal{M}| = v,$$
$$|\mathcal{E}| = 2\frac{\lambda k(k-1)}{v(v-1)},$$
$$K = \frac{a+b}{2}k, \qquad R = \frac{(a+b)\lambda(v-1)}{k-1},$$
$$\Lambda = 2(a+b)\lambda, \qquad r = 2\frac{\lambda(v-1)}{k-1}.$$

Proof. Let A_1 be a $b \times k$ array such that each row of A_1 consists of a block of D (note: we do not care the ordering of elements). Let $A_1 = [A_{11}|A_{12}]$, where A_{11} and A_{12} are $b \times k'$ submatrices. Then the $b' \times k$ array

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{12} & A_{11} \end{bmatrix}$$

is a authentication system we want, where $b' = 2\lambda k(k-1)/\{v(v-1)\}$. Now, we verify that this is the desired authentication system. For any distinct messages m and n, let $\lambda_{ij}(i,j,=1,2)$ be the number of rows l of A_1 such that m and n are contained in the l-th row of A_{1i} and A_{1j}, respectively. Note that $\lambda_{11}+\lambda_{12}+\lambda_{21}+\lambda_{22} = \lambda$, since A_1 is made from a (v,k,λ)-BIBD. For the below half of A, we define λ'_{ij}'s similarly to λ_{ij}'s then we have $\lambda'_{11} = \lambda_{22}$, $\lambda'_{12} = \lambda_{21}$, $\lambda'_{21} = \lambda_{12}$ and $\lambda'_{22} = \lambda_{11}$, thus

$$\begin{aligned}\Lambda &= 2a\lambda_{11} + (a+b)(\lambda_{12}+\lambda_{21}) + 2b\lambda_{22} + 2a\lambda'_{11} + (a+b)(\lambda'_{12}+\lambda'_{21}) + 2b\lambda'_{22} \\ &= 2(a+b)(\lambda_{11}+\lambda_{12}+\lambda_{21}+\lambda_{22}) = 2(a+b)\lambda,\end{aligned}$$

which is independent of the choice of m and n. Similarly, we can show that $R = \sum_e \gamma(e,m)$ is constant, which complete the proof. **Q.E.D.**

For the next construction, we need the following combinatorial design which was introduced by Fuji-Hara and Kuriki(1988).

Let $(X,\mathcal{B})$ be a (v,k,λ)-BIBD. Suppose that each block $B \in \mathcal{B}$ is partitioned into g subblocks $B_1, B_2, \cdots, B_g$ with cardinalities $k_i = |B_i|$. The collection of the i-th subblocks

B_i's is denoted by $\mathcal{B}_i$ and let $\Pi = \{\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_g\}$. A *BIBD with mutually balanced nested subdesigns* is a triple $(X, \mathcal{B}, \Pi)$ satisfying the following conditions:

(i) each $(X, \mathcal{B}_i)$ is a (v, k_i, λ_i)-BIBD for $i = 1, 2, \cdots, g$,

(ii) for distinct elements x and y of X, the number of blocks in $\mathcal{B}$ containing x and y in the i-th and the j-th the subblocks, respectively, is $\lambda_{i,j}$, which is independent of the choice of x and y. (Note that $\lambda_{i,j} = \lambda_{j,i}$ and $\lambda_i = \lambda_{i,i}$.)

Lemma 4.2 *Assume that the source ditribution is uniform and that g kinds of costs $c_1, c_2, \cdots, c_g$ are assigned to k source states. Let k_i be the number of source states with cost c_i for $i = 1, \cdots, g$. If there is a BIBD with mutually balanced nested subdesigns, then there exist an optimal authentication system with parameters*

$$
\begin{aligned}
&|\mathcal{S}| = k, \qquad |\mathcal{M}| = v, \\
&|\mathcal{E}| = \frac{\lambda k(k-1)}{v(v-1)}, \\
&K = \sum_{i=1}^{g} k_i c_i, \\
&R = \sum_{i=1}^{g}\sum_{i=1}^{g} r_i c_i = \frac{1}{v-1}\sum_{i=1}^{g} c_i \lambda_{i,i}(k_i - 1), \\
&\Lambda = \sum_{i=1}^{g}\sum_{j=1}^{g} \lambda_{i,j}(c_i + c_j) = 2\sum_{i=1}^{g} c_i \sum_{j=1}^{g} \lambda_{i,j}.
\end{aligned}
$$

The proof of Lemma 4.2 is immediate, since we can correspond each element of subblocks B_i to a source state with cost c_i.

