2008

Information theoretic bounds on authentication systems in query model

Reihaneh Safavi-Naini
University of Wollongong, rei@uow.edu.au

Peter R. Wild
Royal Holloway University of London

Publication Details
Information theoretic bounds on authentication systems in query model

Abstract
Authentication codes provide message integrity guarantees in an information theoretic sense within a symmetric key setting. Information theoretic bounds on the success probability of an adversary who has access to previously authenticated messages have been derived by Simmons and Rosenbaum, among others. In this paper, we consider a strong attack scenario where the adversary is adaptive and has access to authentication and verification oracles. We derive information theoretic bounds on the success probability of the adversary and on the key size of the code. This brings the study of unconditionally secure authentication systems on a par with the study of computationally secure ones. We characterize the codes that meet these bounds and compare our result with the earlier ones.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/3213
Information Theoretic Bounds on Authentication Systems in Query Model

Reihaneh Safavi-Naini and Peter R. Wild

Abstract—Authentication codes provide message integrity guarantees in an information theoretic sense within a symmetric key setting. Information theoretic bounds on the success probability of an adversary who has access to previously authenticated messages have been derived by Simmons and Rosenbaum, among others. In this paper, we consider a strong attack scenario where the adversary is adaptive and has access to authentication and verification oracles. We derive information theoretic bounds on the success probability of the adversary and on the key size of the code. This brings the study of unconditionally secure authentication systems on a par with the study of computationally secure ones. We characterize the codes that meet these bounds and compare our result with the earlier ones.

Index Terms—A-codes, authentication system, unconditional security, verification oracle.

I. INTRODUCTION

UNCONDITIONALLY secure authentication systems provide message integrity when the adversary’s computational power is unknown or unlimited. Unconditional security is particularly important when recent advances in quantum computing and prospect of discovery and realization of efficient algorithms for solving “hard” problems, is taken into account.

In an authentication code (A-code) [1], [10], authenticated messages (ciphertexts) encode states of an information source (referred to as plaintexts or source states) by a mapping determined by the shared key (also called the encoding rule). A-codes are symmetric key systems. The receiver verifies the authenticity of a message using the same key as the sender. In a spoofing attack of order \( i \), a message-observing adversary observes \( i \) authenticated messages transmitted by the sender and then tries to construct a fraudulent message called the spoofing message that will be accepted by the receiver. We do not make any assumptions about the computational power of an adversary.

The performance of an A-code is measured by the probability that the spoofing message is accepted by the receiver. Information theoretic bounds [10], [7], [6] for A-codes give fundamental limits on performance of the codes. Rosenbaum [7] and Pei [6] independently derived a bound on the success probability of attackers in spoofing of order \( i \) and employed the bound to derive a lower bound on the key size of A-codes. Extensions and alternative derivations of these bounds are given by a number of authors such as [2] and [4].

We extend this analysis by considering adversaries that may be proactive in gathering information. The adversary might obtain information from the sender by having the sender transmit a message corresponding to source state of the adversary’s choosing or might obtain information from the receiver by sending a message of the adversary’s choosing and observing whether or not the receiver accepts it. Safavi-Naini et al. [8] have considered A-codes with such an adversary in the context of unconditionally secure digital signature schemes (USDS) [9]. This situation, the query model, is modeled in terms of an authentication oracle (A-oracle) that provides the authenticated message corresponding to a query source state (an A-query) in the same way that the sender would and a verification oracle (V-oracle) that provides a response accept or reject to a query message (a V-query) depending on if the receiver would or would not accept the message. This terminology parallels that used for schemes relying on computational security. An attack with access to an A-oracle corresponds to an adaptive chosen plaintext attack, and an attack with access to a V-oracle corresponds to an adaptive chosen ciphertext attack.

In this paper, we study unconditionally secure A-codes (symmetric key) under the query model and derive information theoretic bounds on the success probability of a query attacker.

A. Our Results

We consider an adversary who asks exactly \( i \) queries, observing the responses of the oracle, and then spoofs. We analyze this via an experiment in which the adversary uses a strategy to choose each query adaptively, taking into account all queries and responses previously observed.

1) Bounds on Success Probability: We derive information theoretic bounds on the success probability of the adversary in a general query, response attack model. This can be seen as a generalization of the Rosenbaum–Pei lower bound [7], [6] for spoofing of order \( i \).

2) Constructing Pure Optimal Strategies: An adversary’s success chance is maximized when he uses an optimal strategy. Finding optimal strategies requires solving a constrained maximization problem, taking into account all possible sequences of query and responses, and it results in an adversary strategy that is represented by a sequence of probability distributions. We show that there always exists an optimal strategy for which each of these probability distributions has the property that there
is a unique element with nonzero probability. Such a strategy is called pure and we give a recursive algorithm that constructs this pure optimal strategy.

3) Queries Do Not Decrease Success Chance: It is known that an adversary’s expected chance of spoofing may decrease if the adversary observes a message, compared with his expected chance of spoofing when he spoofs without any observation. A natural question, noting the adversary’s control on the choice of the query, is whether it is always beneficial to the adversary to ask a query if possible. We show that as long as there are “good” queries, asking them will not reduce the average success chance (it may improve it) and so they should be asked. Thus, there is no requirement for the adversary to compute the probabilities in order to make a decision on whether to query in each particular case. In particular, in the case of verification queries for non-trivial schemes, it is always a better strategy to ask the query and then spoof than to spoof without querying.

4) Bounds on Key Entropy: In the case of authentication queries, we use the bound on the probability of success to derive a bound on the entropy of the key space. We establish a combinatorial characterization of the authentication schemes attaining the bound which shows that optimal codes in the authentication query model are also optimal codes in the message observing model.

II. DEFINITIONS

A symmetric key authentication system provides integrity guarantees for two parties, referred to as the sender and the receiver, that share a secret key.

A (symmetric) authentication system consists of two algorithms $\Pi = (\text{Auth}, \text{Ver})$ and is defined over three sets $\mathcal{E}, \mathcal{S},$ and $\mathcal{M}$, which satisfies $\mathcal{M} \subseteq \mathcal{S} \times \mathcal{E}$, and generates a ciphertext $m = \text{Auth}(e, s)$. The entry in row $e$ and column $m$ is $\text{D}(e, m)$ if $\text{Ver}(e, m) = 1$ and $0$ otherwise. Alternatively, we may define its encoding matrix. This matrix has $|\mathcal{S}|$ columns labeled by the source states and has $|\mathcal{E}|$ rows labeled by the encoding rules. The entry in row $e$ and column $s$ is the message $m = \text{Auth}(e, s)$. The set of elements in row $e$ is denoted $\mathcal{M}(e)$ and has exactly $|\mathcal{S}|$ distinct messages. Thus, for an encoding rule $e$, a message $m$ is valid if and only if $m \in \mathcal{M}(e)$.

It is assumed that the adversary knows the encoding matrix but does not know the actual secret encoding rule agreed upon by the sender and the receiver.

A. Adversaries and Success Probability

The traditional adversary model for an authentication code is an adversary who has access to $i$ authenticated messages and attempts to construct a forged message (also called a spoofing message) that would be accepted by the receiver. The best success probability $P_i$ of the adversary in the above attack gives a measure of the security provided by the code.

