Appeared in *Proc. 13th Symp. on Theoretical Aspects of Computer Science (STACS'96)*, Lecture Notes in Computer Science, Berlin: Springer-Verlag, vol. 1046, pp. 387-398, 1996.

A Unified and Generalized Treatment of Authentication Theory

Ueli M. Maurer

Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
E-mail address: maurer@inf.ethz.ch

Abstract. This paper provides a unified and generalized treatment of information-theoretic lower bounds on an opponent's probability of cheating in one-way message authentication. It extends and generalizes, in a number of directions, the substantial body of known results, each of which holds only for a certain restricted scenario. At the same time the treatment of unconditionally-secure authentication is simplified considerably.

Keywords. Cryptography, unconditionally-secure authentication, information theory.

1 Introduction

Authentication theory is concerned with providing evidence to the receiver of a message that it was sent by a specified legitimate sender, even in the presence of an opponent who can intercept messages sent by the legitimate sender and/or send a fraudulent message to the receiver. Authenticity (like confidentiality) can be achieved by cryptographic coding based on a secret key shared by sender and receiver.

This paper is concerned with information-theoretically secure message authentication, i.e., we consider a scenario in which the opponent has unlimited computing power and knows everything about the system, except for the secret key. We consider bounds on how efficiently a secret key shared by sender and receiver can be used or, more precisely, we derive lower bounds on an opponent's cheating probability that no authentication system with a given key size can overcome.

Compared to the theory of secrecy, authentication theory is more subtle and involved. For instance, while Shannon's definition of perfect secrecy [11], which means that ciphertext and plaintext are statistically independent, is obviously the strongest possible definition of secrecy, it is not clear how perfect authenticity should be defined. Shannon [11] proved the well-known result that for any perfect cipher the secret key must be at least as long as the plaintext or, more precisely, that $H(Z) \geq H(X)$ where X and Z denote the message and the secret key, respectively.

After some purely combinatorial lower bound results in authentication theory had been derived [4], [3], Simmons [12] initiated a sequence of research activities on information-theoretic lower bounds in authentication theory [2], [5], [6], [7], [9], [10], [13], [14], [15], [17].

The problem of deciding whether a received message is authentic or not is a hypothesis testing problem. The receiver must decide which of two hypotheses is true: either the message was generated by the legitimate sender knowing the secret key, or by an opponent without *a priori* knowledge of the secret key. The joint probability distribution of the authenticated message and the secret key is different in both cases, and this allows the receiver to distinguish between the two hypotheses. This natural interpretation as a hypothesis testing problem is the key to both a generalized and simplified treatment of lower bound results in authentication theory. It is our hope that this paper provides the right view of a problem whose previous treatment has been quite complicated.

2 Description of the scenario

Consider a scenario in which a sender and a receiver share a secret key Z. The sender wants to send a sequence of plaintext messages $X_1, X_2, \ldots, X_n$, at some independent time instances, in an authenticated manner to the receiver. Each message X_i is authenticated separately by sending an encoded message Y_i which depends (possibly probabilistically) on Z, X_i, and possibly also on the previous plaintext messages $X_1, \ldots, X_{i-1}$ and encoded messages $Y_1, \ldots, Y_{i-1}$. Based on Y_i and Z, and possibly also on $X_1, \ldots, X_{i-1}$ and $Y_1, \ldots, Y_{i-1}$, the receiver decides to either reject the message or accept it as authentic and, in case of acceptance, decodes Y_i to a message $\hat{X}_i$. It is assumed that the receiver is synchronized, i.e., he knows the message number i. We assume that X_i is uniquely determined by $X_1, \ldots, X_{i-1}$, $Y_1, \ldots, Y_i$ and Z and hence, by induction, also by $Y_1, \ldots, Y_i$ and Z alone. This is equivalent to

$$H(X_i | Y_1 \ldots Y_i Z) = 0.$$

Information-theoretic concepts, in particular entropy measures, are reviewed in the Appendix. An authentication code can either provide no secrecy, i.e.

$$H(X_i | Y_1 \ldots Y_i) = 0$$

(or more typically even $H(X_i | Y_i) = 0$), or it can provide some degree of secrecy when

$$H(X_i | Y_1 \ldots Y_i) > 0.$$

Authentication schemes without secrecy are often called Cartesian. Our results apply to both cases.

