# Near-perfect Protection and Key Strategies in Authentication Codes under Spoofing Attack of Order $r$

R. Safavi-Naini *

L. Tombak †

Department of Computer Science
University of Wollongong
Northfields Ave., Wollongong 2522, AUSTRALIA

ABSTRACT. Near-perfect protection is a useful extension of perfect protection which is a necessary condition for authentication systems that satisfy Pei-Rosenbaum's bound. Near-perfect protection implies perfect protection for key strategies, defined in the paper, in which the enemy tries to guess the correct key. We prove a bound on the probability of deception for key strategies, characterize codes that satisfy the bound with equality and conclude the paper with a comparison of this bound and Pei-Rosenbaum's bound.

## 1 Introduction

In this paper we study authentication codes (A-codes) under spoofing attack of order $r$. The following is a brief account of the main results of this study.

We consider the class of $(M, k, E)$ A-codes, where $M$, $k$ and $E$ are the number of cryptograms, source states and encoding rules respectively, and assume that the enemy has intercepted a sequence of $r$ cryptograms, encoded under the same key. An A-code provides perfect protection if the enemy's best strategy is random selection from the remaining, $M-r$, cryptograms. In this case the probability of deception $P_r$ is minimum and we

*Support for this project was partly provided by Australian Research Council grant A49030136.

†Support for this project was provided by Australian Research Council grant A49030136.

have $P_r = (k-r)/(M-r)$. For these A-codes we obtain a lower bound, $E \geq E_r$, on the number of encoding rules. We note that $E_r$ denotes the minimum number of encoding rules and hence if an A-code has $E \geq E_r$ keys, it cannot provide perfect protection.

We say an A-code provides *near-perfect protection* if enemy's best strategy is random selection from the set of valid cryptograms whose size $C_r$, $k-r \leq C_r \leq M-r$, depends only on $r$ and not the actual intercepted sequence. Near-perfect protection is a useful extension of perfect protection. We note that the A-codes that satisfy information theoretic bounds do not necessarily provide perfect protection but we will show that they must provide near-perfect protection.

We will also study key strategies. Key strategies model enemy's attack when he/she attempts at *guessing* the correct key and using it to construct a fraudulent message. We will show that an A-code that provides near-perfect protection provides perfect protection for this subset of strategies and hence the enemy's best strategy is randomly selecting a key, from the subset of keys that are valid for the intercepted sequence. We will derive a bound on $P_r$, characterize the A-codes that satisfy the bound with equality and show that near-perfect protection is a necessary condition for equality in the bound. We will conclude by giving a comparison of this bound and Pei-Rosenbaum's bound.

## 2 Preliminaries

We consider an authentication scenario with three participants: a transmitter and receiver (*communicants*) who want to communicate over a publicly exposed channel and an *enemy* who tries to deceive the receiver into accepting a fraudulent message as genuine. We are only concerned with honest communicants. An $(M,k,E)$ *authentication code* ($A$-code) is a collection $\mathcal{E}$, $|\mathcal{E}| = E$, of mappings, called *encoding rules*, from the set $\mathcal{S}$, $|\mathcal{S}| = k$, of *source states* into the set $\mathcal{M}$, $|\mathcal{M}| = M$, of *codewords*. The code provides protection only if $k < M$. The *incidence matrix* of an $A$-code is a zero-one matrix, $A = [a_{im}]$, of size $E \times M$ in which $a_{im} = 1$ if $m \in \mathcal{M}(e_i)$ and zero otherwise; $\mathcal{M}(e_i)$ is the subset of codewords that are authentic under the key $e_i$. Matrix $A$ has exactly $k$ ones in each row. Let $m^r$ denote a sequence of $r$ distinct cryptograms, $m^r = (m_1^r, m_2^r, ..., m_r^r)$, and use $\mathcal{M}^r$ to denote the collection of all such $m^r$'s. We use, $\mathcal{M}\backslash m^r$ to denote the subset of codewords that do not occur in $m^r$, $\mathcal{E}(m)$ to denote the subset of keys that are incident with $m \in \mathcal{M}$, i.e. $\mathcal{E}(m) = \{e_i \in \mathcal{E} | a_{im} = 1\}$, and $\mathcal{E}(m^r)$ to denote the subset of keys that are incident with all codewords $m_i^r$ occurring in $m^r$. The sequence $m^r$ is authentic under a key $e_i$ if $m_j^r \in \mathcal{M}(e_i)$ for all $1 \leq j \leq r$. For a set $\mathcal{X}$ we use $X$ to denote its cardinality; for example $E(m)$ denotes the cardinality of $\mathcal{E}(m)$. We use $m^r m'$ to denote the sequence obtained by

