Combinatorial Bounds for Authentication Codes with Arbitration

Kaoru KUROSAWA *and* Satoshi OBANA

Department of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan
E-mail kkurosaw@ss.titech.ac.jp

Abstract. Unconditionally secure authentication codes with arbitration (A^2-codes) protect against deceptions from the transmitter and the receiver as well as that from the opponent.
In this paper, we present combinatorial lower bounds on the cheating probabilities for A^2-codes in terms of the number of source states, that of the whole messages and that of messages which the receiver accepts as authentic for each source state. Previously, only entropy based lower bounds were known. Our bounds for the model without secrecy are tight because the A^2-codes given by Johansson meet our bounds with equality.

1 Introduction

In the model of unconditionally secure authentication codes (A-codes) [1], there are three participants, a transmitter, a receiver and an opponent. The opponent tries to cheat the receiver by impersonation attack and substitution attack. This model has been studied extensively so far. Lower bounds on the cheating probabilities based on entropy were given by [2, 3]. Combinatorial lower bounds were given by [4, 5, 6, 7, 8, 9]. In this model, the transmitter and the receiver are both honest and trust each other. However, it is not always the case that the two parties want to trust each other.

Inspired by this problem, Simmons introduced an extended model, A^2-code model, in which there is a fourth person, an arbiter [10, 11]. In this model, caution is taken against deception of the transmitter and the receiver as well as that of the opponent. The arbiter has access to all key information of the transmitter and the receiver, and solves disputes between them. We denote by E_R the set of keys of the receiver and by E_T denotes the set of keys of the transmitter, respectively.

In this model, there are essentially five different kinds of cheatings, impersonation by the opponent, substitution by the opponent, impersonation by the transmitter, impersonation by the receiver and substitution by the receiver. Denote these cheating probabilities by P_I, P_S, P_T, P_{R_0} and P_{R_1}. Johansson showed an entropy based lower bound on these five cheating probabilities [12]. By assuming $\max(P_I, P_S, P_T, P_{R_0}, P_{R_1}) = 1/q$, he also showed a lower bound on the size of keys in terms of q [12]. Recently, Kurosawa showed a more tight lower bound

L.C. Guillou and J.-J. Quisquater (Eds.): Advances in Cryptology - EUROCRYPT '95, LNCS 921, pp. 289-300, 1995.

for a larger set of source states by assuming $P_I = P_S = P_T = P_{R_0} = P_{R_1} = 1/q$ [15]. However, combinatorial lower bounds on the cheating probabilities are not known. (The structure of A^2-codes is not well known.)

In this paper, we present combinatorial lower bounds on $P_I, P_S, P_T, P_{R_0}, P_{R_1}$, $|E_R|$ and $|E_T|$. First, we show the following bounds for a A^2-code model without secrecy. Let $|S|$ denote the number of source states and $|M|$ denote that of messages, respectively. Assume that each $f \in E_R$ accepts c messages for each source state s. Let $l \triangleq |M|/c|S|$. Then $P_I \geq 1/l$ and $P_T \geq (c-1)|S|/(|M|-|S|)$. If $P_I = 1/l$, then $P_S \geq 1/l$. For a separable case, if $P_I = 1/l$, then $P_T \geq 1/l$. If $P_I = P_S = P_T = 1/l$, then $|E_R| \geq c|S|(l-1)+1$. Similar bounds are obtained for P_{R_0}, P_{R_1} and $|E_T|$. Our bounds on P_I, P_S, P_T, P_{R_0} and P_{R_1} are tight because the A^2-codes given by Johansson [13, 14] (in which $c = l = q$) meet our bounds with equality.

Further, we show such combinatorial lower bounds for general A^2-codes.

2 Preliminaries

2.1 Authentication code (A-code)

In the model of A-codes, there are three participants, a transmitter T, a receiver R and an opponent O. The transmitter T and thc receiver R share a common encoding rule e. On input a source state s, T computes a message $m = e(s)$ and sends m to R. R accepts or rejects m based on e. An A-code is called an A-code without secrecy if a source state is uniquely determined from a message m. It is possible that more than one message can be used to communicate a particular source state; this is called splitting. Defining

$$M(e,s) \triangleq \{m \mid e(s) = m\}$$

splitting means $|M(e,s)| > 1$. If $|M(e,s)| = 1$ for $\forall e$ and $\forall s$, the A-code is called an A-code without splitting.

