Combinatorial characterizations of authentication codes

D. R. Stinson
Computer Science and Engineering
University of Nebraska
Lincoln, NE 68588-0115
stinson@bibd.unl.edu

Abstract

In this paper, we prove two new combinatorial characterizations of authentication codes. Authentication codes without secrecy are characterized in terms of orthogonal arrays; and general authentication codes are characterized in terms of balanced incomplete block designs.

1 Introduction

In this paper, we prove some new characterizations of authentication codes. By a characterization theorem, we mean a theorem of the form "an authentication code with certain properties exists if and only if a certain combinatorial structure exists". Typically, the properties of the authentication code that are considered are natural, desirable properties such as having the minimum possible deception probabilities and the minimum number of encoding rules.

In the past, bounds have been proved on these quantities, and constructions have been given for classes of authentication codes that meet such bounds with equality. Many of these constructions have used combinatorial designs. The characterizations in this paper show that, in certain cases, the known constructions are essentially the "only way" to obtain codes with the specified properties. Of course, a characterization of this type has intrinsic interest. However, a characterization also proves that it is impossible to find "different" constructions from those already known.

In this paper, we prove two new characterizations of this type. The first result (Theorem 3.1) concerns authentication codes without secrecy, i.e. codes where an observed message can correspond to only one possible source state. Such a code is equivalent to one where a message consists of a source state concatenated with an authenticator. A code where the deception probabilities and the number of encoding rules meet the lower bounds with equality is equivalent to a combinatorial design called an orthogonal array. This characterization has been previously proved in the case where the number of possible

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 62-73, 1992.

source states is at most 1 + the number of possible of authenticators. Here, we extend the characterization so that this assumption is no longer needed. The proof uses an elegant linear-algebraic technique which has not previously been used in authentication theory.

Our second characterization concerns "general" authentication codes. Again, we consider those codes where the deception probabilities and the number of encoding rules are the minimum possible. It has been previously shown that such a code can exist only if a certain balanced incomplete block design (BIBD) exists. Conversely, it has been previously shown that one can use the BIBD to construct the desired code *if the source states are known to be equiprobable.* In this paper, we complete the characterization by showing that the assumption of equiprobable sources is necessary. Our result is stated as Theorem 4.1.

Finally, the second characterization can be extended to include codes that, in addition, provide perfect secrecy. An extra numerical condition is necessary and sufficient to provide secrecy (see Theorem 4.2).

The paper is organized as follows. Section 2 gives necessary background from the theory of authentication codes. In Section 3, we prove our characterization for authentication codes without secrecy. In Section 4, we prove the characterization of general authentication codes.

2 Basic results on authentication codes

The general theory of of unconditional authentication has been developed by Simmons (see e.g. [Si1] and [Si2]), and has been extensively studied in recent years. In this section, we will give a brief review of some relevant known results concerning authentication without secrecy.

In the usual model for authentication, there are three participants: a *transmitter*, a *receiver*, and an *opponent*. The transmitter wants to communicate some information to the receiver using a public commmunications channel. The *source state* (or plaintext) is encrypted to obtain the *message* (ciphertext), which is sent through the channel. An *encoding rule* (or key) e defines the message $e(s)$ to be sent to communicate any source state s. Each encoding rule will be a one-to-one function from the source space to the message space. We assume the transmitter has a key source from which he obtains a key. Prior to any messages being sent, this key is communicated to the receiver by means of a secure channel.

We will use the following notation. Let $\mathcal{S}$ be a set of k source states; let $\mathcal{M}$ be a set of v messages; and let $\mathcal{E}$ be a set of b encoding rules. Since each encoding rule is a one-to-one function from $\mathcal{S}$ to $\mathcal{M}$, we can represent a code by a $b \times k$ matrix, where the rows are indexed by encoding rules, the columns are indexed by source states, and the entry in row e and column s is $e(s)$. We call this matrix the *encoding matrix*. For any encoding rule $e \in \mathcal{E}$, define $M(e) = \{e(s) : s \in \mathcal{S}\}$, i.e. the set of valid messages under encoding rule e. For an encoding rule e, and a message $m \in M(e)$, define $e^{-1}(m) = s$ if $e(s) = m$.

Suppose the opponent has the ability to introduce messages into the channel and/or to modify existing messages. When the opponent places a (new) message m' into the channel, this is called *impersonation*. When the opponent sees a message m and changes it to a message $m' \neq m$, this is called *substitution*. In either case, his goal is to have m' accepted as authentic by the receiver. That is, if e is the encoding rule being used (which is *not* known to the opponent), then the opponent is hoping that $m' = e(s)$ for some source state s.

