1991

Error-correcting codes for authentication and subliminal channels

Reihaneh Safavi-Naini

Jennifer Seberry
University of Wollongong, jennifer_seberry@uow.edu.au

Publication Details

Reihaneh Safavi-Naini and Jennifer Seberry, Error correcting codes for authentication and subliminal channels, IEEE Transactions on Information Theory, 37, (1991), 13-17.

Error-correcting codes for authentication and subliminal channels

Abstract
The application of coding theory to security scenarios is studied. Authentication systems are introduced that are based on algebraic codes and provide high protection against an intruder's impersonation and substitution attacks. It is shown that a subliminal channel can be embedded into these systems and that there is a trade-off between the authentication capability, subliminal capacity and error protection capability.

Disciplines
Physical Sciences and Mathematics

Publication Details
Reihaneh Safavi-Naini and Jennifer Seberry, Error correcting codes for authentication and subliminal channels, IEEE Transactions on Information Theory, 37, (1991), 13-17.

Error-Correcting Codes for Authentication and Subliminal Channels

Reihameh S. Safavi-Naini, *Member, IEEE*, and Jennifer R. Seberry, *Member, IEEE*

Abstract—**The application of coding theory to security scenarios is studied. Authentication systems are introduced that are based on algebraic codes and provide high protection against an intruder's impersonation and substitution attacks. It is shown that a subliminal channel can be embedded into these systems and that there is a trade-off between the authentication capability, subliminal capacity and error protection capability.**

Index Terms—**Authentication code, subliminal channel, McEliece cryptosystem, algebraic code, secrecy.**

I. Introduction

THE MAIN MOTIVATION for the study of coding theory has been the protection of discrete signals from noise. However, the results of these studies have proved beneficial in many other engineering and mathematical contexts. In this paper we look at some possible applications of algebraic codes to security. The most interesting feature of these applications is that they can easily lead to schemes in which the combination of security and protection is possible, and in some cases a trade-off between the two is noticeable. Although we do mention secrecy systems based on algebraic codes, the main aim of the paper is to introduce authentication schemes that are *hard to deceive* and can include subliminal channels. The price to be paid in this case is a reduction in true authentication capability of the communicants.

Section II is devoted to a review of some basic definitions and concepts of coding theory and authentication systems. A more complete treatment of these can be found in [1] and [2] respectively. In Section III, the application of coding theory to secrecy is examined, and in Section IV, authentication systems are introduced that are hard to deceive. In Section V it is shown that subliminal channels can be embedded in these systems and in Section VI some concluding remarks are presented.

II. Background

Let V_n denote the n-dimensional vector space over GF(2). The number of nonzero components of a vector $v = (v_1, v_2, \cdots, v_n)$ is the Hamming weight of v and is denoted by $w_h(v)$. A linear code C of length n, dimension k and minimum distance d is denoted by (n, k, d). The generator matrix G and the parity check matrix H of the code can always be written as

$$G = [I_k | A], \qquad H = [A^T | I_{n-k}],$$

where A is an arbitrary $k \times (n-k)$ binary matrix. A binary k-tuple i is encoded to c, where $c = iG$. A noise vector n added to a codeword c results in a vector $r = c + n$. If $w_h(n) \le t = \lfloor (d-1)/2 \rfloor$, c can be recovered by forming the syndrome vector $\text{syn}(r) = rH^T$, finding the corresponding coset leader e_r and decoding $c = r + e_r$.

We consider the authentication scenario proposed by Simmons [3]. Briefly, a transmitter wants to send the state of a source to a distant receiver over a publicly exposed channel. The enemy tries to fool the receiver into accepting a fraudulent message produced by him/her as a genuine one. Authentication amounts to determining whether or not a received message is in the subset of acceptable messages. An arbiter can always verify the authenticity of the transmitted message.