concatenating $m^r$ and $m'$ and note that $\mathcal{E}(m^r m') = \mathcal{E}(m^r) \bigcap \mathcal{E}(m')$.

An encoding rule may assign two cryptograms to one source state. In this case we have an $A$-code with *splitting*. In this paper we only consider $A$-codes without splitting although some of the results can be generalized to codes with splitting. In an A-code without splitting, a unique source state $s(e_i, m)$ can be determined by an encoding rule $e_i \in \mathcal{E}$ and a cryptogram $m \in M(e_i)$. Similarly a unique source sequence, $s^r = (s(e_i, m_1^r), \cdots, s(e_i, m_r^r))$, can be determined by $e_i$ and $m^r$. We use $P_S(s^r) = P_S(s(e_i, m_1^r), \cdots, s(e_i, m_r^r))$ to denote the probability of a sequence of source states and $P(m^r)$ to denote the probability of a sequence, $m^r$, of codewords. We assume that $P_S(s^r) = 0$ if $s_i^r = s_j^r$ for some $i \neq j$, $1 \leq i, j \leq r$. The communicants use a probability distribution $\pi = (\pi_1, \cdots, \pi_E)$ on the key space as their strategy and use it to choose an encoding rule $e$. The enemy may *impersonate* the transmitter by introducing a codeword $m'$ into the channel or use a *spoofing attack of order* $r$ in which he/she uses the knowledge of a sequence, $m^r$, of $r$ intercepted codewords to construct a fraudulent codeword $m' \in \mathcal{M} \backslash m^r$. The enemy is successful if $m' \in \mathcal{M}(e)$. Impersonation is spoofing of order zero and spoofing of order one is called *substitution*.

Suppose an enemy has intercepted a sequence of $r$ cryptograms. We consider two different types of enemy's action and define two classes of strategies accordingly:

- the enemy tries to construct a valid cryptogram by guessing the correct key; he/she chooses a key $e \in \mathcal{E}(m^r)$, using a probability distribution $p^{m^r}$ on the set $\mathcal{E}(m^r)$, and then randomly selects a cryptogram $m' \in \mathcal{M}(e) \backslash m^r$. The enemy's strategy is the collection $\{p^{m^r}, m^r \in \mathcal{M}^r\}$ where $p^{m^r}$ is a probability distribution on the set $\mathcal{M} \backslash m^r$. This is called a *key strategy*.

- Enemy tries to guess a valid cryptogram; he/she selects a fraudulent cryptogram $m' \in \mathcal{M} \backslash m^r$ using a probability distribution $q^{m^r}$ on $\mathcal{M} \backslash m^r$. Enemy's action in this case is similar to Simmons' model of attack [?], and is given by $\{q^{m^r}, m^r \in \mathcal{M}^r\}$. This is called a *message strategy*.

The relation between the two strategies and their significance is further discussed in the rest of this paper.

We use $P_r^K$ and $P_r^M$ to denote the best probability of success for spoofing attack of order $r$ in the above cases, respectively.

