J. Cryptology (1995) 8: 177–188

Journal of
CRYPTOLOGY

Information-Theoretic Bounds for Authentication Codes and Block Designs*

Dingyi Pei
State Key Laboratory of Information Security,
Graduate School of Academia Sinica, Beijing, P.O. Box 3908,
People's Republic of China

Communicated by James L. Massey

Received 22 March 1992 and revised 18 July 1994

Abstract. Authentication codes with secrecy and with splitting are investigated. An information-theoretic lower bound for the probability of successful deception for a spoofing attack of order r is obtained. The condition necessary on authentication codes to achieve the lower bound is determined as a single simple requirement. Based on the simplicity of the result a construction, by use of so-called partially balanced t-designs, for authentication codes that can achieve the lower bound is suggested.

Key words. Authentication code, Substitution, Impersonation, Spoofing attack, Block design, Partially balance t-design.

1. Introduction

We consider the authentication model that involves three participants: a transmitter, a receiver, and an opponent. The transmitter and receiver trust each other, but the opponent wants to deceive them. The transmitter wishes to send a sequence of source states (plaintexts) $s_1, \ldots, s_r$ to the receiver. In order to enable the receiver to verify the authenticity of these messages as well as to keep the information secret, he encrypts them into a sequence of encoded messages (ciphertexts) $m_1, \ldots, m_r$ by using one of a finite set of encoding rules (keys) which is agreed upon in advance with the receiver. Then the transmitter sends $m_1, \ldots, m_r$ through a public communication channel. We denote by $\mathcal{S}$ the set of all source states, by $\mathcal{E}$ the set of all encoding rules, and by $\mathcal{M}$ the set of all possible encoded messages. Each encoding rule is a mapping from $\mathcal{S}$ to $\mathcal{M}$. The range of the mapping is usually a proper subset of $\mathcal{M}$ and generally different for different encoding rules. Only the messages in the subset corre-

*This research was partially supported by a K. C. Wong Fellowship.

sponding to the agreed-upon encoding rule are acceptable, which is how authentication is achieved.

We assume that the opponent has a complete understanding of the system, including all the encoding rules. The only thing he does not know is the particular encoding rule agreed upon by the transmitter and receiver. We also assume that the opponent has the ability to introduce a message into the channel. After observation of the first r (where $r \geq 0$) messages $m_1, \ldots, m_r$, the opponent places his own message m into the channel, attempting to make the receiver accept it as authentic. This is called a spoofing attack of order r [4].

In this paper we consider authentication systems with secrecy and splitting. In an authentication system without secrecy, called a Cartesian scheme, each encoded message in $\mathcal{M}$ encodes the same source state for all encoding rules for which this encoded message is valid. Therefore, in such a system, once the opponent observes an encoded message, he knows the corresponding source state. In a system with secrecy, the opponent cannot in general determine the corresponding source state from its encoded message without knowing the encoding rule used. In an authentication system with splitting, any of several messages can be used to encode a particular source state for the same encoding rule. However, in order for the receiver to be able to determine the source state uniquely from the encoded message and knowledge of the encoding rule used, there can be at most one source state which is encoded by a particular encoded message in $\mathcal{M}$ under a given encoding rule.

Define

$$\mathcal{S}^r = \{s^r = (s_1, \ldots, s_r) \mid s_i \in \mathcal{S}, 1 \leq i \leq r\}$$

and

$$\mathcal{M}^r = \{m^r = (m_1, \ldots, m_r) \mid m_i \in \mathcal{M}, 1 \leq i \leq r\}.$$

We write E, S, M, S^r, and M^r for the random variables describing the authentication system and taking values e, s, m, s^r, and m^r in $\mathcal{E}$, $\mathcal{S}$, $\mathcal{M}$, $\mathcal{S}^r$, and $\mathcal{M}^r$, respectively.

Let P_r denote the expected probability of successful deception for a spoofing attack of order r. We first recall some previous information-theoretic bounds for P_r. Simmons [12] proved

$$P_0 \geq 2^{H(E|M)-H(E)}, \tag{1}$$

where here and hereafter all logarithms used in entropies are to base 2 and where $H(E|M)$ denotes conditional entropy. Short proofs of (1) were provided by Massey [5] and by Sgarro [10]. Johannesson and Sgarro gave a strengthened bound on P_0 in [3]. Simmons [12] and Brickell [1] proved

$$P_1 \geq 2^{-H(E|M)}. \tag{2}$$

Walker [15] proved

$$P_r \geq 2^{H(E|M^{r+1})-H(E|M^r)}, \qquad r = 0, 1, 2, \ldots, \tag{3}$$

for authentication codes without secrecy and splitting.