We assume independent probability distributions on source states and on encoding rules, respectively. In the impersonation attack, the opponent O sends a message m to the receiver. O succeeds if m is accepted by the receiver as authentic. The impersonation attack probability P_I is defined by

$$P_I \triangleq \max_{m \in M} \Pr[\text{R accepts } m] \tag{2.1}$$

In the substitution attack, O observes a message m that is transmitted by T and substitutes m with another message $\hat{m}$. O succeeds if $\hat{m}$ is accepted by the receiver as authentic. For no splitting, the substitution attack probability P_S is defined by

$$P_S \triangleq \sum_{m \in M} \Pr(M = m) \max_{\hat{m} \neq m} \Pr[\text{R accepts } \hat{m} | \text{R accepts } m] \tag{2.2}$$

For splitting, the maximum is taken over $\hat{m}$ such that the source state conveyed by $\hat{m}$ is different from that of m. Let $S \triangleq \{s\}, E \triangleq \{e\}$ and $M \triangleq \{m\}$. We denote an A-code by (S, E, M).

Proposition 1. *[4] In an A-code without splitting, $P_I \geq |S|/|M|$. The equality holds if and only if* $\Pr[\text{R accepts } m] = |S|/|M|$ *for* $\forall m$.

Proposition 2. *[7] In an A-code without splitting and without secrecy, if $P_I = |S|/|M|$, then $P_S \geq |S|/|M|$.*

Definition 3. An orthogonal array $OA(l, k, \lambda)$ is a $\lambda l^2 \times k$ array of l symbols such that, in any two columns of the array, every one of the possible l^2 pairs of symbols occurs in exactly λ rows.

Proposition 4. *Suppose we have an A-code without splitting and without secrecy such that $P_I = P_S = |S|/|M| = 1/l$.*

1. *$|E| \geq |S|(l-1)+1$. The equality occurs if and only if the incidence matrix of E is an orthogonal array $OA(l, |S|, \lambda)$, where $\lambda = (|S|(l-1)+1)/l^2$ and each $e \in E$ is used with equal probability [8].*
2. *Also, $|E| \geq l^2$ [7].*

Proposition 5. *[9] In a splitting A-code, let $M(e) \triangleq \{m \mid e \text{ accepts } m\}$. Then,*

$$P_I \geq \min_{e \in E} \frac{|M(e)|}{|M|} \qquad P_S \geq \min_{e \in E} \frac{|M(e)| - \max_{s \in S} |M(e,s)|}{|M| - \min_{s \in S} |M(e,s)|}$$

2.2 Authentication code with arbitration (A^2-code)

We denote an A^2-code by (S, M, E_R, E_T), where $S = \{s\}$ is a set of source states, $M = \{m\}$ is a set of messages, $E_R = \{f\}$ is a set of the receiver's decoding rules and $E_T = \{e\}$ is a set of the transmitter's encoding rules.

The selection of e and f may be done in several ways. One choice is to let the receiver R choose his f and then secretly pass this on to the arbiter. In this case, the arbiter constructs e and passes this on to the transmitter T. Another choice is to do the other way around and the third approach is to let the arbiter construct both rules. In any case, on input s, T sends m such that $m = e(s)$ to R. R accepts m iff $f(m)$ is valid. The arbiter accepts m as authentic iff e can generate m.

