New Bound on Authentication Code with Arbitration

Kaoru KUROSAWA

Department of Electrical and Electronic Engineering,
Faculty of Engineering,
Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan
Tel. +81-3-5734-2577
E-mail kkurosaw@ss.titech.ac.jp

Abstract. For the authentication model with arbitration (A^2-code), Johansson showed a lower bound on the size of encoding rules. However, this bound is no longer tight if the size of source states is large. This paper presents a more tight lower bound on the size of encoding rules for large source states. An A^2-code is shown which approximately meets the proposed bound, also. Further, we show that the size of encoding rules for the transmitter can be greatly reduced if the receiver's cheating probability is slightly large.

1 Introduction

As in [8], A^2-code is described as follows. In the model for normal authentication (A-code), the transmitter and the receiver are using the same encoding rule and are thus trusting each other [1] ~ [5]. However, it is no always the case that the two communicating parties want to trust each other. Inspired by this problem Simmons has introduced an extended authentication model [6, 7], here referred to as the authentication model with arbitration (A^2-code). In this model caution is taken against deception from both outsiders (opponent) and insiders (transmitter and receiver). The model includes a fourth person, called the arbiter. The arbiter has access to all key information and is by definition not cheating. The arbiter 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 the following:
I, Impersonation by the opponent. The opponent sends a massage 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

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 140-149, 1994.

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.
$\mathbf{R}_0$, 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 P_I, P_S, P_T, P_{R_0} and P_{R_1}.

Let E_R be a set of the receiver's encoding rules and E_T be a set of the transmitter's encoding rules. Also, let S be a set of source states. Recently, Johansson showed [8] a lower bound on $|E_T|$ and $|E_R|$ to achieve $\max(P_I, P_S, P_T, P_{R_0}, P_{R_1}) = 1/q$. This bound is tight for $|S| \leq q$ because he also showed an A^2-code which meets the bound [9]. However, this bound is no longer tight if $|S| > q + 1$.

On the other hand, it is known that, in A-code, the size of encoding rules is greatly reduced if P_S is slightly greater than its lower bound [11, 12, 13], most notably in [13].

This paper presents a more tight lower bound on $|E_T|$ and $|E_R|$ for $|S| > q+1$ than [8]. An A^2-code is shown which approximately meets the proposed bound, also. Further, we show that $|E_T|$ can be greatly reduced if P_{R_1} is slightly greater than $1/q$.

2 Preliminaries

2.1 Notation

- $|B|$ denotes the cardinality of a set B.
- When we write $X = \{x_{ij}\}$, X denotes a matrix whose (i, j) element is x_{ij}. We denote by x_j the j-th column vector of X. y_j denotes the j-th column vector of Y, etc.
- For a vector y, define $w(y) \triangleq$ the number of nonzero elements of y. We say that $w(y)$ is the weight of y.
- For $x_i = (x_{1i}, x_{2i}, \cdots)^T$ and $x_j = (x_{1j}, x_{2j}, \cdots)^T$, define $x_i \odot x_j = (x_{1i}x_{1j}, x_{2i}x_{2j}, \cdots)^T$.

2.2 Authentication code (A-code)

In the normal model for authentication, there are three participants, a transmitter **T**, a receiver **R** and an opponent **O**. An authentication code (A-code) is **(S,E,M)** such that $\mathbf{S} = \{s\}$ is a set of source states, $\mathbf{E} = \{e\}$ is a set of rules and $\mathbf{M} = \{m\}$ is a set of messages. T and R share e secretly. On input s, T sends m such that $m = e(s)$ to R. R accepts or rejects m based on e.

There are two kinds of attacks of the opponent O, the impersonation attack and the substitution attack. They are defined in the same way as described in

Introduction. The impersonation attack probability $\mathbf{P_I}$ is defined by

$$\mathbf{P_I} \triangleq \max_m \Pr[\mathbf{R} \text{ accepts } m].$$

The substitution attack probability $\mathbf{P_S}$ is defined by

$$\mathbf{P_S} \triangleq \sum_m \Pr(\mathbf{M} = m) \max_{\hat{m} \neq m} \Pr[\mathbf{R} \text{ accepts } \hat{m} \mid \mathbf{R} \text{ accepts } m]$$

Definition 1. A without secrecy A-code is such that $\forall m$ is written as (s, a), where s a a source state and a is an authenticator. For a without secrecy A-code, let $M_s \triangleq \{m | m = (s, a)\}$.

