T-79.7001 Postgraduate Course in Theoretical Computer Science / Theoretical bounds for human mediated data authentication protocols

Vesa Vaskelainen

27.10.2006

Abstract

This survey is predominantly based on the paper written by M. Naor, G. Segev and A. Smith [1]. The message authentication problem is examined here in manual channel model where the sender and receiver are connected by an insecure channel and by a low-bandwidth auxiliary channel, that enables the sender to "manually" authenticate one short message to the receiver. This model is considered in information-theoretic setting where no computational assumptions are made. It will be claimed that for any $0 < \epsilon < 1$ there exists a $\log^* n$-round protocol for authenticating n-bit messages, in which only $2\log(1/\epsilon) + O(1)$ bits are manually authenticated, and proved that any adversary has probability of at most ϵ to cheat the receiver into accepting a fraudulent message.

1 Introduction

Message authentication is a security service for a message receiver to verify whether a message is from a specified legitimate source, even in the presence of an adversary who controls the communication channel. Research on the field has been going on already more than three decades and thus many message authentication protocols have been suggested and throughoutly investigated. Security level of these protocols is determined based on the adversary's computing power.

Security that holds when the adversary is computationally unbounded is called *unconditional security* or *information-theoretic security*. If restrictions are made to the adversary's computing power then security that holds in that case is called *computational security*. Information-theoretic security will be in central concern in this survey, because it allows exact evaluation of the error probabilities. On the other hand we will be able to calculate growth rates and lower bounds for the model parameters as functions on exact error probabilities.

Manual channel model got the formal treatment in the literature by Vaudenay [2] in 2005. In this model the sender and the receiver are connected by a bidirectional insecure channel, and by a unidirectional low-bandwidth auxiliary channel, but do not share any secret information. The low-bandwidth auxiliary channel enables the sender to "manually" authenticate one short string to the receiver. For example, the sender can type a short string and send it to receiver through the auxiliary channel. It is assumed that the adversary can read any message sent over the auxiliary channel, prevent it from being delivered, and insert a new message at any point in time. However, the adversary cannot modify the message sent over this channel.

The rest of the paper is organized as follows. Section 2 gives a detailed description of the protocol in manual channel model and Section 3 states few theoretical results and makes close analysis of the proofs.

2 A message authentication protocol

The notation used in this survey is the following. By $\mathrm{GF}[Q]$ we denote the Galois field with Q elements and by $m = m_1 \dots m_k \in \mathrm{GF}[Q]^k$ a message. With $x \in_{\mathrm{R}} \mathrm{GF}[Q]$ is denoted that element x is chosen uniformly at random from $\mathrm{GF}[Q]$.

For $x \in \mathrm{GF}[Q]$ let $C_x(m) = \sum_{i=1}^{k} m_i x^i$ that is a message parsed a polynomial of degree k over $\mathrm{GF}[Q]$ without the constant term, and evaluated at the point x. Now it holds that for any two different messages $m, \widehat{m} \in \mathrm{GF}[Q]^k$ and for any element $c, \widehat{c} \in \mathrm{GF}[Q]$ the polynomials $C_x(m) + c$ and $C_x(\widehat{m}) + \widehat{c}$ are also different. This follows from the observation that since the messages are different then are also coefficients different in polynomials (c can be equal to $\widehat{c}$ but that cannot make the polynomials the same).

Even though the polynomials are different they can map a certain number of points to the same point. Therefore $\Pr_{x \in_{\mathrm{R}} \mathrm{GF}[Q]}[C_x(m) + c = C_x(\widehat{m}) + \widehat{c}]$ can be greater than $1/Q$, and upper bounding this probability for future reference makes sense since we will use $C(\cdot)$ as a hash function to reduce the length of the message. By the fundamental theorem of algebra we know that a polynomial $P(x)$ of degree d has d values x_i (some of them possibly degenerate) for which $P(x_i) = 0$. Let us write $P(x) = C_x(m) - C_x(\widehat{m}) + c - \widehat{c}$ then $\deg(P(x)) = k$ where it follows that $\max\{|\{x : P(x) = 0\}|\} = k$. There are Q elements in $\mathrm{GF}[Q]$ and thus $\Pr_{x \in_{\mathrm{R}} \mathrm{GF}[Q]}[C_x(m) + c = C_x(\widehat{m}) + \widehat{c}] = \Pr_{x \in_{\mathrm{R}} \mathrm{GF}[Q]}[P(x) = 0] \leq \frac{k}{Q}$.

