October 2005

Bounds on authentication systems in query mode

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

P. Wild
University of London, UK

Bounds on authentication systems in query mode

Abstract

Unconditionally secure authentication codes provide information theoretic security against an adversary who observes authenticated messages and then wants to construct a fraudulent message that is acceptable by the receiver. The attack model for these codes has recently been strengthened and adaptive adversaries with oracle access have been introduced. In this paper we give an analysis of this new model and derive information theoretic bounds on the success probability and key size of the codes. Our analysis treats two games that an adversary can play: an offline attack in which the adversary is allowed to query a verification oracle and then to construct the spoofing query; and an on-line attack in which the adversary interacts with the verification oracle and wins as soon as he constructs an acceptable message. We describe the best strategy of the adversary in each case.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Safavi-Naini, R & Wild, P, Bounds on authentication systems in query mode, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security 2005, 16-19 October 2005, 85-91. Copyright IEEE 2005.

Bounds on Authentication Systems in Query Model

Reihaneh Safavi-Naini
School of Information Technology
and Computer Science
University of Wollongong
Wollongong, Australia
Email: rei@uow.edu.au

Peter Wild
Department of Mathematics
Royal Holloway
University of London
Egham, Surrey TW20 0EX, UK
Email: P.Wild@rhul.ac.uk

***Abstract*— Unconditionally secure authentication codes provide information theoretic security against an adversary who observes authenticated messages and then wants to construct a fraudulent message that is acceptable by the receiver. The attack model for these codes has recently been strengthened and adaptive adversaries with oracle access have been introduced. In this paper we give an analysis of this new model and derive information theoretic bounds on the success probability and key size of the codes. Our analysis treats two games that an adversary can play: an offline attack in which the adversary is allowed to query a verification oracle and then to construct the spoofing query; and an on-line attack in which the adversary interacts with the verification oracle and wins as soon as he constructs an acceptable message. We describe the best strategy of the adversary in each case.**

Keywords: Unconditional security, authentication system, A-codes, verification oracle.

I. Introduction

Unconditionally secure authentication systems provide security for data and origin authentication when the adversary's computational power is unknown or unlimited. Information theoretic security is particularly important when one considers advances in computation such as quantum computing and the growing prospect of development of efficient algorithms for 'hard' problems. In an *Authentication code (A-code)* [1], [5] authenticated messages (*messages*) encode states of an information source (referred to as *source states*) under a mapping determined by a key (*encoding rule*). A-codes are symmetric key systems. The receiver verifies the authenticity of a message using the same key. 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 limiting 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 [5], [3], [2] for A-codes give fundamental limits on performance of the codes. Rosenbaum [3] and Pei [2] 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.

In this analysis of an A-code the adversary gathers information passively by observing valid messages and then attempts to spoof by sending a fraudulent message as the $(i+1)^{th}$ massage, an *impersonation* attack, or by replacing the i^{th} valid message with a fraudulent one, a *substitution* attack. The success probability of these two scenarios are the same (provided the receiver will accept $i+1$ messages).

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 corrsponding 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* [4] have considered A-codes with such an adversary in the context of unconditionally secure digital signature schemes (USDS, Shikata *et al* [**?**]). This situation is modelled in terms of an Authentication Oracle (A-oracle) that provides the authenticated message corresponding a query source state 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 according as the message would be accepted or not by the receiver. 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 under the query model and derive information theoretic bounds on the success probability of a query attacker.

0-7803-9491-7/05/$20.00 ©2005 IEEE

We distinguish two cases according as the attack is on-line or off-line. An off-line attack may arise, for example, when the attacker is able to have access for a short time to the receiver's means of verification but not to the system in which it is integrated. The attacker would use this opportunity to gather information and then attack the system at a later time. An on-line attack may arise, for example, when the attacker is trying to gain access to a secure module such as an ATM.

In an on-line attack each query is also a spoofing attempt and the attacker is successful on the first occasion that the receiver accepts a query as a valid message. In an off-line attack the attacker gathers information from queries and responses before making a spoofing attack on the live system. In this case a query that results in an acceptance does not constitute a successful spoof.

We assume that there is a maximum number, L, of queries that the V-oracle will respond to prior to one further verification (of a final spoofing attempt). This reflects the fact that information about the key is revealed by the verifier's response and that the probability of succesfully spoofing would become equal to 1 if an unlimited number of queries were responded to.

We begin by considering an adversary who asks exactly i V-queries, observes the responses of the V-oracle, and then spoofs. The result of this analysis provides the foundation for the subsequent analysis of all the other attacks. We view this as a game in which the adversary uses a strategy to choose each query adaptively, taking into account all queries and responses previously observed.

