Proceedings of the 9th WSEAS International Conference on Applied Mathematics, Istanbul, Turkey, May 27-29, 2006 (pp546-549)

LOWER BOUND ON THE SIZE OF KEYS IN AUTHENTICATION CODES WITH ARBITRATION*

BOUBACAR ABBA YOU HONG
Department of Mathematics
Harbin Institute of Technology,
Dazhi Street, Harbin 150001
CHINA

Abstract: For the authentication codes with arbitration, Johansson showed lower bounds on the size of keys, but those bounds are no tighter if the size of source states is large. In the present paper , we first present some new lower bounds on the sizes of keys. Next, we discuss the case for large sizes of source states, and then we show that those bounds are tighter.

Key-Words: - Authentication, codes, arbitration, bounds, Keys, sizes.

1 Introduction

In the model for normal 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 and substitution attack. This model has been studied extensively so far. In this model , the transmitter and the receiver are using the same encoding rule and are thus trusting 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 [2,3], here referred to as the authentication codes with arbitration (A^2-codes). In this model , caution is taken against deception by the transmitter and the receiver as well as that by the opponent. This model includes a fourth person , called the arbiter . The arbiter has access to all key information and is by definition not cheating . He does not take part in any communication activities on the Channel but has to solve disputes between the transmitter and the receiver whenever such occur. There are essentially five different kinds of attacks to cheat which are possible. The attacks are following:

I , Impersonation by the opponent. The opponent sends a message to the receiver and succeeds if the message is accepted by the receiver as authentic.

S, Substitution by the opponent. The opponent observes a message that is transmitted and substitutes this message with another. The opponent succeeds if this other message is accepted by the receiver as authentic.

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 the encoding rule.

$\mathbf{R_0}$, 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.

$\mathbf{R_1}$, 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 . For each way of cheating ,we denote the probability of success with $\mathbf{P_I}$, $\mathbf{P_S}$, $\mathbf{P_T}$, $\mathbf{P_{R0}}$ and $\mathbf{P_{R1}}$.

Let $\mathbf{E_R}$ be a set of the receiver's encoding rules and $\mathbf{E_T}$ be a set of the transmitter's encoding rules . Also , let $\boldsymbol{S}$ be a set of source states. Recently, Johansson showed [4] lower bound on $|E_T|$ and $|E_R|$, he established also entropy-based lower bounds on these five cheating probabilities and the sizes of keys [5]. Kaoru K and Obana S showed combinatorial lower bounds on the cheating probabilities (see [6]).

This paper first presents some new lower bounds, and tighter lower bounds on the sizes of keys for large sizes of source states ($|S| > (l+c)/c$) that can be considered as an extension of the bounds established by Kaoru Kurosawa [7]. In fact Kaoru K (see [7]) established some lower bounds but it is in a

*This project is supported by NSF of Heilongjiang Province of China.

special case, because he consider a separable code. Thus contrary to him we suppose that the code is not separable , and then we will give some bounds in a more general case, which are more better than his results.

2 Preliminaries

2.1 Notations and Definition

Let

$S = \{s/s$ is a source state$\}$

$A = \{a / a$ is an authenticator$\}$

$M \subseteq S \times A$,where $m = (s,a) \in M$ is a message

$E_R = \{f / f$ is a key of receiver$\}$

$E_T = \{e / e$ is a key of transmitter$\}$.

Each key of transmitter $e \in E_T$ is a mapping from S to A. Each key of the receiver $f \in E_R$ is a mapping from M to $\{0,1\}$. Let

$E_T \circ E_R = \{(e,f) / e \in E_T, f \in E_R, f(s,s(e)) = 1,$ for all $s \in S\}$.

Note that the probability distribution over M is determined by probability distributions over $E_T \circ E_R$ and S. We denote an A^2-code by (S, M, E_R, E_T), where $\mathcal{X}$ denotes a random variable over X.

Define

$E_R(e) = \{f / \Pr(E_R = f / E_T = e) > 0\}$

$E_T(f) = \{e / \Pr(E_T = e / E_R = f) > 0\}$

$M(f) = \{m / f(m) = 1\}$ $M(e) = \{(s,a) / a = e(s)\}$

$E_R(s,a) = \{f / f \in E_R, f(s,a) = 1\}$

$E_T(s,a) = \{e / e \in E_T, e(s) = a\}$.