We assume that there is some probability distribution on $\mathcal{S}$, which is known to all the participants. Given the probability distribution on the source states, the receiver and transmitter will choose a probability distribution for $\mathcal{E}$, called an *encoding strategy*. Once the transmitter/receiver have chosen the encoding strategy, it is possible to determine, for $i = 0, 1$, a probability denoted P_{d_i}, which is the probability that the opponent can deceive the transmitter/receiver by impersonation and substitution, respectively.

P_{d_0} is calculated as follows. The opponent can compute, for each message m, a quantity $payoff(m)$ which denotes the probability that m will be accepted as authentic by the transmitter/reciever. It is easy to see that

$$payoff(m) = \sum_{\{e \in \mathcal{E} : m \in M(e)\}} p(E = e).$$

Then it follows that

$$\sum_{\{m \in \mathcal{M}\}} payoff(m) = k.$$

Hence, there exists a particular message $m_0 \in \mathcal{M}$ such that $payoff(m_0) \geq k/v$. Further, $P_{d_0} = k/v$ if and only if $payoff(m) = k/v$ for every message m. We summarize this as follows.

Theorem 2.1 *[Si1] $P_{d_0} \geq k/v$. Further, $P_{d_0} = k/v$ if and only if*

$$\sum_{\{e \in \mathcal{E} : m \in M(e)\}} p(E = e) = \frac{k}{v}$$

for every message m.

Now, let's turn our attention to the computation of P_{d_1}. The situation is quite different depending on whether we have an authentication code without secrecy as opposed to a general authentication code. Let's first consider authentication codes without secrecy. This means that $e(s) = e'(s')$ only if $s = s'$; i.e. the message uniquely determines the source state, irrespective of the encoding rule being used. Hence, we can partition the set of messages $\mathcal{M}$ into k subsets $\mathcal{M}_s$, $s \in \mathcal{S}$, such that $\mathcal{M}_s = \{e(s) : e \in \mathcal{E}\}$.

Suppose $P_{d_0} = k/v$. For codes providing authentication without secrecy, this can happen only if $|\mathcal{M}_s| = v/k$ for every source state s. In this situation, we can define a set $\mathcal{A}$ of $\ell = v/k$ *authenticators* and a mapping $\phi : \mathcal{M} \rightarrow \mathcal{A}$ such that, for every $s \in \mathcal{S}$, $\{\phi(m) : m \in \mathcal{M}_s\} = \mathcal{A}$. We can then obtain an isomorphic code by defining for every encoding rule e an *authentication rule* e^ϕ defined by $e^\phi(s) = \phi(e(s))$ for every source state s. In this new code, every message consists of a source state concatenated with an authenticator from $\mathcal{A}$, i.e. source state s is mapped to $(s, e^\phi(s))$, where e^ϕ is an authentication rule. In terms of $\ell = |\mathcal{A}|$, we have $P_{d_0} = 1/\ell$.

We will henceforth assume that every message consists of a source state with a concatenated authenticator, since there is no loss of generality in doing so. Also, we will think of $\mathcal{E}$ as being a collection of authentication rules, and we will speak of an *authentication matrix* rather than an encoding matrix.

Suppose the opponent sees the message $m = (s, a)$ in the channel. He can substitute this message with any message $m' = (s', a')$, where $s' \neq s$. Denote by $payoff(m, m')$ the probability that the message m' will be accepted as authentic, given that m is observed in the channel. Denote by e_0 the authentication rule being used by the transmitter/receiver (again, we emphasize that e_0 is unknown to the opponent). Then we have the following:

$$payoff(m, m') = \frac{\sum_{\{e : e(s)=a, e(s')=a'\}} p(E = e)}{\sum_{\{e : e(s)=a\}} p(E = e)}.$$

Now, it follows that

$$\sum_{a' \in \mathbf{A}} payoff(m, (s', a')) = 1$$

for any $s' \neq s$. Hence, for every s', there exists an authenticator $a' = f(m, s')$ such that $payoff(m, m') \geq 1/\ell$, and it follows that $P_{d_1} \geq 1/\ell$.

Suppose that $P_{d_0} = 1/\ell$. Then, from Theorem 2.1, we have

$$\sum_{\{e : e(s)=a, e(s')=a'\}} p(E = e) = \frac{1}{\ell}.$$

Hence, we obtain the following theorem.

