Lower bounds on the probability of deception in authentication with arbitration

Johansson, Thomas

Published in:
IEEE Transactions on Information Theory

DOI:
10.1109/18.333869

1994

Lower Bounds on the Probability of Deception in Authentication with Arbitration

Thomas Johansson, *Student Member, IEEE*

Abstract—**This paper investigates a model for authentication in which not only an outsider, but also the transmitter or the receiver, may cheat. Lower bounds on the probability of success for different types of deception as well as on the parameters of secure authentication codes are derived. The latter bounds are shown to be tight by demonstrating codes in projective space that meet the bounds with equality.**

Index Terms—**Authentication, authentication codes, arbitration, information-theoretic bounds, unconditional security.**

I. Introduction

THE purpose of conventional authentication codes is to protect the transmitter and the receiver from active deceptions by a third party, the opponent. Two different types of attacks, impersonation and substitution attacks, are usually considered. A model for this scenario has been developed in [1]–[3], and several lower bounds on the probability of successful deception by the opponent have been derived.

The model for conventional authentication is restricted. Because the transmitter and the receiver are using the same secret key, they should trust each other, which is not always the case in reality. The transmitter and the receiver may not even know each other, in which case they definitely do not want to have to trust each other. In such a situation we may think of other types of deceptions like the transmitter sending a message and then later denying having set it or, conversely, the receiver claiming to have received a message that was never sent by the transmitter.

Inspired by this problem Simmons introduced an extended authentication model, here referred to as the *authentication model with arbitration*, [4], [5], or simply the A^2-model. In this model, protection is provided against deceptions both from an outsider (opponent) and from insiders (transmitter and receiver). This model includes a fourth participant that is called the *arbiter*. The arbiter has access to all key information and, by definition, does not cheat. As in the study of conventional authentication, we consider *unconditional security*, i.e., security against attacks performed with unlimited computating power.

The purpose of this paper is to derive lower bounds on the probability of success for the different kinds of deception that can be defined in authentication with arbitration. In Section II we define the model and give an example of an authentication code with arbitration, hereafter called A^2-code. In Sections III–V we derive lower bounds on the probability of success for each of the different kinds of deception. In Section VI these lower bounds are applied to derive bounds on the parameters of unconditionally secure A^2-codes. In Section VI we show that the derived bounds are tight by constructing examples in projective geometry that meet these bounds with equality.

We assume that the reader is familiar with the basic concept of information theory (see for example [6]). As usual, $H(X)$ denotes the entropy of the random variable X, and $I(X;Y)$ denotes the mutual information between X and Y.

II. The Model of Authentication with Arbitration

A brief description of the A^2-model is given in this section. For a more detailed description, we refer to [4], which contains a thorough discussion of the different types of threats.

The main components of the A^2-model are shown in Fig. 1. It includes four different participants: the *transmitter*, the *receiver*, the *opponent*, and the *arbiter*. The transmitter wants to send some information, here called a source state, to the receiver in such a way that the receiver can both recover the transmitted source state and verify that the transmitted message originates from the legitimate transmitter. For this purpose, a source state S from the set $\mathcal{S}$ of possible source states is encoded by the transmitter into a message M from the larger set $\mathcal{M}$ of possible messages. The message M is subsequently transmitted over the channel. The mapping from $\mathcal{S}$ to $\mathcal{M}$ is determined by the transmitter's secret encoding rule E_T chosen from the set $\mathcal{E}_\mathcal{T}$ of possible encoding rules. We may assume that the transmitter uses a mapping $f: \mathcal{S} \times \mathcal{E}_\mathcal{T} \to \mathcal{M}$. The mapping f satisfies

$$f(s, e_t) = f(s', e_t) \text{ implies } s = s'. \tag{1}$$

Manuscript received March 18, 1993; revised December 30, 1993. This work was supported by the TRF under Grant 222 92-662. This work was presented in part at the IEEE International Symposium on Information Theory, San Antonio, TX, January 17–22, 1993.

The author is with the Department of Information Theory, University of Lund, S-221 00 Lund, Sweden.

IEEE Log Number 9405091.

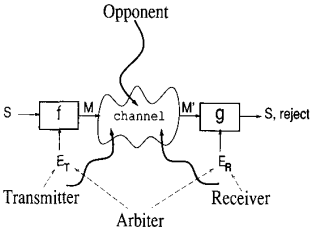

Fig. 1. The model of authentication with arbitration.

In other words, the source state can be recovered uniquely from a transmitted message. The mapping f is deterministic, i.e., a source state cannot be mapped into several messages for a given encoding rule. In authentication theory, this is usually expressed as not allowing *splitting*. This restriction is made for simplicity and most of the results that will be derived are valid also for codes that use splitting.

The opponent has access to the channel in the sense that he can either impersonate the transmitter and send a message or replace a transmitted message with a different one. The receiver must decide whether a received message is valid or not. For this purpose the receiver uses a mapping determined by his own secret encoding rule E_R taken from the set $\mathcal{E}_{\mathcal{R}}$ of possible encoding rules, which determines whether the message is valid or not, and if so also the source state. We may assume a mapping g: $\mathcal{M} \times \mathcal{E}_{\mathcal{R}} \to \mathcal{S} \cup \{\text{reject}\}$, where

$$P(e_t, e_r) \neq 0, \qquad f(s, e_t) = m \text{ implies } g(m, e_r) = s. \tag{2}$$

For the receiver to accept all legal messages from the transmitter and to interpret them to the correct source state, property (2) must hold for all possible pairs (E_T, E_R). However, in general not all pairs (E_T, E_R) will be possible, i.e., have a positive probability to occur.

The arbiter is the supervisory person who has access to all information, including E_T and E_R, but does not take part in any communication activities on the channel. His only task is to resolve possible disputes between the transmitter and the receiver whenever such occur. The arbiter is assumed to be honest.

In the A^2-model the following five types of cheating attacks are considered.

Attack **I**: Impersonation by the opponent—the opponent sends a message to the receiver and succeeds if this message is accepted by the receiver as authentic.

Attack **S**: Substitution by the opponent—the opponent observes a message that is transmitted and replaces this message with another. The opponent is successful if this other message is accepted by the receiver as authentic.

Attack **T**: Impersonation by the transmitter—the transmitter sends a message to the receiver and then denies having sent it. The transmitter succeeds if this message is accepted by the receiver as authentic and if this message is not one of the messages that the transmitter could have generated due to his encoding rule.

Attack $\mathbf{R_0}$: Impersonation by the receiver—the receiver claims to have received a message from the transmitter. The receiver succeeds if this message could have been generated by the transmitter due to his encoding rule.

Attack $\mathbf{R_1}$: Substitution by the receiver—the receiver receives a message from the transmitter, but claims to have received another message. The receiver succeeds if this other message could have been generated by the transmitter due to his encoding rule.

We adopt the Kerckhoffian assumption that everything in the system except the choice of the actual encoding rules is public information. This includes the probability distribution of the source states and of the encoding rules. In all the possible attempts to cheat it is understood that the cheating person uses an optimal strategy when choosing a message, or equivalently, that the cheating person chooses the message that maximizes his chances of success. For the five possible deceptions, we denote the probability of success in each attack by P_I, P_S, P_T, P_{R_0}, and P_{R_1}, respectively. The *overall probability of deception* is denoted by P_D and is defined to be

$$P_D = \max(P_I, P_S, P_T, P_{R_0}, P_{R_1}).$$

The selection of the transmitter's and the receiver's encoding rules may be done in several ways. One choice is to let the receiver choose his own encoding rule E_R and then secretly pass this on to the arbiter. In this case the arbiter constructs the encoding rule E_T and passes this on to the transmitter. Another choice for the setup is to do the other way around and a third approach is to let the arbiter construct both encoding rules. The fact that there are several different ways to construct the encoding rules will influence the definition of the probability of success in some of the attacks.

Finally, we want to point out that the model does not cover all possible ways to cheat. An example of a dispute that is not solved in this model would be if the transmitter claims to have sent a message and the receiver claims that it was never received. The assumption that the arbiter is not cheating is also a major restriction and is something that could be removed if we want to consider a more extended model of authentication, [7], [8].

We now give an example of an unconditionally secure A^2-code.