As usual it is assumed that an opponent knows everything about the system, including the codes used and the plaintext statistics, but that he has no *a priori* information about the secret key. In order to remove a possible source of confusion it should be pointed out that in the literature plaintext message and encoded message are also referred to as source state and message, denoted by S and M, respectively. We follow Massey's terminology [7].

An opponent with read and write access to the communication channel can use either of two different strategies for cheating. In a so-called *impersonation attack* at time i, the opponent waits until he has seen the encoded messages $Y_1, \ldots, Y_{i-1}$ (which he lets pass unchanged to the receiver) and then sends a fraudulent message $\tilde{Y}_i$ which he hopes to be accepted by the receiver as the ith message. In a so-called *substitution attack* at time i, the opponent lets pass messages $Y_1, \ldots, Y_{i-1}$, intercepts Y_i, and replaces it by a different message $\tilde{Y}_i$ which he hopes to be accepted by the receiver. In a substitution attack, an opponent can of course only be considered successful when $\tilde{Y}_i$ is decoded by the receiver to a plaintext message $\hat{X}_i$ different from X_i sent by the sender.

In order to define what it means for an opponent to be successful in an impersonation or a substitution attack, we can distinguish three cases: The opponent is considered successful when

(a) the receiver accepts $\tilde{Y}_i$ as a valid message[1].

(b) the receiver accepts $\tilde{Y}_i$ as a valid message and decodes it to a message $\hat{X}_i$ *known* to the opponent. In other words, an opponent is only considered successful if he also guesses the receiver's decoded message $\hat{X}_i$ correctly.

(c) The receiver accepts $\tilde{Y}_i$ as a valid message and decodes it to a particular message $\hat{X}_i = x$ *chosen* by the opponent. This type of attack depends on a particular value x.

Note that cases (b) and (c) differ from (a) only when the plaintext message is not contained in (or uniquely determined by) the encoded message, i.e., when the system also provides some degree of confidentiality. In this extended abstract we will only consider the first case, but our results can be generalized to the more general cases (b) and (c).

For a given authentication scheme we will denote the probabilities of success for an optimal attack by $P_{I,i}$ for an impersonation attack at time i and by $P_{S,i}$ for a substitution attack at time i. When considering the same probabilities for a particular observed sequence

$$Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$$

of encoded messages and, in case of a substitution attack also for a fixed intercepted message $Y_i = y_i$, then we denote the corresponding probabilities by

$$P_{I,i}(y_1, \ldots, y_{i-1})$$

for an impersonation attack at time i and by

$$P_{S,i}(y_1, \ldots, y_i)$$

[1] In the literature only this case has been considered.

for a substitution attack at time i. Note that, for instance, $P_{I,i}$ is the expected value of $P_{I,i}(y_1, \ldots, y_{i-1})$, i.e.

$$P_{I,i} = \sum_{(y_1,\ldots,y_{i-1})} P_{Y_1,\ldots,Y_{i-1}}(y_1, \ldots, y_{i-1}) \cdot P_{I,i}(y_1, \ldots, y_{i-1}).$$

and

$$P_{S,i} = \sum_{(y_1,\ldots,y_i)} P_{Y_1,\ldots,Y_i}(y_1, \ldots, y_i) \cdot P_{S,i}(y_1, \ldots, y_i).$$

3 Review of previous results

The significance of a lower bound result in authentication theory depends on the generality of the model considered. Instead of reviewing the various papers on the subject in detail, we briefly summarize the various restrictions of the existing results and the generalizations achieved in this paper. We refer to [7], [9] and [17] for reviews of the literature on the subject.

- Some papers consider the authentication of only a single message [4], [5], [7], [10], [12], [16]. Most of the papers dealing with the authentication of several plaintext messages $X_1, X_2, \ldots$ consider only schemes that apply the same encoding rule to every plaintext message X_i, thus assuming that all plaintext messages are different and belong to the same message space [3], [9], [17]. This assumption is necessary to prevent replay attacks in this model, but it appears to be quite unnatural. The only previous papers considering time-dependent encoding rules are [13], [14], and [15].