The main purpose of this paper is to prove that inequality (3) holds for general authentication codes, i.e., codes with secrecy and splitting. In Section 2 we prove our main theory (Theorem 1), which was first presented in the rump session at Asiacrypt '91. The proof of Theorem 1 is based on the method of Massey [5]. It can also be proved by the method of Sgarro [10]. (The latter approach was used in the original version of this paper, see Appendix 7.3C of [8].) Smeets [13], Sgarro [11], and Rosenbaum [7] have all recently given proofs of (3) for general authentication codes. Our proof of (3) is simpler, and this in turn leads to a simpler formulation of the condition for equality to hold. Our approach also suggests a construction, which is based on what we call partially balanced t-designs, for codes that achieve equality in (3).

In Section 3 we discuss some consequences of Theorem 1. In Section 4 we prove (Theorem 6) that if an authentication code (without splitting) has the property that the probabilities P_r $(0 \le r \le t-1)$ achieve their information-theoretic lower bounds and if the number of encoding rules is minimum, then this code corresponds to a partially balanced t-design. Several known partially balanced t-designs are also mentioned.

2. Main Theorem

For any $m^r = (m_1, \ldots, m_r) \in \mathcal{M}^r$ and $e \in \mathcal{E}$, let $f_e(m^r) = (f_e(m_1), \ldots, f_e(m_r))$ denote the unique element $(s_1, \ldots, s_r) \in \mathcal{S}^r$, when it exists, such that $s_i = f_e(m_i)$ $(1 \le i \le r)$ is encoded by m_i under e.

For simplicity, we abbreviate by omitting the names of random variables in a probability distribution when this causes no confusion. For instance, we abbreviate $p(S = s)$ to $p(s)$, $p(E = e | M^r = m^r)$ to $p(e|m^r)$, but $p(M_{r+1} = m | M^r = m^r)$ to $p(M_{r+1} = m|m^r)$ where M_{r+1} denotes the random variable that is the $(r+1)$th encoded message, etc.

We assume that E and S^r are independent, i.e., that $p(e, s^r) = p(e)p(s^r)$ for every $e \in \mathcal{E}$ and $s^r \in \mathcal{S}^r$.

In a system with splitting, the transmitter is free to choose $p(m^r|e, s^r)$ in any manner such that, for any given $s^r \in \mathcal{S}^r$ and $e \in \mathcal{E}$,

$$\sum_{m^r \in \mathcal{M}^r} p(m^r|e, s^r) = 1$$

and

$$p(m^r|e, s^r) = 0 \qquad \text{when} \quad s^r \neq f_e(m^r).$$

We consider only impersonation $(r = 0)$ and plaintext substitution. The latter means that the opponent is considered to be successful only when, after observing a sequence of messages $m_1, \ldots, m_r$, he chooses a fradulent ciphertext m' that is accepted as authentic by the receiver and $f_e(m_i) \neq f_e(m')$ $(1 \le i \le r)$ where e is the key used. If the receiver gets a particular message twice, he cannot decide whether the message was sent twice by the transmitter or was repeated by an opponent. Hence we assume that the transmitter never sends a

particular source state twice under same encoding rule. Accordingly we require that (for $r \geq 2$)

$$p(s^r) > 0$$

only if the components $s_1, \ldots, s_r$ of s^r are pairwise distinct.

For any $m^r = (m_1, \ldots, m_r) \in \mathscr{M}^r$ define

$$\mathscr{E}(m^r) = \left\{ e \in \mathscr{E} \;\middle|\; \begin{array}{l} m_i\ (1 \leq i \leq r) \text{ are acceptable under } e \text{ and} \\ f_e(m_i)\ (1 \leq i \leq r) \text{ are pairwise distinct} \end{array} \right\},$$

i.e., $\mathscr{E}(m^r)$ is the set of all encoding rules under which m^r is valid. The set $\mathscr{E}(m^r)$ may be empty for some m^r.