Simmons [10] derived an information theoretic bound on the success probability of a spoofer when $i = 0$ (an impersonation attack). Rosenbaum [7] and Pei [6] independently derived a general form of the bound for $i > 0$

$$P_i \geq 2^{H(\mathbb{M}^{i+1}) - H(\mathbb{M}^{i})} = 2^{-I(\mathbb{M}; \mathbb{M}^{i})}$$

(1)

where $\mathbb{M}^i$ denotes a random variable associated with the sequence of observed messages $m^i = m_1 m_2 \ldots m_i$.

The bound can be used to derive an information theoretic bound on the entropy or uncertainty (and hence the length) of the key in terms of the success probabilities $P_0, \ldots, P_i$.

1) Adversary With Oracle Access: In [8], the adversary model was strengthened by the addition of access to authentication and verification oracles. This new adversary is adaptive and can ask authentication and verification queries from corresponding oracles. The oracles produce responses to queries in the same way that the legitimate sender and receiver would.

For a given $e \in \mathcal{E}$, an authentication oracle $\text{Auth}(e, \cdot)$ (also called a signature oracle) takes as input a source state $s \in \mathcal{S}$, computes $m = \text{Auth}(e, s)$, and returns response $m$.

A verification oracle $\text{Ver}(\cdot, \cdot)$ receives as input a ciphertext $m \in \mathcal{M}$, computes $b = \text{Ver}(e, m) \in \{0, 1\}$, and returns response $b$.

We use $q$ to denote a query (either an A-query or a V-query $m$) and use $r$ to denote a response (either $m$ or $b$). We denote the set of queries by $Q$ and the set of responses by $R$. Thus, $Q = \mathcal{S}$ and $R = \mathcal{M}$ for A-queries and $Q = \mathcal{M}$ and $R = \{0, 1\}$ for V-queries. Let $x^i = x_1 x_2 \ldots x_i$ denote a sequence of $i$ elements. We also use $x^i$ to denote the set $\{x_1, x_2, \ldots x_i\}$. For
$j < i$, we say $y^j$ is a prefix of $x^i$ if $y^j = x^i, \forall i = 1, \ldots, j$. We use $s^i$, $m^i$, $q^i$, $r^i$, and $(q, r)^i$ to denote a sequence of source states, messages, queries, responses, and query and response pairs, respectively. A strategy $\tau$ of an adversary is a collection of probability distributions that is used to select the queries and also the final spoofing query. If $(q, r)^j$ is a sequence of query and response pairs, then $\tau(q, r)^j$ denotes the probability that $q$ is chosen as the next query (or spoofing message) given that the adversary has asked the sequence $q^j$ of queries and observed the sequence $r^j$ of responses. An adversary’s strategy is a collection of probability distributions $\tau(q, r)^i$.

Let $F^\text{Auth}(e, \cdot), \varnothing(e, \cdot)(i, 1)$ be an adversary that has access to both oracles and uses a strategy $\tau$ to adaptively ask $i$ $A$-queries (receiving the response after each query) and then ask a $V$-query. Let $F^\text{Ver}(e, \cdot)(i, 1)$ be an adversary that has access to only a verification oracle and uses a strategy $\tau$ to adaptively ask $i$ verification queries (receiving the response after each query) and then ask a further verification query.

Consider the following experiments.

Experiment $\text{Exp}_{\Pi, F_{o, r}, (i, 1)}$

$e \leftarrow \mathcal{E}$

\textbf{If} after asking exactly $i$ queries $s^i$ of $\text{Auth}(e, \cdot)$ and receiving corresponding responses $m^i$

$F^\text{Auth}(e, \cdot), \varnothing(e, \cdot)$(i, 1)

makes a query $m$ to the oracle $\text{Ver}(e, \cdot)$ such that the return

$\text{Ver}(e, m) = 1$, and

$m$ had never been returned by the oracle $\text{Auth}(e, \cdot)$

\textbf{then} return 1 \textbf{else} return 0

Experiment $\text{Exp}_{\Pi, F_{v, r}, (i+1)}$

$e \leftarrow \mathcal{E}$

\textbf{If} after asking exactly $i$ queries $m^i$ of $\text{Ver}(e, \cdot)$ and receiving corresponding responses $b^j$

$F^\text{Ver}(e, \cdot), \varnothing(e, \cdot)$ makes a query $m$ to the oracle $\text{Ver}(e, \cdot)$ such that the return

$\text{Ver}(e, m) = 1$, and

$m$ was never asked of the oracle $\text{Ver}(e, \cdot)$

\textbf{then} return 1 \textbf{else} return 0

The output of the experiment is a random variable $\text{Exp}_{\Pi, F_{o, r}, (i, 1)}$ or $\text{Exp}_{\Pi, F_{v, r}, (i+1)}$ on $\{0, 1\}$ corresponding to the success or failure of an adversary who makes $i$ queries to an oracle before spoofing with a (forged) message $m$. Each run of the experiment is one instance of the communicants’ strategy and the adversary’s choices in his attack, and corresponds to a sample point in a probability space where sample points are labeled with a key (the communicants’ choice) and the adversary’s sequence of query and response pairs $(q, r)^i$, $(m, b)$, where $r^i$ is the sequence of responses to the sequence of queries $q^i$ $(g^i \text{ or } m^i)$ and $b = \text{Ver}(e, m)$. Let $p^i_e((q, r)^j)$ denote the probability of the sample point with label $e$, $(q, r)^j$. For the sample points in which the forgery is considered successful the experiment results in 1.

We compute the advantage of the forgers in the previous experiments as the probability of the experiment resulting in 1

\[ \text{Adv}_{\Pi, F_{o, r}, (i, 1)} = Pr[\text{Exp}_{\Pi, F_{o, r}, (i, 1)} = 1] \]
\[ \text{Adv}_{\Pi, F_{v, r}, (i+1)} = Pr[\text{Exp}_{\Pi, F_{v, r}, (i+1)} = 1]. \]

This is the average success probability over all keys (with respect to the distribution given by the communicants’ strategy) when the adversary uses strategy $\tau$. We use the notation $P_i^\tau$ for either of these quantities. This can be written as

\[ P_i^\tau = \sum_{q^i \in Q} \sum_{r^j \in R} \sum_{m \in M} \tau(q^1) \tau(q^2) \cdots \tau(q^i) \tau(r^1) \cdots \tau(r^j) \]
\[ \times \sum_{q^i \in Q} \sum_{r^j \in R} \sum_{m \in M} \tau(q^1) \tau(q^2) \cdots \tau(q^i) \tau(r^1) \cdots \tau(r^j) \]
\[ \times \sum_{e \in \mathcal{E}, \text{Ver}(e, m) = 1} p(e, m, (q, r)^j). \]

The advantage function of $\Pi$ is the advantage of a forger with the highest success probability

\[ \text{Adv}_{\Pi, a}(i, 1) = \max_{F_{o, r}, (i, 1)} Pr[\text{Exp}_{\Pi, F_{o, r}, (i, 1)} = 1] \]
\[ \text{Adv}_{\Pi, a}(i+1) = \max_{F_{v, r}, (i+1)} Pr[\text{Exp}_{\Pi, F_{v, r}, (i+1)} = 1]. \]

The strategy of a forger with this advantage is called an optimal strategy. We write $P_i^\tau$ for either of these quantities.