Definition 2. An A-code is called no splitting if each e generates one message for $\forall s$.

Definition 3. A skeleton matrix for (E, M) is a $|E| \times |M|$ matrix $X = \{x_{ij}\}$ such that

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

2.3 Basic results on A-code

The following observation is a basis for the bound on P_I and P_S.

Claim 4. *Let $X = \{x_{ij}\}$ be a skeleton matrix for (E, M). Suppose that E is uniformly distributed. Then,*

$$\Pr(R \textit{ accepts } m_j) = w(x_j)/|E|, \quad P_I = \max_j w(x_j)/|E|$$

$$\Pr(R \textit{ accepts } m_j | R \textit{ accepts } m_i) = w(x_i \odot x_j)/w(x_i)$$

Let $k \triangleq |\mathbf{S}|$, $v \triangleq |\mathbf{M}|$, $b \triangleq |\mathbf{E}|$, $l \triangleq v/k$. For simplicity, we assume that E is uniformly distributed.

Proposition 5. *[2] $P_{\mathbf{I}} \geq k/v$. For the skeleton matrix $X = \{x_{ij}\}$, $P_{\mathbf{I}} = k/v$ if and only if*

$$w(x_j)/b = k/v \textit{ for } \forall j.$$

Suppose we have a without secrecy A-code with no splitting. Then,

Proposition 6. *[10] If $P_{\mathbf{I}} = k/v = 1/l$, then $P_{\mathbf{S}} \geq 1/l$. For the skeleton matrix $X = \{x_{ij}\}$, $P_I = P_S = 1/l$ if and only if, for $\forall s$, $\forall s'$ such that $s \neq s'$ and for $\forall m_i \in M_s$, $\forall m_j \in M'_s$, $w(x_i \odot w_j)/b = 1/l^2$.*

Proposition 7. *[10, 5] If $P_{\mathbf{I}} = P_{\mathbf{S}} = k/v = 1/l$, then $b \geq \max(l^2,\ k(l-1)+1)$.*

3 New bound for A^2-code

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

A^2-code is 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 a set of the transmitter's encoding rules. Let $E_R \circ E_T$ denote the set of possible pairs of $E_R \times E_T$. At the preprocessing stage, the arbiter sends $f_i \in E_R$ to the receiver R and $e_i \in E_T$ to the transmitter T secretly. e_i (therefore, T) generates one message for each $s \in S$ (that is, no splitting. However, f_i would accept many messages.) R accept $m \in M$ iff $f_i(m)$ is valid. When some dispute happens between T and R, the arbiter accepts m as authentic iff e_i can generate m.

3.2 Johansson's bound

Proposition 8. *[8]. If* $\max(P_I, P_S, P_T, P_{R_0}, P_{R_1}) = 1/q$, *then*

$$|E_R| \geq q^3, \quad |E_T| \geq q^4, \quad |E_R \circ E_T| \geq q^5, \quad |M| \geq q^2|S|$$

4 Generalization of basic results on A-code

Proposition 5 can be generalized as follows.

Lemma 9. *Let* $X = \{x_{ij}\}$ *be a* $b \times v$ *binary matrix. Let the row vectors be* $g_1, g_2, \cdots,$. *Suppose that* $w(g_i) \geq k$ *for* $\forall i$. *Then,*

(1) $\max_i w(x_j)/b \geq k/v$.
(2) The equality holds if and only if $w(x_j) = kb/v$ *for* $\forall j$ *and* $w(g_i) = k$ *for* $\forall i$.

Proof. Denote by N the total number of 1s in X. Then, $N \geq kb$. Therefore, there exists x_j such that $w(x_j)/b \geq N/v \geq kb/v$. (2) is clear from the above discussion. □

Definition 10. Let $I_l(h) \triangleq \{i|(h-1)l+1 \leq i \leq hl\}$. 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 $\forall x_i \in I_l(h_1)$, $\forall x_j \in I_l(h_2)$,

$$w(x_i \odot x_j) = \begin{cases} n_1 & \text{if } h_1 \neq h_2 \\ 0 & \text{if } h_1 = h_2 \text{ and } x_i \neq x_j \end{cases}$$

Then, proposition 7 can be generalized as follows.