The probability distributions for E and S^r together with the splitting strategy $p(m^r|e, s^r)$ determine the probability distribution for M^r. For any $e \in \mathscr{E}$ and $m^r \in \mathscr{M}^r$, if $e \notin \mathscr{E}(m^r)$, then $p(e, m^r) = 0$; if $e \in \mathscr{E}(m^r)$, then

$$p(e, m^r) = p(e)p(\mathscr{S}^r = f_e(m^r))p(m^r|e, \mathscr{S}^r = f_e(m^r)). \tag{4}$$

Let $P_r(m|m^r)$ denote the probability that m would be a valid choice for M_{r+1} given that m^r has been observed. Then

$$P_r(m|m^r) = \sum_{e \in \mathscr{E}(m^r * m)} p(e|m^r),$$

where $m^r * m$ denotes the message sequence $m_1, \ldots, m_r, m$. Given that m^r has been observed, the opponent's optimum strategy is to substitute the message $\hat{m}$ that maximizes $P_r(m|m^r)$. Thus, the unconditional probability of success in an optimum spoofing attack of order r is just

$$P_r = \sum_{m^r \in \mathscr{M}^r} p(m^r) \max_{m \in \mathscr{M}} P_r(m|m^r).$$

Theorem 1. *For any integer $r \geq 0$, the probability of success in an optimum spoofing attack of order r satisfies*

$$P_r \geq 2^{H(E|M^{r+1}) - H(E|M^r)}.$$

Equality holds if and only if, for every $m^r \in \mathscr{M}^r$ and $m \in \mathscr{M}$ for which $\mathscr{E}(m^r * m)$ is not empty,

$$\frac{p(e|m^r)}{p(e|m^r * m)}$$

is independent of m, m^r and $e \in \mathscr{E}(m^r * m)$. When equality holds, the probability P_r equals this constant ratio.

Proof. For a given $m^r \in \mathscr{M}^r$, let

$$\operatorname{supp}(M_{r+1}, E|m^r) = \{(m, e) \mid p(M_{r+1} = m, e|m^r) > 0, m \in \mathscr{M}, e \in \mathscr{E}\}$$

denote the support of the conditional probability distribution of the pair of random variables (M_{r+1}, E) conditioned on $M^r = m^r$. Then underbounding a

maximum by an average gives

$$\begin{aligned}\max_{m\in\mathcal{M}} P_r(m|m^r) &\geq \sum_{m\in\mathcal{M}} p(M_{r+1}=m|m^r)P_r(m|m^r)\\ &= \sum_{(m,e)\in \mathrm{supp}(M_{r+1},E)} p(M_{r+1}=m|m^r)p(e|m^r)\\ &= \tilde{E}\left(\frac{p(M_{r+1}=m|m^r)p(e|m^r)}{p(M_{r+1}=m,e|m^r)}\right),\end{aligned}$$

where $\tilde{E}$ is the conditional expectation given that $\mathcal{M}^r = m^r$. By use of Jensen's inequality, we obtain

$$\begin{aligned}\log \max_{m\in\mathcal{M}} P_r(m|m^r) &\geq \log \tilde{E}\left(\frac{p(M_{r+1}=m|m^r)p(e|m^r)}{p(M_{r+1}=m,e|m^r)}\right)\\ &\geq \tilde{E}\left(\log\frac{p(M_{r+1}=m|m^r)p(e|m^r)}{p(M_{r+1}=m,e|m^r)}\right)\\ &= H(M_{r+1}E|M^r=m^r) - H(M_{r+1}|M^r=m^r)\\ &\quad - H(E|M^r=m^r),\end{aligned}$$

where

$$\begin{aligned}&H(M_{r+1}E|M^r=m^r)\\ &\quad = -\sum_{(m,e)\in\mathrm{supp}(M_{r+1},E)} p(M_{r+1}=m,e|m^r)\log p(M_{r+1}=m,e|m^r),\\ &H(M_{r+1}|M^r=m^r)\\ &\quad = -\sum_{m:p(M_{r+1}=m|m^r)>0} p(M_{r+1}=m|m^r)\log p(M_{r+1}=m|m^r),\end{aligned}$$

and

$$H(E|M^r=m^r) = -\sum_{e\in\mathcal{E}(m^r)} p(e|m^r)\log p(e|m^r).$$

Finally we make another use of Jensen's inequality to obtain

$$\begin{aligned}\log P_r &= \log\sum_{m^r} p(m^r)\max_{m\in\mathcal{M}} P_r(m|m^r)\\ &\geq \sum_{m^r} p(m^r)\log\max_{m\in\mathcal{M}} P_r(m|m^r)\\ &\geq H(M_{r+1}E|M^r) - H(M_{r+1}|M^r) - H(E|M^r)\\ &= H(E|M^{r+1}) - H(E|M^r).\end{aligned}$$