We say that a key $e$ is consistent with a query and response pair $(q, r)$ if the following holds: 1) if $(q, r) = (s, m)$, then it holds that $\text{Auth}(e, s) = m$; and 2) if $(q, r) = (m, b)$, $b \in \{0, 1\}$, then it holds that $\text{Ver}(e, m) = b$. Let $E((q, r)^j)$ denote the set of keys that are consistent with a query response sequence $(q, r)^j$. The conditional probability $p(e((q, r)^j))$ that the key is $e$ given the sequence of query and response pairs $(q, r)^j$ is nonzero only if $e \in E((q, r)^j)$. Similarly, for $m \in M$, let $E((q, r)^j, (m, 1)) = \{ e \in E((q, r)^j) : m \in \mathcal{M}(e) \}$. For $e \in \mathcal{E}$, we put $\gamma(e, m, (q, r)^j) = 1$ if $e \in E((q, r)^j, (m, 1))$ and $m \not\in q^j \cup r^j$; and $\gamma(e, m, (q, r)^j) = 0$ otherwise.

In the following, we assume $e \in \mathcal{E}$ is chosen by the communicants and is unknown to the adversary. We introduce some notation that records probabilities of certain events in the experiments described previously. Put

\[ p^i_e((q, r)^j) = \frac{\prod_{l=1}^{j} \tau(q_l) \gamma(q_l, r_l)}{\tau(q_l) \gamma(q_l, r_l)} \]

where

\[ p(q_l) \gamma(q_l, r_l) = \sum_{e \in \mathcal{E}, \text{Ver}(e, q_l) = r_l} p(e((q, r)^j)) \]
is the conditional probability that $r_j$ is the response to query $q_j$ given that $r_{j-1}$ is the sequence of responses to the sequence of queries $q_{j-1}$. This is the probability in the previous experiments of the instances that have $(e, (q, r))^j$ as the prefix to their label. This probability may be calculated from the communicants’ strategy $p(e)$, the adversary’s strategy $\tau$, and the authentication system $\Pi$. This probability satisfies the following recursion:

$$p_i^\tau((q, r))^j = p_i^\tau((q, r)^{j-1})\tau_{(q, r)^{j-1}}(q_j)p(r_j|q_j, (q, r)^{j-1}).$$

Put

$$(P_i^\tau((q, r)^j), (m, 1)) = \sum_{e \in E} p(e|(q, r)^j)\gamma(e, m, (q, r)^j).$$

This is the probability that the spoofing message $m$ is successful given the sequence $(q, r)^j$. Then

$$P_i^\tau((q, r)^j) = \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^\tau((q, r)^j), (m, 1)).$$

Put

$$P_i^\tau((q, r)^j, q_{j+1}) = \sum_{\tau_{j+1} \in \mathcal{E}} p(\tau_{j+1}|q_{j+1}, (q, r)^j)
\times \sum_{q_{j+1} \in \mathcal{Q}} \tau_{(q, r)^j}(q_{j+1}) \cdots \sum_{q_1 \in \mathcal{Q}} \tau_{(q, r)^{j-1}}(q_1)
\times \sum_{\tau_{\mathcal{R}}} p(r_j|q_j, (q, r)^{j-1})
\times \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^\tau((q, r)^j), (m, 1)).$$

and

$$P_i^\tau((q, r)^j) = \sum_{q_{j+1} \in \mathcal{Q}} \tau_{(q, r)^j}(q_{j+1})P_i^\tau((q, r)^j, q_{j+1})).$$

This is the conditional probability in the previous experiments that the instances with labels whose sequences of queries and responses are prefixed by $(q, r)^j$ output $1$.

For each $j = 1, \ldots, i$, the advantage of the adversary may be written

$$P_i^\tau = \sum_{(q, r)^j} p_i^\tau((q, r)^j)P_i^\tau((q, r)^j).$$

We write $P_i^\tau$ to denote the maximum of $P_i^\tau$ over all strategies $\tau$.

### III. Optimal Strategies

The adversary’s strategy is a collection of probability distributions $\tau_{(q, r)^j}$ that are used to choose queries. We say that $\tau_{(q, r)^j}$ is pure if there is a unique query, denoted $q_{(q, r)^j}$, with $\tau_{(q, r)^j}(q_{(q, r)^j}) = 1$ (so that $\tau_{(q, r)^j}(q) = 0$ for all other queries $q$). We say that a strategy $\tau$ is pure if $\tau_{(q, r)^j}$ is pure for each $(q, r)^j$.

**Theorem 3.1:** There always exists a pure optimal strategy for an authentication system adversary who has oracle access.

**Proof:** We prove the theorem by constructing a pure strategy that is optimal. Let the adversary have $i$ oracle queries and a single spoofing query. Given any strategy $\tau$ of this adversary, we show how to construct a pure strategy $\tau^p$ whose advantage is at least that of $\tau$, using $i$ recursive steps. Towards this end, we recursively determine strategies $\tau^p_1, \ldots, \tau^p_i$ such that the advantage of an adversary with strategy $\tau^p_i$ is at least that of an adversary with strategy $\tau^p_{i-1}$; and $\tau^p_j$ is pure for all $(q, r)^j$, $j = 1, \ldots, i$. Since $\tau^p_i$ is pure, this will establish our claim by taking $\tau$ to be an optimal strategy.

Now $\tau^p_j$ will differ from $\tau$ only in the distributions $\tau_{(q, r)^j}$ used to choose the spoofing message. Thus, we are considering instances with labels whose sequences of queries and responses have a given prefix $(q, r)^j$. For each $(q, r)^j$, let $m_{(q, r)^j}$ be such that

$$P_i^\tau((q, r)^j), (m_{(q, r)^j}, 1)) = \max_{m \in \mathcal{M}} P_i^\tau((q, r)^j), (m, 1)).$$

Put $\tau^0_{(q, r)^j}(m_{(q, r)^j}) = 1$ (and $0$, otherwise). Thus, the strategy $\tau^0_{(q, r)^j}$ is a pure strategy that chooses the spoofing message optimally. For $j < i$, put $\tau_{(q, r)^j}^0 = \tau_{(q, r)^j}$ for all $(q, r)^j$.

Hence, $\tau^0$ is a strategy that is identical to $\tau$ except that each $\tau_{(q, r)^j}^0$ is a special probability distribution with nonzero probability only corresponding to an optimal spoofing query $m_{(q, r)^j}$.

Note that from (2), we have $p_i^\tau((q, r)^j) = p_i^{\tau^0_j}((q, r)^j)$ for all $(q, r)^j$. Also note that from (8), we have

$$P_i^\tau((q, r)^j), (m, 1)) \leq P_i^{\tau^0_j}((q, r)^j), (m_{(q, r)^j}, 1))$$

for all $m \in \mathcal{M}$ so that

$$P_i^\tau((q, r)^j) = \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^\tau((q, r)^j), (m, 1))$$

$$\leq \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^{\tau^0_j}((q, r)^j), (m_{(q, r)^j}, 1))$$

$$= \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^{\tau^0_j}((q, r)^j), (m, 1))$$

$$= \sum_{m \in \mathcal{M}} \tau_{(q, r)^j}(m)P_i^\tau((q, r)^j)$$

where the last equality uses (5). Now

$$P_i^\tau = \sum_{(q, r)^j} p_i^\tau((q, r)^j)P_i^\tau((q, r)^j)$$

$$\leq \sum_{(q, r)^j} p_i^{\tau^0_j}((q, r)^j)P_i^{\tau^0_j}((q, r)^j)$$

and the probability of success using strategy $\tau^0$ is at least that using $\tau$. 

