Two Constructions of Authentication Codes with Multiple Arbiters*

Shangdi Chen† Hao Ma

College of Science, Civil Aviation University of China, Tianjin, 300300, China

Abstract In this paper two authentication codes with multiple arbiters are constructed to protect the communication system against the attacks from the opponent, transmitter, receiver and dishonest arbiters. The first construction takes advantage of set theory to give an authentication codes with two arbiters that resists collusion attacks from dishonest arbiters and participators availably. The second construction makes full use of of Reed-Solomon-code (RS-code) and (k, n)-threshold scheme to give an authentication codes with n arbiters that effectively prevents multiple arbiters from cheating.

Keywords multiple arbiters, collusion attack, (k, n)-threshold scheme.
MSC 2010 94C30, 94A60, 94A62

1 Introduction

The information superhighway is a hot topic today and an important task of authentication is to determine the legality and the authentic transmitter of the message in the communication. Authentication theory initially considered resisting the opponent with honest transmitter and receiver, however, players in the communication could also deceive each other in the complex society. G. J. Simmons[2] was the first to propose authentication codes with arbitration to solve the distrust between the transmitter and the receiver.

Definition 1 *Let S, E_T, E_R, M be four nonempty finite sets, and $f : S \times E_T \to M$ and $g : M \times E_R \to S \cup \{\text{reject}\}$ be two maps. The six tuple (S, E_T, E_R, M, f, g) is called an authentication code with arbitration (A^2-code), if*

1) The maps f and g are surjective;

*Supported by the National Natural Science Foundation of China(61179026), the Fundamental Research Funds For The Central Universities(3122013K001).

†Corresponding author. E-mail address: sdchen@cauc.edu.cn; 904888796@qq.com

2) For any $m \in M$ and $e_t \in E_T$, if there exists an $s \in S$ satisfying $f(s, e_t) = m$, then such an s is uniquely determined by the given m and e_t;

3) $P(e_r, e_t) \neq 0$ and $f(s, e_t) = m$ implies $g(m, e_r) = s$, otherwise, $g(m, e_r) =$ {reject}.

Notes: *$P(e_r, e_t) \neq 0$ implies that any information s encoded by e_t can be authenticated by e_r.*

S, E_T, E_R and M are called the set of source states, the set of transmitter's encoding rules, the set of receiver's decoding rules and the set of messages, respectively. The cardinals $|S|, |E_T|, |E_R|$ and $|M|$ are called the size parameters of the code.

However, the premises of the codes are that the arbiter must be absolutely honest. Y. Desmedt[9] and T. Johansson[5][10] constructed authentication codes with a single arbiter to resist the deception of the arbiter alone, but there was no effective way to counteract the attacks from the arbiter colluding with a participator, and most of the calculation results were complex. So authentication codes with multiple arbiters appeared.

E. F. Brickell and D. R. Stinson[1] designed an authentication code with multiple arbiters base on the scheme in paper [2] and this construction could protect the system from attacks of several dishonest arbiters, but so many authentication codes were used in this design that the efficiency of the authentication was not good. Zhou Zhi and Hu Zhengming[3] designed an authentication code with mental poker protocol[8] against dishonest arbiters and participators, while the workload was relatively large in the key initialization phase and the system was helpless when faced with attacks from dishonest arbiters colluding with the receiver.

We now study such authentication codes with multiple arbiters that will resist not only attacks from single arbiter but also collusion attacks from dishonest arbiters and participators, and this kind of authentication codes can meet the requirements of users.

2 Construction of authentication code with two arbiters

Let S be a set of r elements, where $r = q^4$, and q is a non-negative integer. All players in communication are: a transmitter T, a receiver R, an opponent O, two arbiters A_1 and A_2.

Let C_Z be a set of messages that Z will accept or send as authentic (Z can be O, T, R, A_1 or A_2).