A construction of a BIBD with mutually balanced nested subdesigns is given by Fuji-Hara and Kuriki(1988) which is based on the familiar method of differences (see also, Wilson(1972, Lemma 5 and Theorem 7) and Jimbo and Kuriki(1983)). For the reader's convenience, we refer their construction.

Lemma 4.3(Fuji-Hara and Kuriki) *Let $v = pf + 1$ be a prime power and $X = GF(v)$*

be a finite field of order v. Let $H_u^p = \{x^i | i \equiv u(\mathrm{mod}\ p)\}$, *where* x *is a primitive element of* X. *We select an element* c_u *from each* H_u^p *and let* $C_p = \{c_1, c_2, \cdots, c_{p-1}\}$. *For any mutually disjoint subsets* $L_1, L_2, \cdots, L_g$ *of* C_p, *let* $B_i = \{lh | l \in L_i, h \in H_0^p\}$ *and* $B = B_1 \cup B_2 \cup \cdots \cup B_g$. *Let* $\mathcal{B} = \{y + cB | y \in X, c \in C_p\}$ *and* $\mathcal{B}_i = \{y + cB_i | y \in X, c \in C_p\}$ *for* $i = 1, \cdots, g$. *Then the triple* $(X, \mathcal{B}, \Pi)$ *is a BIBD with mutually balanced nested subdesigns having the parameters* $k_i = pfl_i, \lambda_i = l_i(fl_i - 1)$ *and* $\lambda_{i,j} = fl_il_j$, *where* $\Pi = \{\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_g\}$.

By Lemma 4.2 and Lemma 4.3, we can obtain the following theorem.

Theorem 4.3 *Let v=pf+1 be a prime power. And let* $k_i = pfl_i$ *for* $i = 1, 2, \cdots, g$, *where* $\sum_{i=1}^{g} l_i \leq p$. *Then there exists an optimal authentication system with parameters of Lemma 4.2.*

5. Optimality for deceiving probability

Finally, we shall mention about optimal authentication system for deceiving probability P_I and P_S. We assume here that the source distribution is general similarly to Section 3. Since we restrict to $c(s) = 1$ for all $s \in S$, we may weaken the condition of optimality from that of Theorem 3.2. This is just the case where Simmons(1982,1984,1985), Brickell(1984) and Stinson(1987) treated. Stinson(1987) gave a construction of authentication systems attaining the bounds of Corollaries 2.3 and 2.4. Here, we shall obtain a general condition to attain the bounds of Corollaries 2.3 and 2.4, which includes Stinson's construction as a special case. We prepare the following two lemmas.

Lemma 5.1. *For any source distribution* $\{P_r(S = s)\}$ *and for any distinct message* m, n,

$$\sum_e P_r(M = m|E = e)\delta(e, n) = \text{ const. } (= \lambda)$$

holds if and only if

$$\sum_e \chi(s, f_e(m))\delta(e, n) = \lambda$$

is satisfied for any distinct m, n, *where*

$$\chi(s, s') = \begin{cases} 1 & \text{if } s = s', \\ 0 & \text{otherwise} \end{cases}$$

for $s, s' \in S$.