## 3 Probability of deception

In a message strategy the communicants use a strategy $\pi$ and the enemy uses a strategy given by $\{q^{m^r}, m^r \in \mathcal{M}^r\}$. The probability of deception

when the enemy has intercepted $m^r$ and wants to introduce the cryptogram $m'$ is the $payoff(m, m')$,

$$payoff(m^r, m') = \frac{\sum_j \pi_j a_{jm_1^r} a_{jm_2^r} \cdots a_{jm_r^r} a_{jm'} P_S(e_j, m^r)}{P(m^r)}. \quad (1)$$

This can be used to find $p_r^M$, probability of deception for the given strategies,

$$p_r^M = \sum_{m^r \in \mathcal{M}^r} \sum_{m' \in \mathcal{M} \setminus m^r} \sum_j \pi_j a_{jm_1^r} a_{jm_2^r} \ldots a_{jm_r^r} a_{jm'} P_S(e_j, m^r) q_{m'}^{m^r}. \quad (2)$$

In a key strategy the enemy's strategy is $\{p^{m^r}, m^r \in \mathcal{M}^r\}$ where $p^{m^r}$ is a probability distribution on the set $\mathcal{E}(m^r)$. Proposition 3.1 gives an expression for, $p_r^K$, the probability of deception in this case.

**Proposition 3.1.**

$$p_r^K = \frac{1}{k-r} \sum_{m^r \in \mathcal{M}^r} \sum_{i=1}^{E} \sum_{j=1}^{E} \pi_j p_i^{m^r} a_{jm_1^r} \ldots a_{jm_r^r} P_S(e_j, m^r) \sum_{m' \in \mathcal{M} \setminus m^r} a_{jm'} a_{im'}. \quad (3)$$

**Proof:** $p_r^K$ is obtained by averaging the probability of success when communicants and the enemy are using their pure strategies. A pure strategy of the communicants is choosing a key $e_i$ and an enemy's pure strategy is choosing a key $e_j$ followed by randomly selecting a cryptogram $m' \in M(e_i)$. Payoff of the game, that is, the probability of success of the enemy when he/she has intercepted a sequence $m^r$ of cryptograms and chooses $e_i$ is,

$$\text{payoff}(m^r, e_i) = \sum_j \frac{\pi_j a_{jm_1^r} \cdots a_{jm_r^r} P_S(m^r, e_j)}{P(m^r)} \times \frac{\sum_{m' \in \mathcal{M} \setminus m^r} a_{im'} a_{jm'}}{k-r}, \quad (4)$$

$$p_r^K = \sum_{m^r, i} P(m^r) p_i^{m^r} payoff(m^r, e_i), \quad (5)$$

and we have,

$$P_r^K = \sum_{m^r} P(m^r) Max_{e_i} payoff(m^r, e_i).$$

□

We note that for any key strategy $\{p^{m^r}, m^r \in \mathcal{M}^r\}$, with probability of deception equal to $p_r^K$, one can obtain a corresponding message strategy

$\{q^{m^r}, m^r \in \mathcal{M}^r\}$ with $p_r^M = p_r^K$ . This can be verified by substituting,

$$q_{m'}^{m^r} = \frac{1}{k-r} \sum_{i=1}^{E} p_i^{m^r} a_{im'}, \ m' \in \mathcal{M} \backslash m^r,$$

in expression (2) which results in (3) and $p_r^M = p_r^K$.

**Corollary 3.1.** $P_r = P_r^M \geq P_r^K$.

## 4 Perfect protection

If enemy's best strategy for any sequence $m^r$ of $r$ cryptograms is random selection from the set of valid cryptograms (or for key strategies, the set of valid keys) then the value of the game is independent of the enemy's strategy. The size of these sets in general depend on $m^r$.