2.1 The model

Three stages of constructions of authentication codes:

1. Key generation and distribution:

a. The key distribution center (KDC) selects q^2 elements in S randomly, and secretly sends them to the receiver as C_R.

b. The KDC chooses q elements randomly from C_R , and secretly sends them to the transmitter as C_T.

c. The KDC selects a set C_{R_1} of $\frac{q^2-q}{2}$ elements from $C_R \backslash C_T$ randomly, and let $C_R \backslash (C_T \bigcup C_{R_1})$ be C_{R_2}.

d. A set C_1 consists of stochastic $q^3 - \frac{q^2-q}{2} - q$ elements from $S \backslash C_R$, and a set C_2 consists of $q^3 - \frac{q^2-q}{2} - q$ elements selected from $S \backslash (C_R \bigcup C_1)$ randomly again by the KDC.

e. A set $C_1 \bigcup C_{R_1} \bigcup C_T$ in S is sent to A_1 secretly as C_{A_1}, and $C_2 \bigcup C_{R_2} \bigcup C_T$ is sent to A_2 as C_{A_2} secretly.

2. Message transmission:

The transmitter is allowed to send a message m that comes from C_T, and the receiver accepts m if and only if $m \in C_R$.

3. Arbitration:

When a dispute between the transmitter and receiver arises, A_1 and A_2 are asked to settle the quarrel. The message is regarded as authentic if and only if both of the arbiters claim it is authentic, i.e., the message $m \in C_{A_1} \bigcap C_{A_2}$.

2.2 Rationality

If m is a legitimate message from the transmitter, $m \in C_T$. Since $C_T \subset C_R$, we have $m \in C_R$, i.e., m is accepted by the receiver by all means.

2.3 Parameters of the authentication code

The code has parameters:

$$|C_T| = q, \quad |C_R| = q^2, \quad |C_{A_1}| = |C_{A_2}| = q^3.$$

Moreover, $C_{A_1} \bigcap C_{A_2} = C_T$, $C_{A_1} \bigcap C_R = C_T \bigcup C_{R_1}$, $C_{A_2} \bigcap C_R = C_T \bigcup C_{R_2}$.

2.4 Probabilities of successful attacks

The system is subject to the following attacks ($i = 1, 2$):

1. Attack O_0 (Impersonation by the opponent):

Without waiting to see any communication, the opponent sends a message to the receiver. He wins if it is accepted as authentic.

$$P_{O_0} = \frac{|C_R|}{|S|} = \frac{q^2}{q^4} = \frac{1}{q^2}.$$

2. Attack O_1 (Substitution by the opponent):

The opponent observes a message that is transmitted and replaces this message with another. The opponent is successful if this other message is accepted by the receiver as authentic.

$$P_{O_1} = \frac{|C_R| - 1}{|S| - 1} = \frac{q^2 - 1}{q^4 - 1} = \frac{1}{q^2 + 1}.$$

3. Attack T (Impersonation by the transmitter):

The transmitter sends a message to the receiver and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic, and if this message is not one of the messages that the transmitter could have generated.

$$P_T = \frac{|C_R \backslash C_T|}{|S \backslash C_T|} = \frac{q^2 - q}{q^4 - q} = \frac{1}{q^2 + q + 1}.$$

4. Attack R_0 (Impersonation by the receiver):

The receiver, without receiving any message from the transmitter, tries to convince the arbiter that he did receive a message. The receiver succeeds if this message could have been generated by the transmitter.

$$P_{R_0} = \frac{|C_T|}{|C_R|} = \frac{q}{q^2} = \frac{1}{q}.$$

5. Attack 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.

$$P_{R_1} = \frac{|C_T| - 1}{|C_R| - 1} = \frac{q - 1}{q^2 - 1} = \frac{1}{q + 1}.$$

6. Attack A_{i_0} (Impersonation by single arbiter):

The arbiter A_i sends a message to the receiver and succeeds if the message is accepted by the receiver as authentic.

$$P_{A_{i_0}} = \frac{|C_T \bigcup C_{R_i}|}{|C_{A_i}|} = \frac{q^2 - \frac{q^2 - q}{2}}{q^3} = \frac{q + 1}{2q^2}.$$

7. Attack A_{i_1} (Substitution by single arbiter):

The arbiter A_i observes a message that is transmitted and replaces this message with another. The arbiter succeeds if the receiver accepts this other message as authentic.

