J. Cryptology (1993) 6: 135–156

Journal of
CRYPTOLOGY

A Lower Bound on Authentication After Having Observed a Sequence of Messages

Ute Rosenbaum
Siemens AG, Otto Hahn-Ring 6,
D-81739 München, Federal Republic of Germany

Communicated by Gustavus J. Simmons

Received 11 June 1991 and revised 15 April 1992

Abstract. In this paper we study authentication systems and consider the following scenario: Each encoding rule is used for the transmission of a sequence of i messages. We prove a lower bound on the probability that a spoofer observing i messages succeeds in generating an authentic message without knowing the encoding rule used. This bound is based on the conditional entropy of the encoding rules when a sequence of messages is known. Authentication systems which meet the bound are investigated and compared with systems that are l-fold secure against spoofing introduced by Massey [8]. We also give a bound for the probability of success if the opponent can choose how many messages he observes before trying to cheat.

Key words. Authentication systems.

1. Introduction

In this paper we study the security of unconditionally secure authentication systems. We use the model of authentication introduced by Simmons [10]. There are three participants: a *transmitter*, a *receiver*, and an *opponent*. The transmitter wants to convey some information to the receiver, whereas the opponent wants to deceive the receiver. The transmitter and receiver are assumed to trust each other and act with the common purpose of preventing the opponent from deceiving the receiver into accepting fraudulent messages.

Formally, an *authentication system* can be described as follows. It consists of a set S of *source states*, a set M of *messages*, and a set E of *encoding rules*. Each encoding rule defines a mapping from the set of source states into the set of messages. We allow *splitting*, that is, a source state can be mapped by one encoding rule to more than one message. Authentication systems where each message uniquely determines the corresponding source state are called *Cartesian*.

Prior to transmission the transmitter and receiver agree upon a common secret encoding rule. The transmitter encodes the source state he wants to convey to the receiver with this encoding rule and sends the obtained message. The receiver accepts the message as authentic if it is the encoding of some source state under the chosen encoding rule.

We assume that the opponent will play as follows. He observes a sequence of $i \geq 0$ messages encoded under the same encoding rule. Then he can play either *impersonation* or *substitution*. When the opponent plays impersonation he originates a message of his own devising, attempting to have the receiver accept this message as authentic. When he plays substitution, he replaces the last message being sent with another message so that the receiver is misled as to the state of the source. We assume Kerckhoffs' principle of crytpography, that is, the only thing the opponent does not know is the actual encoding rule. From knowledge of the authentication system and observed messages encoded by the same encoding rule he can deduce information about the encoding rule used.

Let p_i be the probability of success if the opponent has observed i distinct messages and plays optimally. Our main result (see Theorem 3.1) is that under these hypotheses

$$p_i \geq 2^{-I(E;M|M^i)} = 2^{H(E|M^{i+1})-H(E|M^i)}.$$

We also consider the case where the opponent can choose how many messages he observes before trying to cheat. By P_l we denote the probability of success if he can observe at most l messages and again plays to his best. We show (Theorem 4.1) that

$$P_l \geq 2^{-[1/(l+1)]H(E)}.$$

We also prove necessary and sufficient conditions for authentication systems to hold the bounds for p_i and P_l with equality. One result is that if the bound for P_l is met, the encoding rules must be equally distributed and we have

$$P_l = |E|^{-1/(l+1)}.$$

For Cartesian authentication systems and under more stringent conditions than we impose, the bound $P_l = |E|^{-1/(l+1)}$ has been proved by Fåk [6], generalizing the work of Gilbert *et al.* [7] who proved this bound for $l = 1$. Various authors have studied the case where the opponent is restricted to observing at most one message. Under this assumption Simmons has shown the lower bounds for p_0 and P_1. He called an authentication system *perfect* if $P_1 = 2^{-(1/2)H(E)}$ holds (see [10]–[13]). A bound for p_1 has been shown by Brickell and Simmons in [2]. Recently, Walker [18] proved the bounds for p_i and P_l for a special class of authentication systems, namely, Cartesian authentication systems without splitting.

The aim of this paper is to show that these bounds also hold in general authentication systems that allow splitting and provide secrecy.

The paper is structured as follows. In Section 2 we describe more formally authentication systems and the opponent's role. We introduce probability functions on the encoding rules and on the sequences of source states. This enables us to prove formulas for the probability that the transmitter sends a sequence of messages and for the probability that the opponent is successful in cheating.

In Section 3 we prove the lower bound for the probability p_i of the opponent's success if he has observed a sequence of i messages. We prove properties of authentication systems in which this bound holds with equality and investigate authentication systems which meet this bound for all $i \leq l$.

In Section 4 we assume that the opponent can choose how many messages of at most l messages he observes before trying to cheat. We prove a lower bound for the probability P_l of success in this case. In analogy to [10] and [18] we call an authentication system *l-perfect* if this bound is met. For l-perfect authentication systems we prove an upper bound on the number of source states.

In the last section we investigate authentication systems that are l-fold secure against spoofing. This notion was introduced by Massey [8] and investigated by several other authors (see [3], [4], and [17]).

The bounds that we prove in Sections 3 and 4 depend on the entropies of the probability distribution of the encoding rules and messages and on the conditional mutual information. For a probability distribution on a set X, the *entropy* $H(X)$ of X, is defined as follows:

$$H(X) = -\sum_{x \in X} p(x) \cdot \log(p(x)).$$

For a set Y and an element $y \in Y$, the *conditional entropy* $H(X|y)$ is defined to be

$$H(X|y) = -\sum_{x \in X} p(x|y) \cdot \log(p(x|y)).$$

The estimated value $H(X|Y)$ of this conditional entropy can be expressed as

$$H(X|Y) = \sum_{y \in Y} p(y) \cdot H(X|y) = -\sum_{y \in Y} \sum_{x \in X} p(x, y) \cdot \log(p(x|y)).$$

For sets X, Y, and Z the conditional mutual information is defined as

$$I(X; Y|Z) = \sum_{x \in X} \sum_{y \in Y} \sum_{z \in Z} p(x, y, z) \cdot \log\left(\frac{p(x|y, z)}{p(x|z)}\right).$$

It can be interpreted as the average amount of information about $x \in X$ that is given away by the event $Y = y$ when the event $Z = z$ has been observed. From the definition of the mutual information it follows that

$$I(X; Y|Z) = I(Y; X|Z)$$

and

$$I(X; Y|Z) = H(X|Z) - H(X|Y, Z).$$

2. A Model for Authentication

Throughout this paper we use the following notation. The set of messages that encode any source state under an encoding rule $e \in E$ is denoted by $M(e)$. Given a sequence of messages $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^i$, we denote by $E(\mathbf{m}^i)$ the set of encoding rules under which all messages of $\mathbf{m}^i$ can occur, i.e., for all $e \in E(\mathbf{m}^i)$ it is $\{m_1, \ldots, m_i\} \subseteq M(e)$. For an encoding rule $e \in E$ and a natural number i, we define the map f_e:

$$f_e\colon M^i \to S^i \cup \{0\},$$

$$f_e(m_1, \ldots, m_i) = \begin{cases} (s_1, \ldots, s_i) & \text{if there are } s_j \in S \text{ with } e(s_j) = m_j \text{ for } 1 \le j \le i, \\ 0, & \text{otherwise.} \end{cases}$$

If the messages of a sequence $\mathbf{m}^i$ can occur under the encoding rule e, i.e., $e \in E(\mathbf{m}^i)$, the sequence $\mathbf{m}^i$ is decoded to the sequence $f_e(\mathbf{m}^i)$ of source states.

In authentication systems as described above the following problem arises. If the receiver gets a particular message twice he cannot decide if the message was sent by the transmitter or repeated by an opponent. So, if the transmitter wants to communicate a source state twice under the same encoding rule an authentication system without splitting does not provide any security. In an authentication system with splitting, he could use another message to encode the source state. To ensure that no message is repeated we must impose that, for each source state and encoding rule, there are enough messages and that the splitting strategy always yields different messages. Hence splitting does not seem to be an appropriate means of solving the problem. For these reasons we assume that no source state is communicated twice and that the receiver does not accept any message, which is the encoding of any source state already sent before.

Furthermore, we assume that the receiver accepts only those sequences of messages that occur under the chosen encoding rule. To describe this formally we define the function γ in the following way:

$$\gamma\colon E \times M \times M^i \to \{0, 1\},$$

$$\gamma(e, n, \mathbf{m}^i) = \begin{cases} 1 & \text{if } \ e \in E(n, \mathbf{m}^i), \ \ f_e(n) \notin f_e(\mathbf{m}^i), \ \text{ and all} \\ & \text{source states of the sequence } f_e(\mathbf{m}^i) \text{ are different,} \\ 0, & \text{otherwise.} \end{cases}$$

If e is the encoding rule the transmitter and receiver agreed upon and $\mathbf{m}^i$ is a sequence of messages sent by the transmitter, the receiver accepts the message n if and only if $\gamma(e, n, \mathbf{m}^i) = 1$. For a sequence of messages $\mathbf{m}^i$ not valid under the encoding rule e there is $\gamma(e, n, \mathbf{m}^i) = 0$ for all messages n.