In this model, there are five different kinds of attacks.
I, Impersonation by the opponent. The cheating probability P_I is defined in the same way as eq.(2.1). S, Substitution by the opponent. The cheating probability P_S is defined in the same way as eq.(2.2). T, Impersonation by the transmitter. The transmitter sends a message to the receiver and denies having sent it. The transmitter succeeds if the message is accepted by the receiver as authentic and if

the message is not one of the messages that the transmitter could have generated due to his encoding rule. This cheating probability P_T is defined as follows

$$P_T \triangleq \max_{e \in E_T} \max_{m \in M} \Pr[\text{R accepts } m \text{ and } m \text{ is not generated by } e | \text{T has } e] \quad (2.3)$$

R_0, Impersonation by the receiver. The receiver claims to have received a message from the transmitter. The receiver succeeds if the message could have been generated by the transmitter due to his encoding rule. This cheating probability P_{R_0} is defined by

$$P_{R_0} \triangleq \max_{f \in E_R} \max_{m \in M} \Pr[\text{Arbiter (or T) accepts } m | \text{R has } f \in E_R] \quad (2.4)$$

R_1, Substitution by the receiver. The receiver receives a message from the transmitter but claims to have received another message. The receiver succeeds if this other message could have been generated by the transmitter due to his encoding rule. This cheating probability P_{R_1} is defined by

$$\begin{aligned} P_{R_1} \triangleq & \max_{f \in E_R} \sum_{m \in M} \Pr(m) \\ & \max_{\hat{m} \neq m} \Pr[\text{Arbiter (or T) accepts } \hat{m} | \text{R has } f \text{ and T sends } m] \quad (2.5) \end{aligned}$$

Let

$$E_R \circ E_T \triangleq \{(e, f) \mid \Pr[\text{T has } e \in E_T \text{ and R has } f \in E_R] > 0\}$$

For A^2-codes, Johansson showed an information theoretic bound such as follows.

Proposition 6. *[12] In an A^2-code without splitting*

$$\begin{array}{ll} P_I \geq 2^{-\inf I(E_R;M)} & P_{R_0} \geq 2^{-\inf I(E_T;M|E_R)} \\ P_S \geq 2^{-\inf I(E_R;M'|M)} & P_{R_1} \geq 2^{-\inf I(E_T;M'|E_R,M)} \\ P_T \geq 2^{-\inf I(E_R;M|E_T)} & \end{array}$$

where $I(X;Y)$ denotes the mutual entropy of X and Y.

Proposition 7. *[12]*

$$\begin{array}{ll} |E_R| \geq (P_I P_S P_T)^{-1} & |E_R \circ E_T| \geq (P_I P_S P_T P_{R_0} P_{R_1})^{-1} \\ |E_T| \geq (P_I P_S P_{R_0} P_{R_1})^{-1} & \end{array}$$

3 Combinatorial bounds for A^2-codes without secrecy

In this section, we present combinatorial lower bounds for A^2-codes without splitting and without secrecy. To derive our bounds, we develop three techniques. The first technique is a reduction of an A^2-code to an A-code. The second one is a restriction of messages which is described by the following Theorem.

Theorem 8. *For an A-code (S, E, M), consider a subcode $(S, E, \hat{M})$ such that $\hat{M} \subseteq M$. Then, for $\forall m \in \hat{M}$,*

$$\begin{aligned} &\Pr[R \textit{ accepts } m \textit{ in the original } A\textit{-code}] \\ &= \Pr[R \textit{ accepts } m \textit{ in the subcode}] \end{aligned}$$

The third technique is given by the following Theorem. This technique will be a basic Theorem for A-codes.

Theorem 9. *In an A-code without splitting (S, E, M), if $\Pr[R \textit{ accepts } m] = 1/l$ for $\forall m$, then $|M| = |S|l$.*

Proof. Let $X = \{x_{ij}\}$ be the incidence matrix of E. That is,

$$x_{ij} = \begin{cases} 1 & \text{if } e_i \in E \text{ accepts } s_j \in S \\ 0 & \text{otherwise} \end{cases}$$

Then, $\Pr[\text{R accepts } m_j] = \sum_i \Pr[e = e_i]x_{ij}$. If $\Pr[\text{R accepts } m_j] = 1/l$ for $\forall m_j$, then

$$\begin{aligned} |M|/l = \sum_j \Pr[\text{R accepts } m_j] &= \sum_j \sum_i \Pr[e = e_i]x_{ij} \\ = \sum_i \Pr[e = e_i] \sum_j x_{ij} &= \sum_i \Pr[e = e_i]|S| \\ = |S| & \end{aligned}$$

