A^3-codes under Collusion Attacks

Yejing Wang and Rei Safavi-Naini

School of IT and CS, University of Wollongong,
Northfields Ave., Wollongong 2522, Australia
{yw17, rei}@uow.edu.au

Abstract. An A^3-code is an extension of A-code in which none of the three participants, transmitter, receiver and arbiter, is assumed trusted. In this paper we extend the previous model of A^3-codes by allowing transmitter and receiver not only to individually attack the system but also collude with the arbiter against the other. We derive information-theoretic lower bounds on success probability of various attacks, and combinatorial lower bounds on the size of key spaces. We also study combinatorial structure of optimal A^3-code against collusion attacks and give a construction of an optimal code.

1 Introduction

Authentication codes (A-codes) [7] provide protection for two trustworthy participants against an active spoofer tampering with the messages sent by a *transmitter* to a *receiver* over a public channel. In this model transmitter and receiver are assumed trusted. An extension of this model is an *authentication codes with arbitration* [8], or A^2-codes for short, in which transmitter and receiver are not trusted: transmitter may deny a message that he/she has sent, and receiver may attribute a fraudulent message to the transmitter. In an A^2-code a trusted third party, called *arbiter*, resolves the dispute between transmitter and receiver. A^2-codes have been studied by various authors [3], [4] and [6].

Brickell and Stinson ([1]) introduced authentication code with dishonest arbiter(s), or A^3-code, in which the arbiter may tamper with the communication but it will remain trusted in her arbitration. In an A^3-code each participant in the system has some secret key information which is used to protect him/her against attacks in the system. These codes have been also studied in [2], [3] and [9], where some constructions were given. However none of these constructions protect against collusion attacks.

Collusion attacks in A-codes are studied in various extensions of A-codes, such as multisender schemes [10] where unauthorised groups of senders can collude to construct a fraudulent message that is attributed to an authorised group, and multreceiver schemes where unauthorised groups of receivers collude to construct a fraudulent message that is attributed to the transmitter. The model studied in [3] is an extension of multreceiver schemes where transmitter can collude with unauthorised groups of receivers. In the former two cases no arbitration is required as at least one side in the communication is trusted, that is

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 390–398, 1999.

receiver in a multisender scheme and transmitter in a multireceiver scheme are assumed trusted. However in the last case none of the sides is trusted and there can be a dispute between a receiver and a colluding group of the sender and receivers. The suggestion for resolving the dispute is to either include a trusted arbiter or, take the majority vote of the receivers.

In this paper we extend the attack model of A^3-codes to include collusion between arbiter and transmitter or receiver, against the other participants. For example, the arbiter may collude with the transmitter to construct a message that the transmitter can later deny sending it, or she may collude with the receiver to impersonate the sender or substitute a message that he has sent. We assume that the arbiter always honestly follows the arbitration rules. These rules are public and collusion with a participant effectively means that the arbiter will make her key information available to that participant.

The paper is organised as follows. In Section 2 we introduce the model and derive information theoretic bounds on success probabilities of various attacks, and combinatorial bounds on the size of key spaces for each participant. Section 3 gives combinatorial structure of Cartesian optimal A^3-codes. Section 4 gives a construction for such codes.

2 Model and Bounds

There are three participants: a *transmitter*, T, a *receiver*, R and an *arbiter*, A, none of them is assumed trusted. T wants to send a source state s, $s \in S$, to R over a public channel. Each participant has some secret *key*. T uses his key information to construct a message $m \in M$ for a source state s to be sent over the channel. R uses her key information to verify authenticity of a received message and finally A who does not know the key information of T and R will use her key information to resolve a dispute between the two. Transmitter's key, e_t, determines the encoding function $e_t : S \to M$ used by the transmitter, and receiver's key, e_r, determines the verification function $e_r : M \to S \cup \{F\}$ and so the subset of M that R will accept as valid message. Arbiter's key, e_a, determines a subset $M(e_a) \subset M$, which the arbiter accepts as valid.

There is also an *outsider*, O, who has no key information. A colluding group of attackers in general use their knowledge of the system, their key information and all the previous communicated messages to construct fraudulent messages.

The system has the following stages.

Key Distribution: during which a triple (e_t, e_r, e_a) of keys for the three participants T, R, and A is generated and each participant's key is securely delivered to him/her. This stage can be either performed by a trusted party, or by a collaboration of the three principals. A valid triple has the property that if $e_t(s) = m$ then $e_r(m) = s$ and $e_a(m) = s$.