$$P_{A_{i_1}} = \frac{|C_T \bigcup C_{R_i}| - 1}{|C_{A_i}| - 1} = \frac{q^2 - \frac{q^2 - q}{2} - 1}{q^3 - 1} = \frac{q + 2}{2(q^2 + q + 1)}.$$

8. Collusion Attack $\overline{TA_i}$:

T and A_i, collude to construct a message which is not valid under C_T and T wins if it is accepted by the receiver.

$$P_{\overline{TA_i}} = \frac{|(C_R \cap C_{A_i}) \setminus C_T|}{|C_{A_i} \setminus C_T|} = \frac{\frac{q^2-q}{2}}{q^3-q} = \frac{1}{2q+2}.$$

9. Collusion Attack $\overline{R_0A_i}$:

Without receiving any message from the transmitter, R and A_i collude to construct a message m then R claims that m is sent by the transmitter. They succeed if $m \in C_T$.

$$P_{\overline{R_0A_i}} = \frac{|C_T|}{|C_R \cap C_{A_i}|} = \frac{q}{q+\frac{q^2-q}{2}} = \frac{2}{q+1}.$$

10. Collusion Attack $\overline{R_1A_i}$:

Having received a legitimate message m from the transmitter, R and A_i collude to construct another message m' and R claims m' is sent by the transmitter. They succeed if $m' \in C_T$.

$$P_{\overline{R_1A_i}} = \frac{|C_T|-1}{|C_R \cap C_{A_i}|-1} = \frac{q-1}{q+\frac{q^2-q}{2}-1} = \frac{2}{q+2}.$$

11. Collusion Attack $\overline{TA_1A_2}$:

Both A_1 and A_2, collude with T to construct a message which is not valid under C_T and they win if the message is not accepted by all players in the communication except for the receiver R.

$$P_{\overline{TA_1A_2}} = \frac{|C_R \setminus C_T|}{|(C_{A_1} \cup C_{A_2}) \setminus C_T|} = \frac{q^2-q}{2q^3-2q} = \frac{1}{2q+2}.$$

The overall probability of deception, P_D[5], defined as the maximum of the probabilities of success in all allowed attacks, is in this case taken over all eleven types of attacks.

$$P_D = \overline{R_0A_i} = \frac{2}{q+1}.$$

This construction provides an authentication code with two arbiters that will efficiently protect the communication against not only the attacks from single participator, but also the attacks from the collusion of arbiter and one player of the communication. Furthermore, even if both arbiters are dishonest, they won't make sure of success when they help the transmitter cheat by reason of $P_{TA_1A_2} = P_{TA_i}$. It has an advantage of the scheme in paper [3].

3 Construction of authentication code with n arbiters

Any (n, k, d)-linear code has a property that $d \leq n-k+1$, and the (n, k, d)-linear code is Maximum Distance Separable Code ((n, k) MDS-code)[11] if $d = n-k+1$.

The generator matrix G of MDS-code is a $k \times n$ matrix, where optional k columns of matrix G are linearly independent.

A (k, n)-threshold scheme[12] has a property that some data D is divided into n pieces $D_1, D_2, ..., D_n$ in such a way that:

(1) Knowledge of any k or more D_i pieces makes D easily computable;

(2) Knowledge of any k-1 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Paper [7] tells us that (k, n)-threshold scheme can be proposed with (n, k) Reed-Solomon-code (RS-code) which is an important kind of MDS-codes, therefore we design a new authentication code with the help of (k, n)-threshold scheme next.

3.1 The model

All players in the communication are: a transmitter T, a receiver R, an opponent O, n arbiters $A_1, A_2, ...,$and A_n.