Hence, $|M| = l|S|$. □

For an A^2-code (S, M, E_R, E_T), we define a decoding rule of the receiver $f \in E_R$ as follows.

$$f(m) = \begin{cases} s \in S & \text{if } m \text{ is accepted as } s. \\ \text{reject} & \text{if } m \text{ is rejected.} \end{cases}$$

Let

$$\begin{aligned} M(f, s) &\triangleq \{m \mid f(m) = s\} \\ M(f) &\triangleq \{m \mid f \text{ accepts } m\} \ (= \bigcup_{s \in S} M(f, s)) \\ M_s &\triangleq \{m \mid f(m) = s, f \in E_R\} \ (= \bigcup_{f \in E_R} M(f, s)) \\ E_R(e) &\triangleq \{f \mid \Pr[\text{R has } f | \text{T has } e] > 0\} \end{aligned}$$

3.1 Lower bound on P_I and P_S

To prevent the impersonation attack of the receiver, it must be that $|M(f,s)| > 1$. That is, from a view point of the receiver, A^2-codes must be splitting. To derive our bounds, we assume the following assumption.

Assumption 10. *$|M(f,s)| = c$ for $\forall f \in E_R$ and $\forall s \in S$.*

That is, each $f \in E_R$ accepts c messages for each $s \in S$. For each source state $s_i \in S$, define

$$S_i \triangleq \{s_{i1}, s_{i2}, \ldots, s_{ic}\}, \qquad \hat{S} \triangleq S_1 \cup S_2 \cup \cdots$$

Then, we can consider an A-code without splitting $(\hat{S}, E_R, M)$ which corresponds to the original A^2-code (S, M, E_R, E_T) in a natural way. Clearly, $|\hat{S}| = c|S|$.

Theorem 11. *Under assumption 10, $P_I \geq c|S|/|M|$. The equality holds if and only if*

$$\Pr[R \textit{ accepts } m] = c|S|/|M| \textit{ for } \forall m \in M$$

Proof. It is clear that P_I of the A^2-code is equal to the impersonation attack probability for the splitting A-code $(\hat{S}, E_R, M)$. Apply proposition 1 to $(\hat{S}, E_R, M)$. □

Assumption 12. $P_I = c|S|/|M| = 1/l$.

Theorem 13. *Under assumption 10 and 12, $|M_s| = cl$ for $\forall s \in S$.*

Proof. From assumption 12 and theorem 11,

$$\Pr[\text{R accepts } m] = 1/l \text{ for } \forall m \in M \tag{3.1}$$

We consider a subcode of $(\hat{S}, E_R, M)$ such that the set of messages is restricted to M_s. This is an A-code without splitting in which the number of messages is $|M_s|$ and that of source states is c (from assumption 10). Even for this restricted A-code, we have

$$\Pr[\text{R accepts } m] = 1/l \text{ for } \forall m \in M_s$$

from Theorem 11. Then, from Theorem 9, $|M_s| = cl$ □

Theorem 14. *Under assumption 10 and 12,*

$$P_S \geq 1/l \tag{3.2}$$

Proof. P_S is defined by

$$P_S \triangleq \sum_{m' \in M} \Pr[\text{T sends } m'] \max \Pr[\text{R accepts } m | \text{R accepts } m'] \tag{3.3}$$

Let $m' \in M_{s_i}$. Then, the maximum is taken over $m \in M \backslash M_{s_i}$. For $m' \in M_{s_i}$, define

$$P_I'(m') \overset{\triangle}{=} \max_{m \in M \backslash M_{s_i}} \Pr[\text{R accepts } m | \text{R accepts } m']. \tag{3.4}$$