Lemma 11. *If there exists a* (b, k, l, n_0, n_1) K- *array, then* $b \geq k(l-1)+1$.

Proof. Let $X = \{x_{ij}\}$ be a (b, k, l, n_0, n_1) K- array. Let the row vectors be $g_1, g_2, \cdots, g_b$. Define $z_h = (z_{h,1}, z_{h,2}, \cdots, z_{h,kl})$ as a row vector such that

$$z_{h,j} = \begin{cases} 1 & j \in I_l(h) \\ 0 & \text{otherwise.} \end{cases}$$

for $1 \leq h \leq k$. Let V be a vector space over the real number field spanned by $\{g_1, \cdots, g_b, z_1, \cdots, z_{k-1}\}$. We prove that $\dim V = kl$. First, we show that $z_k \in V$. It is easy to see that $z_k = (\sum g_i)/n_0 - \sum_{i \neq k} z_i$ from the definition of K-array. Thus, $z_k \in V$. Next, define

$$u_p \triangleq (0, \cdots, \underset{(p)}{1}, \cdots, 0)$$

Let V' be the vector space spanned by $\{u_1 \cdots, u_{kl}\}$. It is clear that $V \subseteq V'$. We show the converse. For $\forall h_1$, fix $p \in I_l(h_1)$, arbitrarily. Let the row vectors of X such that $x_{ip} = 1$ be $g'_1, g'_2, \cdots, g'_{n_0}$. Then, from the definition of K-array, we have

$$\sum_{i=1}^{n_0} g'_i = n_0 u_p + n_1 \sum_{i \neq h_1} z_i$$

Hence,

$$u_p = 1/n_0 (\sum_{i=1}^{n_0} g'_i - n_1 \sum_{i \neq h_1} z_i)$$

Thus, $u_p \in V'$ for $1 \leq p \leq kl$. This means that $V' \subseteq V$. Therefore, $\dim V = \dim V' = kl$. Hence, we must have $b + k - 1 \geq kl$. Then, we have this lemma. □

Lemma 12. *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.*

Proof. Clear from proposition 5 and 6. □

4.1 New bound

We present a more tight lower bound on the size of encoding rules than proposition 8 [8] for $| S | > P_{\mathbf{I}}^{-1} + 1$. (We consider without secrecy A^2-codes with no splitting.) Let

$$E_T(f_i) \triangleq \{e_j \mid \Pr(e_j, f_i) > 0\}$$
$$E_R(e_i) \triangleq \{f_j \mid \Pr(e_i, f_j) > 0\}$$
$$M_s \triangleq \{m | m = (s, a)\}.$$

Theorem 13. *Suppose that*

(C1) $P_{\mathbf{I}} = P_{\mathbf{S}} = P_{\mathbf{R}_0} = P_{\mathbf{R}_1} = P_{\mathbf{T}} = 1/q$
(C2) $|\,\mathbf{M}\,| = q^2\,|\,\mathbf{S}\,|$
(C3) $|\,E_{\mathbf{R}}(e_i)\,| = q$.
(C4) *$E_T, E_R, E_T(f_i)$ and $E_R(e_j)$ are uniformly distributed, respectively.*
(C5) *For $\forall s$, there exist $A_1, A_2, \cdots$ such that*

$$M_s = A_1 \cup A_2 \cup \cdots, \quad A_i \cap A_j = \phi, \quad |A_i| = constant.$$

$\forall f_h \in E_R$ accepts just one message in $\forall A_i$.

Then,

$$|E_R| \geq |S|q(q-1)+1, \quad |E_T \circ E_R| \geq (|S|(q-1)+1)|E_R|, \quad |E_T| = |E_T \circ E_R|/q$$

Remark. (1) Our bound is more tight than proposition 8 if $|S| > q+1$.
(2) From proposition 8, $|M| \geq q^2|S|$. (C2) requires that this equality holds.
(3) It is easy to see that $|E_R(e_i)| \geq q$ if $P_T = 1/q$. (C3) requires that this equality holds.
(4) Consider the following situation. T sends $m_i \in M_s$. The opponent changes m_i to $m_j \in M_s$ and R acccpts m_j. In this case, the source state is the same. However, if some dispute happens between T and R, the arbiter does not accept m_j as authentic. This attack should also be considered as a substitution attack of the opponent. We call this attack the second type substitution attack of the opponent.