- Some papers are restricted to deterministic encoding rules referred to as authentication codes without splitting [3], [4], [5], [12], [14], [17].

- Some papers are restricted to authentication without secrecy, i.e. where the encoded message uniquely determines the plaintext message [3], [12], [16], [14], [17]. Such schemes are sometimes referred to as Cartesian.

- In all previous papers it is assumed that the receiver never errs when seeing a valid message, i.e., that his strategy is to accept a message if and only if it is consistent with the key Z. Our results are more general in that we also provide bounds on an opponent's cheating probability for a given tolerable probability of rejecting a valid message. While this generalization does not appear to be of much practical interest, it is useful because it establishes the link to the standard hypothesis testing scenario.

Our results hold in a general model without any of the discussed restrictions. Moreover, we need not assume that $X_1, X_2, \ldots$ are independent and we can allow the encoding rule for message X_i to depend on the previous plaintext messages $X_1, \ldots, X_{i-1}$. Furthermore, as discussed above, the realistic alternative models in which an opponent is considered successful only when he knows (or can choose) the plaintext message to which the receiver decodes the fraudulent message, have not been considered previously.

4 Hypothesis testing

Hypothesis testing is the task of deciding which of two hypotheses, H_0 or H_1, is true, when one is given the value of a random variable U (e.g., the outcome of a measurement). The behavior of U is described by two probability distributions: If H_0 or H_1 is true, then U is distributed according to the distribution $P_{U|H_0}$ or $P_{U|H_1}$, respectively. For ease of notation we will write $P_{U|H_0} = P_U$ or $P_{U|H_1} = Q_U$. A decision rule assigns one of the two hypotheses to each possible u that U can assume. There are two types of possible errors in making a decision. Accepting hypothesis H_1 when H_0 is actually true is called a type I error, and the probability of this event is denoted by α. Accepting hypothesis H_0 when H_1 is actually true is called a type II error, and the probability of this event is denoted by β. The optimal decision rule is given by the famous Neyman-Pearson theorem which states that, for a given maximal tolerable probability β of type II error, α can be minimized by assuming hypothesis H_0 if and only if

$$\log \frac{P_U(u)}{Q_U(u)} \geq T \tag{1}$$

for some threshold T, where here and in the sequel logarithms are to the base 2. (Note that only the existence of T, but not its value is specified by this theorem.) The term on the left of (1) is called the log-likelihood ratio. We refer to [1] for an excellent treatment of hypothesis testing.

Let P_U and Q_U be arbitrary probability distributions over the same finite or countably infinite set $\mathcal{U}$. The expected value of the log-likelihood ratio with respect to P_U is called the discrimination and is defined by

$$L(P_U;Q_U) = \sum_{u\in\mathcal{U}} P_U(u) \log \frac{P_U(u)}{Q_U(u)}.$$

The discrimination is non-negative and is equal to zero if and only if the two distributions are identical.

A well-known result in hypothesis testing (cf. [1], Theorem 4.4.1[2]) provides a relation between the error probabilities α and β and the discrimination $L(P_U;Q_U)$. Let the function $d(\alpha,\beta)$ be defined by

$$\begin{aligned} d(\alpha,\beta) &\stackrel{\triangle}{=} \alpha \log \frac{\alpha}{1-\beta} + (1-\alpha)\log\frac{1-\alpha}{\beta} \\ &= -h(\alpha) - \alpha\log(1-\beta) - (1-\alpha)\log\beta. \end{aligned}$$

where $h(\alpha) \stackrel{\triangle}{=} -\alpha\log\alpha - (1-\alpha)\log(1-\alpha)$ is the binary entropy function.

Lemma 1. *The type I and type II error probabilitites α and β satisfy*

$$d(\alpha,\beta) \;\leq\; L(P_U;Q_U).$$

[2] Note that in our formulation of this result we have exchanged α and β as well as P_U and Q_U.