Authentication codes can achieve these requirements by coding a source state to a *cryptogram* that is easily decodable by the legitimate receiver. An authentication code is a set E of *encoding rules*. Each encoding rule A_i is a one-to-one mapping of the elements of the set of source states S onto the elements of some subset of the set of authentic messages M. The inverse mapping used by the receiver is A_i^{-1} where the index i is the secret key information that the transmitter and receiver share.

An authentication system can provide protection against deception by the enemy only if $|M| > |S|$. We call an authentication system *hard to deceive* if it is easy for the transmitter and receiver in possession of the key information to encode and decode, easy for the arbiter to check the authenticity of a transmitted message, but computationally infeasible for an enemy to succeed in a substitution attack.

III. Coding and Secrecy

Algebraic codes can be used to provide security. The symmetric cryptosystem in Section III-A uses automorphisms of a linear code to provide security.

A. Symmetric Cryptosystem

A linear (n, k, d) code C can be used as a block cipher algorithm. The ciphertext block c corresponding to a plaintext block i is obtained as $c = iG_l$ where G_l is a generator

Manuscript received February 27, 1989; revised May 21, 1990.

The authors are with the Department of Computer Science, University College, Australian Defence Force Academy, University of New South Wales, Australia ACT 2600.

IEEE Log Number 9040132.

matrix of the code. The possible generator matrices are labeled by l, which is the key. The number of possible keys for this system is

$$K = \prod_{i=0}^{k-1} (2^k - 2^i).$$

In this system, the set of cryptograms is always the same (the set of codewords of C), but the generator matrix used determines the actual one-to-one correspondence between the plaintext and the ciphertext. The expansion in the length of the message can be used for error protection purposes or employed as a manipulation detection property of the crypto-algorithm, both using the minimum distance between the cryptograms, which is d in this case.

However, the system *is not secure*, as access to k plaintext/ciphertext pairs enables the enemy to reconstruct the generator matrix.

B. Asymmetric Cryptosystems

One of the earliest and yet resistant public key cryptosystems is the system proposed by McEliece, which is based on the known difficulty of the general decoding problem [4, pp. 108–111].

IV. Codes and Authentication

We propose two authentication systems based on algebraic codes. The encoding rules in each system consist of the composition of two mappings performed in two stages. The first stage, which is common to both systems, serves to add the required redundancy by embedding the set of source states S (represented by the subset of non-zero elements of V_k) into a larger set, $V_{n_1}, n_1 > k$. The specific mapping used in this stage is only known to the communicants. The second stage is aimed mainly at obscuring the first stage transformation by mapping V_{n_1} onto $M \subset V_n$, $n > n_1$, where M is the set of authentic messages, to be defined in each case.

A mapping γ_i of the first stage is specified by a linear code C_i with generator matrix $G_i = [I_k | A]$, where A is an arbitrary $k \times (n_1 - k)$ binary matrix:

$$\gamma_i : \boldsymbol{s} \to \boldsymbol{x}, \qquad \boldsymbol{s} \in S, \qquad \boldsymbol{x} \in V_{n_1},$$

$$\boldsymbol{x} = \boldsymbol{s} G_i.$$

The set of all possible mappings of stage one is denoted by Γ, and $|\Gamma| = 2^{(n_1-k)\times k}$.

The set Δ of mappings of stage two is different for each system and will be defined separately later.

An encoding rule A_l consists of $\gamma_i \in \Gamma$ followed by $\delta_j \in \Delta$.

The elements of V_{n_1} can be partitioned into two subsets $V_{n_1}^1$ and $V_{n_1}^2$, where $V_{n_1}^1$ consists of those elements of V_{n_1} with at least one nonzero component in their first k coordinate places, and $V_{n_1}^2$ consists of those vectors that have these components all zero. Vectors of $V_{n_1}^2$ form a subspace, but the sum of two vectors of $V_{n_1}^1$ can result in a vector of $V_{n_1}^2$. It is noted that only $\boldsymbol{x} \in V_{n_1}^1$ (and not $\boldsymbol{x} \in V_{n_1}^2$) can be in the image of $\gamma \in \Gamma$.