Example 1: As an example of an A^2-code we choose to show the Cartesian product construction for the simplest possible nontrivial case, i.e., $P_D = 1/2$, taken from [4], [5]. Assume there are two possible source states, $\mathcal{S} = \{\text{H}, \text{T}\}$. The Cartesian product construction gives rise to the matrix shown in Table I.

The protocol calls for the receiver to choose (or get from the arbiter) one of the 16 rows as the encoding rule E_R. Assume for example that the row e_1 will be the receiver's encoding rule. Then the receiver will accept the

TABLE I
THE CARTESIAN PRODUCT CONSTRUCTION FOR $|\mathcal{S}| = 2$ AND $P_D = 1/2$.

	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
e_1	H	H	-	-	T	T	-	-
e_2	H	H	-	-	T	-	T	-
e_3	H	H	-	-	-	T	-	T
e_4	H	H	-	-	-	-	T	T
e_5	H	-	H	-	T	T	-	-
e_6	H	-	H	-	T	-	T	-
e_7	H	-	H	-	-	T	-	T
e_8	H	-	H	-	-	-	T	T
e_9	-	H	-	H	T	T	-	-
e_{10}	-	H	-	H	T	-	T	-
e_{11}	-	H	-	H	-	T	-	T
e_{12}	-	H	-	H	-	-	T	T
e_{13}	-	-	H	H	T	T	-	-
e_{14}	-	-	H	H	T	-	T	-
e_{15}	-	-	H	H	-	T	-	T
e_{16}	-	-	H	H	-	-	T	T

messages m_1, m_2, m_5, and m_6 as authentic. The messages m_1, m_2 will be interpreted as the source state H and the messages m_5, m_6 will be interpreted as the source state T. All the other messages are not authentic and will thus be rejected.

The transmitter's encoding rule is a mapping that tells which message corresponds to the source state H and which message corresponds to the source state T. Here one of the messages m_1–m_4 corresponds to H and one of the messages m_5–m_8 corresponds to T. However, this choice must be made in such a way that the receiver accepts the messages as authentic and interprets them to the correct source state; see (2). In this example, the message that corresponds to the source state H must be m_1 or m_2 and the message corresponding to the source state T must be m_5 or m_6. Thus there are four possible ways to choose E_T, namely $\{H \mapsto m_1, T \mapsto m_5\}$, $\{H \mapsto m_1, T \mapsto m_6\}$, $\{H \mapsto m_2, T \mapsto m_5\}$, and $\{H \mapsto m_2, T \mapsto m_6\}$. Note that not all pairs (E_R, E_T) are possible.

By inspection we can check that the probability of success for any kind of deception is $1/2$ and thus $P_D = 1/2$ provided that the encoding rules are uniformly distributed. The parameters of the A^2-code is

$$|\mathcal{S}| = 2, \qquad |\mathcal{M}| + 8, \qquad |\mathcal{E}_{\mathcal{R}}| = 16, \qquad |\mathcal{E}_{\mathcal{T}}| = 16.$$

If we assume the source states and the encoding rules all to be uniformly distributed, then by expressing the parameters in terms of entropy we get $H(S) = 1$, $H(M) = 3$, $H(E_R) = 4$ and $H(E_T) = 4$. We also observe that from the dependence between the keys we have

$$I(E_R; E_T) = 2.$$

III. ATTACKS BY THE OPPONENT

In Section III–V we derive lower bounds on the probability of success for the different attacks in the A^2-model. In this section we consider the two possible attacks by the opponent and we start by deriving two lower bounds on the probability of success for the impersonation attack.

In this kind of deception the opponent simply sends a message and hopes for it to be accepted as authentic. The receiver determines if the message sent is authentic or not using his encoding rule e_r. We define the *authentication function* $\chi(m, e_r)$ to be

$$\chi(m, e_t) = \begin{cases} 1, & \text{if a source state } s \text{ exists such that } f(s, e_t) = m, \\ 0, & \text{otherwise.} \end{cases}$$

When the opponent sends the message m, he is successful if and only if $\chi(m, e_r) = 1$. From the definition of the impersonation attack by the opponent we can thus express the probability of success as

$$P_I = \max_m P(m \text{ valid}), \tag{3a}$$

$$P(m \text{ valid}) = \sum_{e_r \in \mathcal{E}_R} \chi(m, e_r) P(e_r). \tag{3b}$$

Let $P(m, e_r, e_t)$ be the given joint probability distribution in a system where the transmitter generates a message. An important property of the authentication function is that if $\chi(m, e_r) = 0$, then the probability distribution $P(m, e_r) = 0$. This is a fact because if $P(m, e_r) \neq 0$, then m is a message that the transmitter might generate and therefore it must be authentic. This important property is used in the proof of the next theorem.

Another important property stems from the definitions in (3a) and (3b). They show that P_I depends only on the authentication function and on the distribution of the receiver's encoding rules but *not* on the distribution of the messages that are to be transmitted. For conventional authentication this was first discovered in [9], where Simmons' bound was strengthened.

Thus we do not have to restrict ourselves to the given distribution, but can apply the definitions (3a) and (3b) to any pair (M, E_R), where M is a random variable that represents a valid message and E_R is the receiver's encoding rule. Since E_R is the receiver's encoding rule, the joint probability distribution $P(m, e_r)$ for the pair (M, E_R) must have the same marginal distribution $P(e_r)$ as the one given for the receiver's encoding rule. Also, since M occurs only when it is a valid message, we must have that if $\chi(m, e_r) = 0$, then $P(m, e_r) = 0$.

With these properties in mind we state the following theorem.

Theorem 1: For an impersonation attack of type **I** the probability of success is lower bounded by

$$P_I \geq 2^{-\inf I(M; E_R)}, \tag{4}$$

where the infimum is taken over all possible values of the probability distribution $P(m, e_r)$ such that

i) the marginal distribution $P(e_r)$ is the same as for the given system,

ii) the property that if $\chi(m, e_r) = 0$, then $P(m, e_r) = 0$ still holds.

Alternatively, P_I is lower bounded by

$$P_I \geq 2^{-I(E_R; E_T) + I(E_R; E_T|M)}. \tag{5}$$

Proof: The proof of the first inequality is based on the log-sum inequality [10]; similar proofs are given in [9] and in [11]. The complete proof is given in the Appendix. □

The last lower bound (5) is essentially a weaker result than the first lower bound (4). However, the last bound gives an important insight in the dependence between the probability of success in an impersonation attack and the encoding rules due to the transmitter and the receiver. From (5) we see that P_I is lower bounded by an expression that depends on **the information that the transmitter and the receiver have in common**. In the case of conventional authentication the transmitter and the receiver share the same key and (5) would coincide with Simmons' bound, since if $E = E_R = E_T$, we have $-I(E_R; E_T) + I(E_R; E_T|M) = -H(E) + H(E|M) = -I(E; M)$. Also, we see that (4) coincides with the strengthened Simmons' bound in [9].

The second attack from the opponent that can occur is a substitution attack. In this kind of deception the opponent observes a message on the channel and then replaces this with another message, hoping for this other message to be accepted as authentic. The receiver determines if the received message from the opponent is valid or not.

In the substitution case, define the authentication function $\chi(m', m, e_r)$ to be

$$\chi(m', m, e_r) = \begin{cases} 1, & \text{if } m' \text{ is authentic for the receiver's encoding rule } e_r \text{ given} \\ & \text{that } m \text{ was authentic and also that } g(m', e_r) \neq g(m, e_r), \\ 0, & \text{otherwise.} \end{cases}$$

Clearly, if the opponent replaces the message m with m', then he is successful if and only if $\chi(m', m, e_r) = 1$. From the definition of the substitution attack by the opponent, the probability of success may be expressed as

$$P_S = \sum_{m \in \mathcal{M}} P(m) \left[\max_{m'} P(m' \text{ valid}|m) \right] \tag{6a}$$

$$P(m' \text{ valid}|m) = \sum_{e_r \in \mathcal{E}_R} \chi(m', m, e_r) P(e_r|m). \tag{6b}$$

The given system has a probability distribution $P(m, e_r, e_t)$. Assume that the system has at least two different source states. We now introduce a new random variable M' that only takes values $M' = m'$ such that $\chi(m', m, e_r) = 1$. This simply means that m' is an authentic message that does not correspond to the same source state as the message m. It is now possible to construct a joint probability distribution $P(m', m, e_r, e_t)$ such that $P(m, e_r)$ is the distribution given in the system and such that if $\chi(m', m, e_r) = 0$, then the probability distribution $P(m', m, e_r) = 0$.