Suppose the enemy has intercepted a sequence $m^r$ of $r$ cryptograms. An A-code provides *perfect protection for spoofing attack of order* $r$ [?], if

$$payoff(m^r, m') = \frac{k-r}{M-r}, \ \forall m^r \in \mathcal{M}^r, m' \in \mathcal{M} \backslash m^r.$$

In this case the code needs at least $E_r$ encoding rules,

$$E_r = \frac{M(M-1)\cdots(M-r)}{k(k-1)\cdots(k-r)}.$$

If $E < E_r$, there exists $m' \in \mathcal{M} \backslash m^r$ with $payoff(m^r, m') = 0$; that is, there exists a sequence $m^r$ for which the set of valid cryptograms $C_{m^r}$, defined as,

$$C_{m^r} = (\bigcup_{e_i \in \mathcal{E}(m^r)} \mathcal{M}(e_i)) \subset \mathcal{M},$$

has less than $M-r$ elements.

An $A$-code provides *near-perfect protection against spoofing attack of order* $r$ if for any $m^r \in \mathcal{M}^r$, with $E(m^r) > 0$, enemy's best strategy is random selection from $C_{m^r}$, and $C_{m^r} = C_r$. For an $A$-code with near-perfect protection $payoff(m^r, m') = (k-r)/C_r$, $m' \in \mathcal{M} \backslash m^r$ and

$$P_r = P_r^M = \sum_{m^r \in \mathcal{M}^r} P(m^r) \frac{k-r}{C_r} = \frac{k-r}{C_r}.$$

Near-perfect protection against spoofing attack of order $r$ ensures that the enemy's chance of success is independent of the sequence $m^r$ and his/her best strategy is to randomly select a cryptogram from $C_{m^r}$, $C_{m^r} = C_r$.

**Proposition 4.1.** *The number of encoding rules in an A-code that provides near-perfect protection for spoofing of order r satisfies the following bound,*

$$E \geq \frac{1}{P_0 P_1 \cdots P_{r-1}} \times \frac{C_r}{k-r}. \tag{6}$$

*Equality holds if and only if the code satisfies Pei-Rosenbaum's bound of order i, $0 \leq i \leq r$, and $H(\mathcal{E}|\mathcal{M}^{r+1}) = 0$.*

**Proof:** Using Theorem 3.1 in [?] we have

$$P_i \geq 2^{H(\mathcal{E}|\mathcal{M}^{i+1}) - H(\mathcal{E}|\mathcal{M}^i)}.$$

Hence

$$P_0 P_1 \cdots P_r \geq 2^{H(\mathcal{E}|\mathcal{M}^{r+1}) - H(\mathcal{E})}$$

and using $H(\mathcal{E}|\mathcal{M}^{r+1}) \geq 0$ and $H(\mathcal{E}) \leq logE$ we have

$$E \geq \frac{1}{P_0 P_1 \cdots P_r}.$$

The result follows by noting that the code provides near-perfect protection for spoofing of order $r$. □

If the code provides near-perfect protection for spoofing of all orders $i$, $1 \leq i \leq r$ then bound 6 reduces to

$$E \geq \prod_{i=0}^{r} \frac{C_i}{k-i}, \tag{7}$$

where $C_0 = M$.

**Example 4.1:** Consider the incidence matrix of an A-code with $M = 6, k = 3, E = 4$ given below. Let $r = 1$. Then $C_{m^r} = 3$ and bound 7 is satisfied with equality.

| E/M | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 0 | 1 | 1 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 | 0 | 1 |
| 4 | 1 | 0 | 0 | 0 | 1 | 1 |

An *A*-code provides *perfect protection against spoofing attack of order r for key strategies* if, for all $m^r \in \mathcal{M}^r$, the enemy's best strategy is random selection from the set $\mathcal{E}(m^r)$. In section 3 we noted that key strategies form a proper subset of message strategies. Proposition 4.2 shows that if an A-code provides near-perfect protection then it provides perfect protection for

key strategies; hence for an $A$-code with near-perfect protection, enemy's chance of success will be the same if he/she tries to guess the correct key or chooses a valid cryptogram.