We derive two information theoretic bounds. The first bound is a lower bound on the success probably of the adversary, and can be seen as a generalisation of the Rosenbaum-Pei lower bound [3], [2] for spoofing of order i. However despite the similarity of the bounds, the bound in the query case does not lead directly to a bound on the size of the key space. We consider another information theoretic quantity, the entropy of the success probability, and derive a bound on its value that leads to a bound on the size of the key space.

It is known that an adversary's expected chance of spoofing may decrease if the adversary observes a message compared to his expected chance of spoofing when he spoofs without any observation. Although under certain circumstances this may also be true in the case of making a query to a V-oracle, we will show that, unless there is a unique spoofing message which gives maximum probability of success, the average of the success chance after making a V-query is at least equal to the success chance without making that query. Thus, in general, it is always best strategy to ask the query and then spoof.

II. Preliminaries

An authentication code is a 4–tuple, $C = (\mathcal{S}, \mathcal{M}, \mathcal{E}, f)$, where $\mathcal{S}, \mathcal{M}, \mathcal{E}$ are the sets of source states, messages and keys, respectively. The function $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ is a mapping that takes a *source state* s, a key e and generates a corresponding *message* m. For each $e \in \mathcal{E}$, the mapping $e : \mathcal{S} \to \mathcal{M}$ given by $e(s) = f(s, e)$ for all $s \in \mathcal{S}$ is injective. We assume that there is a known probability distribution which models the generation of a sequence of source states that the sender wants to communicate to the receiver. We assume that the source states of such a sequence are distinct. The sender and the receiver choose a probability distribution on $\mathcal{E}$, their *strategy*, which we assume is public, and use it to choose a shared key e. We denote by E the random variable on sample space $\mathcal{E}$ corresponding to this probability distribution. To communicate a source state $s \in \mathcal{S}$ to the receiver, s is encoded under e to produce message $m = e(s)$ which is transmitted by the sender to the receiver. We say that $m \in \mathcal{M}$ is valid with respect to $e \in \mathcal{E}$ if $m = e(s)$ for some $s \in \mathcal{S}$. Let $\mathcal{M}(e) = \{m : \ m \text{ is valid under } e \ \}$. The receiver accepts a message m as authentic if m is valid and its corresponding source state has not been received before. Otherwise m is rejected.

III. V-query model

We consider an adversary with access to a verification oracle.

Definition 3.1: **Verification oracle (V-oracle)**
A verification oracle (V-oracle) implements the verification algorithm with the verifier's key e. The oracle response to a *query* $m \in \mathcal{M}$ is `T` if $m \in \mathcal{M}(e)$ and `F`, otherwise. The query m is called a *verification query*, or a V-query. The set $\mathcal{R} = \{\mathtt{T}, \mathtt{F}\}$ is the set of *responses*.

Let $\mathbf{x}^i = x_1, x_2 \dots x_i$ denote a sequence of i elements. We also use $\mathbf{x}^i$ to denote $\{x_1, x_2 \dots x_i\}$. We use $\mathbf{m}^i$, $\mathbf{q}^i, \mathbf{r}^i, (q, r)^i$ to denote a sequence of observed messages, queries, responses, and query and response pairs, respectively.

We consider two games. Game 1 models off-line attackers. In this attack we assume that the adversary chooses the number $i \leq L$ of queries to make before spoofing.

Definition 3.2: **Game 1**
The game has two steps.
S1: The adversary adaptively sends i queries $\mathbf{q}^i = q_1 \cdots q_i$ to the V-oracle and observes the corresponding responses $\mathbf{r}^i = r_1, \dots, r_i$.
S2: The adversary constructs a *spoofing message* $m \in \mathcal{M}$ and wins if the verifier accepts the message as authentic. The adversary uses a strategy τ to choose the queries: for $j = 1, \dots, i$, the adversary chooses query q_j according to a probability distribution $\tau_{(q,r)^{j-1}}(q_j)$ when the sequence of previous query and response pairs is $(q, r)^{j-1} = ((q_1, r_1), \dots, (q_{j-1}, r_{j-1})$. The adversary chooses the spoofing message m according to a probability distribution $\tau'_{(q,r)^i}(m)$ when the sequence $(q, r)^i$ of query and response pairs has been observed.

Note that the spoofing query must be different from queried messages to be accepted. Game 2 models an online adversary.