From the above derivation, we see that equality holds in this bound if and only if the following two conditions are satisfied:

(i) The probability $P_r(m|m^r)$ is independent of those m and m^r with $p(M_{r+1}=m|m^r)>0$ so that its average and maximum values coincide.

(ii) For every $(m^r * m) \in \mathcal{M}^{r+1}$, if $\mathcal{E}(m^r * m)$ is not empty, then

$$\frac{p(M_{r+1} = m|m^r)p(e|m^r)}{p(M_{r+1} = m, e|m^r)} = \frac{p(e|m^r)}{p(e|m^r * m)}$$

is independent of m, m^r and $e \in \mathcal{E}(m^r * m)$.

Condition (i) can be deduced from condition (ii) since, if $p(M_{r+1} = m|m^r) > 0$, then

$$\begin{aligned} P_r(m|m^r) &= \sum_{e \in \mathcal{E}(m^r * m)} p(e|m^r) \\ &= \frac{p(e|m^r)}{p(e|m^r * m)} \sum_{e \in \mathcal{E}(m^r * m)} p(e|m^r * m) \\ &= \frac{p(e|m^r)}{p(e|m^r * m)}. \end{aligned}$$

This completes the proof of Theorem 1. □

3. Some Consequences

In this section we discuss some consequences of Theorem 1. Let $k = |\mathcal{S}|$, $v = |\mathcal{M}|$, and $b = |\mathcal{E}|$. From now on we consider only authentication codes without splitting. For $s^r \in \mathcal{S}^r$, let

$$\mathcal{M}(s^r) = \{m^r \in \mathcal{M}^r \mid \text{for some } e \in \mathcal{E}, f_e(m^r) = s^r\};$$

for $m^r \in \mathcal{M}^r$, let

$$\mathcal{M}(m^r) = \{m \in \mathcal{M} \mid \mathcal{E}(m^r * m) \text{ is not empty}\}$$

and

$$\mathcal{M}(s, m^r) = \{m \in \mathcal{M}(s) \mid \mathcal{E}(m^r * m) \text{ is not empty}\}.$$

For $e \in \mathcal{E}$, let

$$\mathcal{M}(e) = \{m \in \mathcal{M} \mid \text{for some } s \in \mathcal{S}, f_e(m) = s\}.$$

Finally, for an integer $r > 0$, let

$$\overline{\mathcal{M}^r} = \{m^r \in \mathcal{M}^r \mid \mathcal{E}(m^r) \text{ is not empty}\}.$$

By (4), if $e \in \mathcal{E}(m^r * m)$, we have

$$\begin{aligned} \frac{p(e|m^r)}{p(e|m^r * m)} &= \frac{p(e, m^r)p(m^r * m)}{p(e, m^r * m)p(m^r)} \\ &= \frac{p(f_e(m^r))\sum_{e' \in \mathcal{E}(m^r * m)} p(e')p(f_{e'}(m^r * m))}{p(f_e(m^r * m))\sum_{e' \in \mathcal{E}(m^r)} p(e')p(f_{e'}(m^r))}. \end{aligned} \tag{5}$$

The following result was first proved by Walker [15].

Corollary 2. *If an authentication code is Cartesian, then the equality*

$$P_r = 2^{H(E|M^{r+1})-H(E|M^r)} \tag{6}$$

holds if and only if, for every $m^r = (m_1, \ldots, m_r) \in \overline{\mathcal{M}^r}$, *the sum* $\Sigma_{e \in \mathcal{E}(m^r * m)} p(e)$ *is independent of* $m \in \mathcal{M}(m^r)$, *and the number* $|\mathcal{M}(s, m^r)|$ *is constant for all* m^r *and* s *where* $s \neq f_e(m_i)$ $(1 \leq i \leq r)$. *Furthermore, in this case* $P_r = |\mathcal{M}(x, m^r)|^{-1}$.