There will be a probability distribution on the sequences of source states. For any natural number $i \ge 2$ and any sequence of source states $(s_1, \ldots, s_i) \in S^i$ we denote by $p(s_i | s_1, \ldots, s_{i-1})$ the conditional probability that s_i is the source state being communicated immediately after the sequence $(s_1, \ldots, s_{i-1}) \in S^{i-1}$. Thus the probability of the sequence $\mathbf{s}^i = (s_1, \ldots, s_i) \in S^i$ is given by

$$p(\mathbf{s}^i) = p(s_1, \ldots, s_i) = p(s_i | s_1, \ldots, s_{i-1}) \cdot p(s_1, \ldots, s_{i-1}).$$

By our assumption, for any sequence $(s_1, \ldots, s_i) \in S^i$ of source states with $s_i \in \{s_1, \ldots, s_{i-1}\}$ we have that $p(s_1, \ldots, s_i) = 0$.

Given the probability distribution on the sequences of source states, the transmitter and receiver will determine a probability distribution p on E, called the encoding strategy. If splitting occurs, then they will also determine a probability distribution (called the splitting strategy) to get a message, given a source state and an encoding rule. After selection of the encoding strategy and the splitting strategy, they are independent of the probability distribution of the sequences of source states. Throughout this paper we assume that all encoding rules have a positive probability, i.e., $p(e) \neq 0$ for all $e \in E$.

Given the probability functions on the sequences of source states and the set of encoding rules, and the splitting strategy we can calculate the pobability of a sequence of messages $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^i$. Using $\sum_{e \in E} p(e|\mathbf{m}^i) = 1$ we have

$$\begin{aligned} p(\mathbf{m}^i) &= p(\mathbf{m}^i) \cdot \sum_{e \in E} p(e|\mathbf{m}^i) \\ &= \sum_{e \in E} p(e, \mathbf{m}^i) \\ &= \sum_{e \in E} p(\mathbf{m}^i|e) \cdot p(e). \end{aligned}$$

Note that if the sequence $\mathbf{m}^i$ cannot occur under the encoding rule e, i.e., $e \notin E(\mathbf{m}^i)$, we have $p(\mathbf{m}^i|e) = 0$. Thus, in the expression for $p(\mathbf{m}^i)$ we can restrict the summation to $E(\mathbf{m}^i)$. If $e \in E(\mathbf{m}^i)$ and no splitting occurs, then $p(\mathbf{m}^i|e) = p(f_e(\mathbf{m}^i))$. With splitting we have $p(\mathbf{m}^i|e) = p(f_e(\mathbf{m}^i)) \cdot p(\mathbf{m}^i|f_e(\mathbf{m}^i), e)$, where $p(\mathbf{m}^i|f_e(\mathbf{m}^i), e)$ depends on the splitting strategy being used. We denote by $p(m|\mathbf{m}^i)$ the probability that the transmitter sends the message m immediately after the sequence $\mathbf{m}^i$. Thus we have $p(\mathbf{m}^i, m) = p(m|\mathbf{m}^i) \cdot p(\mathbf{m}^i)$, where $p(\mathbf{m}^i, m)$ denotes the probability of the sequence $(\mathbf{m}^i, m) = (m_1, \ldots, m_i, m) \in M^{i+1}$. Note that $p(\mathbf{m}^i, m)$ and $p(m, \mathbf{m}^i)$ denote different probabilities, namely, the probabilities of the sequences $(\mathbf{m}^i, m) = (m_1, \ldots, m_i, m)$ and $(m, \mathbf{m}^i) = (m, m_1, \ldots, m_i)$.

In the following we describe precisely how the opponent tries to cheat. As mentioned above, after observation of a sequence of messages he can play substitution or impersonation. We assume that the opponent is successful if the receiver accepts the fraudulent message as authentic and, in the case of substitution, is misled as to the state of the source.

Let e be the actual encoding rule and let $\mathbf{m}^i$ be a sequence of messages already sent by the transmitter. Assume that he now sends the message m. If, after having observed $\mathbf{m}^i$ and m, the opponent plays impersonation, he sends his message n after m. The receiver accepts n if n is a possible message under the encoding rule, i.e., $n \in M(e)$, and no source state is repeated, i.e., $f_e(n) \notin f_e(\mathbf{m}^i, m)$. If the opponent plays substitution he substitutes the message m, sent by the transmitter, by his own message n. He is sucessful if the receiver accepts n, i.e., if $n \in M(e)$, and $f_e(n) \notin f_e(\mathbf{m}^i)$, and the receiver is misled as to the state of the source, i.e., $f_e(n) \neq f_e(m)$. Thus, by our rules there is no difference in the acceptance of the message if the opponent plays impersonation or substitution. Therefore, we do not distinguish these two ways of cheating.

The probability that after observation of $\mathbf{m}^i$ the opponent is successful in substituting m is denoted by payoff$(m, \mathbf{m}^i)$. It can be calculated as follows. The probability that the encoding rule e is the actual chosen encoding rule is $p(e|\mathbf{m}^i)$. The opponent is successful if the receiver accepts the message m, i.e., if $\gamma(e, m, \mathbf{m}^i) = 1$. Hence, we have

$$\text{payoff}(m, \mathbf{m}^i) = \sum_{e \in E} p(e|\mathbf{m}^i) \cdot \gamma(e, m, \mathbf{m}^i) = \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i) \cdot \gamma(e, m, \mathbf{m}^i),$$

because $\gamma(e, m, \mathbf{m}^i) = 0$ for all $e \notin E(m, \mathbf{m}^i)$. If m is a message that could be sent after $\mathbf{m}^i$ by the transmitter (that is $p(m|\mathbf{m}^i) \neq 0$), then the probability that the opponent is successful if he sends m is $\text{payoff}(m, \mathbf{m}^i) \neq 0$.

We describe the strategy of the opponent by a probability distribution. The probability that he selects a message m given that he has observed $\mathbf{m}^i$ using strategy q is denoted by $q(m|\mathbf{m}^i)$. The probability that, after observation of $\mathbf{m}^i$, he is successful using strategy q is $\sum_{m \in M} q(m|\mathbf{m}^i) \cdot \text{payoff}(m, \mathbf{m}^i)$. Let $p_i(q)$ be the expected value of the probability that he is successful after observation of i messages. Then

$$p_i(q) = \sum_{\mathbf{m}^i \in M^i} p(\mathbf{m}^i) \sum_{m \in M} q(m|\mathbf{m}^i) \cdot \text{payoff}(m, \mathbf{m}^i).$$

By $p_i(\mathbf{m}^i)$ we denote the maximum probability that the opponent is successful given that he has observed $\mathbf{m}^i$, where the maximum is taken over all strategies. By p_i we denote the expected value of $p_i(\mathbf{m}^i)$. Thus, we have

$$p_i = \sum_{\mathbf{m}^i \in M^i} p(\mathbf{m}^i) \cdot p_i(\mathbf{m}^i).$$

We call a strategy q *optimal* if $p_i(q) = p_i$.

Lemma 2.1. *Let $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$. Then, for each $m \in M$, we have*

$$p_i(\mathbf{m}^i) \geq \text{payoff}(m, \mathbf{m}^i).$$

Proof. Choose $m_0 \in M$ and define a strategy q' by $q'(m|\mathbf{m}^i) = 1$ if $m = m_0$, and by $q'(m|\mathbf{m}^i) = 0$ otherwise. Because we have defined $p_i(\mathbf{m}^i)$ to be the maximum value, we have

$$p_i(\mathbf{m}^i) \geq \sum_{m \in M} q'(m|\mathbf{m}^i) \cdot \text{payoff}(m, \mathbf{m}^i) = \text{payoff}(m_0, \mathbf{m}^i). \qquad \square$$

3. A Lower Bound for p_i

In this section we prove our main result, namely, a lower bound for the probability of success after having observed a sequence of i messages.

For the proof of the theorem we need the following result.

Theorem (Jensen's Inequality). *Let $w_i \in [0, 1]$, $i \in I = \{1, \dots, n\}$, n is some integer, with $\sum_{i \in I} w_i = 1$. If φ is a real function which is convex (i.e., $\varphi'(s) < \varphi'(t)$ for all $a < s < t < b$) on the interval (a, b) and $x_i \in (a, b)$, $i \in I$, then*

$$\varphi\left(\sum_{i \in I} w_i \cdot x_i\right) \leq \sum_{i \in I} w_i \cdot \varphi(x_i).$$

Equality holds if and only if all x_i, $i \in I$, are equal.

This inequality will be applied to the functions $\varphi(x) = -\log(x)$ and $\varphi(x) = x \cdot \log(x)$, which are convex for $x > 0$.

In order to simplify the following statements and proofs, we denote by M_0 the empty sequence. We define $p(M_0) = 1$ and the joint probability $p(x, M_0) = p(x)$. Thus, we get $p(M_0|x) = 1$ and $p(x|M_0) = p(x)$.