Definition 3.3: **Game 2**
The adversary adaptively asks *up to* $L+1$ queries, observing the responses. Each query is also a spoofing message and the adversary succeeds if and as soon as he asks a query that produces the response T.
The adversary uses a strategy τ to choose the queries: for $j = 1, \ldots, L+1$, the adversary chooses the query q_j according to a probability distribution $\tau_{(q,r)^{j-1}}(q_j)$ whenever the sequence of previous query and response pairs is $(q,r)^{j-1}$ with the $j-1$ responses $r_1, \ldots, r_{j-1}$ all equal to F.

In Game 1 the adversary has a single chance of spoofing but in Game 2 he has up to $L+1$ chances (although he might not use them all because he succeeds as soon as a response T is received for some query q_j where $j \leq L+1$).

A. Optimal strategies

Suppose that the adversary has sent a sequence $q = q_1, \ldots, q_i$ of queries and observed a sequence $(q,r)^i = ((q_1,r_1), \ldots, (q_i,r_i))$ of query and response pairs resulting from the adversary's queries and the corresponding responses $r_1, \ldots, r_i$ by the receiver. We write $\mathcal{E}((q,r)^i)$ for the set of encoding rules consistent with these observations and $p(e|(q,r)^i)$ for the probability of event $e \in \mathcal{E}((q,r)^i)$. Similarly, let $\mathcal{E}(m,(q,r)^i) = \{e \in \mathcal{E}((q,r)^i) : m \in \mathcal{M}(e)\}$. Further, if $e \in \mathcal{E}$ and $m \in \mathcal{M}$ we write $\gamma(e,m,(q,r)^i) = 1$ if, when the encoding rule is e, the receiver accepts m after receiving message sequence $q_1, \ldots, q_i$ and $\gamma(e,m,(q,r)^i) = 0$ if m is rejected.

The quantity

$$\textbf{payoff}_T(m,(q,r)^i) = \sum_{e \in E} p(e|(q,r)^i)\gamma(e,m,(q,r)^i)$$

is the probability that the adversary will succeed with spoof m after observing $(q,r)^i$. The maximum probability of success if the adversary spoofs after observing $(q,r)^i$ is $P_i((q,r)^i) = \max_m \textbf{payoff}_T(m,(q,r)^i)$. A strategy τ' with this success probabilityis called optimal and we say that the adversary plays spoofing optimally. We denote by $\hat{m}$ a message such that $\textbf{payoff}_T(\hat{m},(q,r)^i) = P_i((q,r)^i)$. We may assume that ${\tau'}_{(q,r)^i}(m)$ equals 1 for $m = \hat{m}$ and 0 otherwise.

The sequence $(q,r)^i$ that the adversary observes depends on the encoding rule agreed by the sender and the receiver and the strategy used by the adversary to send queries to the receiver. The adversary's strategy, together with the probability distributions on the encoding rules, determines conditional probabilities $\sigma_i((q,r)^j|(q,r)^{j-1})$ for $j = 1, \ldots, i$ that the sequence of j query and response pairs is $(q,r)^j$ given that the sequence of $j-1$ query and response pairs is $(q,r)^{j-1}$. These probability distributions determine probabilities $p((q,r)^i)$ that the sequence of query and response pairs is $(q,r)^i$ under startegy τ. We write $(Q,R)^i$ to denote a random variable that takes values $a_{(q,r)^i}$ with respective probabilities $p((q,r)^i)$. Invariably the strategy τ corresponding to $(Q,R)^i$ will be understood from the context.

In an off-line attack, the adversary may choose the value i at which a spoofing attack is made. The adversary's expected probability of success using strategy τ if the adversary plays spoofing optimally after observing i responses to messages by the receiver is

$$P_i^\tau = \sum_{(q,r)^i} p((q,r)^i)P_i((q,r)^i)$$

Let P_i be the maximum of P_i^τ over all strategies τ and P the maximum of P_i over $i = 0, \ldots, L$. Then P is the adversary's probability of success for an off-line attack if the adversary optimally chooses the number of responses to observe before spoofing and then uses an optimal strategy for sending queries and an optimal strategy for spoofing.

Given a sequence $(q,r)^{i-1}$ of query and response pairs and query q the probability that r is the response r_i to query $q_i = q$ is given by

$$p(r|(q,r)^{i-1},q) = \sum_{e \in E((q,r)^{i-1}):e(q)=r} p(e|(q,r)^{i-1})$$

The expected success probability of an adversary that chooses query $q_i = q$ is therefore

$$P_{(q,r)^{i-1}}(q) = \sum_{r \in R} p(r|(q,r)^{i-1},q)P_i((q,r)^i)$$

where $(q_i,r_i) = (q,r)$. The expected success probability of an adversary who spoofs optimally after making i queries using strategy τ is therefore

$$\sum_{q \in M} \tau_{(q,r)^{i-1}}(q)P_{(q,r)^{i-1}}(q)$$

This is maximised when $\tau_{(q,r)^{i-1}}(q) = 0$ whenever

$$P_{(q,r)^{i-1}}(q) \neq P_{(q,r)^{i-1}} = \max_{m \in \mathcal{M}} P_{(q,r)^{i-1}}(m)$$