Proof. We have

$$\begin{aligned} \lambda &= \sum_e P_r(M = m|E = e)\delta(e, n) \\ &= \sum_e \sum_s P_r(S = s)\chi(s, f_e(m))\delta(e, n) \\ &= \sum_s P_r(S = s) \sum_e \chi(s, f_e(m))\delta(e, n). \end{aligned}$$

This equality must hold for any probability distribution $\{P_r(S=s)\}$, thus the theorem is proved. **Q.E.D.**

Lemma 5.2. *If*

$$\sum_e \chi(s, f_e(m))\delta(e,n) = \lambda$$

holds for any distinct messages m, n, then

$$\sum_e \chi(s, f_e(m)) = const. \tag{5.1}$$

and

$$\lambda = \frac{b(k-1)}{v(v-1)}. \tag{5.2}$$

Proof. By the assumption we have

$$\sum_{n(\neq m)} \sum_e \chi(s, f_e(m))\delta(e,n) = (v-1)\lambda.$$

On the other hand,

$$\sum_e \sum_{n(\neq m)} \chi(s, f_e(m))\delta(e,n) = \sum_e \chi(s, f_e(m))(k-1).$$

Combining these two equalities, we obtain (5.1). Further,

$$\sum_m \sum_s \sum_e \chi(s, f_e(m)) = \sum_m \sum_s \frac{(v-1)\mu}{k-1} = v\frac{k(v-1)\lambda}{k-1}$$

and

$$\sum_m \sum_e \sum_s \chi(s, f_e(m)) = \sum_m \sum_e \delta(e,m) = bk$$

hold. **Q.E.D.**

Theorem 5.1. *If there exists an authentication system satisfying*

$$\sum_e \chi(s, f_e(m))\delta(e,n) = \lambda \tag{5.3}$$

for any distinct messages m, n then this system attains the bound of Corollaries 2.3 and 2.4.

Proof. Recall that $\gamma(e,m,n) = \delta(e,m)\delta(e,n)$ for this case. Then by Lemmas 5.1 and 5.2,

$$\begin{aligned} P_S &= \sum_e \sum_m \sum_{n(\neq m)} r_e^* P_r(M=m|E=e) q^*_{n|m} \delta(e,m)\delta(e,n) \\ &\leq \frac{1}{|\mathcal{E}|} \sum_m \sum_{n(\neq m)} q^*_{n|m} \sum_e P_r(M=m|E=e)\delta(e,n) \\ &= \frac{1}{|\mathcal{E}|} \sum_m \sum_{n(\neq m)} q^*_{n|m}\mu \\ &= \frac{v}{b}\lambda \\ &= \frac{k-1}{v-1}. \end{aligned}$$

Finally, by Lemma 5.2,

$$\sum_e \gamma(e,n) = \sum_e \sum_s \chi(s, f_e(m)) = \text{ const.}$$

holds, hence this authentication system attains the bounds of Corollaries 2.3 and 2.4.

Q.E.D.

The condition of Theorem 5.1 can be combinatorially represented as follows:

Condition 5.1. *Let $A = (a_{ij})$ be an authentication system.*

(1) The number of rows which have message m on j-th column is independent of choice of j and m. The set of rows is denoted by $I(j,m)$.

(2) Each message $n \in \mathcal{M} - \{m\}$ occurs exactly λ times in $I(j,m)$ for any j and m.

Let $A = (a_{ij})$ be an authentication system satisfying Condition 5.1. Then, by taking rows of an authentication system A for a block, we can make a combinatorial system D=$(\mathcal{M}, \mathcal{B})$. For any distinct elements m,n of $\mathcal{M}$, the number of rows containing

m and n such that m appears in i-th column is constant, denoted by λ, therefore the number of rows which contain m and n is λk. Hence, we have the following corollary.

Corollary 5.3. *If there exists an authentication system with v messages, k sources and a constant λ satisfying Condition 5.1, then there exists a $(v, k, \lambda k)$-BIBD.*

It is not known whether the converse of Lemma 5.3 holds or not. However, it is shown by Stinson(1987) that if there exist a (v, k, λ)-BIBD, then there is an authentication system with k sources, v messages and $b = \lambda v(v-1)/(k-1)$ keys. This is the only known construction of authentication systems satisfying Condition 5.1.