Authentication: T uses e_t to generate an authentic message.

Verification: R uses e_r to verify authenticity of a received message m. She will also always ask for the verdict of A on the message. R will only accept a message if both R and A accept the message as authentic. We note that in [3] a

message is acceptable by the receiver if $e_r(m) \in S$. This means that $e_r(m) \in S$ implies $e_a(m) \in S$. We assume $M(e_r) \cap M(e_a) \neq \emptyset$ and so for every message both conditions, $e_r(m) \in S$ and $e_a(m) \in S$, must be checked.

Arbitration: A dispute occurs in a number of situations. In the following we list possible disputes and the rules for resolving the disputes. We note that the rules are public and A's arbitration can be later verified by everyone.

1. **Arbitration Rule I (AR I)**: T denies sending a message m.
   - T wins if m is acceptable by e_r and e_a.
   - T looses otherwise.
2. **Arbitration Rule II (AR II)**: R attributes a message m to T but T denies it.
   - R wins if m is valid under e_a.
   - R looses otherwise.

The system is subject to the following attacks.

1. Attack O_i: Observing a sequence of i legitimate messages $m_1, m_2, \cdots, m_i$, the opponent places another message m into the channel. He is successful if both the receiver and the arbiter accept m as an authentic message.

2. Attack R_i: Receiving a sequence of i legitimate messages, $m_1, m_2, \cdots, m_i$, and using her key, e_r, R claims that she has received a message $m \neq m_1, m_2, \cdots, m_i$. She is successful if A accepts m under the arbitration rule II.

3. Attack A_i: Knowing a sequence of i legitimate messages $m_1, m_2, \cdots, m_i$, and using her key e_a, the arbiter puts another message m into the channel. She is successful if the message is valid for R.

4. Attack T_0: Using his key (an encoding rule) e_t, transmitter sends a fraudulent message m which is not valid under e_t. He succeeds if both the receiver and the arbiter accept the message.

5. Collusion Attack $\overline{RA}_i$: Having received a sequence of i legitimate messages $m_1, m_2, \cdots, m_i$, R and A collude to construct a message which R claims it is sent by the transmitter. They succeed if m can be generated by the transmitter under e_t.

6. Collusion Attack $\overline{TA}$: A and T, using their keys e_t and e_a, collude to construct a message m which is not valid under e_t but using $AR\ I$ makes T a winner.

Let E_T, E_R and E_A be the set of transmitter's, receiver's and arbiter's keys, respectively, and assume $p(x, y, z)$ is the joint probability distribution on $E_T \times E_R \times E_A$. Also assume there is a probability distribution on the set of source states S. Denote the *support* of the joint probability distribution by

$$E_T \circ E_R \circ E_A = \{(e_t, e_r, e_a) : p(e_t, e_r, e_a) > 0\}.$$

The joint probability distribution determines the marginal distributions: $p(e_r, e_a)$, $p(e_t)$, $p(e_r)$ and $p(e_a)$. Similarly denote

$$E_R \circ E_A = \{(e_r, e_a) : p(e_r, e_a) > 0\}.$$

We will also use the following notations.

$$E_{\overline{RA}}(m^i) = \{(e_r, e_a) \in E_R \circ E_A : \text{ both } e_r, e_a \text{ accept } m^i\},$$
$$E_{\overline{RA}}(e_t) = \{(e_r, e_a) \in E_R \circ E_A : p(e_t, e_r, e_a) > 0\}.$$

Let M be the set of all possible messages, and M^i denote the set of sequences of i distinct messages.

Using these notations, success probabilities in various attacks are given as follows.

$$P_{O_i} = \max_{m^i \in M^i} \max_{m \in M} p(R \text{ and } A \text{ accept } m \mid R \text{ and } A \text{ accept } m^i) \quad (1)$$

$$P_{R_i} = \max_{m^i \in M^i, e_r \in E_R} \max_{m \in M} p(A \text{ accepts } m \mid A \text{ accepts } m^i, e_r) \quad (2)$$

$$P_{A_i} = \max_{m^i \in M^i, e_a \in E_A} \max_{m \in M} p(R \text{ accepts } m \mid R \text{ accepts } m^i, e_a) \quad (3)$$

$$P_{T_0} = \max_{e_t \in E_T} \max_{m \notin M(e_t)} p(R \text{ and } A \text{ accept } m \mid e_t) \quad (4)$$

$$P_{\overline{RA}_i} = \max_{m^i \in M^i} \max_{(e_r, e_a) \in E_R \circ E_A} \max_{m \in M} p(T \text{ generates } m \mid T \text{ generates } m^i, e_r, e_a) \quad (5)$$

$$P_{\overline{TA}} = \max_{e_t \in E_T} \max_{e_a \in E_A} \max_{m \in M(e_a) \setminus M(e_t)} p(R \text{ accepts } m \mid e_t, e_a) \quad (6)$$