For $j = 1, \ldots, i$, we recursively define $\tau^j$ assuming $\tau^0 = 0$. Now $\tau^j$ will differ from $\tau^{j-1}$ only in the distributions $\tau^j_{(q, r)}$ only. That is, for all $l = 0, \ldots, i, l \neq j$, we have $\tau^j_{(q, r)} = \tau^{j-1}_{(q, r)}$ for all $(q, r)^{i-j}, l = 0, \ldots, j - 1$, and so these strategies are pure. In this step, $\tau^{j-1}_{(q, r)}$ is replaced by a pure distribution such that $P_{\tau^{j-1}} \geq P_{\tau^j}$.

Consider instances with labels whose sequences of queries and responses have prefix $(q, r)^{i-j}$. For each $(q, r)^{i-j}$, let $q_{(q, r)^{i-j}}$ be such that

$$
P(r|q_{(q, r)^{i-j}}, (q, r)^{j-i}) \times P_{\tau^{j-1}}((q, r)^{j-i}, q_{(q, r)^{i-j}})
= \max_{q \in Q} P(r|q, (q, r)^{i-j}) \times P_{\tau^{j-1}}((q, r)^{j-i}, q_{(q, r)^{i-j}}) \leq P_{\tau^j}((q, r)^{i-j}, q_{(q, r)^{i-j}})
$$

for all $q \in Q$ so that

$$
P_{\tau^{j-1}}((q, r)^{i-j}, q) \leq P_{\tau^j}((q, r)^{i-j}, q_{(q, r)^{i-j}})
$$

and the probability of success using strategy $\tau^j$ is at least that using $\tau^{j-1}$.

The strategy $\tau^j$ is a pure strategy and is optimal if $\tau$ is optimal. We have $\tau_{(q, r)}^j(m, q_{(q, r)^{i-j}}) = 1$ and $P_{\tau^j}((q, r)^{i-j}) = \max_{m \in M} P_{\tau^j}((q, r)^{i-j}, (m, 1))$ and $m_{(q, r)^{i-j}}$ is an optimal spoofing message. Moreover, for each $j = 1, \ldots, i$, we have $\tau_{(q, r)}^j = \tau_{(q, r)^{i-j}}$ and $P_{\tau^j}((q, r)^{i-j}) = \max_{q \in Q} \sum_{r \in R} P_{\tau^j}(r|q, (q, r)^{i-j}) P_{\tau^j}(q_{(q, r)^{i-j}}, r)\).}

Thus, $\tau_{(q, r)}^j$ is an optimal query.

A. Bounds on Success Probability

We consider an adversary that uses strategy $\tau$ to make $i$ queries (either A-queries or V-queries) to an oracle and then constructs a spoofing query. Now $p_{\tau^j}((q, r)^{i-j})$ is the probability that the resulting sequence of query and response pairs is $(q, r)^{i-j}$. We write $Q^*(R^*)$ to denote a random variable that takes the values $(q, r)^{i-j}$ with respective probabilities $p_{\tau^j}((q, r)^{i-j})$. The source distribution and the communicants’ strategy determine a distribution $P(m)$ on $M$. Let $P(m| (q, r)^{i-j})$ be the probability that a message $m$ is transmitted by the sender as the next message given the sequence of query and response pairs $(q, r)^{i-j}$.

**Theorem 3.2:** Let $\Pi$ be an authentication system and let $P_{\tau^j}$ be the probability of success of an adversary who spoofs optimally after making $i$ oracle queries using strategy $\tau$. Then

$$
P_{\tau^j} \geq 2^H(E|M_\Pi(Q^*(R^*)) - H(E|Q^*(R^*))) = 2^{-I(E; M_\Pi(Q^*(R^*))}
$$

Moreover, equality holds if and only if, for all $(q, r)^{i-j} \in (Q \times R)^{i-j}$, $P(m| (q, r)^{i-j}) = 0$ and all $m \in M$ with $P(m| (q, r)^{i-j}) \neq 0$, we have $P_{\tau^j}((q, r)^{i-j}, (m, 1)) = P_{\tau^j}((q, r)^{i-j})$ and $p(m| (q, r)^{i-j})$ is constant for all $e \in \mathcal{E}(q^*(r^*))$, $(m, 1)$. □

The proof of Theorem 3.2 is given in the Appendix. It is an adaptation of the proof of Theorem 3.1 of Rosenbaum [7]. This bound is analogous to Rosenbaum’s bound for a message-observing adversary, with the difference being that the distribution associated with the random variable $(Q^*, R^*)$ depends on both the adversary’s and the communicants’ strategies while in the message observing case it is determined by the communicants’ strategy and the source state distribution. This means that unlike the case of a message observing adversary where the best success chance is bounded by the quantity $I(E; M|M^*)$ that he cannot change, the case of an adaptive adversary with access to query oracles allows him to influence $I(E; M|M_\Pi(Q^*, R^*))$ and so have a higher bound on the success chance. The bound depends on the query strategy and applies to any spoofing strategy. For good authentication systems, the best spoofing strategy should meet the bound with equality.

As in [7], we have the following generalization. Let the values $p^*(e, m, (q, r)^{i-j})$ for $e \in \mathcal{E}$, $m \in M$ and sequence $(q, r)^{i-j}$ of query and response pairs be a joint probability distribution on $\mathcal{E} \times M \times (Q \times R)^{i-j}$ such that, if $\gamma(e, m, (q, r)^{i-j}) = 0$, then $p^*(e, m, (q, r)^{i-j}) = 0$ and, for all $e$ and $(q, r)^{i-j}$, $\sum_m p^*(e, m, (q, r)^{i-j}) = p_{\tau^j}(e, (q, r)^{i-j})$, the probability that the encoding rule is $e$ and, for strategy $\tau$, the sequence of query and response pairs is $(q, r)^{i-j}$. We write $M^*$ to denote a random variable that takes values $m \in M^*$ with respective probabilities $p^*(m) = \sum_{(q, r)^{i-j}} p^*(e, m, (q, r)^{i-j})$. The bound in Theorem 3.2 becomes

$$
P_{\tau^j} \geq 2^H(E|M^*_\Pi(Q^*(R^*)) - H(E|Q^*(R^*)) = 2^{-I(E; M_\Pi^*(Q^*(R^*))}.
$$

B. Authentication Queries

When the adversary has access to an authentication oracle, the sample points have labels with sequences of queries and
responses of the form \( ((s,m)^j, (m,b)) \), and the probability of output 1 for a given sequence of queries and responses is given by

\[
P^\tau_i \left( ((s,m)^j), (m,1) \right) = \sum_{e \in \mathcal{E}((s,m)^j)} p(e|(s,m)^j) \gamma(e, m, (s,m)^j)
\]

where \( \mathcal{E}((s,m)^j) \) is the set of keys that satisfy Auth(e, s_j) = m_j, j = 1, \ldots, i. Theorem 3.2 in its generalized form [expression (10)] can be written as follows.