Now we will construct a protocol for manual channel model. Protocol P_k is the k-round protocol which applies a sequence of hash functions $C^1, \ldots, C^{k-1}$ during its execution in order to obtain a shorter and shorter message for manual authentication. Defining parameters for the protocol are n which is the length of the input message, e which is the adversary's forgery probability and each C^j $(j = 1, \ldots, k-1)$ parses n_j-bit strings to polynomials over $\mathrm{GF}[Q]$, where $n_1 = n$. Moreover each Q_j is chosen such that,

$$\frac{2^{k-j} n_j}{\epsilon} \leq Q_j < \frac{2^{k-j+1} n_j}{\epsilon} \tag{1}$$

and for the next round,

$$n_{j+1} = \lceil 2 \log Q_j \rceil. \tag{2}$$

For analysis purposes we still need to make difference between strings x that are sent by sender ($\mathcal{S}$) or by receiver ($\mathcal{R}$) and the strings $\widehat{x}$ that are actually received by other party. This is because the adversary can replace any string sent by any one of parties over the insecure channel. In the protocol addition and multiplication are operations of the Galois field $\mathrm{GF}[Q]$ and $\langle u, v \rangle$ denotes the concatenation of the strings u and v. Protocol is described in Figure 1.

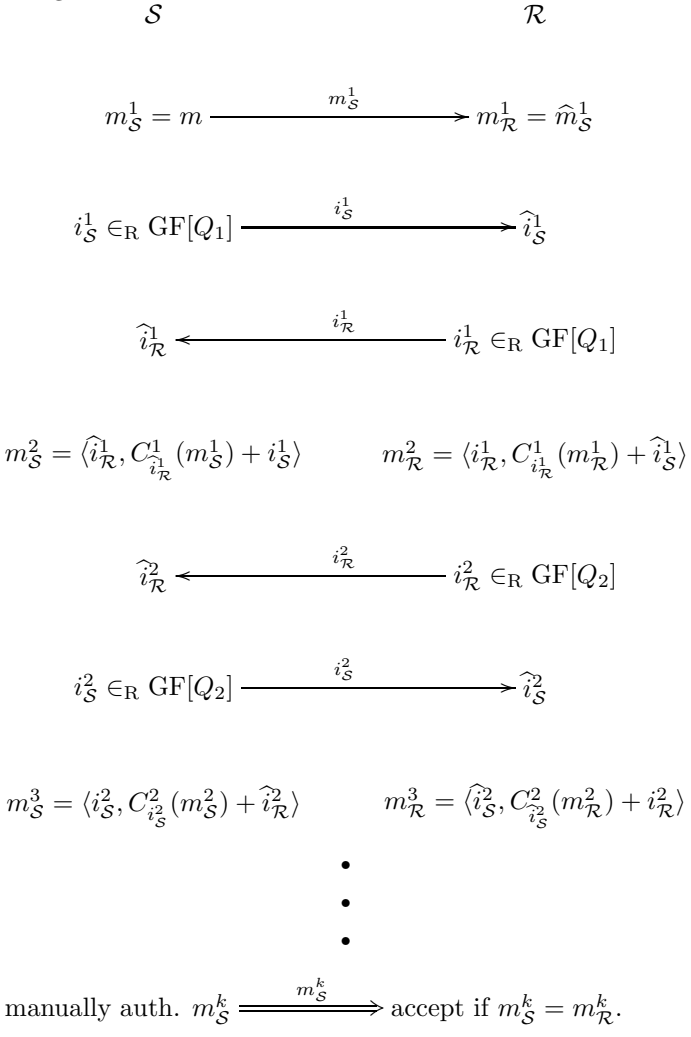

Figure 1: The k-round authentication protocol for manual channel model. First two strings ($m^1_{\mathcal{S}}$ and $i^1_{\mathcal{S}}$) can be sent together, and therefore the protocol requires only k rounds of communication. The first and the second round are different, though the only difference is that the roles of the sender and the receiver are changed. We can see that if $\mathcal{S}$ and $\mathcal{R}$ are interchanged in the second round then it is analogical with the first round (after $m^1_{\mathcal{S}}$ is sent). Rounds after the second round until $k-1$:th round are analogical with the first or the second round depending on is the number of round odd or even.