We note that P_{O_i} and P_{T_0} are different from similar attacks given in [3] as we define success of an attacker as successful verification by the receiver and successful acceptance by the arbiter while in [3] only the first condition is required.

2.1 Information Theoretic Bounds

We will use following notations throughout the paper.

$$E_X(m^i) = \{e_x \in E_X : m^i \text{ is available for } e_x\}.$$
$$E_X(e_y) = \{e_x \in E_X : p(e_x, e_y) > 0\}.$$
$$M(e_y) = \{m \in M : m \text{ is available for } e_y\}.$$

Theorem 1 gives the information-theoretic lower bounds on the above 6 types of attack.

Theorem 1. *In an A^3-code against collusion attacks we have*

1. $P_{O_i} \geq 2^{H(E_R, E_A | M^{i+1}) - H(E_R, E_A | M^i)}$.
2. $P_{R_i} \geq 2^{H(E_A | M^{i+1}, E_R) - H(E_A | M^i, E_R)}$.
3. $P_{A_i} \geq 2^{H(E_R | M^{i+1}, E_A) - H(E_R | M^i, E_A)}$.
4. $P_{T_0} \geq 2^{H(E_R, E_A | M, E_T) - H(E_R, E_A | E_T)}$.
5. $P_{\overline{RA}_i} \geq 2^{H(E_T | M^{i+1}, E_R, E_A) - H(E_T | M^i, E_R, E_A)}$.
6. $P_{\overline{TA}} \geq 2^{H(E_R | M, E_T, E_A) - H(E_R | E_T, E_A)}$.

for $i = 0, 1, 2, \cdots$.

2.2 Combinatorial Bounds on Key Spaces

To derive combinatorial bounds we will *assume that the probability distribution on $E_T \circ E_R \circ E_A$ is uniform.* With this assumption we have the following theorem.

Theorem 2. *In an A^3-code if all six kinds of attacks meet their lower bounds, then*

1. $|E_T| \geq (\prod_{i=0}^{l} P_{\overline{RA_i}})^{-1} (\prod_{i=0}^{l} P_{O_i})^{-1}$.
2. $|E_R| \geq P_{T_0}^{-1} (\prod_{i=0}^{l} P_{O_i})^{-1} (\prod_{i=0}^{l} P_{R_i})$.
3. $|E_A| \geq P_{T_0}^{-1} (\prod_{i=0}^{l} P_{O_i})^{-1} P_{\overline{TA}} (\prod_{i=0}^{l} P_{A_i})$.
4. $|E_R \circ E_A| \geq P_{T_0}^{-1} (\prod_{i=0}^{l} P_{O_i})^{-1}$.

An A^3-code is called *l-optimal* if,
(i) all six types of attacks meet their lower bounds in theorem 1, and
(ii) all inequalities in theorem 2 are satisfied with equalities.

In the following we give structural properties of l-optimal codes in order to analyse their combinatorial structure.

Corollary 1. *In an optimal A^3-code against collusion attacks the following properties are satisfied.*

1. *If $E_{\overline{RA}}(m^i) \neq \emptyset$, then $|E_{\overline{RA}}(m^i)|$ is independent of m^i.*
2. *If $E_T(m^i) \cap E_T(e_r, e_a) \neq \emptyset$, then $|E_T(m^i) \cap E_T(e_r, e_a)|$ is independent of m^i, e_r and e_a.*
3. *If $E_R(m^i) \cap E_R(e_a) \neq \emptyset$, then $|E_R(m^i) \cap E_R(e_a)|$ is independent of m^i and e_a.*
4. *If $E_A(m^i) \cap E_A(e_r) \neq \emptyset$, then $|E_A(m^i) \cap E_A(e_r)|$ is independent of m^i and e_r.*
5. *If $E_T(m^i) \neq \emptyset$, then $|E_T(m^i)|$ is independent of m^i.*
6. *If $E_R(m^i) \neq \emptyset$, then $|E_R(m^i)|$ is independent of m^i.*
7. *If $E_A(m^i) \neq \emptyset$, then $|E_A(m^i)|$ is independent of m^i.*

An A^3-code is called a *Cartesian A^3-code* if for any message m, there is a unique source state s which can be encoded to m.