This criterion determines a distribution $\tau_{(q,r)^{i-1}}(q)$ of an optimal strategy τ. For example the adversary may choose a query $\hat{q}$ such that

$$P_{(q,r)^{i-1}}(\hat{q}) = \max_{m \in \mathcal{M}} P_{(q,r)^{i-1}}(m)$$

with probablility $\tau_{(q,r)^{i-1}}(\hat{q}) = 1$ and all other queries $q \neq \hat{q}$ with probablility $\tau_{(q,r)^{i-1}}(q) = 0$.

A similar argument with $P_{(q,r)^{i-1}}$ in the role of $P_i((q,r)^i)$ leads to a criterion for a distribution $\tau_{(q,r)^{i-2}}(q)$ of an optimal strategy τ. Also similarly the distributions $\tau_{(q,r)^j}(q)$ for $j = i-2, \ldots, 0$ of an optimal strategy τ may be determined. That is, an optimal strategy is one by which the adversary always chooses a query that maximizes the expected success probability.

In an on-line attack, each query is a spoofing attempt and so the adversary continues to make (up to $L+1$) queries only if the response to each previous query is rejection. Denoting the probability that the adversary is successful using strategy τ by P^τ, the probability that the adversary is unsuccessful in spoofing using strategy τ is given by

$$1 - P^\tau = \sum p((q,r)^L)(1 - P_L((q,r)^L))$$

where the sum is over those sequences $(q,r)^L$ such that r_j is rejection for each query $q_j, j = 1, \ldots, L$. Let P be the maximum of P^τ over all strategies τ. Then P is the adversary's probability of success in an on-line attack if the adversary uses an optimal strategy. In the event that each of the first L queries produces the response F the adversary's best strategy is to choose query q_{L+1} that maximises the expected probability of success, *ie* to choose $q_{L+1} = q_{(q,r)^L}$ such that the expected success probability

$$P_{(q,r)^L}(q_{(q,r)^L}) = \mathbf{payoff}_T(q_{(q,r)^L}, (q,r)^L)$$

is equal to the maximum, $P_L((q,r)^L)$ (where $r_j = \mathtt{F}, j = 1, \ldots, L$). In the event that each of the first $L-1$ queries produces the response F the adversaries best strategy is to choose a query q_L that maximises the expected probability of success

$$\begin{aligned} P_{(q,r)^{L-1}}(q_L) = \mathbf{payoff}_T(q_L, (q,r)^{L-1}) + \\ (1 - \mathbf{payoff}_T(q_L, (q,r)^{L-1})) \times \\ P_{(q,r)^{L-1},(q_L,\mathtt{F})}(q_{(q,r)^{L-1},(q_L,\mathtt{F})}) \end{aligned}$$

In a similar way, as in the off-line attack, it follows that, for $j = L+1, \ldots, 1$, the choice of query q_j that maximises the expected success probability provides an optimal strategy τ.

B. Bounds on success probability

Consider an adversary who spoofs after observing i query and response pairs arising from strategy τ. Let the values $p^*(e, m, (q,r)^i)$ for $e \in \mathcal{E}$, $m \in \mathcal{M}$ and sequence $(q,r)^i$ of query and response pairs be a joint probability distribution on $\mathcal{E} \times \mathcal{M} \times (\mathcal{M} \times \mathcal{R})^i$ such that, if $\gamma(e, m, (q,r)^i) = 0$ then $p^*(e, m, (q,r)^i) = 0$ and, for all e and $(q,r)^i$, $\sum_m p^*(e, m, (q,r)^i) = p(e, (q,r)^i)$, the probability that the encoding rule is e and, for strategy τ, the sequence of query and response pairs is $(q,r)^i$. We write M^* to denote a random variable that takes values a_m with respective probabilities $p^*(m) = \sum_{e,(q,r)^i} p^*(e, m, (q,r)^i)$. The proof of Theorem 3.1 of Rosenbaum [3] may be adapted to establish the following theorem giving an information theoretic expression that bounds the probability of success of the adversary. This bound is completely analogous to the bound for a message-observing adversary, the only difference being that it depends on the entropy of the key given query and response information rather than given observed message information.