For the substitution attack by the opponent we state the following theorem.

Theorem 2: For a substitution attack of type **S** the probability of success is lower bounded by

$$P_S \geq 2^{-\inf I(M'; E_R|M)}, \tag{7}$$

where the infimum is taken over all possible values of the probability distribution $P(m', m, e_r)$ such that

i) the marginal distribution $P(m, e_r)$ is the same as for the given system,

ii) the property that if $\chi(m', m, e_r) = 0$, then $P(m', m, e_r) = 0$ holds.

Alternatively, P_S is lower bounded by

$$P_S \geq 2^{-I(E_R; E_T|M)}. \tag{8}$$

We can see that in this case the probability of success in a substitution attack by the opponent is lower bounded by an expression that depends on the secret information shared between the transmitter and the receiver after the observation of one transmitted message.

IV. Attacks by the Transmitter

We now consider the impersonation attack from the transmitter. In this kind of deception the transmitter sends a message that could not have been generated using his encoding rule E_T. The transmitter succeeds in his attack if the receiver accepts the message as authentic.

In this case, we define the authentication function $\chi(m, e_r, e_t)$ to be

$$\chi(m, e_r, e_t) = \begin{cases} 1, & \text{if a source state } s \text{ exists such that } g(m, e_r) = s \\ & \text{but } f(s, e_t) \neq m, \\ 0, & \text{otherwise.} \end{cases}$$

The transmitter now succeeds in his attack when sending the message m if and only if $\chi(m, e_r, e_t) = 1$.

Example 2: Consider the Cartesian product construction given in Example 1. Assume that the transmitter's encoding rule is the mapping $\{H \mapsto m_1, T \mapsto m_5\}$. This gives four possible encoding rules for the receiver, namely e_1, e_2, e_5, and e_6. Assume that the transmitter sends the message m_2 to the receiver as his attack. Since $\chi(m_2, e_1) = 1$, $\chi(m_2, e_2) = 1$, $\chi(m_2, e_5) = 0$, and $\chi(m_2, e_6) = 0$, he will be successful in two cases out of four and if the encoding rules are uniformly distributed we have by symmetry $P_T = 1/2$.

The case of a cheating transmitter is modeled in the following way. Consider the transmitter as an opponent who has access to the encoding rule E_T. A receiver accepts messages according to the above authentication function. Thus, the transmitter is successful when sending the message m if and only if $\chi(m, e_r, e_t) = 1$. Since the key setup in the A^2-model includes a possibility for the transmitter to construct his own encoding rule, we must be aware of the fact that the definition of the probability of deception will be different from the case of substitution by the opponent. Here we must instead maximize over the transmitter's encoding rules. For the impersonation attack by the transmitter the probability of success is expressed as

$$P_T = \max_{e_t \in \mathscr{E}_T} \left[\max_m P(m \text{ valid}|e_t) \right], \tag{9a}$$

$$P(m \text{ valid}|e_t) = \sum_{e_r \in \mathscr{E}_R} \chi(m, e_r, e_t) P(e_r|e_t). \tag{9b}$$

Let $n(e_r)$ be the number of authentic messages for the receiver's encoding rule e_r. We will assume that $\min_{e_r \in \mathscr{E}_R} n(e_r) > |S|$. This guarantees that for each of the receiver's encoding rules there is at least one message for which $\chi(m, e_r, e_t) = 1$. The system has a given probability distribution $P(e_r, e_t)$ on the encoding rules. Assume that the random variable M only takes values $M = m$ such that $\chi(m, e_r, e_t) = 1$. Then a joint probability distribution $P(m, e_r, e_t)$ exists such that $P(e_r, e_t)$ is the distribution given in the system and for which we have that if $\chi(m, e_r, e_t) = 0$, then the joint probability distribution $P(m, e_r, e_t) = 0$.

For impersonation by the transmitter we then state the following theorem.

Theorem 3: For an impersonation attack of type **T** the probability of success is lower bounded by

$$P_T \geq 2^{-\inf I(M; E_R|E_T)}, \tag{10}$$

where the infimum is taken over all possible values of the joint probability distribution $P(m, e_r, e_t)$ such that

i) the marginal distribution $P(e_r, e_t)$ is the same as for the given system;

ii) the property that if $\chi(m, e_r, e_t) = 0$, then $P(m, e_r, e_t) = 0$ still holds.

Alternatively, P_T is lower bounded by

$$P_T \geq 2^{-H(E_R|E_T)}. \tag{11}$$

From the second inequality we see that the probability of success is lower bounded by an expression depending on the transmitter's uncertainty about the receiver's encoding rule.

V. Attacks by the Receiver

This section considers the last two types of deceptions, i.e., the impersonation attack and the substitution attack by the receiver. We start with the impersonation attack.

In this kind of deception the receiver claims to have received a message from the transmitter. The receiver succeeds in his attack if this message could have been generated by the transmitter due to his encoding rule E_T.

Example 3: Consider again the Cartesian product construction given in Example 1. Assume that $E_R = e_1$ and that the receiver tries to claim that he received a message corresponding to source state H. He then must choose one of the two messages m_1 and m_2. For the transmitter, only one of these messages corresponds to source state H

and if the receiver picks the wrong one he will not be successful. Thus, the probability of success is 1/2.

Define the authentication function $\chi(m, e_t)$ to be

$$\chi(m, e_r) = \begin{cases} 1, & \text{if } m \text{ is authentic for the receiver's encoding rule } e_r, \\ 0, & \text{otherwise.} \end{cases}$$

If the receiver claims to have received m, he succeeds in his attack if and only if $\chi(m, e_t) = 1$. This case of a cheating receiver is modeled in the following way.

Consider the receiver as an opponent who has access to the encoding rule E_R. Now imagine another receiver who is only accepting messages that can be generated by the transmitter, or equivalently accepts messages due to the above defined authentication function. Thus the receiver is successful when sending the message m if and only if $\chi(m, e_t) = 1$.

The model includes a possibility for the receiver to choose the encoding rule himself. Thus, from the definition of receiver's impersonation attack, the probability of success is expressed as

$$P_{R_0} = \max_{e_r \in \mathscr{E}_{\mathscr{R}}} \left[\max_m P(m \text{ valid}|e_r) \right], \tag{12a}$$

$$P(m \text{ valid}|e_r) = \sum_{e_t \in \mathscr{E}_{\mathscr{T}}} \chi(m, e_t) P(e_t|e_r). \tag{12b}$$

We introduce the random variable M that only takes values $M = m$ such that $\chi(m, e_t) = 1$. Consider a joint probability distribution $P(m, e_r, e_t)$ such that $P(e_r, e_t)$ is the distribution given in the system and such that if $\chi(m, e_t) = 0$, then the joint probability distribution $P(m, e_t) = 0$. One such distribution is the distribution given in the system when we consider M as the message that the transmitter generates.

For impersonation by the receiver we state the following theorem.

Theorem 4: For an impersonation attack of type $\mathbf{R_0}$ the probability of success is lower bounded by

$$P_{R_0} \geq 2^{-\inf I(M; E_T|E_R)}, \tag{13}$$

where the infimum is taken over all possible values of the joint probability distribution $P(m, e_r, e_t)$ such that

i) the marginal distribution $P(e_r, e_t)$ is the same as for the given system,

ii) the property that if $\chi(m, e_t) = 0$ then $P(m, e_t) = 0$ still holds.

Alternatively, P_{R_0} is lower bounded by

$$P_{R_0} \geq 2^{-I(M; E_T|E_R)}. \tag{14}$$

The last type of deception to consider is the substitution attack by the receiver. In this kind of deception the receiver has received a message from the transmitter, but claims to have received another message. The receiver succeeds in his attack if this other message is a message that could have been generated by the transmitter due to his encoding rule E_T.