Lemma 4.1: Every nonzero element of $V_{n_1}^1$ is in the image of exactly $2^{(n_1-k)(k-1)}$ mappings $\gamma_i \in \Gamma$.

Proof: See Appendix A. □

We propose two possible choices of Δ with the corresponding Ms by employing the cryptosystems discussed in the previous section. It will be shown that the asymmetric system is hard to deceive.

A. Symmetric Authentication System

In the symmetric system proposed, M is the set of nonzero elements of an (n, n_1, d) code C and δ_j is defined by a generator matrix J_j of C:

$$\delta_j : \boldsymbol{x} \to \boldsymbol{m}, \qquad \boldsymbol{x} \in V_{n_1}, \qquad \boldsymbol{m} \in M,$$

$$\boldsymbol{m} = \boldsymbol{x} J_j.$$

The code is publicly known but the specific generator matrix used is the secret key information shared by the transmitter and receiver.

As noted earlier the number of possible j is

$$|\Delta| = \prod_{i=0}^{n_1-1} (2^{n_1} - 2^i).$$

Altogether, the number of possible (γ_i, δ_j) pairs is $|\Gamma| \times |\Delta|$, but the number of distinct encoding rules is

$$\prod_{i=0}^{k-1} (2^{n_1} - 2^i).$$

Example 4.1: Let $k = 2$, $n_1 = 4$, $n = 5$. Γ consists of $(4, 2, d_i)$ codes C_i where

$$G_i = [I_2 | G_i^*], \qquad G_i^* = \begin{bmatrix} \alpha_0 & \alpha_1 \\ \alpha_2 & \alpha_3 \end{bmatrix}.$$

G_i^* is an arbitrary 2×2 matrix with index $i = \sum_{j=0}^{3} \alpha_j \times 2^j$. M is the set of codewords of C, a four-dimensional subspace of V_5:

$$C = \{00000, 10001, 01001, 00101, 00011, 11000, 10100, 10010,$$
$$01100, 01010, 00110, 11101, 10111, 11011, 01111, 11110\}.$$

A mapping $\delta_j \in \Delta$ is given by a generator matrix J_j of the code C. The number of such matrices is

$$\prod_{i=0}^{3} (2^4 - 2^i) = 20160.$$

As an example let the encoding rule be specified by the generator matrices G_5 of the first stage and J of the second stage, where

$$G_5 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \qquad J = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Composition of the mappings of the two stages results in a matrix T

$$T = G_5 J = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

such that

$$\boldsymbol{m} = \boldsymbol{s} T,$$

e.g., the source state $s=[1\ 0]$ results in the cryptogram $m=[1\ 0\ 1\ 0\ 0]$.

Let $P_A(\cdot)$ denote probability distribution on the set A. The following theorem ensures the security of the system in an impersonation attack.

Theorem 4.1: If $P_S(\cdot)$, $P_\Gamma(\cdot)$ and $P_\Delta(\cdot)$ are uniform, then $P_M(\cdot)$ is uniform.

Proof: See Appendix A. □

In an impersonation attack, since the enemy has not yet intercepted any cryptogram, he/she does not have a better strategy than random selection with uniform distribution from M, and in this case his/her probability of success is

$$\frac{2^k-1}{2^{n_1}-1}.$$

Suppose the enemy intercepts a cryptogram m and he/she would like to substitute it with m' such that his/her probability of success is maximized. This corresponds to finding the subset $L_m \subset M$ such that $P(m'|m)$ is maximum for $m' \in L_m$, where $P(m'|m)$ is the probability of m' being a valid cryptogram when m is the intercepted cryptogram. But,

$$P(m'|m)=\frac{P(m'm)}{P(m)}=\frac{1}{P(m)}\times\sum_{x'x}P_\Delta(m'm|x'x)P(x'x),$$