Theorem 2.2 *[St2] Suppose we have an authentication code without secrecy in which* $P_{d_0} = k/v = 1/\ell$. *Then* $P_{d_1} \geq 1/\ell$. *Further,* $P_{d_1} = 1/\ell$ *if and only if*

$$\sum_{\{e:e(s)=a,e(s')=a'\}} p(E=e) = \frac{1}{\ell^2}$$

for every s, s', a, a', $s \neq s'$.

The above considerations also lead to a lower bound on the number of authentication rules and a characterization as to when equality can occur. We give this characterization in terms of orthogonal arrays, which we now define. An *orthogonal array* $OA(n, k, \lambda)$ is a $\lambda n^2 \times k$ array of n symbols, such that in any two columns of the array every one of the possible n^2 pairs of symbols occurs in exactly λ rows. If $\lambda = 1$, then we write $OA(n, k)$. Orthogonal arrays are well-studied structures in combinatorial design theory, and are equivalent to other structures such as transversal designs, mutually orthogonal Latin squares and nets.

Theorem 2.3 *[St2] Suppose we have an authentication code without secrecy in which* $P_{d_0} = P_{d_1} = k/v = 1/\ell$. *Then* $b \geq \ell^2$, *and equality occurs if and only if the authentication matrix is an orthogonal array* $OA(\ell, k)$ *and the authentication rules are used with equal probability.*

Proof: Suppose $P_{d_0} = P_{d_1} = k/v = 1/\ell$. Let $s \neq s'$. Then, for every a, a', $|\{e : e(s) = a, e(s') = a'\}| \geq 1$. Hence, $b \geq \ell^2$.

In order that $b = \ell^2$, it must be the case that $|\{e : e(s) = a, e(s') = a'\}| = 1$ for every s, s', a, a', where $s \neq s'$; and $p(E = e) = 1/\ell^2$ for every $e \in \mathcal{E}$. The authentication matrix is clearly an orthogonal array $OA(\ell, k)$.

Conversely, suppose we start with an orthogonal array $OA(\ell, k)$. Use each row as an authentication rule with equal probability $1/\ell^2$. Then we obtain a code with the stated properties. □

The above theorem provides a nice characterization, as far as it goes. However, existence of an $OA(\ell, k)$ requires that $k \leq \ell + 1$. The two parameters k and ℓ are independent parameters, so it is also of interest to characterize authentication codes in

the situation $k > \ell + 1$; i.e. when $v < k^2 - k$. We shall do this in Section 3. The characterization involves orthogonal arrays with $\lambda > 1$.

Let's turn to general authentication codes. Now, the set $\mathcal{E}$ is a set of encoding rules. As before, we compute a quantity $payoff(m, m')$ which is the property that the receiver will be deceived by a substitution of m by m'. We have

$$payoff(m, m') = \frac{\sum_{\{e: m, m' \in M(e)\}} p(E = e)p(S = e^{-1}(m))}{\sum_{\{e: m \in M(e)\}} p(E = e)p(S = e^{-1}(m))}.$$

Fix a message m. Then we can compute $\sum_{m' \neq m} payoff(m, m') = k - 1$. Hence, there exists a message $m' = f(m)$ such that

$$payoff(m, m') \geq \frac{k-1}{v-1},$$

and it follows that $P_{d_1} \geq (k-1)/(v-1)$.

Theorem 2.4 *[Ma], [St1] In any authentication code, $P_{d_1} \geq (k-1)/(v-1)$. Further, $P_{d_1} = (k-1)/(v-1)$ if and only if*

$$\frac{\sum_{\{e: m, m' \in M(e)\}} p(E = e)p(S = e^{-1}(m))}{\sum_{\{e: m \in M(e)\}} p(E = e)p(S = e^{-1}(m))} = \frac{k-1}{v-1}$$

for all $m, m', m \neq m'$.

If we have a code in which $P_{d_0} = k/v$ and $P_{d_1} = (k-1)/(v-1)$, then we can obtain an immediate lower bound on the number of encoding rules and a partial characterization. We need the concept of a *balanced incomplete block design*, or BIBD. A (v, k, λ)–BIBD is a pair $(X, \mathcal{A})$, where $|X| = v$ is a set of elements called *points* and $\mathcal{A}$ is a family of k–subsets of X (called *blocks*) such that every pair of points occurs in exactly λ blocks. It is not difficult to see that every point occurs in precisely $r = \lambda(v-1)/(k-1)$ blocks and that the total number of blocks is $b = \lambda v(v-1)/(k(k-1))$.