Theorem 3.1. *Let A be an authentication system and let p_i be the maximal probability of deception after observation of i messages. Then*

$$p_i \geq 2^{H(E|M^{i+1})-H(E|M^i)} = 2^{-I(E;M|M^i)}.$$

Moreover, equality holds if and only if, for all $\mathbf{m}^i \in M^i$ with $p(\mathbf{m}^i) \neq 0$ and all $m \in M$ with $p(m|\mathbf{m}^i) \neq 0$, the following conditions are satisfied:

(a) *The probability payoff$(m, \mathbf{m}^i)$ that m is accepted as authentic if $\mathbf{m}^i$ was observed satisfies $p_i = \text{payoff}(m, \mathbf{m}^i)$.*

(b) *The conditional probability $p(m|e, \mathbf{m}^i)$ that m is the next message sent by the transmitter, given that e is the actual encoding rule and the sequence $\mathbf{m}^i$ has already been sent, is constant for all $e \in E(m, \mathbf{m}^i)$.*

Proof. From the definition of the conditional mutual information we have

$$I(E; M|M^i) = H(E|M^i) - H(E|M^{i+1}) = H(M|M^i) - H(M|E, M^i).$$

Thus, it is sufficient to show

$$\log(p_i) \geq H(M|E, M^i) - H(M|M^i).$$

Let $\mathbf{m}^i \in M^i$ be a sequence of messages with $p(\mathbf{m}^i) \neq 0$, and let $m \in M$ be a message with $p(m|\mathbf{m}^i) \neq 0$. In the first step of the proof we show the following inequality:

$$p(m|\mathbf{m}^i)\cdot\log(p(m|\mathbf{m}^i)) \leq \sum_{e \in E(m, \mathbf{m}^i)} p(e, m|\mathbf{m}^i)\cdot\log(\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)), \quad (1)$$

which is fundamental for the proof of the theorem.

From $p(m|\mathbf{m}^i) \neq 0$ it follows that $E(m, \mathbf{m}^i) \neq \emptyset$ and $\text{payoff}(m, \mathbf{m}^i) \neq 0$. Thus we can define a probability distribution $\psi_{m,\mathbf{m}^i}$ on the encoding rules $E(m, \mathbf{m}^i)$ by

$$\psi_{m,\mathbf{m}^i}(e) := \frac{p(e|\mathbf{m}^i)\cdot\gamma(e, m, \mathbf{m}^i)}{\text{payoff}(m, \mathbf{m}^i)}.$$

Because $\text{payoff}(m, \mathbf{m}^i) = \sum_{e \in E(m,\mathbf{m}^i)} p(e|\mathbf{m}^i)\cdot\gamma(e, m, \mathbf{m}^i)$ then $\sum_{e \in E(m,\mathbf{m}^i)} \psi_{m,\mathbf{m}^i}(e) = 1$, thus $\psi_{m,\mathbf{m}^i}$ is a probability distribution.

We use $\gamma(e, m, \mathbf{m}^i) = 1$ if $p(m|e, \mathbf{m}^i) \neq 0$, in order to rewrite the conditional probability $p(m|\mathbf{m}^i)$ as

$$\begin{aligned} p(m|\mathbf{m}^i) &= \sum_{e \in E(m,\mathbf{m}^i)} p(e, m|\mathbf{m}^i) \\ &= \sum_{e \in E(m,\mathbf{m}^i)} p(e|\mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i) \\ &= \sum_{e \in E(m,\mathbf{m}^i)} p(e|\mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)\cdot\gamma(e, m, \mathbf{m}^i). \end{aligned}$$

By the definition of $\psi_{m,\mathbf{m}^i}$, we get

$$p(m|\mathbf{m}^i) = \sum_{e \in E(m,\mathbf{m}^i)} \psi_{m,\mathbf{m}^i}(e)\cdot\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i).$$

Using Jensen's inequality for $\varphi(x) = x\cdot\log(x)$ at $x = p(m|\mathbf{m}^i) = \sum_{e \in E(m,\mathbf{m}^i)} w_e \cdot x_e$

with $w_e = \psi_{m,\mathbf{m}^i}(e)$, and $x_e = \text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)$, we have

$$\begin{aligned} p(m|\mathbf{m}^i)\cdot\log(p(m|\mathbf{m}^i)) &\le \sum_{e\in E(m,\mathbf{m}^i)} \psi_{m,\mathbf{m}^i}(e)\cdot(\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)) \\ &\quad\cdot\log(\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)) \\ &= \sum_{e\in E(m,\mathbf{m}^i)} p(e, m|\mathbf{m}^i)\cdot\log(\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)), \end{aligned}$$

by the definition of $\psi_{m,\mathbf{m}^i}$. This shows (1).

In the second step of the proof we show, for $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, the inequality

$$H(M|\mathbf{m}^i) \ge -\log(p_i(\mathbf{m}^i)) + H(M|E, \mathbf{m}^i).$$

By definition of $H(M|\mathbf{m}^i)$ and use of inequality (1) we get

$$\begin{aligned} H(M|\mathbf{m}^i) &= -\sum_{m\in M} p(m|\mathbf{m}^i)\cdot\log(p(m|\mathbf{m}^i)) \\ &\ge -\sum_{m\in M}\sum_{e\in E(m,\mathbf{m}^i)} p(e, m|\mathbf{m}^i)\cdot\log(\text{payoff}(m, \mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)) \\ &= -\sum_{m\in M} p(m|\mathbf{m}^i)\cdot\log(\text{payoff}(m, \mathbf{m}^i)) \\ &\quad -\sum_{m\in M}\sum_{e\in E(m,\mathbf{m}^i)} p(e|\mathbf{m}^i)\cdot p(m|e, \mathbf{m}^i)\cdot\log(p(m|e, \mathbf{m}^i)). \end{aligned}$$

Now we use the definition of $H(M|E, \mathbf{m}^i)$ and get

$$H(M|\mathbf{m}^i) \ge -\sum_{m\in M} p(m|\mathbf{m}^i)\cdot\log(\text{payoff}(m, \mathbf{m}^i)) + H(M|E, \mathbf{m}^i).$$

By Lemma 2.1, $p_i(\mathbf{m}^i) \ge \text{payoff}(m, \mathbf{m}^i)$. Thus we have

$$\begin{aligned} H(M|\mathbf{m}^i) &\ge -\log(p_i(\mathbf{m}^i))\cdot\sum_{m\in M} p(m|\mathbf{m}^i) + H(M|E, \mathbf{m}^i) \qquad (2) \\ &= -\log(p_i(\mathbf{m}^i)) + H(M|E, \mathbf{m}^i). \end{aligned}$$

Hence, we have shown the second step.

In the third step we eventually show the inequality for p_i. By definition of p_i and using Jensen's inequality for $\varphi(x) = -\log(x)$ we get

$$\log(p_i) = \log\left(\sum_{\mathbf{m}^i\in M^i} p(\mathbf{m}^i)\cdot p_i(\mathbf{m}^i)\right) \ge \sum_{\mathbf{m}^i\in M^i} p(\mathbf{m}^i)\cdot\log(p_i(\mathbf{m}^i)). \qquad (3)$$

The lower bound of $\log(p_i(\mathbf{m}^i))$ proved in step 2 yields

$$\sum_{\mathbf{m}^i\in M^i} p(\mathbf{m}^i)\cdot\log(p_i(\mathbf{m}^i)) \ge \sum_{\mathbf{m}^i\in M^i} p(\mathbf{m}^i)\cdot(H(M|E, \mathbf{m}^i) - H(M|\mathbf{m}^i)).$$

Together we get

$$\log(p_i) \ge \sum_{\mathbf{m}^i\in M^i} p(\mathbf{m}^i)\cdot(H(M|E, \mathbf{m}^i) - H(M|\mathbf{m}^i)) = H(M|E, M^i) - H(M|M^i),$$

using the definition of $H(M|E, M^i)$ and $H(M|M^i)$.

This shows the first statement of the theorem.

We have $\log(p_i) = H(M|E, M^i) - H(M|M^i)$ if and only if equality is attained in inequalities (1)–(3) used in the proof. Thus, equality holds if and only if the following conditions are satisfied for each $\mathbf{m}^i \in M^i$ with $p(\mathbf{m}^i) \neq 0$:

(1) For each $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$, $\text{payoff}(m, \mathbf{m}^i) \cdot p(m|e, \mathbf{m}^i)$ is a constant for all $e \in E(m, \mathbf{m}^i)$.

(2) For each $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$,

$$\text{payoff}(m, \mathbf{m}^i) = p_i(\mathbf{m}^i).$$

(3) The probability $p_i(\mathbf{m}^i)$ is constant.

These conditions are equivalent to the following claim:

For each $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$, the following conditions hold:

(a) The probability $\text{payoff}(m, \mathbf{m}^i)$ that m is accepted as authentic, given that $\mathbf{m}^i$ has been observed, is $\text{payoff}(m, \mathbf{m}^i) = p_i$.

(b) The conditional probability $p(m|e, \mathbf{m}^i)$ is constant for all $e \in E(m, \mathbf{m}^i)$. □

There are authentication systems which reach the bound proved in Theorem 3.1. The authentication systems, constructed in Chapters 6 and 7 of [4], based on t-$(v, k, 1)$ Steiner systems and transversal designs $\text{TD}_\lambda(t, k, n)$ reach the bound for all $i \in \{0, \ldots, t-1\}$, if all sequences of different source state of length $\leq t$ are equally probable. The authentication systems, constructed in Theorem 3.3 of [17] based on authentication perpendicular arrays $\text{APA}_\lambda(t, k, v)$ also reach the bound for all $i \in \{0, \ldots, t-1\}$, if all sequences of different source state of length $\leq t$ are equally probable. The authentication systems, constructed in Theorem 5.3 of [17], based on tranversal designs $\text{TD}_\lambda(t, k, n)$ reach the bound for all $i \in \{0, \ldots, t-1\}$. These authentication systems are Cartesian and have no splitting; hence, condition (b) for equality in Theorem 3.1 is true for any distribution of the source states.

Remarks. 1. The probability of success p_i after having observed a sequence of i messages does not depend on the probability $p(m|e, \mathbf{m}^i)$ that m is the next message sent by the transmitter, given that e is the actual encoding rule and $\mathbf{m}^i$ has been observed. However, in the theorem proved above, the lower bound does depend on this probability.