In particular, for $\alpha = 0$ we have $-\log\beta \leq L(P_U;Q_U)$ which is equivalent to

$$\beta \geq 2^{-L(P_U;Q_U)}.$$

Consider the special case of hypothesis testing where $U = [S,T]$ consists of a pair of random variables S and T, where $P_U = P_{ST}$ is the actual joint distribution of this pair and where $Q_U = P_S P_T$ is the product of the two marginal distributions. This case will be important in the analysis of impersonation attacks. Note that P_{ST} and $P_S P_T$ are both probability distributions over the same set $\mathcal{S} \times \mathcal{T}$ when S and T take on values in $\mathcal{S}$ and $\mathcal{T}$, respectively. We have

$$\begin{aligned} L(P_{ST};P_S P_T) &= \sum_{s,t} P_{ST}(s,t) \log \frac{P_{ST}(s,t)}{P_S(s)P_T(t)} \\ &= H(S) + H(T) - H(ST) \\ &= I(S;T) \qquad (2) \end{aligned}$$

where the entropy $H(S)$ of a random variable S and the other information theoretic quantities are defined in the Appendix. We also refer to [1] for an excellent introduction to information theory. The second and third step of (2) follow from these definitions. We have $L(P_{ST};P_S P_T) = 0$ if and only if the two distributions P_{ST} and $P_S P_T$ are identical, i.e., if and only if S and T are statistically independent. This fact is needed for deriving the conditions for equality in the lower bounds, which is omitted in this extended abstract.

Consider now a hypothesis testing scenario in which the distributions P_U and Q_U depend on the value of an additional random variable V known to the testing person, i.e., we consider a collection of pairs $(P_{U|V=v}, Q_{U|V=v})$ of distributions, each pair ocurring with probability $P_V(v)$. The hypothesis testing strategy may depend on the value v of V, and for each v we can define $\alpha(v)$ and $\beta(v)$ as the error probabilities of type I and II, respectively, given that $V = v$. An elternative form of Lemma 1 is

$$d(\alpha(v), \beta(v)) \ \leq \ L(P_{U|V=v}; Q_{U|V=v}). \qquad (3)$$

The following lemma provides a lower bound similar to Lemma 1 where α and β are taken as the average (over values of V) error probabilities.

Lemma 2. *The average error probabilities of type I and II,*

$$\alpha = \sum_v P_V(v)\alpha(v) \quad \text{and} \quad \beta = \sum_v P_V(v)\beta(v),$$

respectively, satisfy

$$d(\alpha,\beta) \ \leq \ \sum_v P_V(v) L(P_{U|V=v}; Q_{U|V=v}).$$

Proof (sketch): The function $d(\alpha,\beta)$ is a convex-∪ function in both its arguments and hence one can apply Jensen's inequality (cf. [1]). □

Lemma 2 holds of course also for distributions conditioned on the event that a further random variable W takes on a particular value w known to the testing person, i.e., for pairs $(P_{U|V=v,W=w}, Q_{U|V=v,W=w})$ of distributions. The two error probabilities $\alpha(v,w)$ and $\beta(v,w)$ also depend on w. The following corollary follows directly from Lemma 2.

Corollary 3. *The average error probabilities of type I and II, over choices of V,*

$$\alpha(w) = \sum_v P_V(v)\alpha(v,w) \quad \text{and} \quad \beta(w) = \sum_v P_V(v)\beta(v,w),$$

respectively, satisfy

$$d(\alpha(w), \beta(w)) \;\leq\; \sum_v P_V(v) L(P_{U|V=v,W=w}; Q_{U|V=v,W=w}).$$

In analogy to above, consider the special cases of hypothesis testing where $U = [S,T]$ consists of a pair of random variables S and T whose distribution depends on a random variable V, and consider the collection of pairs of distributions

$$(P_{U|V=v}, Q_{U|V=v}) = (P_{ST|V=v}, P_{S|V=v}P_{T|V=v}),$$

each pair ocurring with probability $P_V(v)$. Then the expression on the left side of the inequality in Lemma 2 becomes

$$\begin{aligned}\sum_v P_V(v) L(P_{U|V=v}; Q_{U|V=v}) &= \sum_v P_V(v) L(P_{ST|V=v}, P_{S|V=v}P_{T|V=v}) \\ &= \sum_v P_V(v) I(S;T|V=v) \\ &= I(S;T|V). \end{aligned} \tag{4}$$