We say that E_R and E_T are uniform if $\Pr(E_R = f), \Pr(E_T = e), \Pr(E_R = f / E_T = e)$ and $\Pr(E_T = e / E_R = f)$ are all uniformly distributed.

2.2 Some known results

Definition 1 An A^2-code is called without secrecy if m is written as $m = (s,a)$, where $s \in S$ and a is an authenticator.

Definition 2 We say that an A-code is (l , c)-splitting if

$$|M|/|S| = l,$$

$$|Split(e,s)| = c, \ \forall e \in E \text{ and } \forall s \in S$$

Consider an A^2-code without secrecy (S, M, E_R, E_T), for $f \in E_R$ and $s \in S$, let

$$Split(f,s) = \{(s,a) / f(s,a) = valid\}$$

Definition 3 We say that an A^2-code is an (l, c) A^2-code if $|M|/|S| = l$ and

$$|Split(f,s)| = c \ \forall f \in E_R \text{ and } \forall s \in S.$$

Definition 4 [7] A skeleton matrix for (E , M) is a $|E| \times |M|$ matrix $X = \{x_{ij}\}$ such that

$$x_{ij} = \begin{cases} 1 & if \quad e_i accepts (or\ could\ generate) m_j \\ 0 & otherwise \end{cases}$$

Definition 5[7] Let $I_l(h) = \{i / (h-1)l + 1 \le i \le hl\}$.

We say that a $b \times kl$ binary matrix $X = \{x_{ij}\}$ is a (b,k,l,n_0,n_1) K-array if the following conditions are satisfied.

(1) $w(x_i) = n_0$ for $\forall i$.

(2) For $\forall h_1$, $\forall h_2$ and for $\forall x_i \in I_l(h_1)$, $\forall x_j \in I_l(h_2)$,

$$w(x_i \circ x_j) = \begin{cases} n_1 & if \quad h_1 \ne h_2 \\ 0 & if \quad h_1 = h_2 \quad and \quad x_i \ne x_j \end{cases}$$

Lemma 6 [7] If there exists a (b,k,l,n_0,n_1) K-array, then $b \ge k(l-1)+1$.

Lemma 7 [7] Suppose we have a without secrecy A-code (E,M,S) in which $P_I = P_S = |S|/|M| = 1/l$ .Then, the skeleton matrix for (E,M) is a $(|E|, |S|, l, |E|/l, |E|/l^2)$ K-array.

Definition 8 An orthogonal array $OA_\lambda(k,n)$ is an $\lambda n^2 \times k$ array of n symbols such that, in any 2 columns of the array, every one of the possible n^2 pairs of symbols occurs in exactly λ rows.

Proposition 9 [8] (Rao bound). If there exists an $OA_\lambda(k,n)$, then $\lambda n^2 \ge k(n-1)+1$.

Lemma 10 [8] In an optimal (l , c) A^2-code with respect to cheating probabilities ,

$$|E_R| = (l^2(l-1))/(c^2(c-1)) \text{ if and only if}$$

$|E_R(s,a) \cap E_R(s',a') \cap E_R(s',a'')| = 1$, for all $(s,a),(s',a'),(s',a'') \in S \times A$ such that $s \ne s', a' \ne a''$.

In this case ,

$$|E_R(s,a) \cap E_R(s',a')| = (l-1)/(c-1) \quad (1)$$

$$|E_R(s',a') \cap E_R(s',a'')| = l/c \quad (2)$$

$$|E_R(s,a)| = (l(l-1))/(c(c-1)) \quad (3).$$

2.3 Lower bounds

Johansson [5] derived lower bounds on the sizes of

keys as follows

Proposition 1 [5]

$|E_R| \geq (P_I P_S P_T)^{-1}$, $|E_T| \geq \left(P_I P_S P_{R_0} P_{R_1}\right)^{-1}$

$|E_R \circ E_T| \geq \left(P_I P_S P_T P_{R_0} P_{R_1}\right)^{-1}$, $|M| \geq \left(P_I P_{R_0}\right)^{-1} |S|$

Corollary1 If $P_I = P_S = c/l$, $P_T = (c-1)/(l-1)$, $P_{R_0} = P_{R_1} = 1/c$, then

$|E_R| \geq \frac{l^2(l-1)}{c^2(c-1)}$, $|E_T| \geq l^2$, $|E_R \circ E_T| \geq \frac{l^2(l-1)}{c-1}$, $|M| \geq l|S|$

We say that an (l, c) A^2-code is optimal if all the above bounds are met.