For this reason our result can be generalized as follows. Consider a probability distribution $p^*(e, m, \mathbf{m}^i)$ that satisfies the following conditions:

— p^* matches the actual joint distribution of the encoding rules and the sequences of i messages, that is

$$p^*(e, \mathbf{m}^i) = p(e, m^i)$$

for all $e \in E$ and $\mathbf{m}^i \in M^i$.

— If $\gamma(e, m, \mathbf{m}^i) = 0$, then $p^*(e, m, \mathbf{m}^i) = 0$ also.

Given that e is the actual encoding rule and $\mathbf{m}^i$ has been observed, there is a probability function $p^*(s|f_e(\mathbf{m}^i))$ and, for $m \in M(e)$, a splitting strategy $p^*(m|f_e(m), e, \mathbf{m}^i)$ such that $p^*(m|e, \mathbf{m}^i)$ is the resulting probability function of the next message.

We denote by $I(E; M^*|M^i)$ the conditional mutual information with respect to the probability distribution p^*. Because p^* satisfies the above conditions, we can substitute p by p^* in the whole proof of Theorem 3.1. Hence it also follows that

$$p_i \geq 2^{-I(E;M^*|M^i)}.$$

Equality holds if and only if, for all $\mathbf{m}^i \in M^i$ with $p^*(\mathbf{m}^i) = p(\mathbf{m}^i) \neq 0$ and all $m \in M$ with $p^*(m|\mathbf{m}^i) \neq 0$, the following conditions are satisfied:

(a) The probability payoff$(m, \mathbf{m}^i)$ that m is accepted as authentic if $\mathbf{m}^i$ was observed satisfies $p_i = \text{payoff}(m, \mathbf{m}^i)$.

(b) The conditional probability $p^*(m|e, \mathbf{m}^i)$ is constant for all $e \in E(m, \mathbf{m}^i)$.

If we take the infimum of $I(E; M^*|M^i)$ over all probability distributions satisfying the above conditions, we get

$$p_i \geq 2^{-\inf I(E;M^*|M^i)}.$$

2. In [14] Simmons and Smeets have introduced a model of authentication systems that can be used without the constraint that source states cannot be repeated. In addition to an "ordinary" authentication system a set K of *keys* and a (not secret) *scheduling function* f: $K \times N \to E$ is required. Prior to transmission, a secret key k is chosen. Using k, an encoding rule $e_i = f(k, i)$ for the transmission of the ith source state is selected by the scheduling function. By E_i we denote the subset of encoding rules that could be used for the transmission of the ith source state.

In these sequential authentication systems (see [15]) the probability of deception using an impersonation attack or a substitution attack is (in general) different. With the same proof as for Theroem 3.1 it can be shown that a similar bound holds. For a substitution attack we have

$$p_{Si} \geq 2^{-I(E_i;M^*|M^i)} = 2^{-I(K;M^*|M^i)};$$

similarly for an impersonation attack we have

$$p_{Ii} \geq 2^{-I(E_{i+1};M^*|M^i)} = 2^{-I(K;M^*|M^i)}.$$

These inequalities have also been shown in [15].

Corollary 3.2. *Let A be an authentication system for which $p_i = 2^{-I(E;M|M^i)}$ holds, i is a nonnegative integer. Then, for all $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and for all $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$, we have*:

(i) *The conditional probability $p(m|e, \mathbf{m}^i)$ is a positive constant for all $e \in E(m, \mathbf{m}^i)$.*

(ii) *The probability* payoff$(m, \mathbf{m}^i)$ *that m is accepted as authentic, given that $\mathbf{m}^i$ has been observed, is*

$$\text{payoff}(m, \mathbf{m}^i) = \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i).$$

(iii) *The conditional probability $p(e|\mathbf{m}^i, m)$ satisfies*

$$p(e|\mathbf{m}^i, m) = \frac{p(e|\mathbf{m}^i)}{\sum_{j \in E(\mathbf{m}^i, m)} p(j|\mathbf{m}^i)}.$$

Proof. Let $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$.

(i) By Theorem 3.1 $p(m|e, \mathbf{m}^i)$ is constant for all $e \in E(m, \mathbf{m}^i)$. Since

$$\sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i) \cdot p(m|e, \mathbf{m}^i) = p(m|\mathbf{m}^i) \neq 0,$$

the conditional probability $p(m|e, \mathbf{m}^i)$ is a positive constant.

(ii) For all $e \in E(m, \mathbf{m}^i)$, it follows that $\gamma(e, m, \mathbf{m}^i) = 1$ from $p(m|e, \mathbf{m}^i) \neq 0$. Thus payoff$(m, \mathbf{m}^i) = \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i)$.

(iii) By $\mathbf{m}^{i+1}$ we denote the sequence $(\mathbf{m}^i, m)$ of messages. The joint probability $p(e, \mathbf{m}^{i+1})$ can be written as

$$p(e, \mathbf{m}^{i+1}) = p(e|\mathbf{m}^{i+1}) \cdot p(\mathbf{m}^{i+1})$$

and

$$p(e, \mathbf{m}^{i+1}) = p(m|e, \mathbf{m}^i) \cdot p(e, \mathbf{m}^i) = p(m|e, \mathbf{m}^i) \cdot p(e|\mathbf{m}^i) \cdot p(\mathbf{m}^i).$$

Together we have

$$p(e|\mathbf{m}^{i+1}) = \frac{p(m|e, \mathbf{m}^i) \cdot p(e|\mathbf{m}^i) \cdot p(\mathbf{m}^i)}{p(\mathbf{m}^{i+1})}.$$

The probability of the sequence $\mathbf{m}^{i+1}$ can be expressed as

$$p(\mathbf{m}^{i+1}) = \sum_{j \in E(\mathbf{m}^{i+1})} p(j, \mathbf{m}^{i+1}) = \sum_{j \in E(\mathbf{m}^{i+1})} p(m|j, \mathbf{m}^i) \cdot p(j|\mathbf{m}^i) \cdot p(\mathbf{m}^i),$$

so

$$p(e|\mathbf{m}^{i+1}) = \frac{p(m|e, \mathbf{m}^i) \cdot p(e|\mathbf{m}^i) \cdot p(\mathbf{m}^i)}{\sum_{j \in E(\mathbf{m}^{i+1})} p(m|j, \mathbf{m}^i) \cdot p(j|\mathbf{m}^i) \cdot p(\mathbf{m}^i)}.$$

By hypothesis it follows from (i) that $p(m|j, \mathbf{m}^i)$ is a positive constant for all $j \in E(\mathbf{m}^{i+1})$. Because $p(m|j, \mathbf{m}^i)$ is constant, and the fact that $p(\mathbf{m}^i)$ is independent from j, we can cancel these terms in the above expression for $p(e|\mathbf{m}^{i+1})$. Hence,

$$p(e|\mathbf{m}^{i+1}) = \frac{p(e|\mathbf{m}^i)}{\sum_{j \in E(\mathbf{m}^{i+1})} p(j|\mathbf{m}^i)}. \qquad \square$$

In the following we consider authentication systems that reach the bound for the probability of success p_i, proved in Theorem 3.1, for all $i \in \{0, \ldots, l\}$, where l is some nonnegative integer. The next lemma says in particular that, under the equality assumption, the conditional probability $p(e|\mathbf{m}^{i+1})$ does not depend on the probability $p(f_e(\mathbf{m}^{i+1}))$ of the corresponding source states.

Lemma 3.3. *Let A be an authentication system for which $p_i = 2^{-I(E; M|M^i)}$ holds for all $i \in \{0, \ldots, l\}$, l is a nonnegative integer. Then, for $i \in \{1, \ldots, l+1\}$ for all $\mathbf{m}^i \in M^i$, with $p(m^i) \neq 0$, and all $e \in E(\mathbf{m}^i)$, we have*

$$p(e|\mathbf{m}^i) = \frac{p(e)}{\sum_{j \in E(\mathbf{m}^i)} p(j)}$$

and

$$\sum_{e \in E(\mathbf{m}^i)} p(e) = p_0 \times \cdots \times p_{i-1}.$$

Furthermore, $p(\mathbf{m}^i|e)$ is a positive constant for all $e \in E(\mathbf{m}^i)$.

Proof. Let $i \in \{0, \ldots, l\}$, let $\mathbf{m}^{i+1} = (m_1, \ldots, m_i, m_{i+1}) \in M^{i+1}$ be a sequence of messages with $p(\mathbf{m}^{i+1}) \neq 0$, and let $e \in E(\mathbf{m}^{i+1})$. If $\mathbf{m}^i = (m_1, \ldots, m_i)$, then $0 \neq p(\mathbf{m}^{i+1}) = p(m_i|\mathbf{m}^i) \cdot p(\mathbf{m}^i)$ and so we have $p(\mathbf{m}^i) \neq 0$ and $p(m_{i+1}|\mathbf{m}^i) \neq 0$.