We define the authentication function $\chi(m', m, e_t)$ to be

$$\chi(m', m, e_t) = \begin{cases} 1, & \text{if a source state } s' \text{ exists such that } f(s', e_t) = m' \\ & \text{given that a source state } s \text{ exists such that} \\ & f(s, e_t) = m \text{ and also that } m \neq m', \\ 0, & \text{otherwise.} \end{cases}$$

If the receiver receives m but claims to have received m', he succeeds in his attack if and only if $\chi(m', m, e_t) = 1$. This case of the receiver cheating is modeled in the following way.

Consider the receiver as an opponent who has access to the encoding rule E_R and has observed a message m from the transmitter. The receiver tries to replace this message with another message m'. Imagine another receiver who only accepts messages that can be generated by the transmitter. The receiver will be successful when sending the message m' if and only if $\chi(m', m, e_t) = 1$.

As before, the receiver may have the possibility of choosing his own encoding rule. From the definition of the substitution attack by the receiver, we express the probability of success as

$$P_{R_1} = \max_{e_r \in \mathscr{E}_{\mathscr{R}}} \sum_{\substack{m \in \mathscr{M} \\ P(m, e_r) \neq 0}} P(m|e_r) \left[\max_{m'} P(m' \text{ valid}|m, e_r) \right], \tag{15a}$$

$$P(m' \text{ valid}|m, e_r) = \sum_{e_t \in \mathscr{E}_{\mathscr{T}}} \chi(m', m, e_t) P(e_t|m, e_r). \tag{15b}$$

Assume that $|\mathscr{S}| \geq 2$. Introduce the random variable M' that only takes values such that $\chi(m', m, e_t) = 1$. We then construct a joint probability distribution $P(m', m, e_r, e_t)$ such that $P(m, e_r, e_t)$ is the distribution given in the system and such that if $\chi(m', m, e_t) = 0$, then the probability distribution $P(m', m, e_t) = 0$.

For the substitution attack we state the following theorem.

Theorem 5: For a substitution attack of type $\mathbf{R_1}$ the probability of success is lower bounded by

$$P_{R_1} \geq 2^{-\inf I(M'; E_T|M, E_R)}, \tag{16}$$

where the infimum is taken over all possible values of the joint probability distribution $P(m', m, e_r, e_t)$ such that

i) the marginal distribution $P(m, e_r, e_t)$ is the same as for the given system,

ii) the property that if $\chi(m', m, e_t) = 0$, then $P(m', m, e_t) = 0$ still holds.

Alternatively, P_{R_1} is lower bounded by

$$P_{R_1} \geq 2^{-H(E_T|M, E_R)}. \tag{17}$$

For the attacks by the receiver, the probability of success depends on the uncertainty about the transmitter's key for the receiver. For the impersonation attack R_0 we observe that to have a good protection, the transmitter must give away a lot of information about his key to the receiver. This is an analog to the impersonation attack I, where the transmitter/receiver must give away information about the common part of their keys. Considering multiple use of the codes, this determines the amount of new key entropy that has to be added for each use.

VI. Combinatorial Lower Bounds

After having obtained lower bounds on the probability of success for each type of deception, we are now ready to give some combinatorial lower bounds on the number of encoding rules and on the number of messages that are necessary in an A^2-code.

We distinguish between two different types of A^2-codes. Recall that $n(e_r)$ is the number of authentic messages for the receiver's encoding rule e_r. We define an A^2-code to be *degenerate* if $|S| = 1$ or $\min_{e_r \in \mathcal{E}_\mathcal{R}} n(e_r) = |S|$. For the authentication codes that only have one source state the whole concept of substitution is not relevant since substitution is not possible. The degenerate A^2-codes that have $\min_{e_r \in \mathcal{E}_\mathcal{R}} n(e_r) = |S|$ have $P_{R_0} = 1$ and hence these codes are not very interesting either.

In the following we exclude the degenerate A^2-codes. Under this assumption there exist distributions for the system such that all lower bounds that have been derived are valid. However, the strong lower bounds of Theorems 1–5 may use *different* joint probability distributions for obtaining maximum. Consider instead the simplified lower bounds of Theorems 1–5. These bounds depend only on the probability distribution $P(m, e_r, e_t)$ given in the system and can thus be used simultaneously. If we assume a system with given probability distribution $P(m, e_r, e_t)$, then all the simplified lower bounds are valid for this distribution. We intend to combine these bounds to obtain lower bounds on the number of messages and on the number of encoding rules, which we refer to as combinatorial bounds.

Recall that in general not all pairs (E_R, E_T) will be possible. Therefore, consider the set of possible pairs (E_R, E_T) and denote this set by $\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}$. This is the private information that the arbiter may want to store.

Assume that we want to construct an A^2-code such that the probability of deception is at most $1/q$, $P_D \leq 1/q$. Assume also a uniform probability distribution on the source states. Let the number of source states for a symmetric source be $|\mathcal{S}|$. Then we have the following lower bounds on the number of encoding rules and on the number of messages.

Theorem 6: An A^2-code for $\mathcal{S}$ must satisfy

$$|\mathcal{E}_\mathcal{R}| \geq (P_I P_S P_T)^{-1},$$

$$|\mathcal{E}_\mathcal{T}| \geq (P_I P_S P_{R_0} P_{R_1})^{-1},$$

$$|\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}| \geq (P_I P_S P_T P_{R_0} P_{R_1})^{-1},$$

$$|\mathcal{M}| \geq (P_I P_{R_0})^{-1} |\mathcal{S}|.$$

In particular, if the overall probability of deception is $P_D = 1/q$, then

$$|\mathcal{E}_\mathcal{R}| \geq q^3,$$

$$|\mathcal{E}_\mathcal{T}| \geq q^4,$$

$$|\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}| \geq q^5,$$

$$|\mathcal{M}| \geq q^2 |\mathcal{S}|.$$

Proof: Using the bounds (5), (8), and (11) we have $P_I P_S P_T \geq 2^{-H(E_R)}$. Since $H(E_R) \leq \log |\mathcal{E}_\mathcal{R}|$ we have

$$|\mathcal{E}_\mathcal{R}| \geq 2^{H(E_R)} \geq (P_I P_S P_T)^{-1}.$$

Thus if $P_D = 1/q$, we get $|\mathcal{E}_\mathcal{R}| \geq q^3$.

For the number of encoding rules for the transmitter we use the bounds (5), (8), (14), and (17). We have $P_I P_S P_{R_0} P_{R_1} \geq 2^{-H(E_T)}$. Since $H(E_T) \leq \log |\mathcal{E}_\mathcal{T}|$ we have

$$|\mathcal{E}_\mathcal{T}| \geq 2^{H(E_T)} \geq (P_I P_S P_{R_0} P_{R_1})^{-1}.$$

Particularly if $P_D + 1/q$, we get $|\mathcal{E}_\mathcal{T}| \geq q^4$.

For the set $\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}$ we use the bounds (5), (8), (11), (14), and (17). We obtain $P_I P_S P_T P_{R_0} P_{R_1} \geq 2^{-H(E_R, E_T)}$. Since $H(E_R, E_T) \leq \log |\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}|$, we have

$$|\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}| \geq 2^{H(E_R, E_T)} \geq (P_I P_S P_T P_{R_0} P_{R_1})^{-1}.$$

If $P_D = 1/q$, we get $|\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}| \geq q^5$.

Finally, the lower bound valid on the number of messages is proved. First we note that (5) can be rewritten as $P_I \geq 2^{-I(M; E_T) + I(M; E_T | E_R)}$. Using this inequality and (14), we get $P_I P_{R_0} \geq 2^{-I(M; E_T)}$, or

$$2^{I(M; E_T)} \geq (P_I P_{R_0})^{-1}.$$

Now use the fact that $H(M|E_T) = H(S) = \log |\mathcal{S}|$. This gives

$$2^{H(M)} \geq (P_I P_{R_0})^{-1} |\mathcal{S}|.$$

Since $H(M) \leq \log |\mathcal{M}|$, we have $|\mathcal{M}| \geq (P_I P_{R_0})^{-1} |\mathcal{S}|$. If $P_D = 1/q$, we also get $|\mathcal{M}| \geq q^2 |\mathcal{S}|$. □

We continue by giving some definitions related to the derived bounds. In [4] Simmons defined an authentication code to be *equitable* if the probabilities of success for all types of deception are the same, i.e., if $P_I = P_S = P_T =$

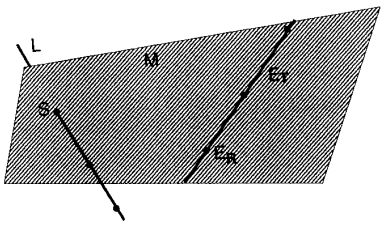

Fig. 2. The connection between the variables in Construction I.