3 New bound for A^2-code

Let A^2-code be a (S, M, E_R, E_T) such that S is a set of source states, M is a set of messages, E_R is a set of the receiver's encoding rules and E_T is the set of the transmitter's encoding rules. Inspired by Johansson 's bound , we will established some new bounds on the sizes of keys.

Proposition 3.1 Consider an (l, c) A^2-code, we have $|E_R| \geq (P_I P_S)^{-1}$, and $|E_T| \geq \left(P_{R_0} P_{R_1}\right)^{-1}$

Proof P_I, P_S, P_T being probabilities, then it obvious that $P_I P_S P_T \leq P_I P_S$, so we can deduce that $(P_I P_S P_T)^{-1} \geq (P_I P_S)^{-1}$. By using proposition 1, we may get $|E_R| \geq (P_I P_S)^{-1}$.

The similar way can be used to prove $|E_T| \geq \left(P_{R_0} P_{R_1}\right)^{-1}$.

Corollary3.1 Suppose that $P_I = P_S = c/l$, $P_T = (c-1)/(l-1)$, and $P_{R_0} = P_{R_1} = 1/c$, then we have $|E_R| \geq (l/c)^2$, and $|E_T| \geq c^2$.

4 Tighter Lower Bound on the sizes of Keys for large $|S|$

In this section we present lower bound on $|E_R|$ and $|E_T|$ for large $|S|$, i.e., $|S| > (l+c)/c$ and we will prove that those bounds are tighter than Corollary 3.1. It was shown that Corollary 1is no tighter if $|S| > c+1$.

We consider an A^2-code without secrecy

(S, M, E_R, E_T) and

let, $E_R(e) = \{f / \Pr(E_R = f / E_T = e) > 0\}$,

$E_T(f) = \{e / \Pr(E_T = e / E_R = f) > 0\}$

Theorem 4.1 Assume that

a) $P_I = P_S = c/l$, $P_T = (c-1)/(l-1)$ $P_{R_0} = P_{R_1} = 1/c$

b) $|M| = l|S|$

c) $|E_R(e)| = \frac{l-1}{c-1}$

d) E_T, E_R , $E_T(f)$ and $E_R(e)$ are uniformly distributed , respectively .

Then ,

$|E_R| \geq |S|(l-c)+1$; $|E_T \circ E_R| \geq (|S|(l-1)+1)|E_R(e)|$;

$|E_T| = |E_T \circ E_R| / |E_R(e)|$

Proof According to corollary 1, $|M| \geq l|S|$. (b) requires that the equality hold. It is easy to see that $|E_R(e)| \geq \frac{l-1}{c-1}$ if $P_T = (c-1)/(l-1)$. (c) requires that this equality hold.

Let $X = \{x_{ij}\}$ be the skeleton matrix for (E_R, M) (see Def. 4) we will prove that X is a $(|E_R|, c|S|, l/c, c|E_R|/l, c^2|E_R|/l^2)$ K-array(seeDef.5).Let $M(f) = \{m / f \text{ accepts } m\} = \{m / f(m) = 1\}$, $M(f,s) = \{m / m \in M(f), m = (s,a)\}$.In an optimal ($l$,$c$)-A^2-code, we have by definition $P_I = |E_R(m)| / |E_R| = c/l$, where $m = (s,a)$, then we have $|E_R(m)| = c|E_R|/l$ (referring to lemma 10), thus X satisfies (1) of Def.5.From the fact that $P_S = |E_R(m) \cap E_R(m')| / |E_R(m)| = c/l$, $m = (s,a)$, $m' = (s',a')$ such that $m \neq m'$, we may get $|E_R(m) \cap E_R(m')| = c|E_R(m)|/l$.

Therefore $|E_R(m) \cap E_R(m')| = c^2|E_R|/l^2$. So we may have

$$|E_R(m) \cap E_R(m')| = \begin{cases} c^2|E_R|/l^2 & if \quad s \neq s' \\ 0 & if \quad s = s' \quad and\, a \neq a' \end{cases}$$

Then, it is easy to see that X satisfies the condition (2) of Def.5.Therefore X is a $(|E_R|, c|S|, l/c, c|E_R|/l, c^2|E_R|/l^2)$ K-array.