The authentication code with n arbiters is constructed as follow:

1. Key initialization phase

a. The KDC selects any (n, k) RS-code over F_q, whose generator matrix G is a $k \times n$ matrix, where q is a power of a prime. As (n, k) RS-code is also (n, k) *MDS*-code, optional k columns of matrix G are linearly independent. Rewrite

$$G = (\overline{G_1}, \overline{G_2}, ..., \overline{G_n}),$$

where $\overline{G_i}$ is a k-dimensional column vector over F_q, $i = 1, 2, ..., n$.

b. The KDC selects a set C_R of r elements from F_q and send it to the receiver as the set of legitimate messages.

c. The set of k elements C_T is selected from C_R randomly $(k < r)$ by the KDC, then C_T is sent to the transmitter secretly.

d. The KDC chooses a k-dimensional row vector $\overline{u} = (u_1, u_2, ..., u_k) \in F_q^{(k)}$ with $u_i \neq u_j$ if $i \neq j$. The KDC calculates the equation:

$$\overline{v} = (v_1, v_2, ..., v_n) = \overline{u}[\overline{G_1}, \overline{G_2}, ..., \overline{G_n}],$$

then v_i and $\overline{G_i}$ are transmitted to unique arbiter A_i secretly, $i = 1, 2, ..., n$.

2. Message transmission

If m is a legitimate message from the transmitter, $m \in C_T$. Since $C_T \subset C_R$, m is accepted by the receiver for $m \in C_R$.

3. Arbitration

The transmitter and the receiver will appeal to arbiters in case of a dispute between them. In case of a dispute, like the arbitration stage in paper [4], the keys

of optional k arbiters $A_{i_1}, A_{i_2}, ..., A_{i_k}$ are secretly selected to construct a system of linear homogeneous equations over F_q:

$$\overline{v} = (v_{i_1}, v_{i_2}, ..., v_{i_k}) = \overline{u}[\overline{G_{i_1}}, \overline{G_{i_2}}, ..., \overline{G_{i_k}}].$$

In the process no arbiter can get the keys of other arbiters.

Because optional k columns of matrix G are linearly independent, $[\overline{G_{i_1}}, \overline{G_{i_2}}, ..., \overline{G_{i_k}}]$ is a nonsingular $k \times k$ matrix, there will be unique solution $\overline{u}=(u_1,u_2,...,u_k)$, where $\{u_1, u_2, ..., u_k\} = C_T$. The message m is regarded as authentic if and only if the message $m \in C_T$.

3.2 Rationality

If m is a legitimate message from the transmitter, $m \in C_T$. Since $C_T \subset C_R$, m is accepted by the receiver by all means.

3.3 Probabilities of successful attacks

The system is subject to the following attacks($0 \le j < k$):

1. Attack O_j :

The opponent intercepts j legitimate messages $m_1, m_2, ..., m_j$ and substitutes a different message m. He wins if m is accepted as authentic by the receiver.

$$P_{O_j} = \frac{|C_R| - j}{|F_q| - j} = \frac{r - j}{q - j}.$$

2. Attack T (Impersonation by the transmitter):

The transmitter sends a message to the receiver and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic, and if this message is not one of the messages that the transmitter could have generated.

$$P_T = \frac{|C_R \backslash C_T|}{|F_q|} = \frac{r - k}{q}.$$

3. Attack R_j :

Having accepted j legitimate messages $m_1, m_2, ..., m_j$, the receiver constructs a new message m and claims it is sent by the transmitter. He succeeds if $m \in C_T$.

$$P_{R_j} = \frac{|C_T| - j}{|C_R| - j} = \frac{k - j}{r - j}.$$

Let $\overline{Z_jA}$ be the attacks from collusion of Z and less than k arbiters, Z may be O or R. $\overline{Z_0A}$ is impersonation and $\overline{Z_jA}$ ($1 \le j < k$) is substitution,respectively. Let $\overline{TA}$ be the attack from collusion of T and less than k dishonest arbiters. Then the following collusion attacks are discussed:

4. Collusion Attack $\overline{O_jA}$:

The opponent intercepts j legitimate messages $m_1, m_2, ..., m_j$ and substitutes a different message m with the help of the dishonest arbiters. He wins if m is accepted as authentic by the receiver.