Similarly, when $(P_{U|V=v}, Q_{U|V=v}) = (P_{ST|V=v,W=w}, P_{S|V=v,W=w}P_{T|V=v,W=w})$, each pair ocurring with probability $P_{VW}(v,w)$, Then the expression on the left side of the inequality in Corollary 3 becomes

$$\sum_v P_V(v) L(P_{U|V=v,W=w}; Q_{U|V=v,W=w}) = I(S;T|V, W=w). \tag{5}$$

5 Impersonation attacks

Let us now return to the analysis of message authentication. The problem of deciding whether a received message $\tilde{Y}$ is authentic or not can be viewed as a hypothesis testing problem. H_0 corresponds to the hypothesis that the message is authentic, and H_1 corresponds to the hypothesis that the message has been generated by an opponent. Referring to Section 4, we are interested in proving lower bounds on β, for a given tolerated upper bound on α. Such a result is stated in the form $d(\alpha,\beta) \leq B$ for some bound B which for $\alpha = 0$ implies $-\log\beta \leq B$:

$$d(\alpha,\beta) \leq B \quad \Longrightarrow \quad \beta \geq 2^{-B}. \tag{6}$$

Consider an impersonation attack on the ith message X_i. The receiver knows Z and the messages $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$, and sees a message $\overline{Y}_i$, which could either be a correct message $\overline{Y}_i = Y_i$ sent by the legitimate receiver (hypothesis H_0) or a fraudulent message $\overline{Y}_i = \tilde{Y}_i$ inserted by an opponent (hypothesis H_1). A potential opponent would choose $\tilde{Y}_i$ depending on the observed messages $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$, but without further knowledge about the secret key. In its most general form, an opponents strategy for impersonation at time i can hence be described by an arbitrary probability distribution $Q_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$, where we have used the symbol Q instead of P to distinguish this distribution from the actual distribution $P_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$ induced by a legitimate sender. Note that in a deterministic (non-splitting) strategy, $Q_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$ is equal to 1 for one particular value y_i and zero otherwise.

Consider probability distributions conditioned on the event $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$. Under hypothesis H_0, the pair $[\overline{Y}_i, Z]$ (seen by the receiver) is generated according to the probability distribution $P_{Y_i Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$, whereas under hypothesis H_1, $[\overline{Y}_1, Z]$ is generated according to the distribution $Q_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}} \cdot P_{Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$.

An information-theoretic lower bound is obtained by observing that one admissible (but generally not optimal) strategy is to let

$$Q_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}} = P_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}.$$

Observe that the distribution $P_{\tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$ is known to the opponent. Recall the definitions of $P_{I,i}$ and $P_{I,i}(y_1, \ldots, y_{i-1})$ from Section 2. The following theorem generalizes results of several papers, including those by Walker [17], Rosenbaum [9], and Smeets [14].

Theorem 4. *For every authentication scheme,*

$$d(\alpha, P_{I,i}(y_1, \ldots, y_{i-1})) \;\leq\; I(Y_i; Z|Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1})$$

and, for $\alpha = 0$,

$$P_{I,i}(y_1, \ldots, y_{i-1}) \;\geq\; 2^{-I(Y_i;Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1})}.$$

Furthermore,

$$d(\alpha, P_{I,i}) \;\leq\; I(Y_i; Z|Y_1 \ldots Y_{i-1})$$

and, for $\alpha = 0$,

$$P_{I,i} \;\geq\; 2^{-I(Y_i;Z|Y_1 \ldots Y_{i-1})}.$$

Proof. The first inequality follows from (3) for $v = [y_1, \ldots, y_{i-1}]$, $U = [Y_i, Z]$, $P_U = P_{Y_i Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$ and $Q_U = P_{Y_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}} \cdot P_{Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$. The third inequality follows from Lemma 2, and the second and fourth inequalities follow from (6). □