**Proposition 4.2.** *If an A-code provides near-perfect protection then the code provides perfect protection for key strategies and* $P_r = P_r^M = P_r^K$.

**Proof:** We have

$$P_r = P_r^M = \sum_{m^r \in \mathcal{M}^r} P(m^r) \frac{(k-r)}{C_r}.$$

On the other hand using (4) we obtain,

$$payoff(m^r, e_i) = \sum_{j=1}^{E} \sum_{m' \in \mathcal{M} \setminus m^r} \frac{\pi_j a_{jm_1^r} \ldots a_{jm_r^r} P_S(m^r, e_j) a_{im'} a_{jm'}}{(k-r)P(m^r)}. \quad (8)$$

Since the A-code provides near-perfect protection, we have

$$\sum_{j=1}^{E} \frac{\pi_j a_{jm_1^r} \ldots a_{jm_r^r} a_{jm'} P_S(m^r, e_j)}{P(m^r)} = \frac{k-r}{C_r},$$

which implies that

$$payoff(m^r, e_i) = \frac{k-r}{C_r}.$$

Using (3) we have,

$$P_r^K = \sum_{m^r \in \mathcal{M}^r} P(m^r) \frac{k-r}{C_r} = P_r^M.$$

□

**Corollary 4.1.** *Let* $P_r = \dfrac{k-r}{M-r}$. *Then the enemy's best strategy is the random key strategy.*

## 5 Information theoretic bounds

Pei-Rosenbaum [?, ?] bound is the main information-theoretic lower bound on $P_r$. For $r = 0$, this bound reduces to Simmons' bound [?] for impersonation. Proposition 5.1 shows that equality in the bound is obtained for A-codes with near-perfect protection and a *matching source*, that is, a source whose probability distribution satisfies condition 2 of this proposition. In theorem 5.2 we obtain a second bound on $P_r^K$ (and hence $P_r$) and then give a comparison of the two bounds.

**Theorem 5.1 (theorem 3.1 [14]).**

$$P_r \geq 2^{-(H(E|M^r)-H(E|M^{r+1}))}, \tag{9}$$

*and equality holds if and only if,*

1. *the probability that $m'$ is accepted as authentic if $m^r$ is observed is constant and $P_r = payoff(m', m^r)$.*
2. *the conditional probability $p(m'|e, m^r)$ that $m'$ is the next cryptogram sent by the transmitter, given that $e$ is the actual encoding rule and sequence $m^r$ is received, is constant for all $e \in \mathcal{E}(m, m^r)$.*

Bound (9) is applicable to a general $A$-codes. For $A$-codes without splitting the equality in bound 9 can be obtained by another set of conditions given in proposition 5.1.

Let $P_S(m'|e_i, m^r)$ denote the probability of the *source state* that is mapped to $m'$ when $m^r$ is received and $e_i$ is used by the communicants.

**Proposition 5.1.** *For an $A$-code without splitting equality in (9) is obtained if and only if*

1. *the code provides near-perfect protection for spoofing attack of order $r$;*
2. *$P_S(m'|e_i, m^r)$ is independent of $e_i$, for all $m^r \in \mathcal{M}^r$, $m' \in \mathcal{M}\backslash m^r$ with $E(m^r, m') > 0$.*

*Moreover in the case of equality $P_r = (k-r)/C_r$.*

**Proof:** *Necessity.* Using condition 1 of theorem 5.1 and expression (1) we have,

$$\sum_{m' \in \mathcal{M}\backslash m^r} P_r = C_{m_r} P_r = \sum_{m'} payoff(m^r, m') = (k-r),$$

and hence $C_{m_r}$. We also have,

$$\begin{aligned} p(m'|e_j, m^r) &= \frac{p(e_j, m', m^r)}{p(e_j, m^r)} = \frac{\pi_j a_{jm_1^r} \cdots a_{jm_r^r} a_{jm'} P_S(e_j, m^r, m')}{\pi_j a_{jm_1^r} \cdots a_{jm_r^r} P_S(e_j, m^r)} \\ &= P_S(m'|e_j, m^r), \end{aligned} \tag{10}$$

which completes the proof. Proof of sufficiency can be given in a similar way. □

A second information-theoretic bound on $P_r$ can be obtained by generalizing a bound originally proved by Brickell-Simmons [?] and later tightened

by Stinson [?]. Our proof shows that this lower bound is in fact a lower bound on $P_r^K$. It also gives a characterization of authentication systems that satisfy the bound with equality.