Proof. Since the code is Cartesian, for every $s \in \mathcal{S}$ with $s \neq f_e(m_i)$ $(1 \leq i \leq r)$, we have

$$\sum_{e \in \mathcal{E}(m^r)} p(e) = \sum_{m \in \mathcal{M}(s, m^r)} \sum_{e \in \mathcal{E}(m^r * m)} p(e).$$

For a fixed $m^r \in \overline{\mathcal{M}_r}$, the source sequence $f_e(m^r)$ is the same for all $e \in \mathcal{E}(m^r)$. By Theorem 1 and (5), we know that

$$\frac{p(e|m^r)}{p(e|m^r * m)} = \frac{\Sigma_{e' \in \mathcal{E}(m^r * m)} p(e')}{\Sigma_{e' \in \mathcal{E}(m^r)} p(e')}$$

is independent of m^r and m. Therefore the sum $\Sigma_{e \in \mathcal{E}(m^r * m)} p(e)$ is independent of $m \in \mathcal{M}(m^r)$ and

$$\frac{p(e|m^r)}{p(e|m^r * m)} = |\mathcal{M}(s, m^r)|^{-1}.$$

The proof of the "if" part is just the inverse of above argument. □

We define the following property of the probability distribution for $\mathcal{S}^r$:

Property $(*)$. For any given $m^r \in \overline{\mathcal{M}^r}$, the probability $p(f_e(m^r))$ is constant for all $e \in \mathcal{E}(m^r)$.

We call the source r-uniform if $p(s^r)$ is constant for all s^r with nonzero probability. Property $(*)$ is weaker than requiring $p(f_e(m^r))$ to be the uniform distribution, since $p(f_e(m^r))$ may have different values for different m^r in the former case.

Corollary 3. *Suppose that the source has property* $(*)$ *for* r *and* $r + 1$ (*only for* 1 *if* $r = 0$), *then equality* (6) *holds if and only if the probability* $P_r(m|m^r)$ *is constant for* $(m^r * m) \in \mathcal{M}^{r+1}$.

Proof. Using property $(*)$ for r and $r + 1$ in (5), for $e \in \mathcal{E}(m^r * m)$, we have

$$\frac{p(e|m^r)}{p(e|m^r * m)} = \frac{\Sigma_{e' \in \mathcal{E}(m^r * m)} p(e')}{\Sigma_{e^* \in \mathcal{E}(m^r)} p(e')}.$$

On the other hand,

$$P_r(m|m^r) = \sum_{e \in \mathscr{E}(m^r * m)} p(e|m^r) = \sum_{e \in \mathscr{E}(m^r * m)} \frac{p(e, m^r)}{p(m^r)} = \frac{\sum_{e \in \mathscr{E}(m^r * m)} p(e)}{\sum_{e \in \mathscr{E}(m^r)} p(e)}.$$

The corollary now follows from Theorem 1. □

Corollary 4. *If* $P_r = 2^{H(E|M^{r+1}) - H(E|M^r)}$ *for* $r = 0, 1, \ldots, t-1$ $(t \leq k)$, *then*:

(i) *Property* $(*)$ *holds for* $1 \leq r \leq t$.

(ii) *For any given* $m^r \in \mathscr{M}^r$ $(1 \leq r \leq t)$,

$$\sum_{e \in \mathscr{E}(m^r)} p(e) = P_0 P_1 \cdots P_{r-1},$$

where

$$P_r = \frac{\sum_{e \in \mathscr{E}(m^r * m)} p(e)}{\sum_{e \in \mathscr{E}(m^r)} p(e)}$$

when $(m^r * m) \in \overline{\mathscr{M}^{r+1}}$.

(iii) $P_0 = k/v$ *and for any given* $m^r \in \mathscr{M}^r$ $(1 \leq r \leq t-1)$, $|\mathscr{M}(m^r)| = (k-r)P_r^{-1}$.

(iv) $|\overline{\mathscr{M}^1}| = v$ *and* $|\overline{M^r}| = \binom{k}{r}(P_0 P_1 \cdots P_{r-1})^{-1}$.