Theorem 2.5 *[Ma], [St2] Suppose we have an authentication code in which $P_{d_0} = k/v$ and $P_{d_1} = (k-1)/(v-1)$. Then $b \geq (v^2 - v)/(k^2 - k)$, and equality can occur only if the rows of the encoding matrix, taken as unordered sets, form a $(v, k, 1)$–BIBD.*

Proof: For every two distinct messages, m, m', $|\{e : m, m' \in M(e)\}| \geq 1$. Hence, $b \geq (v^2 - v)/(k^2 - k)$. If $b = (v^2 - v)/(k^2 - k)$, then $|\{e : m, m' \in M(e)\}| = 1$ for every m, m'. □

The following partial converse was shown in [St2].

Theorem 2.6 *[St1] Suppose there is a $(v,k,1)$–BIBD. Then there exists an authentication code for k equiprobable sources in which $P_{d_0} = k/v$, $P_{d_1} = (k-1)/(v-1)$ and $b = (v^2-v)/(k^2-k)$.*

Proof: For every block $A \in \mathcal{A}$, arbitrarily define an encoding rule e_A such that $\{e_A(s) : s \in \mathcal{S}\} = A$. Use every encoding rule with equal probability $1/b$. □

In Section 4, we complete the characterization by showing that existence of an authentication code with $P_{d_0} = k/v$, $P_{d_1} = (k-1)/(v-1)$ and $b = (v^2-v)/(k^2-k)$ *requires* that the source states and encoding rules be equiprobable.

3 Authentication without secrecy

Suppose there is an authentication code (without secrecy) for k source states, having b authentication rules and ℓ authenticators, such that $P_{d_0} = P_{d_1} = 1/\ell$. Denote $\mathcal{M} = \mathcal{S} \times \mathcal{A}$; $\mathcal{M}$ is the set of messages. For an authentication rule $e \in \mathcal{E}$, $M(e) = \{(s, e(s)) : s \in \mathcal{S}\}$ is the set of messages arising from authentication rule e.

Define a $k\ell$–dimensional real vector space V having as its basis $\mathbf{B} = \{\overline{m} : m \in \mathcal{M}\}$. For every authentication rule $e \in \mathcal{E}$, define a vector $\overline{e} = \sum_{s \in \mathcal{S}} \overline{(s, e(s))}$. For every $s \in \mathcal{S}$, define $\overline{v_s} = \sum_{a \in \mathcal{A}} \overline{(s,a)}$. Next, define $\overline{X} = \sum_{m \in \mathcal{M}} \overline{m} = \sum_{s \in \mathcal{S}} \overline{v_s}$. Finally, for every $m = (s,a) \in \mathcal{M}$, define $\overline{v_m} = \ell \sum_{e \in \mathcal{E}, e(s)=a} p(E=e)\overline{e}$.

Using Theorems 2.1 and 2.2, it is not difficult to see that

$$\overline{v_m} = \overline{m} + \frac{1}{\ell}(\overline{X} - \overline{v_s}). \tag{1}$$

Now fix a source state $s_j \in \mathcal{S}$. Define $V' = \langle \mathbf{B}' \rangle$, where

$$\mathbf{B}' = \{\overline{v_s} : s \in \mathcal{S}, s \neq s_j\} \bigcup \{\overline{e} : e \in \mathcal{E}\}.$$

Note that the dimension of V' is at most $b + k - 1$. We shall prove that $V' = V$.

First, from Theorem 2.1, we observe that

$$\ell \sum_{e \in \mathcal{E}} p(E=e)\overline{e} = \overline{X}, \tag{2}$$

so $\overline{X} \in V'$. Next, we have

$$\overline{v_{s_j}} = \overline{X} - \sum_{s \in \mathcal{S}, s \neq s_j} \overline{v_s},$$

so $\overline{v_{s_j}} \in V'$. At this point, we have $\{\overline{v_s} : s \in \mathcal{S}\} \subseteq V'$. Then it follows from Equation (1) that

$$\overline{v_m} - \frac{1}{\ell}(\overline{X} - \overline{v_s}) = \overline{m} \in V'$$

for any $m \in \mathcal{M}$. Hence, $V' = V$.

Since V has dimension $k\ell$ and it is generated by $\mathbf{B}'$, a set of $b + k - 1$ vectors, we have that $b \geq k(\ell - 1) + 1$.