Theorem 3.1: Let A be an authentication system and let P_i^τ be the probability of success of an adversary who uses strategy τ and spoofs after observing i query and response pairs. Then

$$P_i^\tau \geq 2^{H(E|M^*,(Q,R)^i) - H(E|(Q,R)^i)} = 2^{-I(E;M^*|(Q,R)^i)}$$

Moreover, equality holds if and only if, for all $(q,r)^i \in (\mathcal{M} \times \mathcal{R})^i$ with $p((q,r)^i) \neq 0$ and all $m \in M$ with $p^*(m|(q,r)^i) \neq 0$, we have $\mathbf{payoff}_\mathtt{T}(m, (q,r)^i) = P_i^\tau$ and $p^*(m|e, (q,r)^i)$ is constant for all $e \in \mathcal{E}(m, (q,r)^i)$.

We have described above an optimal strategy τ in which the next query q_j is determined by the response to the previous query (and therefore in turn by the responses to all previous queries). We may write $q_j = q(r^{j-1}$. The authentication code and such an optimal strategy determines a probability distribtion on sequences r^i of responses correspondingto a random variable R^i for $i = 1, \ldots, L+1$. By Theorem 3.1 we have, for such an optimal strategy τ

$$P_i^\tau \geq 2^{-I(E;M^*|R^i)}$$

The message-observing attacker obtains information from valid messages sent across the channel. The querying attacker obtains information from the responses to the queries. Thus, there are two differences: the former's information, unlike the latter's, depends on the source state distribution; and the latter's expected information is an average of information from valid messages and invalid messages. So, whereas observing a message may decrease the success probability of an adversary - because, for example, it might be that the next most likely message to be observed would have been (had it not been observed) the best choice for spoofing - an adversary always increases his success probability by making an additional query - because his probability of success is an average over the two possible responses.

The following theorem shows that, for $i = 0, \ldots, L-1$, $P_{i+1}((q,r)^{i+1}) \geq P_i((q,r)^i)$. That is, the adversary's success probability in an off-line attack can only get better as more queries are made if an optimal strategy is adopted.

Theorem 3.2: Suppose that an adversary adopts an optimal strategy in an off-line attack on an authentication system A. Then for $i = 0, \ldots, L-1$,

$$P_{i+1}((q,r)^{i+1}) \geq P_i((q,r)^i)$$

Proof: Suppose that $0 \leq i \leq L-1$ and that the adversary has observed the sequence $(q,r)^i$ of query and response pairs. Let q_{i+1} be a query such that there exists a message $\hat{m} \neq q_{i+1}$ with

$$\mathbf{payoff}_\mathtt{T}(\hat{m}, (q,r)^i) = \max_{m \in \mathcal{M}} \mathbf{payoff}_\mathtt{T}(m, (q,r)^i)$$

The expected success probability of the adversary after this query is

$$p(\mathtt{T}|q_{i+1},(q,r)^i)\max_{m\in\mathcal{M}}\mathbf{payoff}_{\mathtt{T}}(m,(q,r)^i,(q_{i+1},\mathtt{T}) + p(\mathtt{F}|q_{i+1},(q,r)^i)\max_{w\in\mathcal{M}}\mathbf{payoff}_{\mathtt{T}}(w,(q,r)^i,(q_{i+1},\mathtt{F})$$

where

$$p(r|q_{i+1},(q,r)^i) = \sum_{e\in\mathcal{E}((q,r)^i,(q_{i+1},r))} p(e|(q,r)^i)$$

denotes the conditional probability that the response is r given the sequence $(q,r)^i$ and the query q_{i+1} and $p(e|(q,r)^i) = \frac{p(e)}{\sum_{e\in\mathcal{E}((q,r)^i)}p(e)}$. But this is

$$\begin{aligned}
&p(\mathtt{T}|q_{i+1},(q,r)^i)\max_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}(m,(q,r)^i,(q_{i+1},\mathtt{T}))}\\
&[p(e|(q,r)^i,(q_{i+1},\mathtt{T}))\gamma(e,m,(q,r),(q_{i+1},\mathtt{T}))]\\
&+p(\mathtt{F}|q_{i+1},(q,r)^i)\max_{w\in\mathcal{M}} \sum_{e\in\mathcal{E}(w,(q,r)^i,(q_{i+1},\mathtt{F}))}\\
&[p(e|(q,r)^i,(q_{i+1},\mathtt{F}))\gamma(e,w,(q,r),(q_{i+1},\mathtt{F}))]
\end{aligned}$$

where

$$p(e|(q,r)^i,(q_{i+1},r) = \frac{p(e|(q,r)^i)}{\sum_{e'\in\mathcal{E}((q,r)^i,(q_{i+1},r))}p(e'|(q,r)^i)}$$