**Theorem 3.3:** Let \( \Pi \) be an authentication system and let \( P^\tau_i \) be the probability of success of an adversary who uses strategy \( \tau \) and spoofs optimally after making \( i \) oracle queries. Then

\[
P^\tau_i \geq 2^{H(E|M^\tau, (S^\tau, M^\tau)^j)} - H(E|S^\tau, M^\tau)^j)
= 2^{H(E|M^\tau, (S^\tau, M^\tau)^j)} - H(E|S^\tau, M^\tau)^j)
\]

Moreover, equality holds if and only if, for all \( (s,m)^j \in (S \times \mathcal{M}) \) with \( p^\tau_i((s,m)^j) \neq 0 \) and all \( m \in \mathcal{M} \) with \( p^\tau_i(m|(s,m)^j) \neq 0 \), we have \( P^\tau_i \left( ((s,m)^j), (m,1) \right) = P^\tau_i \) and \( p^\tau_i(m|(s,m)^j) \) is constant for all \( e \in \mathcal{E}((s,m)^j), (m,1) \).

1) **Bound on the Key Size:** We prove a bound on the key size in terms of the probabilities of success \( P^\tau_j \) for an adversary that has access to \( j \) authentication queries, \( j = 0, \ldots, i \). Let \( \tau \) be a strategy such that for all \( (s,m)^j \), \( j = 0, \ldots, i \), we have \( \tau_e(s, m)^j = 0 \) whenever \( s \in S_j \). We define \( j + 1 \) adversaries \( F_{\tau^j} = F_{\tau^j}^A(e^{(s)}), (m)^j, (m,1), j = 0, \ldots, i \), with strategies \( \tau^0, \ldots, \tau^j \), where \( \tau^j = \tau \). For \( j = 0, \ldots, i \), \( F_{\tau^j} \) uses strategy \( \tau^j \) to ask \( j \) oracle queries and then uses an optimal spoofing strategy that gives him the best success chance. For \( j = 0, \ldots, i \), define \( \tau^j_{(s,m)^j} = \tau_{(s,m)^j} \) for all \( (s,m)^j, \ell = 0, \ldots, j - 1 \). Note that \( \tau^j_{(s,m)^j} \) is the probability distribution used by \( F_{\tau^j} \) to select the spoofing message. Also note that for all \( u = 1, \ldots, j - 1 \), the probability distribution used by the adversary \( F_{\tau^u} \) for selecting queries \( s_t, \ell = 1, \ldots, u \), is the same as the probability distribution used by the adversary \( F_{\tau^j} \).

The lower bound on the success probability of \( F_{\tau^j} \) is

\[
P^\tau_j = 2^{-H(E|M^\tau, (S^\tau, M^\tau)^j)}
\]

where \( (S^\tau, M^\tau)^j \) denotes the random variable that takes values \( (s,m)^j \) with probability \( p^\tau_j((s,m)^j) \) and \( M^\tau \) is a random variable that has the properties described at the end of Section III-A. Since \( p^\tau_j((s,m)^j) = p^\tau_j((s,m)^j) \), we have \( (S^\tau, M^\tau)^j = (S^\tau, M^\tau)^j \).

Let

\[
p^\tau(e, m, (s,m)^j) = p^\tau_j((s,m)^j)p(e|(s,m)^j)\gamma^{j+1}_{(s,m)^j}(s)
\]

where \( s = D(e, m) \) and \( p^\tau(e, m, (s,m)^j) = 0 \), otherwise. This is the distribution on query and response pairs \( (s,m)^j \), keys \( e \), and transmitted messages \( m \), which arises when the source state distribution is \( \gamma^{j+1}_{(s,m)^j} \). Then, \( p^\tau(e, m, (s,m)^j) = 0 \), if \( \gamma(e, (s,m)^j, m) = 0 \).

Now \( \gamma^{j+1}_{(s,m)^j}(s) \) is the distribution used by \( F_{\tau^j+1} \) for selection of the \( j + 1 \) query \( s^{j+1} \). The random variable \( M_{j+1}^{j+1} \) has distribution satisfying

\[
p \left( M_{j+1}^{j+1} = m \big| (s,m)^j \right)
= \sum_{s \in S} \sum_{c \in \mathcal{C}(e, s)} \gamma^{j+1}_{(s,m)^j}(s)p(e|(s,m)^j)
= \sum_{e \in \mathcal{E}((s,m)^j)} \gamma^{j+1}_{(s,m)^j}(D(e, m))p(e|(s,m)^j)
\]

and

\[
p \left( M_{j+1}^{j+1} = m \big| (s,m)^j \right)
= \sum_{(s,m)^j} \sum_{c \in \mathcal{C}(e, s)} \gamma^{j+1}_{(s,m)^j}(s)p(e|(s,m)^j)
\]

Thus, \( M_{j+1}^{j+1} \) satisfies the conditions on \( M^* \) described at the end of Section III-A, and we have

\[
P_{\tau^j} \geq 2^{-H(E|M_{j+1}^{j+1}, (S^\tau, M^\tau)^j)}
\]

where \( M_{j+1}^{j+1} \) has the same distribution as responses to query \( q_{j+1} = s_{j+1} \) by the adversary \( F_{\tau^j+1} \).

Equivalently, the inequality may be written as

\[
\log_2 P_{\tau^j} \geq -I \left( E; M_{j+1}^{j+1} \big| (S^\tau, M^\tau)^j \right)
= -H(E|S^\tau, M^\tau)^j + H \left( E(S^\tau, M^\tau)^j, M_{j+1}^{j+1} \right).
\]

**Theorem 3.4:** Let \( \Pi \) be an authentication system. Then

\[\Pi_{j=0}^i P_j \leq 2^{-H(E)}\]

**Proof:** For adversaries \( F_{\tau^j}, j = 0, \ldots, i \), as described previously, we have

\[
\log_2 P_{\tau^j} \geq \log_2 P_{\tau^j+1} \geq -I \left( E; M_{j+1}^{j+1} \big| (S^\tau, M^\tau)^j \right)
= -H(E|S^\tau, M^\tau)^j + H \left( E(S^\tau, M^\tau)^j, M_{j+1}^{j+1} \right).
\]

Note that

\[
H \left( E; S_j^\tau \big| (S^\tau, M^\tau)^j \right)
= H \left( E(S^\tau, M^\tau)^j \right)
+ H \left( S_j^\tau | E(S^\tau, M^\tau)^j \right)
= H \left( S_j^\tau | (S^\tau, M^\tau)^j \right) + H(E|(S^\tau, M^\tau)^j)
\]

and since \( H \left( S_j^\tau | (S^\tau, M^\tau)^j \right) \neq 0 \), we have

\[
H \left( S_j^\tau | (S^\tau, M^\tau)^j \right) = H \left( E(S^\tau, M^\tau)^j \right) - H(E|(S^\tau, M^\tau)^j).
\]
Hence
\[
\log_2 (\prod_{j=0}^{t} P_j) \\
\geq (-H(E) + H(E| M_{i-1}^j)) \\
+ (-H(E| S^j, M_{i-1}^j) + H(E| S^j, M_{i-1}^j, M_{i-1}^{j+1})) \\
+ \cdots + (-H(E| S^j, M_{i-1}^j, M_{i-1}^{j+t}) + H(E| S^j, M_{i-1}^j, M_{i-1}^{j+t+1})) \\
= -H(E) + (H(E| M_{i-1}^j) - H(E| S^j, M_{i-1}^j)) \\
+ \cdots + (H(E| S^j, M_{i-1}^j, M_{i-1}^{j+t}) - H(E| S^j, M_{i-1}^j)) \\
+ H(E| S^j, M_{i-1}^j, M_{i-1}^{j+t+1}) \\
\geq -H(E).
\]
\[\square\]

Let \( P_d = \max_i P_i \). Then, it follows that \( P_d \geq 2^{-m_{i-1}} \).