This means that in a Cartesian code M can be partitioned into $M(s_1)$, $M(s_2), \cdots$ such that messages in $M(s_j)$ only correspond to s_j.

More precisely, for an $s \in S$ and $(e_r, e_a) \in E_R \circ E_A$, define

$$M(s) = \{m : s \text{ can be encoded to } m \text{ by some } e_t \in E_T\}.$$

Then using Corollary 1, we have $|M(s)| = \frac{|E_T|}{|E_T(m)|}$ is a constant. So

$$\frac{|M|}{|S|} = |M(s)| \text{ for all } s \in S. \tag{7}$$

3 Connection with Combinatorial Designs

In this section we study the combinatorial structure of Cartesian l-optimal A^3-code against collusion attacks. In particular we give a combinatorial structure of E_T, E_R, E_A and $E_R \circ E_A$.

First we recall some definitions.

Definition 1. *A block design is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a set of v points and $\mathcal{B}$ is a family of k-subsets (called blocks) of $\mathcal{V}$.*

Definition 2. *A block design $(\mathcal{V}, \mathcal{B})$ is called α-resolvable if the block set B is partitioned into classes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_n$ with the property that in each class, every point occurs in exactly α blocks.*

We will be interested in α-resolvable designs with the following property: There is an integer $l, 0 < l < n$, such that property **(P1)** below is satisfied.

(P1) Any collection of i blocks, from i different classes either intersect in μ_i points or do not intersect, $i\,(1 \leq i \leq l+1)$.

For each participant we define an incidence structure which defines the mapping given by the participant's keys. For receiver and arbiter, the incidence structure is given by a $0,1$ matrix, whose rows are labelled by the participant's keys and columns are labelled by M, and the element in row e and column m is 1 if $e(m) \in S$ and 0, otherwise. For transmitter, it is given by a matrix whose rows are labelled by transmitter's key, and its columns are labelled by S and the element in row e and column s is m if $e_t(s) = m$.

In the following subsections we will study the relationships between combinatorial designs and each participant's incidence structure.

3.1 E_R

Theorem 3. *In an l-optimal A^3-code against collusion attacks, design $(E_R, \{E_R(m) : m \in M\})$ is $\alpha(R)$-resolvable with property* **(P1)**. *It has the parameters:*

$\alpha(R) = \frac{|M|}{|S|} P_{A_0}$,

$\mu_i(R) = |E_R|(P_{O_0} P_{O_1} \cdots P_{O_{i-1}})(P_{R_0} P_{R_1} \cdots P_{R_{i-1}})^{-1},\ 1 \leq i \leq l+1.$

3.2 E_A

By 7 of Corollary 1 $|E_A(m)|$ is a constant. So $(E_A, \{E_A(m) : m \in M\})$ forms a block design.

Theorem 4. *In an l-optimal A^3-code against collusion attacks, design $(E_A, \{E_A(m) : m \in M\})$ is $\alpha(A)$-resolvable with property* **(P1)**. *It has the parameters:*

$\alpha(A) = \frac{|M|}{|S|} P_{R_0}$,

$\mu_i(A) = |E_A|(P_{O_0} P_{O_1} \cdots P_{O_{i-1}})(P_{A_0} P_{A_1} \cdots P_{A_{i-1}})^{-1},\ 1 \leq i \leq l+1.$

3.3 $E_R \circ E_A$

Note that in an optimal code $E_R \circ E_A$ corresponds to an α-resolvable design as well. It has the following properties:

(P2) For any collection of $l+1$ blocks $B_{j_1}, B_{j_2}, \cdots, B_{j_{l+1}}$ from different classes $\mathcal{C}_{j_1}, \mathcal{C}_{j_2}, \cdots, \mathcal{C}_{j_{l+1}}$, and any $u\,(\neq j_1, j_2, \cdots, j_{l+1})$, there exists a unique block $B_u \in \mathcal{C}_u$ such that

$$B_{j_1} \cap \cdots \cap B_{j_{l+1}} \cap B_u = B_{j_1} \cap \cdots \cap B_{j_{l+1}},$$

if $B_{j_1} \cap \cdots \cap B_{j_{l+1}} \neq \emptyset$. Furthermore, for any $B \in \mathcal{C}_u \backslash \{B_u\}$, $|B_{j_1} \cap \cdots \cap B_{j_{l+1}} \cap B| = 1$.