Now, let's consider the case of equality, i.e. $b = k(\ell - 1) + 1$. In this case, $\mathbf{B}'$ is a basis for V. We shall show that every authentication rule is used with equal probability $1/b$, and that the matrix of authentication rules is an orthogonal array $OA(\ell, k, \lambda)$, where $\lambda = b/\ell^2$.

Fix an authentication rule $e_i \in \mathcal{E}$. Using Equations (1) and (2), we compute

$$\begin{aligned} \sum_{m \in M(e_i)} \overline{v_m} &= \overline{e_i} + \frac{k-1}{\ell}\overline{X} \\ &= \overline{e_i} + (k-1)\sum_{e \in \mathcal{E}} p(E = e)\overline{e} \end{aligned}$$

But we also have that $\overline{v_m} = \ell \sum_{e \in \mathcal{E}, e(s) = a} p(E = e)\overline{e}$, where $m = (s, a)$, by definition. Hence, we have

$$\sum_{m \in M(e_i)} \overline{v_m} = \ell \sum_{m \in M(e_i)} \sum_{\{e : m \in M(e)\}} p(E = e)\overline{e}.$$

Since $\mathbf{B}'$ is a basis for V, we can extract the coefficient of $\overline{e_i}$ and we obtain $\ell k p(E = e_i) = 1 + (k-1)p(E = e_i)$. Hence, $p(E = e_i) = 1/(k(\ell - 1) + 1) = 1/b$. Since e_i was an arbitrary authentication rule, it follows that all authentication rules are used with equal probability $1/b$.

Now, define the $b \times k$ authentication matrix $M = (a_{ij})$ where $a_{ij} = e_i(s_j)$, $1 \leq i \leq b$, $1 \leq j \leq k$.

Consider any message $m = (s, a)$; since $p(E = e) = 1/b$ for any e, we have the

equation

$$\overline{v_m} = \frac{\ell}{b} \sum_{e \in \mathcal{E}, e(s)=a} \overline{e} = \frac{1}{\ell}(\overline{X} - \overline{v_s}) + \overline{m}.$$

We write this equation with respect to the basis $\mathbf{B}$. Define $r_m = |\{e \in \mathcal{E}, e(s) = a\}|$, and for any $m' = (s', a')$, $s' \neq s$, define $\lambda_{mm'} = |\{e \in \mathcal{E}, e(s) = a, e(s') = a'\}|$. Then we obtain the following relation:

$$\frac{\ell}{b}(r_m \overline{m} + \sum_{m'=(s',a'), s' \neq s} \lambda_{mm'} \overline{m'}) = \overline{m} + \frac{1}{\ell} \sum_{m'=(s',a'), s' \neq s} \overline{m'}.$$

Extracting the coefficient of $\overline{m}$, we see that $r_m = b/\ell$. Then extracting the coefficient of any $\overline{m'}$ $(m' = (s', a'), s' \neq s)$, we see that $\lambda_{mm'} = b/\ell^2$. Since m is an arbitrary message, it follows that the authentication matrix M is an $OA(\ell, k, \lambda)$.

Conversely, suppose we start with an orthogonal array $OA(\ell, k, \lambda)$. Use each row as an authentication rule with equal probability $1/(\lambda \ell^2)$. Then we obtain a code with $P_{d_0} = P_{d_1} = 1/\ell$.

We summarize the above discussion in the following theorem, which complements Theorem 2.3.

Theorem 3.1 *Suppose we have an authentication code without secrecy in which $P_{d_0} = P_{d_1} = k/v = 1/\ell$. Then $b \geq k(\ell - 1) + 1$, and equality occurs if and only if the authentication matrix is an orthogonal array $OA(\ell, k, \lambda)$ where $\lambda = (k(\ell - 1) + 1)/\ell^2$ and the authentication rules are used with equal probability.*

4 General authentication codes

Suppose there is an authentication code for k source states, having b encoding rules and v messages, such that $P_{d_0} = k/v$ and $P_{d_1} = (k-1)/(v-1)$. Recalling Theorem 2.5, we know that $b \geq v(v-1)/(k(k-1))$ and equality can occur only if the encoding matrix is a $(v, k, 1)$−**BIBD**. Here, we consider the case of equality, i.e. $b = v(v-1)/(k(k-1))$.