References

[1] T. Beth, D. Jungnickel, H. Lenz(1986), *Design Theory*, Bibliographisches Institut Mannheim.

[2] E. F. Brickell(1984), A Few Results in Message Authentication, *Congressus Numerantium* **43**, 141-154.

[3] R. Fuji-Hara and S. Kuriki(1988), Constructions of balanced arrays with s symbols, submitted.

[4] M. Jimbo and S. Kuriki(1983), Constructions of nested designs, *ARS Combinatoria* **16**, 275-285.

[5] G. J. Simmons(1982), A Game Theory Model of Digital Message Authentication, *Congressus Numerantium* **34**, 413-424.

[6] G. J. Simmons(1984), Message Authentication: A Game on Hypergraphs, *Congressus Numerantium* **45**, 161-192.

[7] G. J. Simmons(1985), Authentication Theory/Coding Theory, in " *Advances in Cryptology: Proceedings of CRYPTO 84*", Lecture Notes in Computer Science, **196**, 411-432, Springer Verlag, Berlin.

[8] D. R. Stinson(1987), Some Constructions and Bounds for Authentication Codes, *CRYPTO 86 Proceedings, Lecture Notes in Computer Science*, **263**, 418-425, Springer Verlag, Berlin. [9] R. M. Wilson(1972), Cyclotomy and Difference Families in Elementary Abelian groups,*Journal of Number Theory*, **4**, 220-245.

Appendix. The existence of the value of substitution game

Here, we shall show the existence of the value of the substitution game.

Let $\{r_e\} = \{P_r(E = e)\}$ be mixed strategies for the transmitter and receiver, and let $\{q_{n|m}\} = \{P_r(N = n|M = m)\}$ be mixed strategies for the opponent when the message m is sent by the transmitter. Then the expected loss is

$$v(r, q) = \sum_e \sum_m \sum_n r_e P(M = m|E = e)\gamma(e, m, n)q_{n|m}.$$

The transmitter and receiver want to minimize $\max_q v(r, q)$ with respect to $\{r_e\}$, and the opponent wants to maximize $\min_r v(r, q)$ with respect to the strategies $\{q_{n|m}\}$. The computing problem of $\min_r \max_q v(r, q)$ is equivalent to solve the following linear programming.

Problem I:

$\min \sum_m v_m$

subject to

$$\sum_e r_e P(M = m|E = e)\gamma(e, m, n) \leq v_m, \qquad \text{for any } m \text{ and } n.$$
$$\sum_e r_e = 1, \qquad r_e \geq 0.$$

On the other hand, to get the value $\max_q \min_r v(r, q)$ is equivalent to solve the following linear programming.

Problem II:

$\max v$

subject to

$$\sum_m \sum_n P(M = m|E = e)\gamma(e, m, n)q_{n|m} \geq v \qquad \text{for any } e,$$
$$\sum_n q_{n|m} = 1 \qquad \text{for any } m, \qquad q_{n|m} \geq 0.$$

These problems are dual each other. By the well-known duality theorem, they have

the same optimal solution for objective functions if one of these problem has a feasible solution. And it is obvious that there are feasible solutions for these problems. Hence we have the following theorem:

Theorem A.1. *There exist the value of the substitution game.*

Let $\{r_e^*\}$ and $\{q_{n|m}^*\}$ are optimal strategies for the substitution game. Then the following corollary holds.

Corollary A.2.

$$\sum_e r_e^* P(M=m|E=e)\gamma(e,m,n) \begin{cases} = v_m & \text{if } q_{n|m}^* > 0, \\ \leq v_m & \text{if } q_{n|m}^* = 0, \end{cases}$$

and

$$\sum_m \sum_n P(M=m|E=e)\gamma(e,m,n) q_{n|m}^* \begin{cases} = V_S & \text{if } r_e^* > 0, \\ \geq V_S & \text{if } r_e^* = 0, \end{cases}$$

where V_S is the value of substitution game and $V_S = \sum_m v_m$.