Using Corollary 3.2 we express $p(e|\mathbf{m}^{i+1})$ in terms of $p(j|\mathbf{m}^i)$ with $j \in E(\mathbf{m}^{i+1})$:

$$p(e|\mathbf{m}^{i+1}) = \frac{p(e|\mathbf{m}^i)}{\sum_{j \in E(\mathbf{m}^{i+1})} p(j|\mathbf{m}^i)}.$$

For $i = 0$ we have $p(e|\mathbf{m}^0) = p(e)$, so, with $\mathbf{m}^1 = (m)$, we get

$$p(e|m) = \frac{p(e)}{\sum_{j \in E(m)} p(j)}.$$

Suppose that, for an $i < l$, we have shown that $p(e|\mathbf{m}^i) = p(e)/\sum_{e' \in E(\mathbf{m}^i)} p(e')$ for all $e \in E(\mathbf{m}^i)$. Because $E(\mathbf{m}^{i+1}) \subseteq E(\mathbf{m}^i)$,

$$p(e|\mathbf{m}^{i+1}) = \frac{p(e|\mathbf{m}^i)}{\sum_{j \in E(\mathbf{m}^{i+1})} p(j|\mathbf{m}^i)} = \frac{p(e)/\sum_{e' \in E(\mathbf{m}^i)} p(e')}{\sum_{j \in E(\mathbf{m}^{i+1})} p(j)/\sum_{e' \in E(\mathbf{m}^i)} p(e')};$$

canceling $\sum_{e' \in E(\mathbf{m}^i)} p(e')$ we get

$$p(e|\mathbf{m}^{i+1}) = \frac{p(e)}{\sum_{j \in E(\mathbf{m}^{i+1})} p(j)}.$$

This proves the first assertion of the lemma.

By Corollary 3.2, $p_i = \text{payoff}(m_{i+1}, \mathbf{m}^i) = \sum_{e \in E(m_{i+1}, \mathbf{m}^i)} p(e|\mathbf{m}^i)$. Thus, for $i = 0$, we get

$$p_0 = \text{payoff}(m) = \sum_{e \in E(m)} p(e).$$

Now suppose that, for $i, i < l$, we have shown $\sum_{e \in E(\mathbf{m}^i)} p(e) = p_0 \times \cdots \times p_{i-1}$. From $p_i = \text{payoff}(m_{i+1}, m^i) = \sum_{e \in E(m_{i+1}, \mathbf{m}^i)} p(e|\mathbf{m}^i)$ and the above expression for $p(e|\mathbf{m}^i)$ we get

$$p_i = \frac{\sum_{e \in E(m_{i+1}, \mathbf{m}^i)} p(e)}{\sum_{e \in E(\mathbf{m}^i)} p(e)}.$$

Replacing $\sum_{e \in E(\mathbf{m}^i)} p(e)$ by $p_0 \times \cdots \times p_{i-1}$ yields

$$\sum_{e \in E(m_{i+1}, \mathbf{m}^i)} p(e) = p_0 \times \cdots \times p_i.$$

Now let $i \in \{1, \ldots, l+1\}$, let $\mathbf{m}^i \in M^i$ with $p(\mathbf{m}^i) \neq 0$, and let $e \in E(\mathbf{m}^i)$. Using the formulas proved above for $p(e|\mathbf{m}^i)$ and $\sum_{e \in E(\mathbf{m}^i)} p(e)$ we get

$$\begin{aligned} p(\mathbf{m}^i|e) &= \frac{p(\mathbf{m}^i) \cdot p(e|\mathbf{m}^i)}{p(e)} \\ &= \frac{p(\mathbf{m}^i)}{p(e)} \cdot \frac{p(e)}{\sum_{j \in E(\mathbf{m}^i)} p(j)} \\ &= \frac{p(\mathbf{m}^i)}{p_0 \times \cdots \times p_{i-1}}. \end{aligned}$$

Since this is independent of e and $p(\mathbf{m}^i) \neq 0$ the conditional probability $p(\mathbf{m}^i|e)$ is a positive constant for all $e \in E(\mathbf{m}^i)$. □

In the next lemma we prove a simple formula for the probability p_i of success under the assumption that the encoding rules are equally probable or that the conditional entropy $H(E|M^{l+1})$ is zero. In the latter case it also follows that the encoding rules must be equally probable.

Lemma 3.4. *Let A be an authentication system in which $p_i = 2^{-I(E;M|M^i)}$ holds for all $i \in \{0, \dots, l\}$, and where l is a nonnegative integer. Suppose furthermore that either*

(a) *the encoding rules are equally probable, or*
(b) $H(E|M^{l+1}) = 0$.

Then, for each $i \in \{1, \dots, l+1\}$, the number of encoding rules $|E(\mathbf{m}^i)|$ is constant for all $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and

$$p_i = \frac{|E(\mathbf{m}^{i+1})|}{|E(\mathbf{m}^i)|}$$

for $i = 0, \dots, l$. Moreover, if $H(E|M^{l+1}) = 0$, for any $e \in E$,

$$p(e) = p_0 \times \cdots \times p_l,$$

i.e., the encoding rules are equally probable.

Proof. (a) For an $i \in \{0, \dots, l\}$ consider an $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and an $m \in M$, with $p(m|\mathbf{m}^i) \neq 0$. From $p_i = 2^{-I(E;M|M^i)}$ it follows, using Corollary 3.2, that

$$p_i = \text{payoff}(m, \mathbf{m}^i) = \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i).$$

By hypothesis the encoding rules are equally probable so $p(e)$ is constant for all $e \in E$. Thus, we can cancel $p(e)$ in the expression for $p(e|\mathbf{m}^i)$ derived in Lemma 3.3 and get

$$p(e|\mathbf{m}^i) = \frac{p(e)}{\sum_{j \in E(\mathbf{m}^i)} p(j)} = \frac{1}{|E(\mathbf{m}^i)|}.$$

Together we have

$$p_i = \sum_{e \in E(m, \mathbf{m}^i)} \frac{1}{|E(\mathbf{m}^i)|} = \frac{|E(m, \mathbf{m}^i)|}{|E(\mathbf{m}^i)|}.$$

Since this is true for all $i \in \{0, \dots, l\}$, we get, for all $\mathbf{m}^{i+1} \in M^{i+1}$, with $p(\mathbf{m}^{i+1}) \neq 0$,

$$|E(\mathbf{m}^{i+1})| = p_0 \times \cdots \times p_i \cdot |E|,$$

in particular, $|E(\mathbf{m}^{i+1})|$ is constant.

(b) Suppose that $H(E|M^{l+1}) = 0$. Let $\mathbf{m}^{l+1} \in M^{l+1}$ and let $e \in E$, with $p(e, \mathbf{m}^{l+1}) \neq 0$. Because $H(E|M^{l+1}) = 0$, we have $p(e|\mathbf{m}^{l+1}) = 1$, therefore $E(\mathbf{m}^{l+1}) = \{e\}$.

Let $e \in E$ and let $\mathbf{s}^{l+1} \in S^{l+1}$ be a sequence of source states with $p(\mathbf{s}^{l+1}) \neq 0$. By $\mathbf{m}^{l+1}$ we denote the sequence of messages if $\mathbf{s}^{l+1}$ is encoded with e. By construction,

$p(e|\mathbf{m}^{l+1}) = 1$, therefore $E(\mathbf{m}^{l+1}) = \{e\}$ and so

$$\sum_{j \in E(\mathbf{m}^{l+1})} p(j) = p(e).$$

By Lemma 3.3,

$$\sum_{j \in E(\mathbf{m}^{l+1})} p(j) = p_0 \times \cdots \times p_l.$$

Together we have

$$p(e) = p_0 \times \cdots \times p_l.$$

Hence the encoding rules are equally probable. The rest follows from (a). □

4. Perfect Authentication Systems

In the last section we have obtained a lower bound of the probability of success for the opponent, if he has observed a sequence of $i \geq 0$ messages and if he uses an optimal strategy. In this section we turn our attention to the following scenario.

The opponent knows that the transmitter sends at most l messages encoded by the same encoding rule. Therefore, he can choose how many messages he wants to observe before he tries to cheat. We assume that he uses a strategy Q, i.e., a probability distribution Q on the set $\{0, \ldots, l\}$, to determine how many messages he shall observe. If $Q(i)$ denotes the probability that he observes i messages, then, according to the strategy q, he substitutes the ith message. The probability $P_l(Q, q)$ of success of this scenario can be calculated as

$$P_l(Q, q) = \sum_{i=1}^{l} Q(i) \cdot p_i(q).$$

We denote the maximum value of $P_l(Q, q)$ by P_l, where the maximum is taken over all strategies Q and q. We call the strategies Q and q *optimal* if $P_l(Q, q) = P_l$.

The following strategy Q^*, q^* is easily seen to be optimal. For each $i \in \{0, \ldots, l\}$ we choose an optimal strategy q^*, thus $p_i = p_i(q^*)$. Now we select a $j \in \{0, \ldots, l\}$ with $p_j \geq p_i$, for $0 \leq i \leq l$. Then we define $Q^*(j) = 1$ and $Q^*(i) = 0$ for $i \neq j$. Note that in order to choose this strategy, the opponent must be able to calculate the probabilities of success p_i.

In the following theorem we prove a lower bound for P_l and give necessary and sufficient conditions for the case of equality.

Theorem 4.1. *Let A be an authentication system, and let P_l be the probability of success after observation of at most l messages. Then*

$$P_l \geq 2^{-[1/(l+1)]H(E)}.$$

Equality holds if and only if the following conditions are satisfied:

(1) *The encoding rules are equally probable.*

(2) *For each $i \in \{1, \ldots, l+1\}$ for all $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, we have*

$$|E(\mathbf{m}^i)| = |E|^{(l+1-i)/(l+1)}.$$

(3) *For each* $i \in \{1, \ldots, l+1\}$ *for all* $\mathbf{m}^i \in M^i$, *with* $p(\mathbf{m}^i) \neq 0$, *the conditional probability* $p(\mathbf{m}^i | e)$ *is constant for all* $e \in E(\mathbf{m}^i)$.