Then, this is the impersonation attack probability against an A-code without splitting $(\hat{S} \backslash S_i, E_R, M \backslash M_{s_i})$, where the probability distribution on E_R is conditioned by the fact that R accepts m'. Then, from proposition 1,

$$P_I'(m') \geq \frac{|\hat{S} \backslash S_i|}{|M \backslash M_{s_i}|}.$$

Now

$$|\hat{S} \backslash S_i| = |\hat{S}| - |S_i| = c|S| - c = c(|S| - 1), \qquad |M \backslash M_{s_i}| = |M| - |M_{s_i}| = cl|S| - cl$$

from assumption 12 and Theorem 13. Therefore, we have $P_I'(m') \geq 1/l$ for $\forall m'$. Then, we have eq.(3.2) from eq.(3.3) and eq.(3.4). □

3.2 Lower bound on P_T

Let $h \overset{\triangle}{=} \min_{e \in E_T} |E_R(e)|$.

Theorem 15. *Under assumption 10, $P_T \geq \max\{(c-1)|S|/(|M| - |S|), 1/h\}$.*

Proof. It is easy to see that $P_T \geq 1/h$.
Suppose that the transmitter T has an encoding rule $e \in E_T$. Let $m_i = e(s_i)$ for $i = 1, 2, \ldots, |S|$. T must send m to R such that $m \neq m_i$ for $\forall i$ for cheating. Consider the following subcode of $(\hat{S}, E_R, M)$ such as follows. Let X be the incidence matrix of $E_R(e)$ which is a $|E_R(e)| \times |M|$ binary matrix. Remove the columns corresponding to $\{m_i | i = 1, 2, \cdots, |S|\}$ from this matrix. Then, we obtain an incidence matrix of an A-code without splitting $(S', E_R(e), M \backslash \{m_i\})$, where $|S'| = |\hat{S}| - |S| = c|S| - |S| = (c-1)|S|$. Theorem 11 holds for this subcode. The best strategy of the transmitter is at least as good as the impersonation attack against this modified A-code. Then from proposition 1, we have

$$P_T \geq \max_{e \in E_T} \frac{|S'|}{|M \backslash \{m_i\}|} = \frac{(c-1)|S|}{|M| - |S|}$$

□

Corollary 16. *Under assumption 10 and 12,*

$$P_T \geq \max\{(c-1)/(lc-1), 1/h\}. \quad \textit{Further, if } c = l = q, \textit{ then} \quad P_T \geq \frac{1}{q+1}$$

Next, we consider a separable case.

Assumption 17. *For $\forall s$, M_s can be grouped into $A_1^s, A_2^s, \ldots$ in such a way that $|A_i^s \cap M(f, s)| = 1$ for $\forall s$, $\forall A_i^s$ and $\forall f \in E_R$. An A^2-code given by [14] satisfies this assumption.*

Lemma 18. *Under assumption 10, 12 and 17,* $|A_i^s| = l$ *and* $|\{A_i^s\}| = c$ *for* $\forall s$.

Proof. The proof is almost the same as that of Theorem 13. We consider a subcode of $(\hat{S}, E_R, M)$ such that the set of messages is restricted to A_i. In this restricted A-code, the number of messages is $|A_i|$ and that of source states is 1 from assumption 17. From Theorem 11, assumption 12 and Theorem 11, even for this restricted A-code, Pr[R accepts m] $= 1/l$ for $\forall m \in A_i$. Then, from Theorem 9, $|A_i^s| = 1 \times l = l$. From Theorem 13, $|\{A_i^s\}| = |M_s|/|A_i| = c$ □

Theorem 19. *Under assumption 10, 12 and 17,* $P_T \geq \max\{1/l, 1/h\}$.