Consider now scenario (b) mentioned in Section 2, i.e., in addition to having $\tilde{Y}_i$ accepted by the receiver the opponent also wants to know the message $\hat{X}_i$ the receiver decodes it to. One admissible (but generally not optimal) strategy is to choose the pair $[\tilde{X}_i, \tilde{Y}_i]$ according to some distribution $Q_{\tilde{X}_i \tilde{Y}_i|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}}$. Using similar arguments as those used above one can prove the following bound on the average probability $P'_{I,i}$ of cheating in an optimal attack:

$$P'_{I,i} \ \geq \ 2^{-I(X_iY_i;Z|Y_1,\ldots,Y_{i-1})}.$$

Consider now scenario (c) mentioned in Section 2, i.e., in addition to having $\tilde{Y}_i$ accepted by the receiver, the opponent also wants the decoded message $\hat{X}_i$ to be equal to a particular value x. One can prove the following bound on the average probability $P''_{I,i,x}$ of cheating in an optimal attack

$$P''_{I,i,x} \ \geq \ 2^{-I(X_iY_i;Z|Y_1,\ldots,Y_{i-1},X_i=x)}.$$

6 Substitution attacks

When an opponent guesses the secret key Z correctly, he can launch any attack of his choice, for instance any of the three forms of substitution attacks. In this section we therefore derive lower bounds on an opponent's probability of guessing the correct value of Z.

Let S be a random variable. The entropy $H(S)$ is the expected value of $-\log P_S(S)$. Because the minimum of the values occurring in the averaging, $\min_s(-\log P_S(s))$, is upper bounded by the average, it is straight-forward to prove that

$$\min_s(-\log P_S(s)) = -\log(\max_s P_S(s)) \leq H(S)$$

and hence that the probability of guessing S correctly when knowing only P_S is lower bounded by

$$\max_s P_S(s) \geq 2^{-H(S)}.$$

Similarly, and by application of Jensen's inequality, one obtains

$$\sum_t P_T(t) \max_s P_{S|T}(s,t) \geq 2^{-H(S|T)}$$

as a lower bound on the average (over choices of T) probability of guessing S correctly when knowing $P_{S|T}$ and T. These observations lead to the following theorem which generalizes results in the literature.

Theorem 5. *We have*

$$P_{S,i}(y_1,\ldots,y_i) \geq 2^{-H(Z|Y_1=y_1,\ldots,Y_i=y_i)} \tag{7}$$

and

$$P_{S,i} \geq 2^{-H(Z|Y_1,\ldots,Y_i)}. \tag{8}$$

These bounds also hold for the other two types (b) and (c) of substitution attacks.

The jounal version of this paper will describe an alternative derivation of a more general version of these results by using the results on hypothesis testing.

7 Conclusions

The results of this paper can be combined as described in the following. When a sequence of n messages $X_1, \ldots, X_n$ is to be authenticated, an opponent could choose the type of attack with the highest success probability. A secret key Z is used optimally when the maximum of these probabilities is minimal. If it is required that a legitimate message is always accepted ($\alpha = 0$) in all of these possible attacks, we obtain

$$\begin{aligned} -\sum_{i=1}^{n} \log P_{I,i} - \log P_{S,n} &\leq \sum_{i=1}^{n} I(Y_i; Z|Y_1 \ldots Y_{i-1}) + H(Z|Y_1 \ldots Y_n) \\ &= H(Z). \end{aligned}$$

The following theorem follows from the fact that $-log(.)$ is a convex-$\cup$ function. It generalizes results of Walker [17] and Rosenbaum [9] and states that for a secret key of a given size, the effective security achievable in any authentication scheme for n messages corresponds at most to the difficulty of guessing a secret key whose size is $n+1$ times smaller than the size of the actual secret key. In other words, a part of the secret key is consumed by each message to be authenticated, and the number of key bits consumed by a message corresponds to the negative logarithm of the desirable maximal probability of cheating.

Theorem 6. *For every authentication scheme for authenticating n messages $X_1, \ldots, X_n$ in which the legitimate receiver never rejects a valid message, we have*

$$\max(P_{I,1},, \ldots, P_{I,n}, P_{S,n}) \geq \frac{H(Z)}{n+1}.$$

Appendix

This appendix gives a brief summary of important information-theoretic concepts. All logarithms are to the base 2. The entropy $H(S)$ of a random variable S is defined by

$$H(S) \;=\; -\sum_{s \in \mathcal{S}: P_S(s) \neq 0} P_S(s) \log P_S(s),$$

the conditional entropy of S, given that the random variable T takes on the value t is defined by

$$H(S|T=t) \;=\; -\sum_{s \in \mathcal{S}: P_{S|T=t}(s) \neq 0} P_{S|T=t}(s) \log P_{S|T=t}(s),$$

and the conditional entropy of S, given T is defined by

$$\begin{aligned} H(S|T) &= \sum_{t \in \mathcal{T}} P_T(t) H(S|T=t) \\ &= -\sum_{(s,t) \in \mathcal{S} \times \mathcal{T}: P_{ST}(s,t) \neq 0} P_{ST}(s,t) \log P_{S|T}(s,t). \end{aligned}$$