From Theorem 2.4, it must be the case that

$$\sum_{\{e:m,m' \in M(e)\}} p(E = e)p(S = e^{-1}(m)) = \sum_{\{e:m,m^* \in M(e)\}} p(E = e)p(S = e^{-1}(m))$$

for all $m \neq m', m \neq m^*$. As noted earlier, since $b = v(v-1)/(k(k-1))$, it follows that $|\{e : m, m' \in M(e)\}| = 1$ for all $m \neq m'$. Hence, it follows that

$$p(E = e)p(S = s) = p(E = e')p(S = s')$$

if $e(s) = e'(s')$.

For any $m \in \mathcal{M}$, let

$$x_m = \sum_{\{e:m \in M(e)\}} p(E = e)p(S = e^{-1}(m)).$$

Then,

$$p(S = s)p(E = e) = \frac{x_m}{r}$$

for all e, s such that $e(s) = m$ (recall that $r = (v-1)/(k-1)$ is the number of encoding rules in which any message m occurs). Also, note that $\sum_{m \in \mathcal{M}} x_m = 1$.

Now, for any $e \in \mathcal{E}$, we have

$$p(E = e) = \sum_{s \in \mathcal{S}} p(E = e)p(S = s) = \sum_{m \in M(e)} \frac{x_m}{r}. \tag{3}$$

Fix a message m_0. Now, applying Theorem 2.1 and Equation (3), we get the following:

$$\begin{aligned} \frac{k}{v} &= \sum_{\{e:m_0 \in M(e)\}} p(E = e) \\ &= \sum_{\{e:m_0 \in M(e)\}} \sum_{m \in M(e)} \frac{x_m}{r} \\ &= x_{m_0} + \frac{1}{r} \sum_{m \in \mathcal{M}, m \neq m_0} x_m \\ &= (1 - \frac{1}{r})x_{m_0} + \frac{1}{r} \end{aligned}$$

since $\sum_{m \in \mathcal{M}} x_m = 1$. Solving for x_{m_0}, we get

$$x_{m_0} = (\frac{k}{v} - \frac{1}{r})\frac{r}{r-1} = \frac{r}{bk}.$$

This quantity is independent of m_0, so we have

$$p(E = e)p(S = s) = \frac{1}{bk}$$

for all $s \in \mathcal{S}, e \in \mathcal{E}$. Fixing e and summing over s, we get $p(E = e) = 1/b$ for every $e \in \mathcal{E}$. Similarly, fixing s and summing over e, we get $p(S = s) = 1/k$ for every $s \in \mathcal{S}$. Hence

both the set of source states and the set of encoding rules must be equiprobable in order to obtain the desired deception probabilities.

Summarizing this discussion, we have our main theorem.

Theorem 4.1 *Suppose we have an authentication code in which* $P_{d_0} = k/v$ *and* $P_{d_1} = (k-1)/(v-1)$. *Then* $b \geq (v^2 - v)/(k^2 - k)$, *and equality occurs if and only if the rows of the encoding matrix (taken as unordered sets) form a* $(v, k, 1)$*−BIBD, and both the source states and encoding rules are equiprobable.*

We can extend this result to include codes that provide perfect secrecy. The following theorem follows immediately from Theorem 2.5 and [St2, Theorem 6.4].

Theorem 4.2 *Suppose we have an authentication code which provides perfect secrecy and in which* $P_{d_0} = k/v$ *and* $P_{d_1} = (k-1)/(v-1)$. *Then* $b \geq (v^2 - v)/(k^2 - k)$, *and equality occurs if and only if* $v - 1 \equiv 0 \bmod k(k-1)$, *there exists a* $(v, k, 1)$*−BIBD, and both the source states and encoding rules are equiprobable.*

Acknowledgements

This research was supported by NSERC grant A9287 and by the Center for Communication and Information Science at the University of Nebraska.

This paper is a preliminary version. A final version has been submitted for publication in Designs, Codes and Cryptography.

References

[Ma] J. L. Massey. *Cryptography - a selective survey*, in *Digital Communications*, North-Holland (pub.) (1986), 3–21.

[Si1] G. J. Simmons. *Message authentication: a game on hypergraphs*, Congr. Numer. **45** (1984), 161–192.

[Si2] G. J. Simmons. *Authentication theory / coding theory*, Lecture Notes in Comput. Sci. **196** (1985), 411–432 (proceedings of CRYPTO 84).

[St1] D. R. Stinson. *Some constructions and bounds for authentication codes*, J. Cryptology **1** (1988), 37–51.

[St2] D. R. Stinson. *The combinatorics of authentication and secrecy codes*, J. Cryptology **2** (1990), 23–49.