Hence this is:

$$\begin{aligned}
&\max_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}(m,(q,r)^i,(q_{i+1},\mathtt{T}))} [p(e|(q,r)^i)\times\\
&\qquad \gamma(e,m,(q,r),(q_{i+1},\mathtt{T}))]\\
&+\max_{w\in\mathcal{M}} \sum_{e\in\mathcal{E}(w,(q,r)^i,(q_{i+1},\mathtt{F}))} [p(e|(q,r)^i)\times\\
&\qquad \gamma(e,w,(q,r),(q_{i+1},\mathtt{F}))]\\
&\geq \max_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}(m,(q,r)^i,(q_{i+1},\mathtt{T}))} [p(e|(q,r)^i)\times\\
&\qquad \gamma(e,m,(q,r),(q_{i+1},\mathtt{T})) + p(e|(q,r)^i)\times\\
&\qquad \gamma(e,m,(q,r),(q_{i+1},\mathtt{F}))]\\
&= \max_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}(m,(q,r)^i)} p(e|(q,r)^i)\times\\
&\qquad \gamma(e,m,(q,r)^i,(q_{i+1},r))\\
&= \sum_{e\in\mathcal{E}(\hat{m},(q,r)^i)} p(e|(q,r)^i)\gamma(e,\hat{m},(q,r)^i)\\
&= P_i((q,r)^i).
\end{aligned}$$

It follows immediately that $P_{i+1}((q,r)^{i+1}) \geq P_i((q,r)^i)$ as an optimal strategy must do at least as well as a strategy that chooses q_{i+1}. ■

C. Bounds on key entropy

We find a bound on the key entropy by considering a different game that the adversary may play. Instead of querying with the objective of being able to spoof optimally, the adversary may try to query to obtain the maximum possible amount of information from the responses. We consider the mutual information between the key and such responses and so obtain a bound on the key entropy, that is the size of the key.

Suppose the adversary can ask L queries using strategy τ and his aim is to maximize the information obtained from these queries. To find the best strategy of the attacker we will use an approach similar to Section **??**. For a given a the sequence $(q,r)^i$, a query q will have the response $r = T$ with probability $p(T|q,(q,r)^i)$ and F with probability $p(F|q,(q,r)^i$. Let R_i denote a binary random variable associated with this probability distribution. Note that $p(r|q,(q,r)^i) = \mathbf{payoff}_r(q,(q,r)^i)$ is the (conditional) probability that the response is r to query q given the sequence $(q,r)^i$ of query and response pairs. We have $\mathbf{payoff}_{\mathtt{F}}(q,(q,r)^i) = 1 - \mathbf{payoff}_{\mathtt{T}}(q,(q,r)^i)$. Then

$$\begin{aligned}
&H(R_{i+1}|q,(q,r)^i) =\\
&-\sum_{r\in\mathcal{R}}\mathbf{payoff}_r(q,(q,r)^i)\log\mathbf{payoff}_r(q,(q,r)^i) =\\
&-\sum_{r\in\mathcal{R}}\sum_{e\in\mathcal{E}(q,(q,r)^i)} p(e,r|q,(q,r)^i)\times\\
&\qquad\qquad \log\mathbf{payoff}_r(q,(q,r)^i)
\end{aligned}$$

This is the uncertainty in the response to query q assuming that query and response pairs $(q,r)^i$ had been observed.

Now consider a game where the adversary uses a strategy τ to select queries and his aim is to learn as much as possible from the responses. Let

$$U_i((q,r)^i) = \max_{q\in\mathcal{M}} H(R_{i+1}|q,(q,r)^i)$$

This is the maximum information the adversary can obtain from the response r_{i+1} after the sequence $(q,r)^i$ of query and responses. Although querying with a query that attains this maximum may not lead to maximizing the total information in the sequence of responses, we can use $U_i((q,r)^i)$ to obtain a lower bound on this total information and therefore a lower bound on the key entropy. To this end we let

$$U_i^\tau = \min_{(q,r)^i} U_i((q,r)^i)$$

where the minimum is over all query and response sequences $(q,r)^i$ with non-zero probability for strategy τ.

Given a query and response sequence $(q,r)^L$ the adversary's best strategy is to choose with non-zero probability $\tau_{(q,r)^L}(q)$ only those queries q such that the information obtained $H(R_{L+1}|q,(q,r)^L)$ is equal to

the maximum, $U_L((q,r)^L)$. Given a query and response sequence $(q,r)^{L-1}$ the adversary's best strategy is choose with non-zero probability $\tau_{(q,r)^{L-1}}(q)$ only those queries q such that the expected information gain

$$H(R_L|q,(q,r)^{L-1}) + \sum_{r\in\mathcal{R}} p(r|q,(q,r)^{L-1})U_L((q,r)^{L-1},(q,r))$$

is a maximum. As $U_{L-1}((q,r)^{L-1}) = (\max_{q\in\mathcal{M}} H(R_L|q,(q,r)^{L-1})$ and by the definition of U_i^τ we clearly have that this maximum is at least $U_{L-1}^\tau + U_L^\tau$.