IV. “Good” Queries Do Not Decrease Success Probability

It is well known that for a message observing adversary, observing an extra message may reduce the success probability of the adversary. For example, Massey [3] defined onefold secure A-codes as codes that provide perfect protection against spoofing of order 0 and 1. For such codes with \( k \) source states and \( v \) messages, we have \( P_0 = \frac{k}{v} \) and \( P_1 = \frac{k-1}{v} \). Moreover, the probability of success in spoofing of order 0 is \( \frac{k}{v} \) for each spoofing message \( m \) and the probability of success in spoofing of order 1 is \( \frac{k-1}{v} \) for each observed message \( m \) and spoofing message \( m' \neq m \). Thus, for these codes, observing any message will reduce the success probability of the adversary.

The passive message observing adversary obtains information from valid messages sent across the channel. On the other hand, the active querying adversary obtains information from the responses to the queries. Thus, there is a difference: in the latter, the adversary can control the amount of information that he receives.

Since adversaries with oracle access have some control of the information that they receive a natural question is whether asking queries is always helpful to such adversaries. For every query, the adversary may calculate his best success chance before and after the query is asked and choose the one that gives him the higher success chance. Of course, the probability of success is unchanged if the adversary repeats a query that has been made before, so we only need to consider the case where the adversary makes distinct queries. We call a query “good” if it is distinct from previous queries and if asking it will not reduce the success chance of the adversary. Otherwise, a query is “bad.” In the following, we show that the adversary only needs to look for “good” queries and if there is one then he can be guaranteed that asking the query will not decrease his success chance.

The following theorem gives conditions under which a query is good. It follows that, in all but those special cases where no query satisfies these conditions, asking another query is helpful and the adversary’s probability of success is at least as great with the extra query.

Theorem 4.1: Let \( \tau \) be a strategy of an adversary who asks \( i \) oracle queries and then constructs a spoofing query for an authentication system \( \Pi \). Suppose that the adversary modifies the strategy to ask one extra oracle query and then spoof optimally.

Then, an extra query \( q \) is good if it is distinct from previous queries and the following occurs: 1) in the case of verification queries, \( q \) is distinct from the unique optimal spoofing message for strategy \( \tau \) should one exist; and 2) in the case of authentication queries, there exists an optimal spoofing message \( \hat{m} \) for strategy \( \tau \) such that any key consistent with the previous query and response pairs is not consistent with \((q, \hat{m})\).

If there exists a good extra query for every sequence of query and response pairs arising from \( \tau \), then for a suitable modification, the adversary’s probability of success is at least \( P_\tau^i \).

Proof: Suppose that the adversary has observed the sequence \((q, r)^i\) of query and response pairs.

The expected success probability of the adversary after another query \((q_{i+1})\) is

\[
\sum_{r_{i+1} \in R} p(r_{i+1}|q_{i+1}, (q, r)^i) \max_{m \in M} \left\{ \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, m, (q, r)^i+1) \right\}
\]

where \( p(r_{i+1}|q_{i+1}, (q, r)^i) = \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \) is the conditional probability that the response is \( r_{i+1} \) given the sequence \((q, r)^i\) and the query \( q_{i+1} \). However

\[
p(e|(q, r)^i) = \frac{\sum_{c' \in E((q, r)^i)} p(e'(q, r)^i)}{p(e'(q, r)^i)}
\]

so this is

\[
\sum_{r_{i+1} \in R} \max_{m \in M} \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, m, (q, r)^i+1)
\]

\[
\geq \max_{m \in M} \sum_{r_{i+1} \in R} \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, m, (q, r)^i+1)
\]

\[
= \max_{m \in M} \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, m, (q, r)^i, (q_{i+1}, \hat{r}))
\]

where \( \hat{r} = \text{Ver}(e, q_{i+1}) \) or \( \text{Auth}(e, q_{i+1}) \).

Suppose that \( q_{i+1} \) is distinct from \( q_1, \ldots, q_i \) and the following occurs: 1) if \( q_{i+1} \in M \), then there exists \( \hat{m} \neq q_{i+1} \) with \( P_\tau^i((q, r)^i, (\hat{m}, 1)) = \max_{m \in M} \{ P_\tau^i((q, r)^i, (m, 1)) \} \), and 2) if \( q_{i+1} \in S \), then under any key \( e \in E((q, r)^i) \), there exists a message \( \hat{m} \in M \) with \( \hat{m} \neq \text{Auth}(e, q_{i+1}) \) and \( P_\tau^i((q, r)^i, (\hat{m}, 1)) = \max_{m \in M} P_\tau^i((q, r)^i, (m, 1)) \).

With \( \hat{m} \) so defined, we have

\[
\gamma(e, \hat{m}, (q, r)^i, (q_{i+1}, \hat{r})) = \gamma(e, \hat{m}, (q, r)^i)
\]

and so

\[
\max_{m \in M} \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, m, (q, r)^i, (q_{i+1}, \hat{r}))
\]

\[
= \sum_{e \in E((q, r)^i)} p(e|(q, r)^i) \gamma(e, \hat{m}, (q, r)^i) = P_\tau^i((q, r)^i).
\]

Thus, \( q_{i+1} \) is a good query.
It follows immediately that if there exists a good extra query for every sequence of query and response pairs arising from $\tau$, then the adversary’s probability of success for a modified strategy that chooses such a query with probability 1 is at least

$$\sum_{q \in \mathcal{Q}} p(q)^i P_j^r((q, r)^i) P_j^r((q, r)^i) = P_j^r$$

and the result follows. □

Note that for verification queries the condition for existence of a good query is nearly always satisfied. The exception is when $|\mathcal{M}\setminus \mathcal{F}| = 1$ and so the available query is the spoofing query. As long as $|\mathcal{M}\setminus \mathcal{F}| > 1$, there will be a good query and so the success chance of the adversary would not be reduced if that query is asked. Note, however, that there is no guarantee that the success chance will be improved by asking a query. For example, in the onefold secure A-codes of Massey [3], the success chance is $\frac{k}{n}$ either with or without a verification query. A query has probability $\frac{k}{n}$ of producing response 1 and probability $\frac{n-k}{n}$ of response 0. If the response is 1, then the success chance is reduced to $\frac{k-1}{n-1}$, while if the response is 0, the success chance is increased to $\frac{k+1}{n+1}$. Thus, the success chance if the adversary asks a verification query is $\frac{k}{n} + \frac{n-k}{n} \cdot \frac{k}{n} = \frac{k}{n}$.

In the case of authentication queries, the theorem may not imply the existence of a good query. This is the case if for some sequence of query and response pairs $(q, r)^i$ arising from $\tau$ every optimal spoofing message $m$ has the property that for any $q \in S^i \mathcal{Q}$ there is an $e \in \mathcal{E}(q, r)^i$ such that $\text{Auth}(e, q) = m$. This is the case for the onefold secure A-codes of Massey [3], where any authentication query reduces the success chance from $\frac{k}{n}$ to $\frac{k-i}{n-i}$.

Note that Theorem 4.1 is helpful as it provides the adversary with a method to determine whether he should ask a query or not: he simply checks whether there are good queries, and if there are, then he is guaranteed to do better if he asks them.

V. OPTIMAL CODES

We consider optimal authentication codes that satisfy the bound $Pd \geq 2^{-\frac{M_{j+1}}{2}}$ with equality. We use an argument similar to Rosenbaum [7] and obtain a combinatorial characterization of such authentication codes analogous to that in the message-observing adversary setting. The codes will have minimum number of keys and limit the best success chance of an imposter with access to $i$ queries to its minimum (that is, satisfy bound of Theorem 3.2 with equality).