Proof. It is clear that $P_T \geq 1/h$.
Suppose that the transmitter has $e \in E_T$. Let $m_i = e(s_i)$ for $i = 1, 2, \ldots, |S|$. For simplicity, suppose that $m_i \in A_1^{s_i}$ for $i = 1, 2, \ldots, |S|$. As in the proof of Theorem 15, we consider an A-code without splitting $(S', E_R(e), M \backslash \{A_i^{s_i}\})$ such that $|S'| = (c-1)|S|$. Then, as in that proof, we have

$$P_T \geq \max_{e \in E_T} \frac{|S'|}{|M \backslash \{A_i^{s_i}\}|}$$

From assumption 12, and lemma 18,

$$|M \backslash \{A_i^{s_i}\}| \quad = \quad |M| - \sum |A_1^{s_i}| \quad = \quad |M| - l|S| \quad = \quad lc|S| - l|S|$$

Then, $P_T \geq (c-1)|S|/(lc|S| - l|S|) = 1/l$ □

3.3 Lower bound on P_{R_0} and P_{R_1}

Let $E_T(f) \triangleq \{e \mid \Pr[\text{T has } e | \text{R has } f] > 0\}$. Suppose that R has f. Then, R knows that T has some $e \in E_T(f)$. Consider an A-code $(S, E_T(f), M(f))$. It is an A-code without splitting and without secrecy because the original A^2-code is so. Let $P_I(f)$ and $P_S(f)$ denote the impersonation attack probability and the substitution attack probability, respectively. Then it is easy to see that

$$P_{R_0} = \max_{f \in E_R} P_I(f) \qquad\qquad P_{R_1} = \max_{f \in E_R} P_S(f)$$

(Remember that the arbiter accepts m as authentic iff e can generate m.) From assumption 10, $|M(f)| = c|S|$. Now, from proposition 1, we have Theorem 20.

Theorem 20. *Under assumption 10,*

1. $P_{R_0} \geq 1/c$
2. *If* $P_{R_0} = 1/c$, *then* $P_{R_1} \geq 1/c$.

3.4 Tightness

Corollary 21. *Suppose that $c = l = q$. Then*

1. $P_I \geq 1/q$, $P_T \geq 1/(q+1)$, $P_{R_0} \geq 1/q$.
2. *If* $P_I = 1/q$, *then* $P_S \geq 1/q$, *If* $P_{R_0} = 1/q$, *then* $P_{R_1} \geq 1/q$.
3. *Under assumption 17, if* $P_I = 1/q$, *then* $P_T \geq 1/q$.

Corollary 21 is tight because all the bounds are satisfied with equality by the A^2-codes given by Johansson [13, 14].

3.5 Lower bound on $|E_R|, |E_R \circ E_T|$ and $|E_T|$

In this subsection, we show more tight lower bounds on $|E_R|, |E_R \circ E_T|$ and $|E_T|$ than proposition 7.

Assumption 22. $P_I = P_S = P_T = c|S|/|M| = 1/l$

Theorem 23. *Under assumption 10, 17 and 22,* $|E_R| \geq c|S|(l-1)+1$. *The equality holds if and only if the incidence matrix of* E_R *is an orthogonal array* $OA(l, c|S|, \lambda)$ *where* $\lambda = (c|S|(l-1)+1)/l^2$ *and each* $f \in E_R$ *is used with equal probability.*

Proof. From assumption 17, we can consider that our A-code without splitting $(\hat{S}, E_R, M)$ is without secrecy. Remember that $|\hat{S}| = c|S|$. For this A-code without secrecy, let $\hat{P}_I$ and $\hat{P}_S$ be the impersonation attack probability and the substitution attack probability, respectively. Then, clearly $\hat{P}_I = P_I = c|S|/|M|$. From assumption 22, $\hat{P}_S = \max\{P_S, P_T\} = c|S|/|M|$. Now, from proposition 4, we have this Theorem. □

Remark. From proposition 7, we have another bound such that $|E_R| \geq l^3$. If $c|S| \geq l^2 + l + 1$, Theorem 23 is more tight than this bound.

Assumption 24. $P_{R_0} = P_{R_1} = 1/c$

Theorem 25. *Under assumption 10 and 24,* $E_T(f) \geq \max\{c^2, |S|(c-1)+1\}$.