where $P_\Delta(m'm|x'x)$ is the total probability of the mappings δ such that

$$\delta: x' \to m', \qquad \delta: x \to m.$$

This probability is

$$\frac{1}{(2^{n_1}-1)(2^{n_1}-2)}$$

and hence

$$P(m'|m)=\frac{P_\Delta(m'm|x'x)}{P(m)}\times\sum_{x'x}P(x'x)=\frac{1}{2^{n_1}-2},$$

which clearly shows that the interception of a cryptogram does not help the enemy in devising a strategy better than random selection with uniform distribution, and his/her probability of success in this case is

$$\frac{2^k-2}{2^{n_1}-2}.$$

However, the interception of the second cryptogram raises the probability of success of the enemy to one! This is because of the linearity of the system, which ensures $b=m+m'$ is a valid cryptogram under the authentication key used for m and m'.

B. Asymmetric Authentication

As was noted earlier the symmetric system is not hard to deceive. The following system overcomes this difficulty by employing the asymmetric cryptosystem mentioned in Section III-A.

Let C be a linear (n,k,d) code with an easy decoding algorithm corresponding to the generator matrix G and parity check matrix H (e.g., Goppa code). The structure of G is scrambled to $G'=SGP$ where P is a permutation matrix and S is a nonsingular $k\times k$ binary matrix. Matrix G' is made public. The set of authentic messages M is

$$M=\bigcup_{c\in C}S_n^t(c),$$

$$S_n^t(c)=\{m\in V_n \mid 0\le w_h(m+c)\le t,\ c\in C\},$$

$$|S_n^t(c)|=\sigma_n^t=\sum_{i=0}^{t}\binom{n}{i}.$$

An encoding rule A_i consists of a linear map $\gamma_i\in\Gamma$ followed by a probabilistic mapping δ defined as

$$\delta: x\to m, \qquad x\in V_{n_1}^1, \qquad m\in M,$$

$$m=xG'+n,$$

where n is selected randomly with uniform distribution from the set $S_n^t(\mathbf{0})$ (of size σ_n^t). The image of $V_{n_1}^1$ under δ is $Y\subset M$. Let Y_x denote the set of possible images of $x\in V_{n_1}^1$ ($Y=S_n^t(c_x)$ where $c_x=xG'$); then for $x,x'\in V_{n_1}^1$ we have

$$Y=\bigcup_{x\in V_{n_1}^1}Y_x, \qquad Y_x\cap Y_{x'}=\varnothing, \qquad x\ne x'.$$

Lemma 4.2: The probability distribution over Y is uniform.

Proof: Follows from uniform distribution over $V_{n_1}^1$ and $S_n^t(\mathbf{0})$. □

The system satisfies the requirements of a *hard to deceive* authentication system as follows.

- Encoding is easy. The cryptogram corresponding to s under a key i is m where
$$x=sG_i, \qquad m=(xG')+n.$$
- The receiver can easily decode the message because he/she knows S and P and hence
$$mP^{-1}=(xSGP)P^{-1}+nP^{-1}=(xS)G+n'.$$
P is a permutation matrix, so P^{-1} is also a permutation matrix, and thus:
$$w_h(n')=w_h(n)\le t.$$
Now (xS) can be recovered using the easy decoding algorithm, and, as S is nonsingular, x can be found and its corresponding s is the first k components of x as C_i is systematic.
- It is easy for the arbiter to check the authenticity of a received message as he/she also knows P and S matrices and is able to use the easy decoding algorithm to remove the noise. His/her successful decoding proves the authenticity of the cryptogram.
- Impersonation and substitution are hard because, from Lemma 4.2, the best strategy for impersonation is random selection with uniform distribution from Y of size $\sigma_n^t(2^{n_1}-2^{n_1-k})$. Interception of a cryptogram m will affect the optimum strategy by reducing the size of the set of possible cryptograms by at most σ_n^t. Cryptograms that are close to m will be accepted by the receiver with a high probability but they are not good choices as they are decoded to the same s.