If equality holds, then it follows by Theorem 3.4 that

$$P_j = Pd \quad \text{for} \quad j = 0, \ldots, i \quad \text{and} \quad \text{the proof of the theorem shows that} \quad H(E((S^i \mathcal{M}), M_{j+1}^i)) = 0 \quad \text{and} \quad H((S^j \mathcal{M})^j((S^i \mathcal{M})^j, M_{j+1}^i)) = 0 \quad \text{for} \quad j = 1, \ldots, i.$$ 

Further, equality holds in Theorem 3.3 and so, for an optimal strategy $\tau^*$ (having the properties described above the statement of Theorem 3.4), $p^*(m_e, (s, m)^i)$ is constant for all $e \in \mathcal{E}(s^i, m)^i(m, 1)$ and $P_j = P_j^r((s, m)^i, (m, 1)).$

Since $p^*(m_e, (s, m)^i)$ is independent of $e$, it follows that

$$p(e|(s^i, m)^i, (m, 1)) = \frac{p(e|(s^i, m)^i)}{\sum_{e' \in \mathcal{E}(s^i, m)^i(m, 1)} p(e'(s^i, m)^i)} \quad (11)$$

and we have

$$p(e|(s^i, m)^i, (m, 1)) = P_j^r((s^i, m)^i, (m, 1)) = Pd.$$

Using an argument by induction on the number $j$ of query and response pairs gives

$$p(e|(s^i, m)^j, (m, 1)) = \frac{p(e)}{\sum_{e' \in \mathcal{E}(s^i, m)^j(m, 1)} p(e')} \quad (12)$$

for all $j = 0, \ldots, i$. Further, another induction, on the number $j$ of terms in the product, gives

$$\sum_{e' \in \mathcal{E}(s^i, m)^j} p(e') = \prod_{l=0}^{j-1} P_l \quad (13)$$

for all $j = 0, \ldots, i$. (See Appendix for proofs of these equations.)

Let $s^{i+1}$ be a sequence of distinct source states and let $e \in \mathcal{E}$. Let $m^{i+1}$ be the sequence of messages with $m_j = \text{Auth}(e, s_j)$ for $j = 1, \ldots, i + 1$. Then, $p(e|(s, m)^{i+1}) \neq 0$ and since $H(E((S^i \mathcal{M}), M^{i+1}_j)) = 0$, we have $p(e|(s, m)^{i+1}) = 1$ and $\mathcal{E}(s^i, m)^j(m^{i+1}_j, 1) = \{e\}$. Hence, $p(e) = \sum_{e' \in \mathcal{E}(s^i, m)^j(m^{i+1}_j, 1)} p(e') = \prod_{j=0}^{i} P_j$. Thus, the distribution $p(e)$ is uniform.

It follows that

$$p(e|(s^i, m)^j) = \frac{p(e)}{\sum_{e' \in \mathcal{E}(s^i, m)^j} p(e')} = \frac{1}{|\mathcal{E}(s^i, m)^j|}$$

and $|\mathcal{E}(s^i, m)^j| = \prod_{l=0}^{j-1} |\mathcal{E}_l| = Pd^{i+1}|\mathcal{E}_l|$. Since $|\mathcal{E}(s^i, m)^{i+1}| = 1$, we have $|\mathcal{E}_l| = Pd^{i+1}$ and $|\mathcal{E}(s^i, m)^j| = Pd^{i+1-j}$. Thus, $Pd^{i+1-j}$ is an integer $q$ and $|\mathcal{E}_l| = q^{i+1}$.

Thus, the optimal authentication systems determine a combinatorial structure. We may identify a pair $(e, s, m)$ with an incidence in a combinatorial design.

The previous results show that an optimal authentication code corresponds to a combinatorial design in which any $j$ query response pairs $(s, m)^j$ are incident with a constant number $q^{i+1-j}$ encoding rules. Since $H((S^j \mathcal{M})^i | M_{j+1}^i = 0$, the authentication code is Cartesian and it follows that it is optimal in the message observing setting also. The authentication systems arising from Reed–Solomon codes (or orthogonal arrays) (see [5]) that are optimal in the message observing adversary setting also provide examples of optimal codes in our query oracle setting.

VI. CONCLUDING REMARKS

We have given an analysis of authentication systems for an adversary with access to oracle queries. We derived information theoretic bounds on the best success probability of an adversary using a strategy $\tau$ to ask $i$ queries and then construct a spoofing query. This bound can be seen as a generalization of the Simmons and Rosenbaum bound and is derived using the same technique. The adaptive adversary, however, has the ability to
influence the bound through his querying strategy as well as his spoofing strategy while for a message observing adversary the bound is only affected by this latter strategy. We also derived a bound on the key entropy for an adaptive adversary with access to \( i \) authentication queries and showed that in this case for an authentication system with probability of deception \( Pd \) the key entropy is at least \( (i+1)\log Pd \). This is similar to the known result for a message observing adversary.

We gave a combinatorial characterization of authentication codes that meet the bounds and showed that optimal codes (having the least success probability and the smallest number of keys) correspond to orthogonal arrays. This is analogous to the message observing case.

We gave a result to show that, in the query oracle model, as long as there is always a good query, then asking that query is helpful to the adversary.

**APPENDIX**

**Proof of Theorem 3.2:** The following proof is a direct application of the proof used in [7] to the situation where the adversary makes oracle queries instead of observing messages.

We will use Jensen’s inequality for convex functions. A real function \( \phi \) is convex on the interval \((a, b)\) if \( \phi'(r) < \phi'(s) \) for all \( a < r < s < b \).

**Theorem 7.1 (Jensen’s Inequality) [11]:** Let \( w_i, i = 1, \ldots, n \) be nonnegative numbers such that \( \sum_i w_i = 1 \). Let \( \phi \) be a real function that is convex on the interval \((a, b)\) and let \( x_i \in (a, b), i = 1, \ldots, n \).

\[
\phi \left( \sum_i w_i \cdot x_i \right) \leq \sum_i w_i \phi(x_i) \tag{14}
\]

and equality holds if and only if all \( x_i \) are equal.

The proof of Theorem 3.2 proceeds as follows.

Let

\[
\Psi_{(q,r)^i, m}(e) = \frac{p(e, (q,r)^i)\gamma(e, m, (q,r)^i)}{P_i^T((q,r)^i), (m, 1))}.
\]

Because

\[
P_i^T((q,r)^i), (m, 1)) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, (q,r)^i)\gamma(e, m, (q,r)^i)
\]

it follows that \( \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} \Psi_{(q,r)^i, m}(e) = 1 \) and \( \Psi_{(q,r)^i, m}(e) \) is a probability distribution on \( \mathcal{E}((q,r)^i), (m, 1)) \).