Proof. For $(m^r * m) \in \overline{\mathscr{M}^{r+1}}$ and $e \in \mathscr{E}(m^r * m)$ we have, by Theorem 1,

$$P_r = \frac{p(e|m^r)}{p(e|m^r * m)} = \frac{p(f_e(m^r))\sum_{e' \in \mathscr{E}(m^r * m)} p(e')p(f_{e'}(m^r * m))}{p(f_e(m^r * m))\sum_{e' \in \mathscr{E}(m^r)} p(e')p(f_{e'}(m^r))}$$

for $0 \leq r \leq t-1$. By the above equality for $r = 0$, we see that (i) and (ii) hold for $r = 1$. Then (i) and (ii) can be proved by induction on r.

To show (iii), we have

$$\sum_{m \in \mathscr{M}} \sum_{e \in \mathscr{E}(m)} p(e) = k \sum_{e \in \mathscr{E}} p(e) = k,$$

and

$$\sum_{m \in \mathscr{M}(m^r)} \sum_{e \in \mathscr{E}(m^r * m)} p(e) = (k-r) \sum_{e \in \mathscr{E}(m^r)} p(e).$$

Thus (iii) follows from (ii).

Finally, it is trivial that $|\overline{\mathcal{M}^1}| = v$. By (iii), when $r \geq 2$, we have

$$|\overline{\mathcal{M}^r}| = \frac{1}{r} \sum_{m^{r-1} \in \overline{\mathcal{M}^{r-1}}} |\mathcal{M}(m^{r-1})| = \frac{(k-r+1)|\overline{\mathcal{M}^{r-1}}|}{rP_{r-1}}.$$

Thus (iv) follows by induction on r. □

4. Constructions of Authentication Codes that Achieve the Information-Theoretic Lower Bounds

Besides the information-theoretic lower bound discussed above, Massey [4] proved that

$$P_r \geq \frac{k-r}{v-r}.$$

We call this lower bound the *combinatorial lower bound.* It was proved that if P_r $(0 \leq r \leq t-1)$ achieve their combinatorial lower bounds, then the number $|\mathcal{E}(m^r)|$ is constant for all $m^r \in \mathcal{M}^r$ with pairwise different components. An authentication code that achieves combinatorial lower bounds for P_r $(0 \leq r \leq t-1)$ with equiprobable source states corresponds to a t-design (see [9] and [2]). In this section we discuss the same problem for the information-theoretic bound.

Definition 5. Let v, k, λ, t be positive integers with $t \leq k$. A $t-(v, k; \lambda, 0)$ design is a pair $(\mathcal{M}, \mathcal{E})$, where $\mathcal{M}$ is a set of v points and $\mathcal{E}$ is a family of k-subsets (called blocks) of $\mathcal{M}$ such that any t-subset of $\mathcal{M}$ either occurs in exactly λ blocks or does not occur in any block.

If every t-subset of $\mathcal{M}$ always occurs in exactly λ blocks, then a $t-(v, k; \lambda, 0)$ design is just a $t-(v, k, \lambda)$ design. That is, the concept of a $t-(v, k; \lambda, 0)$ design is a generalization of the well-known concept of a t-design. We call a $t-(v, k; \lambda, 0)$ design a *partially balanced* t-design.

Theorem 6. *Suppose an authentication code has the property that*

$$P_r = 2^{H(E|M^{r+1}) - H(E|M^r)} \qquad (0 \leq r \leq t-1, t < k).$$

Then $b \geq (P_0 P_1 \cdots P_{t-1})^{-1}$, *where equality holds if and only if the sets* $\{\mathcal{M}(e)\}$ $(e \in \mathcal{E})$ *form an* $r-(v, k; \lambda_r, 0)$ *design for* $2 \leq r \leq t$ *and a* $1-(v, k, \lambda_1)$ *design simultaneously where* $\lambda_t = 1$, $\lambda_r = (P_r P_{r+1} \cdots P_{t-1})^{-1}$ $(1 \leq r \leq t-1)$, *the encoding rules are equally probable, and the probability distributions for* S^r $(1 \leq r \leq t)$ *satisfy property* $(*)$.