4.2 Proof

Let $X = \{x_{ij}\}$ be the skeleton matrix for (E_R, M) (see Def.3). We will show that X is a $(|E_R|, q|S|, q, |E_R|/q, |E_R|/q^2)$ K- array (see Def.10). Let

$$M_{f_i} \triangleq \{m \mid f_i \text{ accepts m }\}, \quad M_{f_i}(s) \triangleq \{m \mid m \in M_{f_i}, m = (s,a)\}.$$

Lemma 14. **(1)** *$w(x_i) = |E_R|/q$ for $\forall i$.*
(2) $|\,E_{\mathbf{T}}(f_i)\,| \geq |\,\mathbf{S}\,|\,(q-1)+1$
(3) $|\,M_{f_i}\,| = q\,|\,\mathbf{S}\,|$
(4) $|\,M_{f_i}(s)\,| = q$

Proof. Consider a A-code $(S, M_{f_i}, E_T(f_i))$ in which the arbiter is a receiver and the receiver is an opponent. Let $Y = \{y_{ij}\}$ be the skeleton matrix for $(E_T(f_i), M_{f_i})$. Each row vector of Y has a constant weight $|S|$ because $\forall e_j$ generates one message for each s (no splitting). Then, from lemma 9,

$$1/q = P_{R_0} = \max_i w(y_i)/|E_T(f_i)| \geq |S|/|M_{f_i}| \tag{1}$$

Therefore, $|M_{f_i}| \geq q|S|$. Now, we have shown that the weight of each row vector of X is at least $q|S|$. Then, from lemma 9 and (C2),

$$1/q = P_I = \max_i w(x_i)/|E_R| \geq q|S|/|M| = 1/q$$

This means that $\max_i w(x_i)/|E_R| = q|S|/|M|$. Then, again from lemma 9, we have

$$w(x_i) = |E_R|/q \quad \text{for } \forall i, \quad \text{and } |M_{f_i}| = q|S| \quad \text{for } \forall i$$

Then, we see that the equality of eq.(1) is also satisfied. That is,

$$1/q = P_{R_1} = P_{R_0} = |S|/|M_{f_i}|$$

Now, from lemma 11 and 12, we have (2) of this lemma. Finally, we will prove (4). Let $W = \{w_{ij}\}$ be the skeleton matrix for $(E_T(f_i), M_{f_i}(s))$. The weight of each row vector of W is 1 from the second sentence of this proof. Then, from lemma 9, we have

$$1/q = P_{R_0} = \max_i w(w_i)/|E_T(f_i)| \geq 1/|M_{f_i}(s)|$$

Therefore, $|M_{f_i}(s)| \geq q$. On the other hand, $q|S| = |M_{f_i}| = \sum_s |M_{f_i}(s)| \geq q|S|$. Hence, we must have $|M_{f_i}(s)| = q$. □

¿From lemma 14, we see that X satisfies the condition (1) of Def.10.

Lemma 15. $|M_s| = q^2$.

Proof. Let $Y = \{y_{ij}\}$ be the skeleton matrix for (E_R, M_s). Each row vector of Y has the weight $|M_{f_i}(s)| = q$ from lemma 14. Then, from lemma 9,

$$1/q = P_I = \max_i w(y_i)/|E_R| \geq q/|M_s|$$

Therefore, $|M_s| \geq q^2$. On the other hand, $q^2|S| = |M| = \sum_s |M_s| \geq q^2|S|$. Hence, it must be that $|M_s| = q^2$. □

Let $F_i \triangleq \{f_u \mid f_u \text{ accepts } m_i\}$. Note that $|F_i| = w(x_i) = |E_R|/q$ from lemma 14.