Proof. From proposition 4. □

Theorem 26. *Under assumption 10 and 24,*

$$|E_R \circ E_T| \geq |E_R| \times \max\{c^2, |S|(c-1)+1\}.$$

Proof. From Theorem 25. □

From Theorem 19, if $P_T = 1/l$, then $l \leq h = \min_e |E_R(e)|$

Assumption 27. *For* $\forall e \in E_T, |E_R(e)| = l$

Theorem 28. *Under assumption 10, 24 and 27,*

$$|E_T| \geq \frac{|E_R|}{l} \times \max\{c^2, |S|(c-1)+1\}.$$

Proof. From assumption 27, $l \times |E_T| = |E_R \circ E_T|$. Then, from Theorem 26, Theorem 28 holds. □

4 Combinatorial bounds for general A^2-codes

In this section, we show combinatorial bounds for general A^2-codes without splitting.

Theorem 29.

$$P_I \geq \min_{f \in E_R} \frac{|M(f)|}{|M|} \qquad P_S \geq \min_{f \in E_R} \frac{|M(f)| - \max_{s \in S} |M(f,s)|}{|M| - \min_{s \in S} |M(f,s)|}$$

Proof. We consider a splitting A-code (S, E_R, M) which corresponds to the original A^2-code (S, M, E_R, E_T) in a natural way (where $|M(f,s)| > 1$). From proposition 5, we have this theorem. □

Theorem 30. $$P_T \geq \min_{f \in E_R} \frac{|M(f)| - |S|}{|M| - |S|}$$

The proof is almost the same as that of theorem 15.

Theorem 31. $$P_{R_0} \geq \max_{f \in E_R} \frac{|S|}{|M(f)|}$$

Proof. We consider an A-code without splitting $(S, E_T(f), M(f))$ as shown in subsection 3.3. From proposition 1, we have this theorem. □

Theorem 32. $$P_{R_1} \geq \max_{f \in E_R} \frac{|S| - 1}{|M(f)| - \min_{s \in S} |M(f,s)|}$$

Proof. Fix $f \in E_R$ and $m \in M(f)$ arbitrarily. For $\forall m' \in M(f) - M(f, f(m))$, let

$$P_{m'} \triangleq \Pr[\text{Arbiter accepts } m' \mid \text{R has } f \text{ and T sends } m]$$

Then

$$P_{m'} = \frac{\sum_{\{e \mid m, m' \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}$$

Now, we have

$$\begin{aligned}
&\sum_{m' \in M(f)} P_{m'} \\
&= \frac{\sum_{m' \in M(f)} \sum_{\{e \mid \exists s: m' = e(s), m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_s \sum_{m' \in M(f)} \sum_{\{e \mid m' = e(s), m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_s \sum_{\{e \mid m \in M(e)\}} |\{m' \mid m' = e(s)\}| \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_s \sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= |S|
\end{aligned}$$

Further,

$$\begin{aligned}
&\sum_{m' \in M(f,f(m))} P_{m'} \\
&= \frac{\sum_{m' \in M(f,f(m))} \sum_{\{e \mid \exists s : m' = e(s), m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_{m' \in M(f,f(m))} \sum_{\{e \mid m' = e(f(m)), m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_{\{e \mid m \in M(e)\}} |\{m' \mid m' = e(f(m))\}| \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= \frac{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]}{\sum_{\{e \mid m \in M(e)\}} \Pr[E_T = e | E_R = f] \Pr[S = f(m)]} \\
&= 1
\end{aligned}$$

Hence, $\displaystyle\sum_{m' \in M(f) \backslash M(f,f(m))} P_{m'} = \sum_{m' \in M(f)} P_{m'} - \sum_{m' \in M(f,f(m))} P_{m'} = |S| - 1$

Therefore, there exists $\hat{m}' \in M(f) \backslash M(f, f(m))$ such that

$$P_{\hat{m}'} \geq \frac{|S| - 1}{|M(f)| - |M(f, f(m))|}$$

Thus

$$\begin{aligned}
P_{R_1} &\triangleq \max_{f \in E_R} \sum_{m \in M} \Pr(m) \max_{\hat{m} \neq m} \Pr[\text{Arbiter accepts } \hat{m} | \text{R has } f \text{ and T sends } m] \\
&\geq \max_{f \in E_R} P_{\hat{m}'} \\
&\geq \max_{f \in E_R} \frac{|S| - 1}{|M(f)| - \min_{s \in S} |M(f, s)|}
\end{aligned}$$