$P_{R_0} = P_{R_1}$. We define an authentication code that permits arbitration to be *perfect* if

$$|\mathscr{E}_{\mathscr{R}}| = \frac{1}{P_I P_S P_T}$$

and

$$|\mathscr{E}_{\mathscr{T}}| = \frac{1}{P_I P_S P_{R_0} P_{R_1}}.$$

Also we define an A^2-code to be *equitably perfect* if for $P_D = 1/q$ we have $|\mathscr{E}_{\mathscr{R}}| = q^3$ and $|\mathscr{E}_{\mathscr{T}}| = q^4$.

We end the section with a note on the Cartesian product construction obtained by applying the combinatorial bounds.

Example 4 (Example 1, Continued): In Example 1 we gave an example of an A^2-code using the Cartesian product construction for the case $P_D = 1/2$. Let us examine the parameters of this code and compare them with the combinatorial lower bounds derived in this section. For $|\mathscr{S}| = 2$ and $P_D = 1/2$ we found before that in the Cartesian product construction the cardinality parameters were $|\mathscr{M}| = 8$, $|\mathscr{E}_{\mathscr{R}}| = 16$, and $|\mathscr{E}_{\mathscr{T}}| = 16$. However, Theorem 6 gives the bounds $|\mathscr{E}_{\mathscr{R}}| \geq 8$, $|\mathscr{E}_{\mathscr{T}}| \geq 16$, and $|\mathscr{M}| \geq 8$.

We see that the number of encoding rules for the receiver does not meet the lower bound of Theorem 6 with equality and thus this construction is not perfect due to the combinatorial lower bounds. Indeed, it is possible to find a construction that is equitably perfect for the case $|\mathscr{S}| = 2$ and $P_D = 1/2$. We use the reduced matrix shown in Table II instead.

For this matrix we have $|\mathscr{E}_{\mathscr{R}}| = 8$. The transmitter will have as encoding rule one of the four messages $m_1, \cdots, m_4$ to transmit H and one of the four messages $m_5, \cdots, m_8$ to transmit T. Thus $|\mathscr{E}_{\mathscr{T}}| = 16$. The encoding rules are chosen in such a way that the receiver accepts the messages that the transmitter can generate. If the receiver's encoding rule is fixed there are four possible choices for the transmitter's encoding rule. Thus the number of possible choices for the pair (E_R, E_T) is 32. It is also possible to check that $P_D = 1/2$.

VII. Some Constructions and Examples

A natural question to ask is if (infinite) classes of perfect or equitably perfect A^2-codes exist. In this section we show that they do by constructing perfect and equitably perfect A^2-codes in the projective space, [12], in the same manner as was done in [1] in the case of conventional authentication.

TABLE II
An Equitably Perfect A^2-Code for $|\mathscr{S}| = 2$ and $P_D = 1/2$.

	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
e_1	H	H	-	-	T	T	-	-
e_2	H	H	-	-	-	-	T	T
e_3	H	-	H	-	T	-	T	-
e_4	H	-	H	-	-	T	-	T
e_5	-	H	-	H	T	-	T	-
e_6	-	H	-	H	-	T	-	T
e_7	-	-	H	H	T	T	-	-
e_8	-	-	H	H	-	-	T	T

In [1] perfect authentication codes were constructed in a projective plane. We will instead use the projective space of dimension 3, $\mathbf{PG}(3, \mathbb{F}_q)$, to construct perfect and equitably perfect A^2-codes. We give two constructions. We start with the simplest construction which gives us only perfect A^2-codes.

Construction I: Fix a line L in $\mathbf{PG}(3, \mathbb{F}_q)$. The points on L are regarded as source states. The transmitter's encoding rule is a line E_T not intersecting L. The receiver's encoding rule E_R is a point on the line E_T. When the transmitter is to map a source state S into a message that is to be transmitted, this message will be the unique plane $M = \langle E_T, S \rangle$ obtained by joining the line E_T and the point S on L corresponding to the source state. The receiver accepts a message only if the point E_R is contained in the received plane.

The messages are all the planes intersecting the line L in a point. Since E_R lies on the line E_T, properly generated messages by the transmitter will always be accepted by the receiver. These relations are shown in Fig. 2. Let us give the parameters of the constructed A^2-code.

Theorem 7: Construction I gives a *perfect* A^2-code that has the following parameters:

$$|S| = q + 1, \qquad |M| = q^3 + q^2, \qquad |E_R| = q^3 + q^2,$$
$$|E_T| = q^4,$$

and the probabilities of deception are

$$P_I = P_S = P_{R_0} = P_{R_1} = \frac{1}{q}, \quad P_T = \frac{1}{q+1}.$$

Proof: Let us start by proving the cardinality parameters. The source states are the points on a fixed line L. The number of points on any line is $q + 1$. Thus $|\mathscr{S}| = q + 1$. The messages are all planes intersecting the line L in a point. This is the same as all planes not containing the fixed line L. The total number of planes is $q^3 + q^2 + q + 1$ and the number of planes containing the line L is $q + 1$. Thus $|\mathscr{M}| = q^3 + q^2$. The receiver's encoding rules

are all points not on L. Since the number of points is $q^3 + q^2 + q + 1$, we have that $|\mathscr{E}_{\mathscr{R}}| = q^3 + q^2$. The transmitter's encoding rules are all lines having empty intersection with the fixed line L. The total number of lines is $(q^2 + 1)(q^2 + q + 1)$. The number of lines intersecting in a point on L is $q^2 + q + 1$ and one of them is L itself. Since a line ($\neq L$) cannot intersect L in two points there are $(q + 1)(q^2 + q) + 1$ lines that have nonempty intersection with L. From this we conclude that $|\mathscr{E}_{\mathscr{T}}| = q^4$.

Next we compute the probability of success for the different kinds of deception. We assume the encoding rules to be uniformly distributed.

Impersonation by the Opponent, I: The opponent simply sends a message, which is a plane intersecting the line L in a point. This message is accepted by the receiver as authentic only if the encoding rule E_R, which is a point, lies on the plane. The number of points on a plane is $q^2 + q + 1$ and in this case one of them is on L. Since the number of possible E_R's in a message is the same for all possible messages the opponent can do no better than to choose an arbitrary message. Then we have that the number of E_R's accepting the message as authentic is $q^2 + q$ and the total number of the receiver's encoding rules is $q^3 + q^2$. Thus

$$P_I = \frac{q^2 + q}{q^3 + q^2} = \frac{1}{q}.$$

Substitution by the Opponent, S: The opponent has observed a message M and now he replaces this with another message M'. If the plane M intersects the line L in the point S then the message M' must intersect L in another point S' or otherwise both messages correspond to the same source state and the substitution attack would by definition not be successful. The best strategy for the opponent is to choose M' in such a way that the intersection between M and M' is as large as possible. But $M \cap M'$ is always a line, not intersecting L, containing $q + 1$ points. Since the number of possible E_R's for a given message is $q^2 + q$ we have

$$P_S = \frac{q + 1}{q^2 + q} = \frac{1}{q}.$$

Impersonation by the Receiver, R_0: The receiver claims to have received a message M from the transmitter. The receiver succeeds in his cheating if the transmitter's encoding rule E_T lies on the plane M. The receiver can do no better than to choose an arbitrary M containing his own encoding rule E_R. The number of possible E_T's for a message M given E_R is the number of lines on the plane M not intersecting L and containing the point E_R. This number is q, since the number of lines on M containing E_R is $q + 1$ and exactly one of them also contains the point on L. The total number of E_T's for a given E_R is the number of lines containing the fixed point E_R and not intersecting L. This number is q^2 since the number of lines through a point is $q^2 + q + 1$ and $q + 1$ of them will intersect L in a point. Then we have

$$P_{R_0} = \frac{q}{q^2} = \frac{1}{q}.$$

Substitution by the Receiver, R_1: The receiver has received a message M but claims to have received another message M'. The two planes M and M' must intersect L in different points or the substitution attack by the receiver will not be successful. Then $M \cap M'$ will be a line, not intersecting L and the two messages will only have one possible E_T in common. The number of possible E_T's on M is q and thus we have

$$P_{R_1} = \frac{1}{q}.$$

Impersonation by the Transmitter, T: The transmitter sends a message M that does not contain his encoding rule E_T and hopes for the receiver to accept the message as authentic. The transmitter knows that E_R is a point on the given line E_T. Thus, the message M is chosen such that it contains as many points of the line E_T as possible, but not E_T itself. But then it can only contain one point since otherwise E_T would be included. The number of points on the line E_T is $q + 1$. Thus we have

$$P_T = \frac{1}{q + 1}.$$

Finally we verify that the A^2-code is perfect by checking that $P_I P_S P_T = |E_R|^{-1}$ and $P_I P_S P_R T_0 P_{R_1} = |E_T|^{-1}$. □