Asymmetric authentication systems provide security even if a second cryptogram m' is intercepted. The enemy could

succeed in his/her deception if he/she could decode $\boldsymbol{m}$ and $\boldsymbol{m}'$ to obtain $\boldsymbol{x}, \boldsymbol{x}' \in V_{n_1}^1$ and form $\boldsymbol{b} = (\boldsymbol{x} + \boldsymbol{x}')G' + \boldsymbol{n}$, the bogus message that is accepted by the receiver. However, this is not computationally feasible because of the difficulty of the decoding problem.

V. Subliminal Channels

Subliminal channels are introduced by Simmons. He showed it is possible for two parties to communicate over an authentication-without-secrecy channel and exchange information unreadable by the authenticator. The channel through which this information transfer takes place is called the *subliminal channel*. It is pointed out in [5] that in order to communicate H_m bits of information with H_r bits of authentication, $H_r + H_m$ bits in total must be exchanged. In fact the transmitter/receiver can give up some of their authentication capability without the host being aware of it, and use the extra capacity H_s bits to communicate secretly.

We propose two possible modifications of the first stage of the authentication schemes proposed in the previous section to include a subliminal channel in the system. In both cases the second stage remains untouched.

A. Noise Addition

The redundancy added in the first stage can be exploited to establish a subliminal channel between the communicants. The capacity of the channel is equal to the number of redundant bits added.

Suppose the transmitter wants to send s to the receiver using a key i. He/she can include one subliminal bit in his/her message by adding a noise bit to one of the $(n_1 - k)$ last bits of $\boldsymbol{x} = \boldsymbol{s}G_i$ to obtain $\boldsymbol{x}'$. The receiver recovers $\boldsymbol{x}'$ after decoding of the second stage and hence determines s as the first k components of $\boldsymbol{x}'$. Moreover he/she can find any error in the last $(n_1 - k)$ bits, simply by calculating $\boldsymbol{x}^r = \boldsymbol{s}G_i$ and $\boldsymbol{x}' + \boldsymbol{x}^r$. Hence the capacity of the subliminal channel is $\log_2(n_1 - k + 1)$.

In general, the previous procedure allows the communicants to establish a subliminal channel of capacity $(n_1 - k)$ because any error vector $\boldsymbol{e} \in V_{n_1}$ of weight $w_h(\boldsymbol{e}) \le n_1 - k$ whose nonzero components are in the last $n_1 - k$ positions can be determined. Since the code of the first stage is only known to the transmitter and receiver, the information represented by the noise pattern remains exclusive to them.

B. Partitioning of Γ

Another way of embedding a subliminal channel in the system is by partitioning the set Γ into $p = 2^{k(n_1-k)-1}$ subsets E_i such that

$$\Gamma = \bigcup_{i=1}^{p} E_i,$$

$$E_i = \{\gamma_i^0, \gamma_i^1\}, \qquad C_i^0 \cap C_i^1 = \varnothing, \qquad 1 \le i \le p,$$

where $C_i^j \subset V_{n_1}$, $j = 0, 1$ are the sets of nonzero elements of the images of γ_i^j, $j = 0, 1$. This partitioning is only known to the transmitter and receiver. A given key determines the subset E_i to be used for the first stage and the actual code used by the transmitter in E_i for encoding s is determined by the subliminal bit accompanying s, i.e., a subliminal j, $j = 0, 1$, is sent by employing γ_i^j in stage one.

As the receiver has the key, he/she can decode the second stage and obtain $\boldsymbol{x} \in V_{n_1}^1$. Because the codes of the first stage are systematic, the first k bits of $\boldsymbol{x}$ actually determine the s, and it is easy for the receiver to check which generator matrix in E_i is used, hence obtaining the subliminal bit.