Lemma 16. *For $\forall s, \forall s'$ such that $s \neq s'$, and for $\forall m_i \in M_s, \forall m_j \in M_{s'}$,*

$$w(x_i \odot x_j) = |E_{\mathbf{R}}|/q^2.$$

Proof. Suppose that **T** sends $m_i \in M_s$. Consider a substitution attack such that **O** changes m_i to $m_j \in M_{s'}$. This attack is modeled by the skeleton matrix for $(F_i, M_{s'})$. Let the skeleton matrix be $Y = \{y_{ij}\}$. The weight of each row of Y is $|M_{f_h}(s')| = q$ from lemma 5.1(4). Then, from lemma 9 and lemma 15,

$$1/q = P_S \geq \max_j w(y_j)/|F_i| \geq |M_{f_h}(s')|/|M_{s'}| = 1/q.$$

Therefore, from lemma 9, $w(y_j) = |F_i|q^{-1} = |E_R|q^{-2}$ for $\forall j$. It is easy to see that $w(y_j) = w(x_i \odot x_j)$. □

Lemma 17. *For $\forall s$, there exist $A_1 \cdots A_q$ such that*

(1) $M_s = A_1 \cup A_2 \cup \cdots \cup A_q, |A_i| = q$

(2) *For* $\forall A_t, \forall A_u$ *and for* $\forall x_i \in A_t, \forall x_j \in A_u$,

$$w(x_i \odot x_j) = \begin{cases} |E_R|/q^2 & \text{if } A_t \neq A_u \quad (2) \\ 0 & \text{if } A_t = A_u \text{ and } x_i \neq x_j \quad (3) \end{cases}$$

Proof. ¿From lemma 14, $|M_{f_h}(s)| = q$ for $\forall f_h$. Then, from (C5), there exist $A_1 \cdots A_q$ such that $M_s = A_1 \cup A_2 \cup \cdots \cup A_q$ and $\forall f_h$ accepts just one message in $\forall A_t$. Because $|M_s| = q^2$ (from lemma 15), we have $|A_u| = q$.

Since $\forall f_h$ accepts just one message in $\forall A_t$, we have eq.(3). Without loss of generality, let $A_t = A_1$ and let $\hat{M} = A_2 \cup \cdots \cup A_q$. Then, $|\hat{M}| = q(q-1)$. Suppose that **T** sends $m_i \in A_1$. The second type substitution attack (see Remarks 1 (4)) is modeled by the skeleton matrix for $(F_i, \hat{M})$. Let the skeleton matrix be $Y = \{y_{ij}\}$. The weight of each row vector of Y is $|M_{f_h}(s)| - 1 = q - 1$ since m_i is excluded (see lemma 14). Then, from lemma 9,

$$1/q = P_S \geq \max_j w(y_j)/|F_i| \geq (q-1)/|\hat{M}| = 1/q.$$

Therefore, from lemma 9,

$$w(x_i \odot w_j) = w(y_j) = |F_i|q^{-1} = |E_R|q^{-2}$$

for $\forall j$. Thus, eq.(2) is proved. □

¿From lemma 5.3 and 5.4, it is easy to see that X satisfies the condition (2) of Def.4.1. ¿From this fact and from lemma 5.1(1), X is a $(|E_R|, q|S|, q, |E_R|/q, |E_R|/q^2)$ K- array. Therefore, from lemma 11,

$$|E_R| \geq q|S|(q-1) + 1$$

Then, from lemma 5.1(2), $|E_T \circ E_R| \geq (|S|(q-1)+1)|E_R|$.. ¿From (C3), $|E_T| = |E_T \circ E_R|/q$.

5 Construction of A^2-code

We show two A^2-code, α and β. A^2-code α approximately meets the bound of Theorem 13. In A^2-code β, it is shown that $|E_T|$ can be greatly reduced by letting P_{R_1} be slightly greater than $1/q$ (as long as $|S| > q+1$).

Let q be a prime power. Let a source state s be $s = (s_1, s_2, \cdots, s_n)$, where $\forall s_i \in GF(q)$.
In the proposed codes, $f_i \in E_R$ is $f_i = (f_{i1}, f_{i2}, \cdots, f_{i,n+2})$, where $\forall f_{ij} \in GF(q)$. T sends $m = (s_1, s_2, \cdots, s_n, m_1, m_2)$. R accepts m iff

$$m_2 = s_1 f_{i,1} + s_2 f_{i,2} + \cdots + s_n f_{i,n} + f_{i,n+1} + m_1 f_{i,n+2}$$

(A^2-code α)

In this A^2-code, $e_i \in E_T$ is $e_i = (e_{i1}, e_{i2}, \cdots, e_{i,2n+2})$, where $\forall e_{ij} \in GF(q)$. e_i and f_i are related as follows.