Example 5: We here give a small example of how Construction I works in $\mathbf{PG}(3, \mathbb{F}_2)$. We have 15 points, 35 lines, and 15 planes in $\mathbf{PG}(3, \mathbb{F}_2)$. The points are numbered $1, \cdots, 15$. The fixed line L is the line $L = (1, 2, 3)$. Thus the source states are the points 1, 2, and 3. The messages are the 12 planes not containing L. The receiver's encoding rules are the points $4, \cdots, 15$ and the transmitter's encoding rules are the 16 lines (4, 11, 15), (4, 10, 14), (4, 9, 13), (4, 8, 12), (5, 11, 14), (5, 10, 15), (5, 9, 12), (5, 8, 13), (6, 11, 13), (6, 10, 12), (6, 9, 15), (6, 8, 14), (7, 11, 12), (7, 10, 13), (7, 9, 14), (7, 8, 15). The authentication matrix for the receiver is shown in Table III. Note that the rows are now the messages and the columns are the receiver's encoding rules. It can be checked that $P_I = P_S = P_{R_0} = P_{R_1} = 1/2$ and $P_T = 1/3$.

We now make a modification in Construction I in order to obtain an equitable A^2-code.

Construction II (Construction I, Modified): Fix a plane H and a line L on H in $\mathbf{PG}(3, \mathbb{F}_q)$. The points on L are regarded as source states. The transmitter's encoding rule is a line E_T not intersecting L. The receiver's encoding rule E_R is a point on the line E_T and not on the plane H. As before, the message will be the unique plane $M = \langle E_T, S \rangle$ obtained by joining the line E_T and the point on L corresponding to the source state S. Also, the receiver only accepts messages containing the point E_R.

The messages will still be all the planes intersecting the line L in a point. For this construction we state the following theorem.

TABLE III
DECODING MATRIX FOR CONSTRUCTION I IN $\mathbf{PG}(3, \mathbb{F}_2)$.

		Receiver's encoding rule											
		4	5	6	7	8	9	10	11	12	13	14	15
	(1,4,5,10,11,14,15)	1	1	-	-	-	-	1	1	-	-	1	1
	(1,4,5,8,9,12,13)	1	1	-	-	1	1	-	-	1	1	-	-
	(1,6,7,10,11,12,13)	-	-	1	1	-	-	1	1	1	1	-	-
	(1,6,7,8,9,14,15)	-	-	1	1	1	1	-	-	-	-	1	1
	(2,4,6,8,10,12,14)	2	-	2	-	2	-	2	-	2	-	2	-
Message	(2,4,6,9,11,13,15)	2	-	2	-	-	2	-	2	-	2	-	2
	(2,5,7,8,10,13,15)	-	2	-	2	2	-	2	-	-	2	-	2
	(2,5,7,9,11,12,14)	-	2	-	2	-	2	-	2	2	-	2	-
	(3,4,7,8,11,12,15)	3	-	-	3	3	-	-	3	3	-	-	3
	(3,4,7,9,10,13,14)	3	-	-	3	-	3	3	-	-	3	3	-
	(3,5,6,8,11,13,14)	-	3	3	-	3	-	-	3	-	3	3	-
	(3,5,6,9,10,12,15)	-	3	3	-	-	3	3	-	3	-	-	3

Theorem 8: Construction II gives an *equitably perfect* A^2-code that has the following parameters:

$$|S| = q + 1, \qquad |M| = q^3 + q^2, \qquad |E_R| = q^3,$$
$$|E_T| = q^4$$

and the probabilities of deception are

$$P_I = P_S = P_{R_0} = P_{R_1} = P_T = \frac{1}{q}.$$

Proof: The cardinality parameters will remain the same as for the first construction except for the receiver's encoding rules. They are now all points not on the plane H. Thus the number of E_R's is q^3. Let us determine the probability of success for the different kinds of deception.

Impersonation by Opponent, I: The opponent sends the plane M. Since $M \cap H$ is a line that intersects L in a point, we have that the number of possible E_R's on M is q^2. The number of E_R's is q^3 and thus

$$P_I = \frac{q^2}{q^3} = \frac{1}{q}.$$

Substitution by the Opponent, S: The opponent replaces the message M with M' and the messages intersect L in different points. Now $M \cap M'$ is a line and this line intersects H in a point. Thus there are q possible E_R's both on M and M'. But the number of E_R's on M is q^2, so

$$P_S = \frac{q}{q^2} = \frac{1}{q}.$$

Impersonation and Substitution by the Receiver, R_0 and R_1: This derivation is the same as for the first construction and is therefore omitted.

Impersonation by the Transmitter, T: The transmitter sends the message M not containing his encoding rule E_T. Now $E_T \cap H$ is a point and thus there are q points on E_T that are possible E_R's. But M can only contain one of these points and thus we have

$$P_T = \frac{1}{q}. \qquad \square$$

The construction that was given can be used for any number of source states such that $|\mathcal{S}| \leq q + 1$ and if all messages not used are erased, the construction is still equitably perfect.

VIII. CONCLUSIONS AND OPEN PROBLEMS

The main results in this paper are the information-theoretic lower bounds on the probabilities of success for the different kinds of deception, from which we have been able to derive lower bounds on the number of encoding rules and on the number of messages that are necessary in an A^2-code. We have also shown that the combinatorial bounds are tight by constructing A^2-codes in projective space which meet the bounds with equality. The results obtained show many similarities with established results in conventional symmetric authentication. They can be interpreted as a generalization of known results for symmetric authentication systems to corresponding results for asymmetric authentication systems.

Many interesting problems are left open. As the recent development in conventional authentication has shown, it is possible to construct authentication codes where the

source state space grows exponentially with the number of keys if we allow P_S to be slightly greater than P_I, [13]. This is of great practical relevance since we are mostly interested in authenticating long messages. It is of interest to see if any of these ideas can be applied to A^2-codes. Other interesting problems would be to characterize perfect A^2-codes in terms of combinatorial designs and to examine how A^2-codes are related to secrecy. For the latter, we see no obvious way of including secrecy without increasing the key size.

Appendix
Proofs of the Theorems

The proofs that follow are based on some common inequalities. These inequalities are first stated. The most important is the *Log-Sum Inequality*.

Lemma 9 (Log-Sum Inequality): For arbitrary nonnegative numbers $\{a_i\}_{i=1}^n$, $\{b_i\}_{i=1}^n$ we have

$$\sum_{i=1}^{n} a_i \log \frac{a_i}{b_i} \geq a \log \frac{a}{b},$$

where $a = \Sigma_{i=1}^n a_i$, $b = \Sigma_{i=1}^n b_i$. Equality holds if and only if $a_i b = b_i a$ for $i = 1, 2, \cdots, n$.

Proof: See [10]. □

The second inequality that is used is *Jensen's Inequality*.

Lemma 10 (Jensen's Inequality): Let $g(x)$ be a convex function on an interval (a, b) and $x_1, x_2, \cdots, x_n$ are arbitrary real numbers $a < x_i < b$ and $w_1, w_2, \cdots, w_n$ are positive numbers with $\Sigma w_i = 1$. Then

$$g\left(\sum_{i=1}^{n} w_i x_i\right) \leq \sum_{i=1}^{n} w_i g(x_i).$$

Equality holds if and only if $g(x_i)$ takes the same value for each i for which $w_i > 0$.