Paper [7] tells us that $k-1$ arbiters A_{i_1}, A_{i_2},..., and $A_{i_{k-1}}$ won't get any information of C_T and C_R with their secret keys, nor will less than $k-1$ arbiters. Therefore,

$$P_{\overline{O_jA}} = P_{O_j} = \frac{r-j}{q-j}.$$

5. Collusion Attack $\overline{R_jA}$:

Having accepted j legitimate messages $m_1, m_2, ..., m_j$, the receiver constructs a new message m which the receiver claims it is sent by the transmitter with the help of the dishonest arbiters. He succeeds if $m \in C_T$.

The dishonest arbiters have little effect on this attack, too.

$$P_{\overline{R_jA}} = P_{R_j} = \frac{k-j}{r-j}.$$

6. Collusion Attack $\overline{TA}$:

The transmitter sends a message to the receiver colluding with the dishonest arbiters and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic, and if this message is not one of the messages that the transmitter could have generated.

It is the same as the two cases above, so

$$P_{\overline{TA}} = P_T = \frac{r-k}{q}.$$

It does well in preventing less than k arbiters from cheating, what's more, less than k arbiters will not obtain any information while the keys they have are valuable enough to authenticate the message correctly in case of a dispute. The scheme is of both efficiency and safety.

4 Concluding remarks

In this paper, the first construction may have double dishonest arbiters, single player is hard to attack the communication with the help of an arbiter, and even though both arbiters assist the transmitter, it is still difficult for them to cheat successfully. This also demonstrates the safety of the system. The second construction takes full advantage of the generator matrix of the RS-code to obtain a (k, n)-threshold scheme, and collusion between single participator and multiple arbiters won't do harm to the communication. It provides a way to construct authentication codes with the help of other codes and it indeed works.

However, the models in this paper are not perfect. The first construction has a litter larger size, i.e., the request of safety is based on the size of the code; the second one is not very convenient for arbitration.

All in all, authentication codes with multiple arbiters can be made in different ways and it still takes constant effort to construct authentication models with better properties and less costs.

References

[1] E. F. Brickell and D. R. Stinson. Authentication codes with multiple arbiters. In Advances in Cryptology-Eurocrypt'88, Lecture Notes in Computer Science, Springer-Verlag, Berlin: 1988, 330: 51-55.

[2] G. J. Simmons. Message authentication with arbitration of transmitter\receiver disputes. Proceedings of Crypto'87, Lecture Notes in Computer Science304. Berlin: 1987, 151-165.

[3] Zhou Zhi and Hu Zhengming. Authentication code with multiple arbiters. Beijing University of Posts and Telecommunications, 1996, 19(4): 75-80.

[4] Zhou Zhi and Hu Zhengming. The constructions of A^2-codes from conventional A-codes. Journal of Electronics, 1997, 19(4): 489-493.

[5] T. Johansson. Further results on asymmetric authentication schemes. Information and Computation, 151, 1999, 100-133.

[6] Y. Wang and R. Safavi-Naini. A^3-codes under collusion attacks. Proc. of Asiacrypt'99, LNCS 1716, Springer-Verlag, Berlin: 1999, 390-398.

[7] Li Yuanxing and Wang Xinmei. Secret sharing schemes and linear block codes. Journal of China Institute of Communications, 1993, 14(3): 22-28.

[8] Liu Zhen, Yang Xiaoyuan, Yan Botao, Xiao Haiyan. Mental poker protocol without trusted third party. Journal of Computer Applications, 2009, 29(7): 1836-1838.

[9] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. Advances in Cryptology. Proceedings of CRYPT'90, 1990, 537: 179-193.

[10] T. Johansson. Lower bounds on the probability of deception in authentication with arbitration. IEEE Transcations on Information Theory, 1994, 40(5): 1573-1585.

[11] Yang Yixian. The applications of MDS-codes in cryptography. Journal of Beijing University of Posts and Telecommunications, 1988, 11(1): 30-35.

[12] A. Shamir. How to share a secret. Communication of the ACM, 1979, 22(11): 612-613.

[13] Liu Huanping and Yang Yixian. A generalized (k, n)-threshold secret sharing scheme. Journal of China Institute of Communications, 1998, 19(8): 72-77.

[14] Zheng Baodong. A discussion on (k, n) threshold communication secret key sharing systems. Journal of China Institute of Communications, 1994, 15(6): 23-28.