Let $\delta_r(e_i, m^r, m')$ be,

$$\delta_r(e_i, m^r, m') = \frac{\sum_{j=1}^{E} \pi_j a_{jm_1^r} \ldots a_{jm_r^r} a_{jm'} P_S(e_j, m^r)}{\pi_i a_{im_1^r} \ldots a_{im_r^r} a_{im'} P_S(e_i, m^r)}, \tag{11}$$

and $\delta_r = min_{i,m^r,m'} \delta_r(e_i, m^r, m')$.

**Theorem 5.2.**

$$P_r^K \geq \delta_r 2^{-H(E|M^r)}. \tag{12}$$

*In the case of equality the A-code satisfies the following properties:*

*(i)* $E(m^r) = const = \lambda_{r-1}$, *for all* $m^r \in \mathcal{M}^r$ *with* $E(m^r) > 0$;

*(ii)* $E(m^r, m') = const = \lambda_r = \delta_r$ *for all* $m^r \in \mathcal{M}^r$ *and* $m' \in \mathcal{M}^r \backslash m^r$ *with* $E(m^r, m') > 0$;

*(iii)* $\pi_j P_S(e_j, m^r)$ *is independent of* $j$ *for all* $m^r \in \mathcal{M}^r$ *and* $1 \leq j \leq E$;

*(iv)* $P_r^M = P_r^K = \frac{\delta_r}{\lambda_{r-1}} = \frac{\lambda_r}{\lambda_{r-1}} = \frac{k-r}{C_r}$ *and the A-code provides near-perfect protection.* ;

*Moreover the first three conditions are sufficient conditions for an A-code to satisfy bound (12) with equality.*

**Proof:** See appendix.

It is interesting to compare the bounds 9 and 12. Let $\alpha_r$ and $\beta_r$ denote the value of the right hand sides of the two bounds respectively. If an $(M, k, E)$ A-code satisfies $P_r = \alpha_r$ or $P_r = \beta_r$ then it provides near-perfect protection. Hence for all $m^r \in \mathcal{M}^r$ with $E(m^r) > 0$ we must have $C_{m^r} = C_r$ which is a requirement on the incidence matrix of the code. On the other hand if an A-code provides near-perfect protection and there exists a source that satisfies condition 2 of proposition 5.1, then the bound 9 is satisfied with equality and the A-system uses all the redundancy, introduced during the encoding process, for providing protection. However $P_r = \beta_r$ requires the incidence matrix of the A-code to satisfy much stricter conditions.

In general, if $P_r = \alpha_r$ then $\alpha_r \geq \beta_r$ and if $P_r = \beta_r$ then $\beta_r > \alpha_r$.

If the A-code does not provide near-perfect protection neither of the bounds can be satisfied with equality. Proposition 5.2 shows that in some cases bound 9 is a tighter bound. However such a statement, in general, is not possible.