Proof: See [14]. □

This inequality will be used with the fact that $-\log x$ is a convex function for $x > 0$.

The last inequality is the simple fact that taking a maximum results always in something that is greater than or equal to taking the mean value.

Lemma 11: Let $g(x)$ be a function on an interval (a, b) and $x_1, x_2, \cdots, x_n$ are arbitrary real numbers $a < x_i < b$ and $w_1, w_2, \cdots, w_n$ are positive numbers with $\Sigma w_i = 1$. Then

$$\max_{x_i} g(x_i) \geq \sum_{x=1}^{n} w_i g(x_i).$$

We now prove the theorems.

Proof of Theorem 1: We prove the first part of Theorem 1. The proof is based on the log-sum inequality, [10]; similar proofs are given in [9] and [11]. By definition we have

$$I(M; E_R) = \sum_{m \in \mathcal{M}} P(m) \left(\sum_{e_r \in \mathcal{E}_R} P(e_r|m) \log \frac{P(e_r|m)}{P(e_r)} \right).$$

The summation over the receiver's encoding rules can now be restricted to all e_r for which $\chi(m, e_r) = 1$, since $\chi(m, e_r) = 0$ implies that $P(e_r|m) = 0$. So we equivalently write

$$I(M; E_R) = \sum_{m \in \mathcal{M}} P(m) \left(\sum_{e_r \in \mathcal{E}_R} P(e_r|m)\chi(m, e_r) \cdot \log \frac{P(e_r|m)\chi(m, e_r)}{P(e_r)\chi(m, e_r)} \right).$$

Using the log-sum inequality we now rewrite this as the inequality

$$I(M; E_R) \geq \sum_{m \in \mathcal{M}} P(m) \left(\sum_{e_r \in \mathcal{E}_R} P(e_r|m)\chi(m, e_r) \cdot \log \frac{\left(\sum_{e_r \in \mathcal{E}_R} P(e_r|m)\chi(m, e_r) \right)}{\left(\sum_{e_r \in \mathcal{E}_R} P(e_r)\chi(m, e_r) \right)} \right).$$

Since $\Sigma_{e_r \in \mathcal{E}_R} P(e_r|m)\chi(m, e_r) = 1$ and $\Sigma_{e_r \in \mathcal{E}_R} P(e_r)\chi(m, e_r) = P(m \text{ valid})$ the inequality reduces to

$$I(M; E_R) \geq - \sum_{m \in \mathcal{M}} P(m) \log P(m \text{ valid}).$$

Use of Lemma 11 gives

$$\log P_I = \max_m \log P(m \text{ valid}) \geq \sum_{m \in \mathcal{M}} P(m) \log P(m \text{ valid}) \geq -I(M; E_R).$$

We obtain the bound $P_I \geq 2^{-I(M; E_R)}$. Going back to (3a) and (3b) we can see that P_I depends only on two different things, $\chi(m, e_r)$ and $P(e_r)$. This means that we do not have to use the given probability distribution $P(m, e_r)$, but can consider any possible distribution $P(m, e_r)$ such that it leaves the marginal distribution $P(e_r)$ invariant and such that if $\chi(m, e_r) = 0$, then $P(m, e_r) = 0$. The bound $P_I \geq 2^{-I(M; E_R)}$ is then valid for all these possible distributions. Thus we strengthen the obtained bound by taking the infimum over all these possible distributions. The existence of one such distribution is clear from the one given in the system. □

The remaining four proofs can be given in a similar manner, but we instead choose to give a more general proof. We need a general result, which we give as a lemma. This lemma is then specialized to prove the remaining theorems in a very simple way. Note also that from this lemma we can provide simple proofs of similar bounds on other kinds of attack, for example bounds on A^2-codes for multiple use.

We start by giving some general definitions. Let $\mathbf{\Omega}$ denote the cartesian product of some arbitrary sets and let $\omega \in \mathbf{\Omega}$. For example, we can have $\mathbf{\Omega} = \mathcal{M} \times \mathcal{E}_R$ and $\omega = (m, e_r)$. Let $\mathbf{\Omega}$ be a random variable taken from $\mathbf{\Omega}$ and also, let M_x and E_x be random variables taken from $\mathcal{M}_x$ and $\mathcal{E}_x$.

Now we define the authentication function $\chi(m_x, e_x, \omega)$ to be a characteristic function, i.e., it only takes the values 0 and 1. It must also have the property that $\chi(m_x, e_x, \omega) = 0$ implies $P(m_x, e_x|\omega) = 0$ if $P(\omega) \neq 0$.

We assume that the probability of success in a general attack, denoted P_x, is described as

$$P_x = \sum_{\substack{\omega \in \mathbf{\Omega} \\ P(\omega) \neq 0}} P(\omega) \left[\max_{m_x} P(m_x \text{ valid}|\omega) \right], \tag{18a}$$

$$P(m_x \text{ valid}|\omega) = \sum_{e_x \in \mathcal{E}_x} \chi(m_x, e_x, \omega) P(e_x|\omega). \tag{18b}$$

We now have the following.

Lemma 12: The probability of success for a general attack P_x is lower bounded by

$$P_x \geq 2^{-\inf I(M_x; E_x|\Omega)}, \tag{19}$$

where the infimum is taken over all possible values of the joint distribution $P(m_x, e_x, \omega)$ such that

i) the marginal distribution $P(e_x, \omega)$ is the same as for the given system,

ii) the property that if $\chi(m_x, e_x, \omega) = 0$, then $P(m_x, e_x, \omega) = 0$ still holds.

Proof: The proof is similar to the one given in the impersonation case. By definition we have

$$I(M_x; E_x|\Omega) = \sum_{\substack{m_x \in \mathcal{M}_x,\ \omega \in \Omega \\ P(m_x, \omega) \neq 0}} P(m_x, \omega) \left(\sum_{e_x \in \mathcal{E}_x} P(e_x|m_x, \omega) \cdot \log \frac{P(e_x|m_x, \omega)}{P(e_x|\omega)} \right).$$

The summation over the receiver's encoding rules is restricted to all e_x for which $\chi(m_x, e_x, \omega) = 1$, since $\chi(m_x, e_x, \omega) = 0$ implies that $P(e_x|m_x, \omega) = 0$ when $P(m_x, \omega) \neq 0$. We equivalently write

$$I(M_x; E_x|\Omega) = \sum_{\substack{m_x \in \mathcal{M}_x,\ \omega \in \Omega \\ P(m_x, \omega) \neq 0}} P(m_x, \omega) \left(\sum_{e_x \in \mathcal{E}_x} P(e_x|m_x, \omega)\chi(m_x, e_x, \omega) \cdot \log \frac{P(e_x|m_x, \omega)\chi(m_x, e_x, \omega)}{P(e_x|\omega)\chi(m_x, e_x, \omega)} \right).$$

Using the log-sum inequality this is rewritten as the inequality

$$I(M_x; E_x|\Omega) \geq \sum_{\substack{m_x \in \mathcal{M}_x,\ \omega \in \Omega \\ P(m_x, \omega) \neq 0}} P(m_x, \omega) \left(\sum_{e_x \in \mathcal{E}_x} P(e_x|m_x, \omega) \cdot \chi(m_x, e_x, \omega) \cdot \log \frac{\left(\sum_{e_x \in \mathcal{E}_x} P(e_x|m_x, \omega)\chi(m_x, e_x, \omega) \right)}{\left(\sum_{e_x \in \mathcal{E}_x} P(e_x|\omega)\chi(m_x, e_x, \omega) \right)} \right).$$

Since $P(m_x, \omega) \neq 0$ we have that $\sum_{e_x \in \mathcal{E}_x} P(e_x|m_x, \omega)\chi(m_x, e_r, \omega) = 1$ and $\sum_{e_x \in \mathcal{E}_x} P(e_x|\omega)\chi(m_x, e_x, \omega) = P(m_x \text{ valid}|\omega)$. The inequality reduces to

$$I(M_x; E_x|\Omega) \geq - \sum_{\substack{\omega \in \Omega \\ P(\omega) \neq 0}} P(\omega) \sum_{m_x \in \mathcal{M}_x} P(m_x|\omega) \cdot \log P(m_x \text{ valid}|\omega).$$