$$\left.\begin{array}{rcl} e_{i1} & = & f_{i1} + e_{i,n+2} f_{n+2} \\ e_{i2} & = & f_{i2} + e_{i,n+3} f_{i,n+2} \\ & \vdots & \\ e_{in} & = & f_{in} + e_{i,2n+1} f_{i,n+2} \\ e_{i,n+1} & = & f_{i,n+1} + e_{i,2n+2} f_{i,n+2} \end{array}\right\}$$

m_1 and m_2 are computed as follows.

$$m_1 = s_{i1} e_{i,n+2} + s_{i2} e_{i,n+3} + \cdots + s_n e_{i,2n+1} + e_{i,2n+2}$$
$$m_2 = s_1 e_{i,1} + s_2 e_{i,2} + \cdots + s_n e_{i,n} + e_{i,n+1}$$

Theorem 18. *In the above scheme,* $P_{\mathbf{I}} = P_{\mathbf{S}} = P_{\mathbf{R}_0} = P_{\mathbf{R}_1} = P_{\mathbf{T}} = 1/q$, *and*

$$|E_R| = q^2|S|, \quad |E_T \circ E_R| = q^3|S|^2, \quad |E_T| = q^2|S|^2$$

(A^2-code β)

In A^2-code β, $e_i \in E_T$ is $e_i = (e_{i1}, e_{i2}, \cdots, e_{i,n+2}, e_{i,2n+2})$, where $\forall e_{ij} \in GF(q)$. This code is obtained from A^2-code α by letting

$$e_{i,n+3} = e_{i,n+2}^2, \ \cdots, \ e_{i,2n+1} = e_{i,n+2}^n$$

Theorem 19. *In the above scheme,* $P_{\mathbf{I}} = P_{\mathbf{S}} = P_{\mathbf{R}_0} = P_{\mathbf{T}} = 1/q$, $P_{\mathbf{R}_1} \leq n/q$ *and*

$$|E_R| = q^2|S|, \quad |E_T \circ E_R| = q^4|S|, \quad |E_T| = q^3|S|$$

6 Further work

Relationships with error correcting codes and orthogonal arrays will be discussed in the final paper.

References

1. E.N.Gilbert, F.J.MacWilliams and N.J.A.Sloane, "Codes which detect deception", *Bell Syst. Tech. J.*, Vol.53, 1974, pp.405–424
2. G.J.Simmons, "Authentication theory/coding theory", in *Advances in Cryptology, Proceedings of CRYPTO 84*, G.R.Blakley and D.Chaum, Eds.Lecture notes in Computer Science, No.196. New York, NY:Springer, 1985, pp.411–431.
3. J.L.Massey, "Contemporary Cryptology, An Introduction", in *Contemporary Cryptology, The Science of Information Integrity*, G.J.Simmons, Ed., IEEE Press, 1991, pp.3–39.
4. 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.

5. D.R.Stinson, *Combinatorial Characterization of Authentication Codes*, Proceedings Crypto 91, Lecture Notes in Computer Science 576, Springer 1992, pp62–72.
6. G.J.Simmons, "Message authentication with arbitration of transmitter/receiver disputes", in *Proceedings of Eurocrypt '87.*
7. G.J.Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration", in *Journal of Cryptology*, Vol.2, no.2, 1990, pp.77–104.
8. Thomas Johansson,"Lower Bounds on the Probability of Deception in Authentication with Arbitation", in *Proceeding of 1993 IEEE International Symposium on Information Theory,*San Antonio,USA,January 17-22,1993,p.231
9. Thomas Johansson, "On the construction of perfect authentication codes that permit arbitration", Crypto 93
10. D.R.Stinson, "The combinatorics of authentication and secrecy codes", Journal of Cryptology, Vol.2, 1990, pp.23–49.
11. M.N.Wegman and J.L.Carter. *New hash functions and their use in authentication and set equality,* J.Comput.System Sci. 22(1981), 265–279.
12. D.R.Stinson,"Universal Hashing and authentication codes" *Proceeding of Crypto 91,*Santa,Babara,USA,1991,pp.74-85
13. Jürgen Bierbrauter, Thomas Johanssen, Gregory Kabatianskii, Ben Smeets, "On Families of Hash Functions via Geometic Codes Concatination", Crypto 93