(P3) The point set $\mathcal{V}$ is partitioned into subsets $\mathcal{V}_1, \mathcal{V}_2, \cdots, \mathcal{V}_h$ such that for each subset $\mathcal{V}_i$, $(\mathcal{V}_i, \mathcal{B}_i')$ is an α-resolvable design with property **(P1)** and **(P2)**.

Here we use $\mathcal{B}_i'$ to denote $\{B_j \cap \mathcal{V}_i \neq \emptyset : B_j \in \mathcal{B}\}$.

¿From 1 of Corollary 1 we know $|E_{\overline{RA}}(m)|$ is a constant for all $m \in M$. Then $(E_R \circ E_A, \{E_{\overline{RA}}(m) : m \in M\})$ forms a block design. For this block design we have following theorem.

Theorem 5. *In an l-optimal A^3-code against collusion attacks, design $(E_R \circ E_A, \{E_{\overline{RA}}(m) : m \in M\})$ is α-resolvable with properties* **(P1)**, **(P2)** *and* **(P3)**. *It has the parameters:*

$\alpha = \frac{|M|}{|S|} P_{O_0}$,

$\mu_i = |E_R \circ E_A| \prod_{i=0}^{i-1} P_{O_i},\ 1 \leq i \leq l+1.$

3.4 E_T

In order to describe E_T, we recall some definitions to be used later.

Definition 3. *A* t-design *is a block design (V, B) so that any t-subset of V occurs in exactly λ blocks.*

Definition 4. *A* partially balanced t-design *is a block design (V, B), where every t-subset of V either occurs in exactly λ blocks or does not occur in any block.*

We denote this design by $t-(v, k; \{\lambda, 0\})$-design, where v is the total number of points and k is the size of a block.

Definition 5. *A $t-(v, k; \{\lambda, 0\})$-design (V, B) is a* strong partially balanced t-design *if it is a $i-(v, k; \{\lambda_i, 0\})$-design, for any $i, 1 < i < t$, and also a* 1*-design.*

Definition 6. *A $t-(v, k; \{\lambda, 0\})$-design (V, B) is a resolvable partially balanced t-design if the block set can be partitioned into classes $C_1, C_2, \cdots, C_{n'}$ with the property: For each $j (1 \leq j \leq n')$, (V, C_j) is a $t-(v', k; \{\lambda', 0\})$-design.*

Definition 7. *A strong partially balanced $t-(v, k; \{\lambda, 0\})$-design (V, B) is resolvable if it is resolvable with classes $C_1, C_2, \cdots, C_{n'}$ and property: For each $j (1 \leq j \leq n')$, (V, C_j) is a strong partially balanced $t-(v', k; \{\lambda', 0\})$-design.*

Now consider design (M, E_T).

Theorem 6. *In an l-optimal A^3-code against collusion attacks, design (M, E_T) is a $(l+1)-(|M|, |S|; \{\lambda, 0\})$-design which is strong and resolvable, it has parameters as follows:*

$\lambda = \lambda_{l+1} = 1$,
$\lambda_i = (P_{O_i} P_{O_{i+1}} \cdots P_{O_l})^{-1} (P_{\overline{RA_i}} P_{\overline{RA_{i+1}}} \cdots P_{\overline{RA_l}})^{-1},\ 1 \le i \le l$,
$\lambda_i^{'} = (P_{\overline{RA_i}} P_{\overline{RA_{i+1}}} \cdots P_{\overline{RA_l}})^{-1},\ 1 \le i \le l$.

It is known that in an optimal A-code, the transmitter and the receiver have a partially balanced t-design (see [5]), or an orthogonal array if the code is Cartesian (see [1]). In an optimal Cartesian A^2-code the transmitter has a partially balanced t-design, while the receiver has an α-resolvable design (see [6]). Our results in this section show that in an optimal Cartesian A^3-code against collusion attacks, the transmitter has a partially balanced t-design, while the receiver and the arbiter have α-resolvable designs each.

4 Optimal Code from Finite Geometry

In this section we show an example of 1-optimal A^3-code against collusion attacks.