**Proposition 5.2.** *If $P_S(m'|e_i, m^r)$ is independent of $i$ then*

$$\alpha_r \geq \beta_r.$$

**Proof:** If $P(m'|e_i, m^r)$ is independent of $i$ then

$$\begin{aligned} H(E|M^{r+1}) &= \sum_{i,m^{r+1}} P(e_i, m^{r+1}) \log \frac{1}{P(e|m^{r+1})}, \\ &= \sum_{i,m^{r+1}} P(e_i, m^{r+1}) \log \delta(e_i, m^r, m') \geq \log \delta_r \end{aligned}$$

and

$$2^{-(H(E|M^r)-H(E|M^{r+1}))} \geq \delta_r 2^{-H(E|M^r)}.$$

□

## Appendix

**Proof of theorem 5.2:** The proof is similar to Stinson's Lemma 2.7 [?]. We note that using (4) we have

$$\begin{aligned} \text{payoff}(m^r, e_i) = \frac{1}{(k-r)P(m^r)} & \sum_{m' \in \mathcal{M} \setminus m^r} \\ & \delta_r(m^r, m', e_i) P_S(m^r, e_i) \pi_i a_{im_1^r} \ldots a_{im_r^r} a_{im'} \\ = \frac{\pi_i P_S(e_i, m^r) a_{im_1^r} \ldots a_{im_r^r}}{P(m^r)(k-r)} & \\ \sum_{m'} \delta_r(m^r, m', e_i) a_{im'} \geq \frac{\delta_r \pi_i P_S(e_i, m^r)}{P(m^r)}. & \end{aligned} \tag{13}$$

Let $v_r^K(m) = Max_i(\text{payoff}(e_i, m^r))$. Then we have $P_r^K = \sum_{m^r \in \mathcal{M}^r} P(m^r) v_r^K(m^r)$ and [?]

$$H(E|M^r) \quad \geq \quad -log \frac{P_r^K}{\delta_r},$$

which proves the bound.

Equality holds if and only if $\delta_r(e_i, m^r, m') = \delta_r$ is constant and $P_r^K = v_r^K(m^r)$, $\forall m^r$. If $\delta_r(m^r, m', e_i) = \delta_r$, then

$$\delta_r \times \pi_i P_S(e_i, m^r) = \sum_{j=1}^{E} \pi_j a_{jm_1^r} \ldots a_{jm_r^r} a_{jm'} P_S(e_j, m^r),$$

which means that $\pi_i P_S(e_i, m^r)$ is independent of $i$. In this case

$$\delta_r = \sum_j a_{jm_1^r} \ldots a_{jm_r^r} a_{jm'} = \delta_r.$$

Moreover since $P_r^K = v_r^K(m)$ we have,

$$P_r^K = v_r^K(m^r) = Max_i(\text{payoff}(e_i, m^r)) = \frac{\pi_i P_S(e_i, m^r)}{P(m^r)(k-r)} \sum_{m'} \delta_r(m^r, m', e_i)$$
$$= \lambda_r \times \frac{\pi_i P_S(e_i, m^r)}{P(m^r)},$$

and since,

$$P(m^r) = \sum_i \pi_i P_S(e_i, m^r) a_{im_1^r} \ldots a_{im_r^r} = \pi_i P_S(e_i, m^r) \sum_i a_{im_1^r} \ldots a_{im_r^r},$$

we have,

$$P_r^K = \frac{\lambda_r}{\sum_i a_{im_1^r} \ldots a_{im_r^r}}.$$

Hence $\sum_i a_{im_1^r} \ldots a_{im_r^r} = \lambda_{r-1}$ is a constant and $P_r^K = \lambda_r / \lambda_{r-1}$. But for any $m^r \in \mathcal{M}^r$ we have the following equality $\lambda_{r-1} \times (k-r) = \lambda_r \times C_{m^r}$. It implies that $C_{m^r} = C_r$ and $P_r^K = (k-r)/C_r$. Also using expression (1) we have

$$payoff(m^r, m') = \frac{\pi_j P_S(e_j, m^r) \sum_j a_{jm_1^r} \cdots a_{jm_r^r} a_{jm'}}{\pi_j P_S(e_j, m^r) \sum_j a_{jm_1^r} \cdots a_{jm_r^r}} = \frac{\lambda_r}{\lambda_{r-1}} = \frac{k-r}{C_r},$$