Proof. We have

$$\sum_{m^{t-1} \in \overline{\mathscr{M}^{t-1}}} |\mathscr{E}(m^{t-1})| = b\binom{k}{t-1}$$

and

$$(k-t+1) \sum_{m^{t-1} \in \overline{\mathscr{M}^{t-1}}} |\mathscr{E}(m^{t-1})| = \sum_{m^{t-1} \in \overline{\mathscr{M}^{t-1}}} \sum_{m \in \mathscr{M}(m^{t-1})} |\mathscr{E}(m^{t-1} * m)|$$

$$\geq |\overline{\mathscr{M}^{t-1}}|\, |\mathscr{M}(m^{t-1})| \qquad \left(m^{t-1} \in \overline{\mathscr{M}^{t-1}}\right). \quad (7)$$

By using (iii) and (iv) of Corollary 4, we get

$$b \geq \frac{|\overline{\mathscr{M}^{t-1}}|}{\binom{k}{t-1} P_{t-1}} = (P_0 P_1 \cdots P_{t-1})^{-1}.$$

Suppose equality holds in the above bound, then $|\mathscr{E}(m^t)| = 1$ for any $m^t \in \overline{\mathscr{M}^t}$ from (7). By (ii) of Corollary 4, we know $p(e)$ is constant for all $e \in \mathscr{E}$ and

$$P_r = \frac{|\mathscr{E}(m^r * m)|}{|\mathscr{E}(m^r)|}, \qquad 1 \leq r \leq t-1,$$

for any $(m^r * m) \in \overline{\mathscr{M}^{r+1}}$. Therefore the sets $\{\mathscr{M}(e)\}$ form an $r-(v, k;\ \lambda_r, 0)$ design $(1 \leq r \leq t)$ with $\lambda_t = 1$ and

$$\lambda_r = |\mathscr{E}(m^r)| = (P_r P_{r+1} \cdots P_{t-1})^{-1} \ (1 \leq r \leq t-1).$$

By (i) of Corollary 4, property $(*)$ holds for $1 \leq r \leq t$. The proof of the "if" part is easy and is omitted. □

Theorem 6 suggests a way of constructing authentication codes that achieve the information-theoretic lower bounds, i.e., to find partially balanced t-designs.

Now we consider a Cartesian scheme. We 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 the encoded message m. We call this matrix an encoding matrix. The rows (taken as unordered sets) of the encoding matrix form a block design for the v elements of $\mathscr{M}$.

Definition 7. An orthogonal array $\mathrm{OA}_t(n, k)$ is an $n^t \times k$ array of n symbols, such that in any t $(t \leq k)$ columns of the array, any t ordered symbols occur in exactly one row.

Corollary 8. *Suppose a Cartesian authentication code has the property that*

$$P_r = 2^{H(E|M^{r+1})-H(E|M^r)} \qquad (0 \le r \le t-1, t \le k).$$

Then $P_0 = P_1 = \cdots = P_{t-1} = k/v = 1/n$, *and* $b \ge n^t$ *where* n *is an integer. Equality holds if and only if the encoding matrix is an orthogonal array and the encoding rules are equally probable.*

Proof. Let $S = \{s_1, \ldots, s_k\}$. Fix s_j, take $m^r = (m_1, \ldots, m_r) \in \overline{\mathcal{M}^r}$ $(1 \le r \le t-1)$ such that $m_i \notin M(s_j)$ $(1 \le i \le r)$. We have

$$\sum_{m \in \mathcal{M}(s_j)} \sum_{e \in \mathcal{E}(m)} p(e) = 1$$

and

$$\sum_{m \in \mathcal{M}(s_j)} \sum_{e \in \mathcal{E}(m^r * m)} p(e) = \sum_{e \in \mathcal{E}(m^r)} p(e).$$

By (ii) of Corollary 4, we obtain

$$P_0 = P_1 = \cdots = P_{t-1} = |\mathcal{M}(s_j)|^{-1} = n^{-1}.$$

Therefore $b \ge n^t$ by Theorem 6. Furthermore if $b = n^t$, then E has the uniform distribution and $|\mathcal{E}(m^r)| = n^{t-r}$ for any $m^r \in \overline{\mathcal{M}^r}$ $(1 \le r \le t)$.

For any s_j, we have

$$|\mathcal{M}(s_j)| n^{t-1} = \sum_{m \in \mathcal{M}(s_j)} |\mathcal{E}(m)| = n^t$$

(from (ii) of Corollary 4); hence $|\mathcal{M}(s_j)| = n$ $(1 \le j \le k)$. Fix an element $m \in \mathcal{M}(s_j)$, for any $i \ne j$ we have

$$\sum_{m' \in \mathcal{M}(s_i)} |\mathcal{E}(m * m')| = |\mathcal{E}(m)| = n^{t-1}.$$

It follows that $|\mathcal{E}(m * m')| = n^{t-2}$ for any $m' \in \mathcal{M}(s_i)$. By induction, for any integers $1 < j_1 < j_2 < \cdots < j_t < k$ and any messages $m_i \in \mathcal{M}(s_{u_i})$ $(1 \le i \le t)$, we have $|\mathcal{E}(m_1, \ldots, m_t)| = 1$.