Partitioning of the set of codes of Γ is equivalent to reducing the effective size of the key space by a factor of two, hence losing one bit uncertainty about the authentication key. This bit is the capacity of the subliminal channel established between the communicants.

The capacity of the subliminal channel can be increased by using partitions which include subsets E_i of cardinality more than two, resulting in one bit extra subliminal capacity by doubling the size of the subsets E_i.

The communicants can exploit both channels simultaneously. While the first one can be considered as a free channel (as the extra bits are added in the first stage of encoding of the source states), the second one is paid off by the reduction in the effective size of the set of encoding rules, i.e., reduction in authentication capability of the communicants.

Example 5.1: In the Table I of Appendix B we give a partition of the set of codes of Example 4.1 where C_i^j, $j = 0, 1$ and $1 \le i \le 8$ are given in the last two columns of the table. The codes in the first column can be used to send a subliminal zero while the second column is used for sending a subliminal one.

VI. Conclusion

The application of algebraic codes to security can result in cryptographically resistant systems that combine security and error protection. We have used secure systems based on algebraic codes to design the so-called *hard to deceive* authentication codes that can include subliminal channels. The two types of subliminal channels discussed are different by nature and hence can be established simultaneously in a system.

While the first channel is always present in the system, the prerequisite for establishing the second one is the existence of certain types of partitioning of the set of encoding rules. Although an example is provided, the question of what systematic procedure should be used to obtain one, remains unanswered.

Both symmetric and asymmetric authentication codes can also cater for controlling errors by requiring that the codes of the first stage have certain minimum distance or using error correcting capability of the code of the second stage.

The trade-off between authentication capability, subliminal capacity and error control properties of the system, is clearly seen as the minimum distance of the code is the crucial parameter in all these cases.

Acknowledgment

The authors would like to thank Don Coppersmith for his helpful comments and suggestions.

Appendix A

Proof of Lemma 4.1: Let $\boldsymbol{x} \in V_{n_1}^1$ and $\boldsymbol{x} = (x_1, x_2, \cdots, x_k, \cdots, x_{n_1})$ where not all x_i, $1 \le i \le k$ are zero. As γ_i corre-

sponds to a systematic code, $s_x=(x_1,x_2,\cdots,x_k)$ is the unique source state that can be mapped onto x. This requires the row vectors g_i, $1\le i\le k$ of G_i satisfy the following equation:

$$\sum_{i=1}^{k} x_i g_i = x. \tag{1}$$

So $(k-1)$ row vectors of G_i can be chosen arbitrarily and the last row vector g_p with $x_p\neq 0$, is uniquely obtained from (1). The result follows from counting the number of possible G_is.

From these assumptions we have

$$P_{V_{n_1}}(d)=0, \qquad d\in V_{n_1}^2,$$

because none of the $\gamma_i\in\Gamma$ maps an $s\in S$ onto an element of $V_{n_1}^2$. However $P_{V_{n_1}^1}(x)$ is uniform and

$$P_{V_{n_1}^1}(x)=\sum_{s_i\in S} P_S(s_i)P_\Gamma(x|s_i), \qquad x\in V_{n_1}^1,$$

where $P_\Gamma(x|s_i)$ is the total probability of mappings $\gamma_j\in\Gamma$ that map s_i onto x. As γ_j corresponds to a systematic code, there is a unique s_x that can be mapped onto a given x. Hence

$$P_{V_{n_1}^1}(x)=\frac{N_\Gamma(s_x;x)}{|\Gamma|}\times(2^k-1)^{-1}$$

where $N_\Gamma(s_x;x)$ is given by

$$N_\Gamma(s_x;x)=\left|\{\gamma\in\Gamma|\gamma: s_x\to x\}\right|,$$

and from Lemma 4.1 we have

$$P_{V_{n_1}^1}(x)=(2^{n_1}-2^{n_1-k})^{-1}.$$

The uniform distribution of $V_{n_1}^1$ induces a uniform distribution on M as

$$P_M(m)=\sum_{x\in V_{n_1}^1} P_{V_{n_1}^1}(x)P_\Delta(m|x)$$

$$=(2^{n_1}-2^{n_1-k})^{-1}\times\sum_{x\in V_{n_1}^1}\frac{N_\Delta(x;m)}{|\Delta|}$$