and the $A$-code provides near perfect protection for class $M_r$ and perfect protection for class $K_r$. To prove the sufficiency of 1-3 we note that if $\pi_i P_S(e_i, m^r)$ and $\sum_j a_{jm_1^r} \ldots a_{jm_r^r} a_{jm'}$ are constants then from (11) we have $\delta_r(m^r, m', e_i) = \delta_r = \lambda_r$ independent of $m^r, m', i$. Also

$$v_r^K = Max_i(\text{payoff}(m^r, e_i)) = Max_i(\frac{\pi_i P_S(e_i, m^r)\delta_r}{P(m^r)}) = \frac{\delta_r}{\lambda_{r-1}},$$

and $P_r^K = \sum_{m^r} P(m^r) v_r^K(m^r) = \delta_r / \lambda_{r-1} = \lambda_r / \lambda_{r-1}$. To prove condition 5.2 we note that in general $P_r^M \geq P_r^K$. If the $A$-code satisfies conditions 1-3 of theorem 5.2 we have

$$p_r^M(m^r, m') = \frac{\pi_j P_S(e_j, m^r) \sum_j a_{jm_1^r} \cdots a_{jm_r^r} a_{jm'}}{\pi_j P_S(e_j, m^r) \sum_j a_{jm_1^r} \cdots a_{jm_r^r}} = \frac{\lambda_r}{\lambda_{r-1}},$$

and so the best strategy of class $M^r$ is uniform strategy. That is, the $A$-code provides near-perfect protection and so

$$P_r^M = P_r^K = \frac{\lambda_r}{\lambda_{r-1}}.$$

□

## References


[1] V. Fak, Repeated Use of Codes with Detect Deception, *IEEE Transactions on Information Theory*, vol 25, no 2, March (1979), 233–234.

[2] E.F. Brickell, A few results in message authentication, *Congressus Numerantium* 43 (1984), 141–154.

[3] J.L. Massey, *Cryptography, a selective survey*, Digital Communications, ed.E. Biglieri and G. Pratti, Elsevier Science Publ., North-Holland, (1986), 3–25.

[4] D. Pei *Information - Theoretic Bounds for Authentication Codes and PBIB* , Proceedings Asiacrypt, (1991), Rump Session.

[5] G.J. Simmons, A game theory model of digital message authentication, *Congressus Numerantium* 34 (1982), 413–424.

[6] G.J. Simmons, Authentication Theory/Coding Theory, *Proceedings Crypto 84, Lecture Notes in Computer Science* 196 (1985), 411–432.

[7] D.R. Stinson, Some Constructions and Bounds for Authentication Codes, *Journal of Cryptology* 1 (1988), 37–51.

[8] D.R. Stinson, The combinatorics of authentication and secrecy codes, *Journal Cryptology* 2 (1990), 23–49.

[9] D.R. Stinson, Combinatorial characterization of authentication codes, *Proceedings Crypto 91, Lecture Notes in Computer Science* 576 (1992), 62–72.

[10] J.H. Dinitz, D.R. Stinson, *Contemporary Design Theory* , John Wiley and Sons, Inc., New-York, 1992.

[11] R. Safavi-Naini, L. Tombak, Authentication Codes under Impersonation Attack, *Proceedings of Auscrypt 1992, Lecture Notes in Computer Science* 718 (1993), 35–47.

[12] L. Tombak, R. Safavi-Naini, Authentication Codes with Perfect Protection, *Proceedings of Auscrypt 1992, Lecture Notes in Computer Science* 718 (1993), 15–26.

[13] R. Safavi-Naini, L. Tombak, Optimal Authentication Systems, *Proceedings of Auscrypt 1992, Lecture Notes in Computer Science* 765 (1994), 12–27. *Proc. of Eurocrypt 1993*, to appear.

[14] U. Rosenbaum, A Lower Bound on Authentication After Having observed a sequence of messages, *Journal of Cryptology*, No 3, Vol 6 (1993), 135–156.