Now we have

\[
p(m|(q,r)^i) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(m, e|(q,r)^i) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, (q,r)^i)p(m|e, (q,r)^i) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, (q,r)^i)p(m|e, (q,r)^i) \times \gamma(e, m, (q,r)^i) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} \Psi_{(q,r)^i, m}(e) \times P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i).
\]

Using Jensen’s inequality (14) for \( \phi(x) = x \log x \) at \( x = p(m|(q,r)^i) = \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} w_e \cdot x_e \) with \( w_e = \Psi_{(q,r)^i, m}(e) \) and \( x_e = P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i) \), we have

\[
p(m|(q,r)^i) \log p(m|(q,r)^i) 
\leq \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} \Psi_{(q,r)^i, m}(e)P_i^T((q,r)^i), (m, 1)) \times p(m|e, (q,r)^i) \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\leq \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, (q,r)^i)p(m|e, (q,r)^i) \times \gamma(e, m, (q,r)^i) \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\leq \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, (q,r)^i)p(m|e, (q,r)^i) \times \gamma(e, m, (q,r)^i) \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\leq \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} \Psi_{(q,r)^i, m}(e) \times P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i).
\]

We will first show that

\[
H(M|(q,r)^i) \geq \log P_i^T((q,r)^i) + H(M|E, (q,r)^i).
\]

This is true because using (15), we have

\[
H(M|(q,r)^i) = -\sum_{m \in M} p(m|(q,r)^i) \log p(m|(q,r)^i)) 
\geq -\sum_{m \in M} \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, m|q, r)^i \times \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\geq \sum_{m \in M} p(m|(q,r)^i) \log P_i^T((q,r)^i), (m, 1)) - \sum_{m \in M} \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, m|q, r)^i \times \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\geq \sum_{m \in M} \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, m|q, r)^i \times \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\geq \sum_{m \in M} \sum_{e \in \mathcal{E}((q,r)^i), (m, 1))} p(e, m|q, r)^i \times \log [P_i^T((q,r)^i), (m, 1))p(m|e, (q,r)^i)]
\geq H(M|E, (q,r)^i).
\]

Now as the adversary spoofs optimally, we have \( P_i^T((q,r)^i) \geq P_i^T((q,r)^i), (m, 1)) \) and so

\[
H(M|(q,r)^i) \geq -\log P_i^T((q,r)^i) \sum_{m \in M} p(m|(q,r)^i) + H(M|E, (q,r)^i)
\geq -\log P_i^T((q,r)^i) + H(M|E, (q,r)^i).
\]

The final step uses Jensen’s inequality (14) for \( \phi(x) = -\log x \)

\[
\log P_i^T = \log \left[ \sum_{(q,r)^i} p_i^T((q,r)^i) P_i^T((q,r)^i) \right] 
\geq \sum_{(q,r)^i} p_i^T((q,r)^i) \log P((q,r)^i)
\geq \sum_{(q,r)^i} p_i^T((q,r)^i)(H(M|E, (q,r)^i)
\geq -H(M|(q,r)^i))
= H(M|E, (q', R')^i) - H(M|(q', R')^i)
\]

\[
\square
\]
Proof of (11): We show that

\[ p(e|s^*,m^j, (m,1)) = \frac{p(e|s^*,m^j)}{\sum_{e' \in \mathcal{E}(s^*,m^j), (m,1)} P(e'|s^*,m^j)}. \]

Now, for \( p^*(e, (s^*,m)^j, m) \neq 0 \), we have

\[ p^*(e, (s^*,m)^j, m) = p(e|s^*,m^j)^j, (m,1)) p^*(s^*,m)^j, m) \]

and

\[ p^*(e, (s^*,m)^j, m) = p^*(m|e, (s^*,m)^j) p(e|s^*,m^j) p^*(s^*,m)^j. \]

Hence

\[ p(e|s^*,m^j, (m,1)) = \frac{p^*(m|e, (s^*,m)^j) p(e|s^*,m^j) p^*(s^*,m)^j}{p^*(s^*,m)^j, m)}. \]

Now

\[ p^*(s^*,m)^j, m) = \sum_{e' \in \mathcal{E}(s^*,m)^j, (m,1)) p^*(e', (s^*,m)^j, m) \]

\[ = \sum_{e' \in \mathcal{E}(s^*,m)^j, (m,1)) p^*(m|e', (s^*,m)^j) \]

\[ \times p(e'|s^*,m)^j) p^*(s^*,m)^j). \]

Thus

\[ p(e|s^*,m^j, (m,1)) = \frac{p(e|s^*,m^j) p(e|s^*,m^j) p^*(s^*,m)^j)}{\sum_{e' \in \mathcal{E}(s^*,m)^j, (m,1)) p(e'|s^*,m)^j) p^*(s^*,m)^j), \]

where the sum is over \( e' \in \mathcal{E}(s^*,m)^j, (m,1)) \).

However, by Theorem 3.3, \( p^*(m|e', (s^*,m)^j) \) is constant for all \( e' \in \mathcal{E}(s^*,m)^j, (m,1)). \)

so that

\[ p(e|s^*,m^j, (m,1)) = \frac{p(e|s^*,m^j) p(e|s^*,m^j)}{\sum_{e' \in \mathcal{E}(s^*,m)^j, (m,1)) p(e'|s^*,m)^j) p^*(s^*,m)^j) \}

and the result follows.

Proof of (12): We show that

\[ p(e|s^*,m^j) = \frac{P(e)}{\sum_{e' \in \mathcal{E}(s^*,m)^j) P(e')}}, \]

For \( j = 0 \), we have \( p(e|s^*,m^0) = p(e) \), so

\[ p(e|s^*,m) = \frac{p(e)}{\sum_{e' \in \mathcal{E}(s^*,m)^j) P(e')}}, \]

Suppose that \( 1 \leq j \leq i \) and

\[ p(e|s^*,m)^{j-1}) = \frac{p(e)}{\sum_{e' \in \mathcal{E}(s^*,m)^{j-1}) P(e')} \]

for all \( e \in \mathcal{E}(s^*,m)^{j-1}). \)

so that

\[ \mathcal{E}(s^*,m)^{j-1}, (m,1)) = \mathcal{E}(s^*,m)^{j-1}, (s^*, m) \]

and because \( \mathcal{E}(s^*,m)^{j-1}) \subseteq \mathcal{E}(s^*,m)^j) \), we have

\[ p(e|s^*,m)^j) = \frac{p(e|s^*,m)^{j-1})}{\sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) p(e')} \]

\[ \sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) P(e')} \]

\[ = \sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) P(e')} \]

\[ \sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) P(e')} \]

and the result follows. \( \square \)

Proof of (13): We show that

\[ \sum_{e \in \mathcal{E}(s^*,m)^j} P(e) = \prod_{l=0}^{j-1} P_l. \]

For \( j = 1 \), we have

\[ P_0 = P_0^+ ((m,1)) = \sum_{e \in \mathcal{E}(s^*,m)^j) P(e) = \sum_{e \in \mathcal{E}(s^*,m)^j) P(e), \]

Suppose that \( 2 \leq j \leq i + 1 \) and

\[ \sum_{e \in \mathcal{E}(s^*,m)^{j-1}) P(e) = \prod_{l=0}^{j-2} P_l. \]

Now

\[ P_{j-1} = \sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) p(e|s^*,m)^{j-1}) \]

\[ \sum_{e \in \mathcal{E}(s^*,m)^{j-1}, (m,1)) p(e|s^*,m)^{j-1}) \]

so that

\[ P_{j-1} = \sum_{e \in \mathcal{E}(s^*,m)^{j-1}) \sum_{e' \in \mathcal{E}(s^*,m)^{j-1}) P(e')} \]

\[ \sum_{e \in \mathcal{E}(s^*,m)^{j-1}) \prod_{l=0}^{j-1} P_l \]

and the result follows. \( \square \)

REFERENCES