where $P_\Delta(m|x)$ is the total probability of obtaining a cryptogram $m\in Y$ when $x\in V_{n_1}^1$ is obtained after the first stage, $|\Delta|=\prod_{i=0}^{n_1-1}(2^{n_1}-2^i)$ and $N_\Delta(x;m)$ is the number of mappings of Δ that map x onto m. But $N_\Delta(x;m)=\prod_{i=1}^{n_1-1}(2^{n_1}-2^i)$ is independent of x. Hence

$$P_M(m)=(2^{n_1}-1)^{-1}. \qquad \square$$

Appendix B

TABLE I
A Partition of the Set of Codes of Example 4.1

$E_1=\{C_0,C_{14}\}$	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\1&1&0&0\end{bmatrix}$	$\begin{bmatrix}1&0&0&1\\0&1&1&1\\1&1&1&0\end{bmatrix}$
$E_2=\{C_1,C_{15}\}$	$\begin{bmatrix}1&0&1&0\\0&1&0&0\\1&1&1&0\end{bmatrix}$	$\begin{bmatrix}1&0&1&1\\0&1&1&1\\1&1&0&0\end{bmatrix}$
$E_3=\{C_2,C_{12}\}$	$\begin{bmatrix}1&0&0&1\\0&1&0&0\\1&1&0&1\end{bmatrix}$	$\begin{bmatrix}1&0&0&0\\0&1&1&1\\1&1&1&1\end{bmatrix}$
$E_4=\{C_3,C_{13}\}$	$\begin{bmatrix}1&0&1&1\\0&1&0&0\\1&1&1&1\end{bmatrix}$	$\begin{bmatrix}1&0&1&0\\0&1&1&1\\1&1&0&1\end{bmatrix}$
$E_5=\{C_4,C_{10}\}$	$\begin{bmatrix}1&0&0&0\\0&1&1&0\\1&1&1&0\end{bmatrix}$	$\begin{bmatrix}1&0&0&1\\0&1&0&1\\1&1&0&0\end{bmatrix}$
$E_6=\{C_5,C_{11}\}$	$\begin{bmatrix}1&0&1&0\\0&1&1&0\\1&1&0&0\end{bmatrix}$	$\begin{bmatrix}1&0&1&1\\0&1&0&1\\1&1&1&0\end{bmatrix}$
$E_7=\{C_6,C_8\}$	$\begin{bmatrix}1&0&0&1\\0&1&1&0\\1&1&1&1\end{bmatrix}$	$\begin{bmatrix}1&0&0&0\\0&1&0&1\\1&1&0&1\end{bmatrix}$
$E_8=\{C_7,C_9\}$	$\begin{bmatrix}1&0&1&1\\0&1&1&0\\1&1&0&1\end{bmatrix}$	$\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&1&1&1\end{bmatrix}$

References

[1] J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland Publishing Company, 1978.

[2] G. J. Simmons, "Message authentication without secrecy," in *A.A.A.S. Selected Symposia Series*, pp. 105–139, 1982.

[3] ____, "A game theory model of digital message authentication," in *Congressus Numerantium*, vol. 34, pp. 413–424, 1982.

[4] J. Seberry and J. Piepryzk, *Cryptography, An Introduction to Computer Security*. Englewood Cliffs, NJ: Prentice Hall, 1989.

[5] G. J. Simmons, "The prisoner's problem and subliminal channel," in *Proc. CRYPTO '83*, 1983; and in *Advances in Cryptology. Proceedings of CRYPTO '83*. New York: Plenum Press, 1984, pp. 51–67.