Moreover, if equality holds, then

$$P_l = |E|^{-1/(l+1)}.$$

Proof. For simplification we write P instead of P_l. We show the inequality for a strategy Q^* with

$$P(Q^*) = \max\{p_0, \ldots, p_l\}.$$

By definition of P and Q^* we have $P \geq P(Q^*) \geq p_i$ for $i = 0, \ldots, l$. Using Theorem 3.1 we get

$$\begin{aligned} -\log(P^{l+1}) &\leq -\log(P(Q^*)^{l+1}) && \text{(a)} \\ &\leq -\log(p_0 \times p_1 \times \cdots \times p_l) && \text{(b)} \\ &\leq (H(E) - H(E|M)) + (H(E|M) - \mathrm{H}(E|M^2)) + \cdots \\ &\quad + (H(E|M^l) - H(E|M^{l+1})) && \text{(c)} \\ &= H(E) - H(E|M^{l+1}) \\ &\leq H(E), && \text{(d)} \end{aligned}$$

that is the first assertion of the theorem.

We have $-\log(P) = [1/(l+1)]H(E)$ if and only if equality holds in inequalities (a)–(d) used in the above proof. Hence equality holds if and only if the following conditions are satisfied:

(a) Q^* is an optimal strategy.

(b) For each $i \in \{0, \ldots, l\}$ the probability p_i of success after observation of exactly i messages is equal to P,

$$P = p_i.$$

(c) For each $i \in \{0, \ldots, l\}$ there is

$$-\log(p_i) = H(E|M^i) - H(E|M^{i+1}).$$

(d) The conditional entropy $H(E|M^{l+1})$ is equal to 0,

$$H(E|M^{l+1}) = 0,$$

that is, given that $l+1$ different messages have been observed, there is no equivocation about the encoding rule used.

We first show that (a)–(d) imply (1)–(3).

By (c) and (d), hypotheses (b) of Lemma 3.4 hold, so the encoding rules are equally probable. Hence, $H(E) = \log(|E|)$, so $\log(P) = -[1/(l+1)] \log(|E|)$. Also by Lemma 3.4, for all $\mathbf{m}^i \in M^i$, with $p(\mathbf{m}^i) \neq 0$, and $\mathbf{m}^{i+1} \in M^{i+1}$, with $p(\mathbf{m}^{i+1}) \neq 0$, we have

$$p_i = \frac{|E(\mathbf{m}^{i+1})|}{|E(\mathbf{m}^i)|}.$$

By (b), all p_i are all equal to P, so

$$\log(p_i) = -\frac{1}{l+1}\log(|E|).$$

Thus,

$$-\frac{1}{l+1}\log(|E|) = \log(p_i) = \log(|E(\mathbf{m}^{i+1})|) - \log(|E(\mathbf{m}^i)|). \qquad (*)$$

From $H(E|M^{l+1}) = 0$, for all $\mathbf{m}^{l+1} \in M^{l+1}$ with $p(\mathbf{m}^{l+1}) \neq 0$ it follows that $|E(\mathbf{m}^{l+1})| = 1$, thus

$$|E(\mathbf{m}^{l+1})| = |E|^{0/(l+1)}.$$

Suppose that we have shown

$$\frac{(l+1)-(i+1)}{l+1}\log(|E|) = \log(|E(\mathbf{m}^{i+1})|).$$

Using $(*)$ we obtain

$$\begin{aligned}\log(|E(\mathbf{m}^i)|) &= \frac{1}{l+1}\log(|E|) + \log(|E(\mathbf{m}^{i+1})|)\\ &= \frac{1}{l+1}\log(|E|) + \frac{(l+1)-(i+1)}{l+1}\log(|E|)\\ &= \frac{l+1-i}{l+1}\log(|E|).\end{aligned}$$

This shows statement (2).

In view of Lemma 3.4 we have that $p(\mathbf{m}^i|e)$ is a constant for all $e \in E(\mathbf{m}^i)$. This shows statement (3).

Finally we show that (a)–(d) follow from (1)–(3).

In order to do this we calculate the probability of success payoff$(m, \mathbf{m}^i)$, given that the opponent has observed a sequence $\mathbf{m}^i$ of i messages $(0 \leq i \leq l)$ and he substitutes a message m with $p(m|\mathbf{m}^i) \neq 0$. By (3) $p(\mathbf{m}^i, m|e)$ is constant for all $e \in E(m, \mathbf{m}^i)$. Since $p(\mathbf{m}^i, m) \neq 0$ by assumption, $p(\mathbf{m}^i, m|e)$ is positive, thus $\gamma(e, m, \mathbf{m}^i) = 1$ for all $e \in E(m, \mathbf{m}^i)$. Hence we have

$$\begin{aligned}\text{payoff}(m, \mathbf{m}^i) &= \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i)\\ &= \sum_{e \in E(m, \mathbf{m}^i)} \frac{p(\mathbf{m}^i|e)\cdot p(e)}{p(\mathbf{m}^i)}\\ &= \sum_{e \in E(m, \mathbf{m}^i)} \frac{p(\mathbf{m}^i|e)\cdot p(e)}{\sum_{e' \in E(\mathbf{m}^i)} p(\mathbf{m}^i|e')\cdot p(e')},\end{aligned}$$

because $p(\mathbf{m}^i) = \sum_{e' \in E(\mathbf{m}^i)} p(\mathbf{m}^i|e')\cdot p(e')$. By (1) all $p(e)$ are equal and by (3) each $p(\mathbf{m}^i|e)$ is constant for all $e \in E(\mathbf{m}^i)$. Thus we get

$$\text{payoff}(m, \mathbf{m}^i) = \frac{|E(m, \mathbf{m}^i)|}{|E(\mathbf{m}^i)|} = |E|^{-1/(l+1)}$$

using (2). By Theorem 3.1 this shows (c) and (b). Condition (d) follows from $|E(\mathbf{m}^{l+1})| = 1$ if $p(\mathbf{m}^{l+1}) \neq 0$. By definition, Q^* is an optimal strategy, so all is shown. □

For Cartesian authentication systems without splitting, this inequality has already been proved by Walker [18] using $P_l = \sum_{i=0}^{l} [1/(l+1)] p_i$. Generalizing his definition, we call an authentication system *l-perfect* if

$$P_l = 2^{-[1/(l+1)]H(E)},$$

that is, equality holds in the inequality proved in Theorem 4.1.

Note that in l-perfect authentication systems the encoding rules must be equally probable, so that we have $\log(P_l) = -[1/(l+1)] \cdot \log(|E|)$.

Examples of perfect authentication systems can be found in [17] and [9]. The authentication systems, constructed in Theorem 5.3 of [17] based on transversal design $\mathrm{TD}_\lambda(t, k, n)$ are $(t-1)$-perfect for $\lambda = 1$. The perfect authentication systems, constructed in Chapter 7 of [9] are based on Reed–Solomon Codes.

In the following we prove an upper bound on the number of source states in l-perfect authentication systems. In order to do this we first prove a more general result.

Lemma 4.2. *Let A be an authentication system and let l be a positive integer. If there is an encoding rule $e \in E$ and a sequence $\mathbf{s}^{l-1} = (s_1, \ldots, s_{l-1}) \in S^{l-1}$ of source states such that, for all $s, s' \in S \setminus \{s_1, \ldots, s_{l-1}\}$ with $s \neq s'$, the following conditions hold*:

(a) *The set of encoding rules $E(e(\mathbf{s}^{l-1}, s, s'))$, that is, the encoding rules that are possible under the sequence $e(\mathbf{s}^{l-1}, s, s')$ of messages, consists only of the encoding rule e.*

(b) *There is an integer $c > 1$ with $|E(e(\mathbf{s}^{l-1}, s))| \geq c$.*

Then the number of source states is restricted by

$$|S| \leq \frac{|E(e(\mathbf{s}^{l-1}))| - 1}{c - 1} + l - 1.$$

Proof. Let $e \in E$ and let $\mathbf{s}^{l-1} = \{s_1, \ldots, s_{l-1}\} \in S^{l-1}$ be such that conditions (a) and (b) hold. Then, for $s, s' \in S \setminus \{s_1, \ldots, s_{l-1}\}$ with $s \neq s'$, the intersection of $E(e(\mathbf{s}^{l-1}, s))$ and $E(e(\mathbf{s}^{l-1}, s'))$ consists only of e. Hence

$$\sum_{s \in S \setminus \{s_1, \ldots, s_{l-1}\}} |E(e(\mathbf{s}^{l-1}, s)) \setminus \{e\}| \leq |E(e(\mathbf{s}^{l-1})) \setminus \{e\}|.$$

Using (b) we get

$$(|S| - (l-1)) \cdot (c-1) \leq |E(e(\mathbf{s}^{l-1}))| - 1,$$

which proves the lemma. □

Lemma 4.3. *Let A be an l-perfect authentication system. If there is a sequence $\mathbf{s}^{l-1} = (s_1, \ldots, s_{l-1}) \in S^{l-1}$ such that $p(\mathbf{s}^{l-1}, s, s') \neq 0$ for all $s, s' \in S \setminus \{s_1, \ldots, s_{l-1}\}$ with*

$s \neq s'$, then the number of source states is restricted by

$$|S| \leq |E|^{1/(l+1)} + l.$$

Proof. Let $e \in E$ and let $s^{l-1} = (s_1, \ldots, s_{l-1}) \in S^{l-1}$ with $p(\mathbf{s}^{l-1}, s, s') \neq 0$ for all s, $s' \in S \backslash \{s_1, \ldots, s_{l-1}\}$ with $s \neq s'$. By Theorem 4.1 we get $|E(e(\mathbf{s}^{l-1}))| = |E|^{2/(l+1)}$, $|E(e(\mathbf{s}^{l-1}, s))| = |E|^{1/(l+1)}$, and $|E(e(\mathbf{s}^{l-1}, s, s'))| = 1$. Using the above lemma we have

$$|S| \leq \frac{|E|^{2/(l+1)} - 1}{|E|^{1/(l+1)} - 1} + l - 1 = |E|^{1/(l+1)} + l. \qquad \square$$

For Cartesian authentication systems, this bound has been proved for $l = 1$ by [7]; it is not the best bound possible as is shown in [1] for $l = 2$ and in [9].