□

5 Another definition of P_{R_0} and P_{R_1}

We can define P_{R_0} and P_{R_1} in a different way from eq.(2.4) and eq.(2.5). The alternative definitions are

$$P_{R_0} \triangleq \sum_{f \in E_R} \Pr(f) \max_{m \in M} \Pr[\text{Arbiter (or T) accepts } m | \text{R has } f \in E_R]$$

$$\begin{aligned}
P_{R_1} \triangleq &\sum_{f \in E_R} \Pr(f) \sum_{m \in M} \Pr(m) \\
&\max_{\hat{m} \neq m} \Pr[\text{Arbiter (or T) accepts } \hat{m} | \text{R has } f \text{ and T sends } m]
\end{aligned}$$

For the model without secrecy, the lower bounds on the above P_{R_0} and P_{R_1} are the same as those on the original P_{R_0} and P_{R_1}. For the general model, we obtain the following bound.

Theorem 33.

$$P_{R_0} \geq \min_{f \in E_R} \frac{|S|}{|M(f)|} \qquad P_{R_1} \geq \min_{f \in E_R} \frac{|S|-1}{|M(f)| - \min_{s \in S} |M(f,s)|}$$

References

1. G.J.Simmons, "A survey of Information Authentication", in *Contemporary Cryptology, The science of information integrity,* ed. G.J.Simmons, IEEE Press, New York, 1992.
2. G.J.Simmons, "Authentication theory/coding theory", Proceedings of Crypto'84, Lecture Notes in Computer Science, LNCS 196, Springer Verlag, pp.411–431 (1985).
3. E.F.Brickell, "A few results in message authentication", Congresus Numerantium, vol.43, pp.141–154 (1984).
4. G.J.Simmons, "Message authentication: a game on hypergraphs", Congresus Numerantium, vol.45, pp.161–192 (1984).
5. J.L.Massey, *Cryptography – a selective survey,* in *Digital Communications,* North Holland (pub.), pp.3–21, (1986).
6. D.R.Stinson, "Some constructions and bounds for authentication codes", Journal of Cryptology, Vol.1, 1988, pp.37–51, (1988).
7. D.R.Stinson, "The combinatorics of authentication and secrecy codes", Journal of Cryptology, Vol.2, no 1, 1990, pp.23–49, (1990).
8. D.R.Stinson, "Combinatorial Characterization of Authentication Codes", Proceedings of Crypto'91, Lecture Notes in Computer Science, LNCS 576, Springer Verlag, pp62–72 (1992).
9. Marijke De Soete, "New Bounds and Constructions for Authentication/Secrecy Codes with Splitting", Journal of Cryptology, Vol.3, no 3, 1991, pp173–186 (1991).
10. G.J.Simmons, "Message Authentication with Arbitration of Transmitter/Receiver Disputes", Proceedings of Eurocrypt'87, Lecture Notes in Computer Science, LNCS 304, Springer Verlag, pp.150–16 (1987)
11. G.J.Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration", Journal of Cryptology, Vol.2, no.2, 1990, pp.77–104 (1990).
12. Thomas Johansson, "Lower Bounds on the Probability of Deception in Authentication with Arbitration", In *Proceedings of 1993 IEEE International Symposium on Information Theory,* San Antonio, USA, January 17–22, 1993, pp.231.
13. Thomas Johansson, "Lower Bounds on the Probability of Deception in Authentication with Arbitration", submitted to IEEE Trans. on IT (private communication).
14. Thomas Johansson, "On the construction of perfect authentication codes that permit arbitration", Proceedings of Crypto'93, Lecture Notes in Computer Science, LNCS 773, Springer Verlag, pp.341-354 (1993).
15. K.Kurosawa, "New bound on authentication code with arbitration", Proceedings of Crypto'94, Lecture Notes in Computer Science, LNCS 899, Springer Verlag, pp.140–149 (1994).