Let $\mathcal{M}(s_j) = \{m_{j1}, \ldots, m_{jn}\}$ $(1 \le j \le k)$ and $\mathcal{E} = \{e_1, \ldots, e_{n^t}\}$. Put

$$a_{ij} = r \qquad \text{if} \quad e_i(s_j) = m_{jr}.$$

Then $A = (a_{ij})$ is an orthogonal array $\mathrm{OA}_t(n, k)$. □

The result of Corollary 8 was proved by Stinson [14, Theorems 5.2 and 5.3]. The orthogonal array $\mathrm{OA}_t(n, k)$ is equivalent to the transversal design $\mathrm{TD}_1(t, k, n)$ discussed there. It is easy to see that the orthogonal array $\mathrm{OA}_t(n, k)$ is an $r - (kn, k; n^{t-r}, 0)$ design for $2 \le r \le t$ and a $1 - (kn, k, n^{t-1})$ design simultaneously.

So far we have seen that a t-design and an orthogonal array are also partially balanced t-designs with the property mentioned above. A partially balanced incomplete block design (PBIB) with two associate classes, in which one of the parameters λ_1 and λ_2 is zero, is also a $2-(v,k;\lambda,0)$ design and a $1-(v,k,r)$ design as well. The reader is referred to [6] or [16] for the definition of a PBIB. Recently the author has found a new class of partially balanced t-design for any positive integer t which will be described in a latter paper.

Acknowledgments

The author wishes to thank Professor J. L. Massey for helpful discussions.

References

[1] E. F. Brickell, A few results in message authentication. *Congr. Numer.*, **43** (1984), 141–154.
[2] M. De Soete, Some constructions for authentication-secrecy does. In *Advances in Cryptology–Eurocrypt '88*. Lecture Notes in Computer Science, Vol. 330, Springer-Verlag, Berlin, 1988, pp. 57–75.
[3] R. Johannesson and A. Sgarro, Strengthening Simmons' bound on impersonation. *IEEE Trans. Inform. Theory*, **37**(4) (1991), 1182–1185.
[4] J. L. Massey, Cryptography—a selective survey. *Alta Frequenza*, **LV**(1) (1986), 4–11.
[5] J. L. Massey, Contemporary cryptology: an introduction. In *Contemporary Cryptology* (edited by G. J. Simmons). IEEE Press, New York, 1991, pp. 1–39.
[6] D. K. Ray-Chaudhuri, Application of the geometry of quadrics for constructing PBIB design. *Ann. of Math. Statist.*, **33** (1962), 1175–1186.
[7] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages. *J. Cryptology*, **6** (1993), 135–156.
[8] R. Safavi-Naini and L. Tombak, Optimal authentication systems. In *Advances in Cryptology—Eurocrypt '93*. Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, Berlin, 1994, pp. 12–27.
[9] P. Schöbi, Perfect authentication systems for data sources with arbitrary statistics. Presented at Eurocrypt '86.
[10] A. Sgarro, Informational divergence bounds for authentication codes. In *Advances in Cryptology —Eurocrypt '89*, Lecture Notes in Computer Science, Vol. 434, Springer-Verlag, Berlin, 1990, pp. 93–101.
[11] A. Sgarro, Information-theoretic bounds for authentication frauds. *J. Comput. Security*, **2** (1993), 53–63.
[12] G. J. Simmons, Authentication theory/coding theory. In *Advances in Cryptology—Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, Berlin 1985, pp. 411–431.
[13] B. Smeets, A short proof of a lower bound on the probability of deception in multiple authentication, to appear.
[14] D. R. Stinson, The combinatorics of authentication and secrecy codes. *J. Cryptology*, **2** (1990), 23–49.
[15] M. Walker, Information-theoretic bounds for authentication schemes. *J. Cryptology*, **2** (1990), 131–143.
[16] Z. Wan, Z. Dai, X. Feng, and B. Yang, *Studies in Finite Geometries and Incomplete Block Designs* (in Chinese). Science Press, Beijing, 1966.