Let $GF(q)$ be a field of q elements, $PG(n, q)$ be a n-dimensional projective space over $GF(q)$. Every point on $PG(n, q)$ has a homogeneous coordinate $(x_0, x_1, x_2, \cdots, x_n)$, here not all x_i are zero. Two homogeneous coordinates $(x_0, x_1, \cdots, x_n)$ and $(x_0^{'}, x_1^{'}, \cdots, x_n^{'})$ identify the same point if and only if there is a nonzero constant c such that $(x_0, x_1, \cdots, x_n) = c(x_0^{'}, x_1^{'}, \cdots, x_n^{'})$. A *$k$-flat* H_k $(0 \le k \le n)$ on $PG(n, q)$ is defined as a system of $n-k$ linear equations:

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \cdots + a_{1n}x_n = b_1, \\ a_{20}x_0 + a_{21}x_1 + \cdots + a_{2n}x_n = b_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n-k,0}x_0 + a_{n-k,1}x_1 + \cdots + a_{n-k,n}x_n = b_{n-k}, \end{cases}$$

where the rank of coefficient matrix (a_{ij}) is $n-k$. Thus a 0-flat is a point, a 1-flat is a line, a 2-flat is a plane, and so on.

Now consider $PG(4, q)$ to construct our code. Let each message correspond to a 3-flat in $PG(4, q)$. Fix a line L_S in $PG(4, q)$. Let the points on L_S be regarded as source states. Let the transmitter's encoding rule be a 2-flat e_t not intersecting L_S. Let the receiver's decoding rule and the arbiter's arbitration rule be points e_r and e_a, respectively. The pair (e_t, e_r, e_a) is valid if and only if e_r, e_a are on e_t. A source state s will be encoded to $m =< s, e_t >$ which is a 3-flat passing through s and e_t. The receiver accepts a message m if and only if e_r is in m, the arbiter arbitrates that m should be accepted by the receiver if and only if e_a is in m. This code is optimal with the parameters:

$$
\begin{aligned}
|S| &= q+1,\\
|M| &= q^4+q^3,\\
|E_T| &= q^6,\\
|E_R| &= q^4+q^3+q^2,\\
|E_A| &= q^4+q^3+q^2,
\end{aligned}
$$

5 Conclusion

In this paper we introduced a new model for A^3-codes, obtained information theoretic and combinatorial bounds on security and efficiency parameters of the codes, defined optimal codes and finally derived combinatorial structure of optimal Cartesian codes. Our study of the optimal A^3-codes is limited to Cartesian codes. Combinatorial structure of optimal A^3-codes in the general case is an open problem.

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,* volume 330, pages 51-55. Springer-Verlag, Berlin, Heidelberg, New York, 1988. 390, 397
2. Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attack. In *Advances in Cryptology-CRYPTO'90, Lecture Notes in Computer Science,* volume 537, pages 177-188. Springer-Verlag, Berlin, Heidelberg, New York, 1990. 390
3. T. Johansson. Further results on asymmetric authentication schemes. Information and Computation, 151, 1999. 390, 391, 393
4. S. Obana and K. Kurosawa. A^2-code=affine resolvable + BIBD. In *Proc. of ICICS, Lecture Notes in Computer Science, volume* 1334, pages 118-129. Springer-Verlag, Berlin, Heidelberg, New York, 1997. 390
5. D. Pei. Information-theoretic bounds for authentication codes and block designs. *Journal of Cryptology,* 8:177-188, 1995. 397
6. D. Pei, Y. Li, Y. Wang, and R. Safavi-Naini. Characterization of optimal authentication codes with arbitration. In *Proceeding of A CISP '99, Lecture Notes in Computer Science,* volume 1587, pages 303-313. Springer-Verlag, Berlin, Heidelberg, New York, 1999. 390, 397
7. G. J. Simmons. Authentication theory/coding theory. In *Advances in Cryptology-CRYPTO'84, Lecture Notes in Computer Science,* volume 196, pages 411-431. Springer-Verlag, Berlin, Heidelberg, New York, 1984. 390
8. G. J. Simmons. A cartesian construction for uncondetionally secure authentication codes that permit arbitration. *Journal of Cryptology,* 2:77-104, 1990. 390
9. R. Taylor. Near optimal unconditionally secure authentication. In *Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science,* volume 950, pages 244-253. Springer-Verlag, Berlin, Heidelberg, New York, 1994. 390
10. Y. Frankel Y. Desmedt and M. Yung. Multi-receiver/multi-sender network securety: efficient authenticated multicast/feedback. In *IEEE Infocom,* pages 2045-2054, 1992. 390