Thus according to Lemma6, $|E_R| \geq c|S|((l/c)-1)+1$, and then the conclusion.In [7], Kaoru K has proved that the encoding matrix of E_T is an $OA_1(|S|, l)$, then by Proposition 9, we have $|E_T| \geq |S|(l-1)+1$.

We know that $|E_R \circ E_T| \geq |E_T||E_R(e)|$, therefore we may have the conclusion.

From (c), we have $|E_T| = |E_T \circ E_R| / |E_R(e)|$.

Theorem 4.2 In an optimal (l , c) A^2-code , we have
(1) $|E_R(m)| = c|E_R|/l$
(2) $|M(f)| = c|S|$
(3) $|M(f,s)| = c$
(4) $|E_T(f)| \geq |S|(c-1)+1$

Proof Let A^2-code (S, M, E_R, E_T), then we can consider an A-code $(S, M(f), E_T(f))$, for any $f \in E_R$. Let $P_I(f)$ and $P_S(f)$ denote the P_I and P_S of this A-code respectively, then $P_{R_0} = \max_{f \in E_R} P_I(f)$, and $P_{R_1} = \max_{f \in E_R} P_S(f)$. Note that $P_I(f) = P_S(f) = |S|/|M(f)|$.

We have $1/c = P_{R_0} \geq P_I(f) = |S|/|M(f)|$, therefore $|M(f)| \geq c|S|$. Moreover , we have

$c/l = P_I = \max_m |E_R(m)|/|E_R| \geq c|S|/|M| = c/l$, this means $|E_R(m)|/|E_R| = c|S|/|M|$, we can see easily that $|E_R(m)| = c|E_R|/l$, and $|M(f)| = c|S|$, (1) and (2) are proved.

Then $1/c = P_{R_0} = P_{R_1} = |S|/|M(f)|$

$1/c = P_{R_0} = |E_T(m) \cap E_T(f)|/|E_T(f)| \geq 1/|M(f,s)|$

therefore $|M(f,s)| \geq c$. On other way ,

$c|S| = |M(f)| = \sum_s |M(f,s)| \geq c|S|$. Hence, we must have $|M(f,s)| = c$.

We have $P_I(f) = P_S(f) = |S|/|M(f)| = 1/c$, thus by lemma7 the skeleton matrix for $(E_T(f), M(f))$ is a $(|E_T(f)|, |S|, c, |E_T(f)|/c, |E_T(f)|/c^2)$,

by lemma 6, we get the conclusion (4).

5 Conclusion

In this paper, we have given some new lower bounds on the sizes of keys in authentication codes with arbitration. Further, we have shown tighter bounds on the sizes of keys of the transmitter and the receiver for large sizes of source states than before. These bounds can be considered as an extension of Rao bound and Kageyama's bound.

References

[1] G.J.Simmons, "A survey of Information Authentication", *in Contemporary Cryptology*, *The science of information integrity*, ed. G.J.Simmons, IEEE Press NewYork ,1992.

[2] G.J.Simmons, Message authentication with arbitration of transmitter/receiver disputes, in *proceedings of Eurocrypt'87*

[3] G.J.Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that permit Arbitration", *in J. of Cryptology*, Vol.2, No.2, 1990, pp.77-104.

[4] Thomas Johansson, "Lower Bounds on the probability of Deception in Authentication with Arbitration", in Proceeding of 1993 IEEE *International Symposium on Information Theory*, San Antonio, USA, January 17-22, 1993,p.231.

[5] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, IEEE Trans. *On IT*, Vol.40, No.5 (1994) pp.1573-1585.

[6] Kaoru K, Obana S, Combinatorial Bounds on Authentication Codes with Arbitration, *Designs, codes and Cryptography*, 22, 265-281, 2001.

[7] Kaoru K, New Bound on Authentication Codes with Arbitration, 1998, *Springer-Verlag.*

[8] Kaoru K, Obana S, Combinatorial Classification of Optimal Authentication Codes with Arbitration, *Designs, Codes* and *Cryptography*,20,281-305,2000.