One can further define

$$H(S|T,V=v)=\sum_{t\in\mathcal{T}}P_{T|V}(t,v)H(S|T=t,V=v)$$

The mutual information between S and T is defined by

$$I(S;T)=H(S)-H(S|T)$$

which is equal to $H(T)-H(T|S)$. The conditional mutual information between S and T, given an event $V=v$, or given the random variable V, are defined by

$$I(S;T|V=v)=H(S|V=v)-H(S|T,V=v)$$

and

$$I(S;T|V)=H(S|V)-H(S|TV)=\sum_{v}P_V(v)I(S;T|V=v),$$

respectively. A further quantity of interest is

$$\begin{aligned}I(S;T|V,W=w) &= H(S|V,W=w)-H(S|TV,W=w)\\ &= \sum_{v}P_{V|W}(v,w)I(S;T|V=v,W=w).\end{aligned}$$

References

[1] R. E. Blahut, *Principles and practice of information theory*, Addison-Wesley, 1987.

[2] E.F. Brickell, A few results in message authentication, *Congressus Numerantium*, vol. 43, pp. 141-154, 1984.

[3] V. Fåk, Repeated use of codes which detect deception, *IEEE Trans. on Information Theory*, Vol. 25, No. 2, 1979, pp. 233-234.

[4] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell Syst. Tech. J.*, Vol. 53, No. 3, 1974, pp. 405-424.

[5] R. Johannesson and A. Sgarro, Strengthening Simmons' bound on impersonation, *IEEE Trans. on Information Theory*, Vol. 37, No. 4, 1991, pp. 1182–1185.

[6] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, *IEEE Trans. on Information Theory*, Vol. 40, No. 5, 1994, pp. 1573-1585.

[7] J.L. Massey, Contemporary cryptology – an Introduction, in *Contemporary cryptology – the science of information integrity*, G.J. Simmons (Ed.), IEEE Press, 1992.

[8] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120–126.

[9] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, *J. of Cryptology*, Vol. 6, No. 3, 1993, pp. 135–156.

[10] A. Sgarro, Information divergence bounds for authentication codes, *Advances in Cryptology – Eurocrypt '89*, J.-J. Quisquater and J. Vandewalle (Eds.), Lecture Notes in Computer Science, No. 434. Berlin: Springer Verlag, 1985, pp. 93-101.

[11] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, Oct. 1949, pp. 656-715.

[12] G. J. Simmons, Authentication theory/coding theory, in *Advances in Cryptology – CRYPTO 84*, G.R. Blakley and D. Chaum (Eds.), Lecture Notes in Computer Science, No. 196, Berlin: Springer Verlag, 1985, pp. 411–431.

[13] G.J. Simmons and B. Smeets, A paradoxical result in unconditionally secure authentication codes – and an explanation, in *Cryptography and Coding II*, C. Mitchell, Ed., Oxford: Clarendon, 1992, pp. 231-258.

[14] B. Smeets, Bounds on the Probability of Deception in Multiple Authentication, *IEEE Trans. on Information Theory*, Vol. 40, No. 5, 1994, pp. 1586-1591.

[15] B. Smeets, P. Vanroose, and Zhe-Xian Wan, On the construction of authentication codes with secrecy and codes which stand against spoofing attacks of order $L \geq 2$, *Advances in Cryptology – Eurocrypt '90*, I.B. Damgård, Ed., Lecture Notes in Computer Science, No. 473, Berlin: Springer Verlag, 1991, pp.306-312.

[16] D. R. Stinson, Some constructions and bounds for authentication codes, *J. of Cryptology*, Vol. 1, No. 1, 1988, pp 37-51.

[17] M. Walker, Information-theoretic bounds for authentication schemes, *J. of Cryptology*, Vol 2, No. 3, 1990, pp. 131–143.