5. Authentication Systems that are l-Fold Secure Against Spoofing

In this section we consider the relations between authentication systems that reach the lower bound for p_i of Theorem 3.1 and authentication systems that are l-fold secure against spoofing.

Throughout this section we assume that each sequence of different source states of length i, $i \in \{1, \ldots, l + 1\}$, can occur. By S^{i*} we denote the set of sequences of different source states of length i. Thus we have $p(\mathbf{s}^i) \neq 0$ for all $\mathbf{s}^i \in S^{i*}$. Since we already assumed $p(e) \neq 0$ for all $e \in E$, we now have $p(m) \neq 0$ for all $m \in M$. By M^{i*} we denote the set of sequences of different messages of length i.

In [8] Massey has shown that the probability of success of an opponent who knows the authentication system is always greater or equal to the probability of guessing an authentic message. If the opponent has observed i different messages, the probability of guessing an authentic message is the number of messages the receiver would accept as authentic divided by the number of messages not observed. The number of messages the receiver would accept is at least $|S| - i$, so we have

$$p_i \geq \frac{|S| - i}{|M| - i}.$$

Massey called an authentication system *l-fold secure against spoofing*, if, for all $i \in \{0, \ldots, l\}$, one has

$$p_i = \frac{|S| - i}{|M| - i}.$$

In the following lemma we give a characterization for such authentication systems.

Lemma 5.1. *An authentication system A is l-fold secure against spoofing if and only if:*

(a) *For each $i \in \{0, \ldots, l\}$, for all sequences of different messages $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^{i*}$, and for all $m \in M \backslash \{m_1, \ldots, m_i\}$ the probability* payoff$(m, \mathbf{m}^i)$ *that m is accepted as authentic given that $\mathbf{m}^i$ has been observed is constant.*

(b) *No splitting occurs.*

(c) *For each* $i \in \{1, \ldots, l+1\}$ *and for all* $\mathbf{m}^i \in M^{i*}$, $p(\mathbf{m}^i) \neq 0$.

Proof. Let $i \in \{0, \ldots, l\}$, let $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^{i*}$ be a sequence of different messages with $p(\mathbf{m}^i) \neq 0$, and let $m \in M \backslash \{m_1, \ldots, m_i\}$. The probability that m is accepted as authentic, given that $\mathbf{m}^i$ has been observed, is

$$\text{payoff}(m, \mathbf{m}^i) = \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i) \cdot \gamma(e, m, \mathbf{m}^i).$$

Summation over all $m \in M \backslash \{m_1, \ldots, m_i\}$ yields

$$\begin{aligned}
\sum_{m \in M \backslash \{m_1, \ldots, m_i\}} \text{payoff}(m, \mathbf{m}^i) &= \sum_{m \in M \backslash \{m_1, \ldots, m_i\}} \sum_{e \in E(m, \mathbf{m}^i)} p(e|\mathbf{m}^i) \cdot \gamma(e, m, \mathbf{m}^i) \\
&= \sum_{e \in E(\mathbf{m}^i)} \sum_{m \in M(e) \backslash \{m_1, \ldots, m_i\}} p(e|\mathbf{m}^i) \cdot \gamma(e, m, \mathbf{m}^i) \\
&= \sum_{e \in E(\mathbf{m}^i)} p(e|\mathbf{m}^i) \sum_{m \in M(e) \backslash \{m_1, \ldots, m_i\}} \gamma(e, m, \mathbf{m}^i) \\
&\geq |S| - i. \qquad (**)
\end{aligned}$$

Consider now an authentication system A that is l-fold secure against spoofing. Let $i \in \{0, \ldots, l\}$, let $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^{i*}$ be a sequence of different messages, with $p(\mathbf{m}^i) \neq 0$, and let $m \in M \backslash \{m_1, \ldots, m_i\}$. By (**) there exists at least one $m_0 \in M \backslash \{m_1, \ldots, m_i\}$ with $\text{payoff}(m_0, \mathbf{m}^i) \geq (|S| - i)/(|M| - i)$. Suppose that $\text{payoff}(m_0, \mathbf{m}^i) > (|S| - i)/(|M| - i)$. Then $p_i > (|S| - i)/(|M| - i)$, contradicting the hypothesis that A is l-fold secure against spoofing. Thus, $\text{payoff}(m, \mathbf{m}^i) = (|S| - i)/(|M| - i)$ for all $m \in M \backslash \{m_1, \ldots, m_i\}$. In particular, $\text{payoff}(m, \mathbf{m}^i)$ is constant.

In order to show that no splitting occurs, assume that $m_1 \neq m_2$ both encode a source state s under some encoding rule e. Since $m_2 \in M \backslash \{m_1\}$ and $p(m_1) \neq 0$ we get $\text{payoff}(m_2, m_1) = (|S| - 1)/(|M| - 1) \neq 0$, as proved above. However, the receiver does not accept m_2 because it encodes the same source state as m_1. This contradiction shows that no splitting occurs.

It remains to show that $p(\mathbf{m}^i) \neq 0$ for all $\mathbf{m}^i \in M^{i*}$, $i \in \{1, \ldots, l+1\}$. By assumption, $p(m) \neq 0$ for all $m \in M$. Suppose we have shown, for $i \leq l$, that $p(\mathbf{m}^i) \neq 0$ for all $\mathbf{m}^i \in M^{i*}$. Let $\mathbf{m}^{i+1} = (m_1, \ldots, m_{i+1}) \in M^{i+1*}$ be a sequence of different messages. Since no splitting occurs,

$$p(\mathbf{m}^{i+1}) = \sum_{e \in E(\mathbf{m}^{i+1})} p(\mathbf{m}^{i+1}|e) \cdot p(e) = \sum_{e \in E(\mathbf{m}^{i+1})} p(f_e(\mathbf{m}^{i+1})) \cdot p(e).$$

By assumption, $p(m_1, \ldots, m_i) \neq 0$ and $m_{i+1} \notin \{m_1, \ldots, m_i\}$, thus $\text{payoff}(m_{i+1}, (m_1, \ldots, m_i)) = (|S| - i)/(|M| - i) \neq 0$, therefore $E(\mathbf{m}^{i+1}) \neq \varnothing$. Now $p(\mathbf{m}^{i+1}) \neq 0$ follows from the above formula.

Now suppose that, for each $i \in \{0, \ldots, l\}$, for all sequences of different messages $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^{i*}$, and for all $m \in M \backslash \{m_1, \ldots, m_i\}$, the probability $\text{payoff}(m, \mathbf{m}^i)$ is constant and no splitting occurs.

Let $i \in \{0, \ldots, l\}$, let $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^{i*}$, and let $e \in E(\mathbf{m}^i)$. Since there is no splitting, $|M(e) \backslash \{m_1, \ldots, m_i\}| = |S| - i$ and $\gamma(e, m, \mathbf{m}^i) = 1$ for all $m \in M(e) \backslash \{m_1, \ldots, m_i\}$. Using (**) we get $\sum_{m \in M \backslash \{m_1, \ldots, m_i\}} \text{payoff}(m, \mathbf{m}^i) = |S| - i$. By hypothesis, $\text{payoff}(m, \mathbf{m}^i)$ is constant for all $m \in M \backslash \{m_1, \ldots, m_i\}$, therefore $\text{payoff}(m, \mathbf{m}^i) =$

$(|S| - i)/(|M| - i)$. Hence $p_i = (|S| - i)/(|M| - i)$, so A is l-fold secure against spoofing. □

We have two different lower bounds for the probability of success p_i, given that i messages have been observed: the bound proved by Massey is

$$p_i \geq \frac{|S| - i}{|M| - i}, \tag{4}$$

while the bound proved in Section 3 is

$$p_i \geq 2^{H(E|M^{i+1}) - H(E|M^i)}. \tag{5}$$

These bounds are different as shown by the following examples. In both examples the encoding rules are equally probable and there are two source states with respective probabilities 2/3 and 1/3.