Using Lemma 11 and Lemma 10 we get

$$\begin{aligned} \log P_x &= \log \left(\sum_{\substack{\omega \in \Omega \\ P(\omega) \neq 0}} P(\omega) \left[\max_{m_x} P(m_x \text{ valid}|\omega) \right] \right) \\ &\geq \log \left(\sum_{\substack{\omega \in \Omega \\ P(\omega) \neq 0}} P(\omega) \left[\sum_{m_x \in \mathcal{M}_x} P(m_x|\omega) P(m_x \text{ valid}|\omega) \right] \right) \\ &\geq \sum_{\substack{\omega \in \Omega \\ P(\omega) \neq 0}} P(\omega) \left[\sum_{m_x \in \mathcal{M}_x} P(m_x|\omega) \log P(m_x \text{ valid}|\omega) \right] \\ &\geq -I(M_x; E_x|\Omega). \end{aligned}$$

We obtain the bound $P_x \geq 2^{-I(M_x; E_x|\Omega)}$. Going back to (18a) and (18b) we can see that P_x depends only of two different things, $\chi(m_x, e_x, \omega)$ and $P(e_x, \omega)$. Thus we can consider any possible distribution $P(m_x, e_x, \omega)$ such that it leaves the marginal distribution $P(e_x, \omega)$ invariant and such that if $\chi(m_x, e_x, \omega) = 0$, then $P(m_x, e_x, \omega) = 0$. We strengthen the bound by taking the infimum over all these possible distributions.

The existence of a joint distribution $P(m_x, e_x, \omega)$ such that i) and ii) hold must be checked whenever this lemma is used. □

This lemma immediately gives the first part of the remaining proofs. To make things clear, we also prove Theorem 1 again, now giving the full proof.

Proof of Theorem 1: Choose $M_x = M$, $E_x = E_R$, and $\Omega = \emptyset$. Lemma 12 gives the result. The existence of a joint distribution $P(m, e_x)$ such that i) and ii) hold is clear from the one given in the system.

For the second inequality, we consider the given joint distribution $P(m, e_r, e_t)$ in the system. The message M is generated by the transmitter due to his encoding rule E_T. Thus the generated message M and the receiver's encoding rule E_R are independent when E_T is given and we have $P(m|e_r, e_t) = P(m|e_t)$. As a consequence we get

$$I(M; E_R) = I(E_R; E_T) + I(E_R; E_T|M).$$

The given distribution is valid in (4) and if it is used instead of taking the infimum we have

$$P_I \geq 2^{-I(M; E_R)} = 2^{-I(E_R; E_T) + I(E_R; E_T|M)}. \qquad \square$$

Proof of Theorem 2: Choose $M_x = M'$, $E_x = E_R$, and $\Omega = M$. Lemma 11 and Lemma 12 give the result. The existence of a joint distribution $P(m', m, e_r)$ such that i) and ii) hold must be checked. If for every receiver's encoding rule e_r, there are at least two valid messages corresponding to different source states, then such a distribution exists. Thus we must have $|S| \geq 2$.

For the second inequality, consider the joint distribution $P(m', m, e_r, e_t)$, as above. Here both i) and ii) in (7) hold. Since M' is generated from the pair M, E_T, it is independent of E_R and we have $P(m'|m, e_r, e_t) = P(m'|m, e_t)$. From this independence we derive

$$I(M'; E_R|M) = I(E_R; E_T|M) + I(E_R; E_T|M', M).$$

Thus we can modify the lower bound of (7) in the following way:

$$\begin{aligned} P_S &\geq 2^{-I(M';E_R|M)} \\ &= 2^{-I(E_R;E_T|M)+I(E_R;E_T|M',M)} \\ &\geq 2^{-I(E_R;E_T|M)}. \end{aligned}$$ □

Proof of Theorem 3: Choose $M_x = M$, $E_x = E_R$, and $\Omega = E_T$. Lemma 12 gives the result. We now check the existence of a suitable distribution. Assume that the receiver's key e_r and the transmitter's key e_t is given and $P(e_r, e_t) \neq 0$. Then there must exist at least one message m such that $\chi(m, e_r, e_t) = 1$. This will be true if the number of messages accepted by the receiver as authentic due to his encoding rule e_r is larger than the number of source states. This must hold for all possible keys at the receiver and thus $\min_{e_r \in \mathscr{E}_R} n(e_r) > |S|$.

To prove (11) we observe that all valid distributions in (10) have the same marginal distribution $P(e_r, e_t)$ as the distribution given in the system. If we use one of these distributions in (10) we have

$$P_T \geq 2^{-H(E_R|E_T)+H(E_R|M,E_T)} \geq 2^{-H(E_R|E_T)}.$$

The bound is valid for the given distribution of the encoding rules. □

Proof of Theorem 4: Choose $M_x = M$, $E_x = E_T$, and $\Omega = E_R$. Lemma 12 gives the result. It is obvious that a distribution exists, such that i) and ii) in the theorem hold.

For the second inequality, simply choose the joint distribution $P(m, e_r, e_t)$ as for the given system. This distribution is valid in (13) and thus the inequality holds. □

Proof of Theorem 5: Choose $M_x = M'$, $E_x = E_T$, and $\Omega = (M, E_R)$.

Lemma 11 and Lemma 12 give the result. Similarly as in the proof of Theorem 2 a distribution, such that i) and ii) in the theorem hold, exists if $|S| \geq 2$.

To prove (17) we observe that all valid distributions have the same marginal distribution $P(m, e_r, e_t)$ as the one given in the system. Using one such distribution in (16) we have

$$P_{R_1} \geq 2^{-H(E_T|M,E_R)+H(E_T|M',M,E_R)} \geq 2^{-H(E_T|M,E_R)}.$$

The bound is valid for the given distribution. □

ACKNOWLEDGMENT

The author wishes to thank B. Smeets for spending considerable time giving valuable comments on this work.

REFERENCES

[1] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *Bell Syst. Tech. J.*, vol. 53, pp. 405–424, 1974.

[2] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology, Proc. CRYPTO 84*, G. R. Blakley and D. Chaum, Eds., Lecture Notes in Computer Science, Vol. 196. New York: Springer, 1985, pp. 411–431.

[3] J. L. Massey, "Contemporary cryptology, an introduction," in *Contemporary Cryptology, The Science of Information Integrity*, G. J. Simmons, Ed. New York: IEEE Press, 1991, pp. 3–39.

[4] G. J. Simmons, "A Cartesian product construction for unconditionally secure authentication codes that permit arbitration," *J. Cryptology*, vol. 2, no. 2, pp. 77–104, 1990.

[5] ——, "Message authentication with arbitration of transmitter/receiver disputes," in *Proc. Eurocrypt '87*, Amsterdam, The Netherlands, April 13–15, 1987, D. Chaum and W. L. Price, Eds. Berlin: Springer-Verlag, 1988, pp. 151–165.

[6] R. G. Gallager, *Information Theory and Reliable Communications*. New York: Wiley, 1968.

[7] E. F. Brickell and D. R. Stinson, "Authentication codes with multiple arbiters," in *Proc. Eurocrypt '88*, Davos, Switzerland, May 25–27, 1988, C. G. Günter, Ed. Berlin: Springer-Verlag, 1988, pp. 51–55.

[8] Y. Desmedt and M. Yung, "Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attack," in *Proc. Crypto '90*. Berlin: Springer-Verlag, pp. 177–188.

[9] R. Johannesson and A. Sgarro, "Strengthening Simmons' bound on Impersonation," in *IEEE Trans. Inform. Theory*, vol. 37, pp. 1182–1185, July 1991.

[10] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981, p. 48.

[11] B. Smeets, "Bounds on the probability of deception in multiple authentication," *IEEE Trans. Inform. Theory*, see this issue.

[12] Z.-X. Wan, *Geometry of Classical Groups over Finite Fields*. Lund: Studentlitteratur, 1993.

[13] T. Johansson, G. Kabatianskii, and B. Smeets, "On the relation between A-codes and codes correcting independent errors," in *Proc. Eurocrypt '93*, Berlin: Springer-Verlag, 1994, pp. 1–11.

[14] W. Feller, *An introduction to Probability Theory and Its Applications, Vol. 2*. New York: Wiley, 1966, pp. 153–154.