Similarly, for each $i = L-2,\ldots,1$, the adversary may determine a distribution $\tau_{(q,r)^i}$ of an optimal strategy τ. An optimal strategy ensures that the information obtained by the adversary is at least $\sum_{i=0}^{L} U_i^\tau$.

The information obtained from the responses to the adversary's queries give information about the key. We establish a bound on the key entropy in terms of the information obtained from the responses.

We write $\chi(e,m,\mathtt{T},(q,r)^i) = \gamma(e,m,(q,r)^i)$ and $\chi(e,m,\mathtt{F},(q,r)^i) = 1-\gamma(e,m,(q,r)^i)$

Theorem 3.3: Let A be an authentication system and suppose that the adversary uses a strategy τ such that $\tau_{(q,r)^i}(q') \neq 0$ only if $H(R_{i+1}|q',(q,r)^i) = U_i((q,r)^i)$. Then

$$U_i((q,r)^i) \leq H(E|(Q,R)^i) - H(E|(Q,R)^{i+1}).$$

Proof:

Let $p(q',r'|(q,r)^i)$ denote the conditional probability that the response is r' to query q' given that the responses were $r_j, j=1,\ldots,i$ to queries $q_j, j=1,\ldots,i$ respectively. Put

$$\Psi_{q',r',(q,r)^i}(e) = \frac{p(e|(q,r)^i)\chi(e,q',r',(q,r)^i)}{\mathbf{payoff}_{r'}(q',(q,r)^i)}.$$

Then $\Psi_{q',r',(q,r)^i}$ is a probability distribution on $\mathcal{E}$.

Now

$$p(q',r'|(q,r)^i) = \sum_{e\in\mathcal{E}(q',r',(q,r)^i)} p(q',r',e|(q,r)^i) =$$
$$\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [\Psi_{q',r',(q,r)^i}(e)\mathbf{payoff}_{r'}(q',(q,r)^i) \times p(q',r'|e,(q,r)^i)]$$

Hence, by Jensen's inequality [6], we have the following

$$\begin{aligned}
& p(q',r'|(q,r)^i)\log p(q',r'|(q,r)^i) \\
\leq & \sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [\Psi_{q',r',(q,r)^i}(e)\mathbf{payoff}_{r'}(q',(q,r)^i) \times \\
& p(q',r'|e,(q,r)^i)\log(\mathbf{payoff}_{r'}(q',(q,r)^i) \times \\
& p(q',r'|e,(q,r)^i))] \\
= & \sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e|(q,r)^i)p(q',r'|e,(q,r)^i) \\
& \times\chi(e,q',r',(q,r)^i)\log(\mathbf{payoff}_{r'}(q',(q,r)^i) \\
& \times p(q',r'|e,(q,r)^i))]
\end{aligned}$$

We now consider the entropy of of the joint distribution of the random variables Q',R' where the adversary chooses the next query $q' \in Q'$ according to probability distribution $\tau'(q')$ and $r' \in R'$ is distributed with probability dependent on the distribution of q' and the distribution $p(e)$ on the encoding rules. We are interested in the conditional entropy $H(Q',R'|(q,r)^i)$ conditional on responses $r_j, j=1,\ldots,i$ to queries $q_j, j=1,\ldots,i$, respectively.