Example 1. The authentication system is defined by the following matrix:

	s_1	s_2
e_1	m_1, m_2	m_3
e_2	m_4, m_5	m_6

We use a uniform splitting strategy. The entropies satisfy $H(E) = 1$ and $H(E|M) = 0$. Therefore

$$p_0 = \tfrac{1}{2} = 2^{H(E|M) - H(E)} > \tfrac{2}{6} = \frac{|S|}{|M|}.$$

Example 2. The authentication system is defined by the following matrix:

	s_1	s_2
e_1	m_1	m_2
e_2	m_2	m_1
e_3	m_3	m_4
e_4	m_4	m_3

The entropy of the encoding rules is $H(E) = 2$. For a message m there is $p(m) = \frac{1}{4}$ and $p(e|m) = p(m|e) \cdot p(e)/p(m) = p(f_e(m))$, since $p(e) = p(m) = \frac{1}{4}$. Thus, $H(E|m) = -\frac{2}{3}\log(\frac{2}{3}) - \frac{1}{3}\log(\frac{1}{3}) = \log(3) - \frac{2}{3}$. Therefore, $H(E|M) = \log(3) - \frac{2}{3}$ and

$$p_0 = \tfrac{1}{2} = \frac{|S|}{|M|} = 2^{-1} \neq 2^{\log(3) - 2/3 - 2} = 2^{H(E|M) - H(E)}.$$

In the next two lemmas we give necessary and sufficient conditions such that if an authentication system reaches one bound with equality it also meets the other bound. It is obvious that an authentication system that is l-fold secure against spoofing with $l > 0$ is not l-perfect. (For an authentication system that is l-fold secure against spoofing we have $p_{i-1} < p_i$, for $0 < i \le l$, whereas in an l-perfect authentication system all p_i are equal.)

Lemma 5.2. *Let A be an authentication system that is l-fold secure against spoofing. Then*

$$p_i = 2^{-I(E;M|M^i)}$$

for all $i \in \{0, \ldots, l\}$ if and only if, for each $i \in \{1, \ldots, l+1\}$ and for all $\mathbf{m}^i \in M^{i*}$, the conditional probability $p(\mathbf{m}^i|e)$ is a constant for all $e \in E(\mathbf{m}^i)$.

Proof. Suppose $p_i = 2^{-I(E;M|M^i)}$ holds for all $i \in \{0, \ldots, l\}$. Then, by Lemma 3.3, for all $\mathbf{m}^i \in M^i$, $i \in \{1, \ldots, l+1\}$ with $p(\mathbf{m}^i) \neq 0$, it follows that $p(\mathbf{m}^i|e)$ is a positive constant for all $e \in E(\mathbf{m}^i)$. Using Lemma 5.1(c) we see that $p(\mathbf{m}^i) \neq 0$ holds for all $\mathbf{m}^i \in M^{i*}$, $i \in \{1, \ldots, l+1\}$, thus we have proved the assertion.

We suppose now that, for all $\mathbf{m}^i \in M^{i*}$, $i \in \{1, \ldots, l+1\}$, the conditional probability $p(\mathbf{m}^i|e)$ is a constant for all $e \in E(\mathbf{m}^i)$. Using Lemma 5.1(c) it follows from $\sum_{e \in E} p(\mathbf{m}^i|e) = p(\mathbf{m}^i) \neq 0$ that $p(\mathbf{m}^i|e)$ is a positive constant.

Let $i \in \{0, \ldots, l\}$, let $\mathbf{m}^i = (m_1, \ldots, m_i) \in M^i$, and let $m \in M$ with $p(\mathbf{m}^i, m) \neq 0$. Obviously, it follows that $\mathbf{m}^i \in M^{i*}$ and $m \in M \backslash \{m_1, \ldots, m_i\}$. Then, by hypothesis, $p(\mathbf{m}^i, m|e)$ is a positive constant for all $e \in E(\mathbf{m}^i, m)$, and $p(\mathbf{m}^i|e)$ is also a positive constant for all $e \in E(\mathbf{m}^i, m) \subseteq E(\mathbf{m}^i)$. Hence, $p(m|e, \mathbf{m}^i) = p(\mathbf{m}^i, m|e)/p(\mathbf{m}^i|e)$ is a positive constant for all $e \in E(\mathbf{m}^i, m)$. By Lemma 5.1(b) we have $p_i = \text{payoff}(m, \mathbf{m}^i)$. Thus, by Theorem 3.1, the assertion follows. □

Lemma 5.3. *Let A be an authentication system where, for all $i \in \{0, \ldots, l\}$, the probability of success is*

$$p_i = 2^{-I(E;M|M^i)}.$$

Then A is l-fold secure against spoofing if and only if, for each $i \in \{1, \ldots, l+1\}$, for all $\mathbf{m}^i \in M^{i*}$, one has $E(\mathbf{m}^i) \neq \varnothing$ and no splitting occurs.

Proof. If A is l-fold secure against spoofing it follows by Lemma 5.1 that there is no splitting and, for all $i \in \{1, \ldots, l+1\}$, $\mathbf{m}^i \in M^{i*}$, that $p(\mathbf{m}^i) \neq 0$. Because $0 \neq p(\mathbf{m}^i) = \sum_{e \in E(\mathbf{m}^i)} p(\mathbf{m}^i|e)$, we must have $E(\mathbf{m}^i) \neq \varnothing$.

Conversely, suppose that, for each $i \in \{1, \ldots, l+1\}$ and for all $\mathbf{m}^i \in M^{i*}$, we have $E(\mathbf{m}^i) \neq \varnothing$ and no splitting occurs. Thus we have $p(\mathbf{m}^i) = \sum_{e \in E(\mathbf{m}^i)} p(f_e(\mathbf{m}^i)) \cdot p(e)$. By assumption, $p(\mathbf{s}^i) \neq 0$ for all sequences $\mathbf{s}^i \in S^{i*}$ and $p(e) \neq 0$ for all $e \in E$, thus $p(\mathbf{m}^i) \neq 0$ for all $\mathbf{m}^i \in M^{i*}$. Using Theorem 3.1 we get $p_i = \text{payoff}(m, \mathbf{m}^i)$ for all $i \in \{0, \ldots, l\}$ and $(\mathbf{m}^i, m) \in M^{i*}$. Hence, by Lemma 5.1, it follows that A is l-fold secure against spoofing. □

Examples of authentication systems that are $(t-1)$-fold secure against spoofing and that satisfy the bound $p_i = 2^{-I(E;M|M^i)}$ for all $i \in \{0, \ldots, t-1\}$ are the following authentication systems already mentioned in Section 3: the authentication systems, constructed in Chapters 6 and 7 of [4], based on t-$(v, k, 1)$ Steiner systems and tranversal designs $\text{TD}_\lambda(t, k, n)$ for $n = 1$, and the authentication systems, constructed in Theorem 3.3 of [17], based on authentication perpendicular arrays $APA_{\lambda}(t, k, v)$ for $\lambda = 1$. For all these authentication systems we must have that all sequences of different source states of length $\leq t$ are equally probable.

Acknowledgments

I would like to thank Albrecht Beutelspacher (Justus-Liebig-Universität, Giessen) for all his encouragement in carrying out this research. I would also like to thank the referees for their careful reading of the manuscript and their useful comments.

References

[1] Beutelspacher, A., and Rosenbaum, U., Essentially Perfect Authentication Systems, *Advances in Cryptology: Proceedings of EUROCRYPT 1990*, pp. 294–305.

[2] Brickell, E. F., A Few Results in Message Authentication, *Congressus Numerantium*, **43** (1984), 141–154.

[3] Castagnoli, G., Comments on Massey's Concepts of Perfect Secrecy and Perfect Authenticity, *Alta Frequenza* LVI(4) (1987), 227–228.

[4] De Soete, M., Some Constructions for Authentication-Secrecy Codes, *Advances in Cryptology: Proceedings of EUROCRYPT 1988*, pp. 33–39.

[5] De Soete, M., Vedder, K., and Walker M., Cartesian Authentication Schemes, *Advances in Cryptology: Proceedings of EUROCRYPT 1989*, pp. 476–490.

[6] Fåk, V., Repeated Use of Codes which Detect Deception, *IEEE Transactions on Information Theory*, **25**(2) (1979), 233–234.

[7] Gilbert, E. N., MacWilliams, F. J., and Sloane, N. J. A., Codes which Detect Deception, *The Bell System Technical Journal*, **53** (1974), 405–425.

[8] Massey, J. L., Cryptography—A Selective Survey, *Alta Frequenza*, LV(1) (1986), 4–11.

[9] Mitchell, C., Walker, M., and Wild, P., The Combinatorics of Perfect Authentication Schemes, to appear.

[10] Simmons, G. J., A Game Theoretical Model of Digital Message Authentication, *Congressus Numerantium*, **34** (1982), 413–424.

[11] Simmons, G. J., Authentication Theory/Coding Theory, *Advances in Cryptology: Proceedings of CRYPTO 1984*, pp. 411–432.

[12] Simmons, G. J., Message Authentication: A Game on Hypergraphs, *Congressus Numerantium*, **45** (1984), 161–192.

[13] Simmons, G. J., The Practice of Authentication, *Advances in Cryptology: Proceedings of EUROCRYPT 1985*, pp. 261–272.

[14] Simmons, G. J., and Smeets, B., A Paradoxical Result in Unconditionally Secure Authentication Codes—and an Explanation, *IMA Conference on Cryptography and Coding*, Dec. 18–20, 1989, Cirencester, England.

[15] Smeets, B., Bounds on the Probability of Deception in Multiple Authentication, to appear. (Partially presented at the *IEEE Symposium on Information Theory*, Budapest, Hungary, June 1991.)

[16] Stinson, D. R., Some Constructions and Bounds for Authentication Codes, *Journal of Cryptology*, **1** (1988), 37–51.

[17] Stinson, D. R., The Combinatorics of Authentication and Secrecy Codes, *Journal of Cryptology*, **2** (1990), 23–49.

[18] Walker, M., Information-Theoretic Bounds for Authentication Schemes, *Journal of Cryptology*, **2** (1990), 131–143.