We have

$$\begin{aligned}
& H(Q',R'|(q,r)^i) = -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}} [p(q',r'|(q,r)^i) \\
& \times\log p(q',r'|(q,r)^i)] \\
& \geq -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e|(q,r)^i) \times \\
& \qquad p(q',r'|e,(q,r)^i)\chi(e,q',r',(q,r)^i) \times \\
& \qquad \log(\mathbf{payoff}_{r'}(q',(q,r)^i)p(q',r'|e,(q,r)^i))] \\
& = -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e|(q,r)^i)p(q',r'|e,(q,r)^i) \\
& \qquad \times\chi(e,q',r',(q,r)^i)\log\mathbf{payoff}_{r'}(q',(q,r)^i)] \\
& -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e|(q,r)^i)p(q',r'|e,(q,r)^i) \\
& \qquad \times\chi(e,q',r',(q,r)^i)\log p(q',r'|e,(q,r)^i)] \\
& = -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e,q',r'|(q,r)^i) \\
& \qquad \times\log\mathbf{payoff}_{r'}(q',(q,r)^i)] \\
& -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} p(e,q',r'|(q,r)^i)\log p(q',r'|e,(q,r)^i) \\
& = -\sum_{r'\in\mathcal{R}}\sum_{q'\in\mathcal{M}}\sum_{e\in\mathcal{E}(q',r',(q,r)^i)} [p(e,q',r'|(q,r)^i) \\
& \qquad \times\log\mathbf{payoff}_{r'}(q',(q,r)^i)] + H(Q',R'|E,(q,r)^i) \\
& = -\sum_{q'\in\mathcal{M}} \tau'(q') \sum_{r'\in\mathcal{R}}\sum_{e\in\mathcal{E}((q,r)^i)} [p(e,r'|q',(q,r)^i) \\
& \qquad \times\log\mathbf{payoff}_{r'}(q',(q,r)^i)] + H(Q',R'|E,(q,r)^i) \\
& = \sum_{q'\in\mathcal{M}} \tau'(q')H(R_{i+1}|q',(q,r)^i) + H(Q',R'|E,(q,r)^i) \\
& = \sum_{q'\in\mathcal{M}} \tau'(q')U_i((q,r)^i) + H(Q',R'|E,(q,r)^i) \\
& = U_i((q,r)^i) + H(Q',R'|E,(q,r)^i)
\end{aligned}$$

where the second to last equality holds provided τ' satisfies $\tau'(q') = 0$ unless $H(R_{i+1}|q',(q,r)^i) = U_i((q,r)^i)$.

This can be written as

$$\begin{aligned}
U_i((q,r)^i) &\leq H(Q',R'|(q,r)^i) - H(Q',R'|E,(q,r)^i) \\
&= H(E|(q,r)^i) - H(E|Q',R',(q,r)^i)
\end{aligned}$$

Thus, since $U_i^\tau \leq U_i((q,r)^i)$ for all $(q,r)^i$ by definition,

$$\begin{aligned} U_i^\tau &\leq H(E|(Q,R)^i) - H(E|Q',R',(Q,R)^i) \\ &= H(E|(Q,R)^i) - H(E|(Q,R)^{i+1}) \end{aligned}$$

if $\tau_{(q,r)^i}(q') = \tau'(q')$

■

This means that the reduction in uncertainty about the key in step i, will be lower bounded by U_i^τ for an adversary's strategy that maximizes the expected conditional entropy $\sum_{q\in\mathcal{M}} \tau_{(q,r)^i}(q) H(R_{i+1}|q,(q,r)^i)$.

Since $H(E) = H(E|(Q,R)^{L+1}) + \sum_{j=0}^{L}(H(E|(Q,R)^j) - H(E|(Q,R)^{j+1}))$ we obtain from the bound in Theorem 3.3 a bound on the key entropy of an A-code.

Theorem 3.4: For an A-code, $(\mathcal{S},\mathcal{M},\mathcal{E},f)$, we have the following bound

$$H(E) \geq \sum_{j=0}^{L} U_j^\tau$$

for any adversary strategy τ which chooses queries q_{j+1} such that $H(R_{j+1}|q_{j+1},(q,r)^j)$ is a maximum, $j = 0,\ldots,L$.

IV. Concluding Remarks

We have given an analysis of two games played by an adversary in the verication query model of an A-code and derived bounds on success probability of the adversary and the size of the key space. The bounds on the success probability of a V-query adversary in Game 1 generalise known bounds on the success probability of a message observing adversary.

We showed that, in general, asking a query before spoofing is the best strategy. This is not the case for a message observing adversary where observing a message may reduce his success chance and the best strategy might be spoofing without observing a message.

References

[1] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, 'Codes which detect deception', *Bell System Tech. J.* **53**(3) (1974) 405–424.

[2] D. Pei, 'Information-theoretic bounds for authentication codes and block designs', *Journal of Cryptology* **8** (1995), 177-188.

[3] U. Rosenbaum, 'A lower bound on authentication after having observed a sequence of messages', *Journal of Cryptology* 6 (1993), 135-156.

[4] R. Safavi-Naini, L. McAven and M. Yung, 'General Group Authentication Codes and Their Relation to "Unconditionally Secure Signatures"', Public Key Cryptography 2004, LNCS 2947, pp 231-248.

[5] G. J. Simmons, 'Authentication theory/coding theory', *Crypto'84* LNCS **196** (Springer–Verlag, 1984) 411–431.

[6] http://planetmath.org/encyclopedia/JensensInequality.html