If for all input messages m, whenever there is no interference by the adversary in the execution, the receiver accepts m with probability 1 then the authentication protocol is said to be *perfectly complete*. With this protocol that is clearly the case. If there is no interference by the adversary, that is $m^1_{\mathcal{R}} = m^1_{\mathcal{S}}$ and for all j, $1 \leq j \leq k-1$, hold that $\widehat{i}^j_{\mathcal{R}} = i^j_{\mathcal{R}}$ and $\widehat{i}^j_{\mathcal{S}} = i^j_{\mathcal{S}}$ then $m^{j+1}_{\mathcal{R}} = m^{j+1}_{\mathcal{S}}$ which leads to $m^k_{\mathcal{R}} = m^k_{\mathcal{S}}$ and that means that the receiver accepts.

Note that an important property in this setting is that the parties will each be able to choose the Q_j's in deterministic way and after the Q_j is chosen then representations of GF$[Q_j]$ can also be get in deterministic way. Remember that the order of of a Galois field completely specifies the field. This avoids us to explicitly specify these parameters in the description of the protocol which could cause security problems (see an example from [3]). One possible solution is to choose Q_j as the smallest prime number in the interval (1) (assuming that it exists always). For the Galois field of order p which is prime we know that we can construct GF$[p]$ using the integers $\{1, 2, \ldots, p-1\}$ and *modulo* p addition and multiplication. The representation of the field element in bits then can be just a binary representation of the integer.

3 Analysis of the protocol

In this section we prove that a computationally unbounded adversary has probability of at most ϵ to cheat the receiver into accepting a fraudulent message in the protocol P_k. We also examine the proof that for any integer $k \geq 3$, and any integer n and $0 < \epsilon < 1$, the protocol P_k enables the sender to authenticate an n-bit input message to the receiver, while manually authenticating at most $2\log(1/\epsilon) + 2\log^{(k-1)} n + \mathrm{O}(1)$ bits.

Lemma 3.1 *Any computationally unbounded adversary has probability of at most ϵ to cheat the receiver into accepting a fraudulent message in protocol P_k.*

Proof. Let us assume an execution of the protocol P_k in which an adversary cheats the receiver into accepting a fraudulent message, then it corresponds to situation where the receiver gets a message $m^1_{\mathcal{R}}$ which is different than the message that was sent by the sender $m^1_{\mathcal{S}}$ but the receiver checks in the end that $m^k_{\mathcal{S}} = m^k_{\mathcal{R}}$ and accepts the message $m^1_{\mathcal{R}}$. Then it must be that during the rounds from 1 to $k-1$ at some round j, $m^j_{\mathcal{S}} \neq m^j_{\mathcal{R}}$, but on the next round, $m^{j+1}_{\mathcal{S}} = m^{j+1}_{\mathcal{R}}$. We denote this event by D_j. Other notation used in this proof is the following. For any variable y that occurs during this execution let $T(y)$ be the moment of time at which the variable y is fixed. Time moments $T(x_1)$ and $T(x_2)$ occur in time such that either $T(x_1) < T(x_2)$ or $T(x_1) \geq T(x_2)$ which means that either x_1 is fixed before x_2 or x_1 is fixed at the same time or later than x_2.

In [1] is given a more practical example where $T(i^j_{\mathcal{R}})$ denotes the time in which $\mathcal{R}$ sent $i^j_{\mathcal{R}}$ and $T(\widehat{i}^j_{\mathcal{R}})$ denotes the time in which $\mathcal{S}$ received from the adversary $\widehat{i}^j_{\mathcal{R}}$ corresponding to $i^j_{\mathcal{R}}$. However, now the comparison of times when choosing of $i^j_{\mathcal{R}}$ and $\widehat{i}^j_{\mathcal{R}}$ occurred is not exact based on $T(i^j_{\mathcal{R}})$ and $T(\widehat{i}^j_{\mathcal{R}})$ if no assumption of delays on transmission or channel are made. For clarity, I consider here $T(i^j_{\mathcal{R}})$ denote the time when $i^j_{\mathcal{R}}$ was chosen by the receiver and $T(\widehat{i}^j_{\mathcal{R}})$ denotes the time when $\widehat{i}^j_{\mathcal{R}}$ was chosen by the adversary.

Structure of $m^{j+1}_{\mathcal{S}} = \langle \widehat{i}^j_{\mathcal{R}}, C^j_{\widehat{i}^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} \rangle$ and $m^{j+1}_{\mathcal{R}} = \langle i^j_{\mathcal{R}}, C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i}^j_{\mathcal{S}} \rangle$ on the odd round and structure of $m^{j+1}_{\mathcal{S}} = \langle i^j_{\mathcal{S}}, C^j_{i^j_{\mathcal{S}}}(m^j_{\mathcal{S}}) + \widehat{i}^j_{\mathcal{R}} \rangle$ and $m^{j+1}_{\mathcal{R}} = \langle \widehat{i}^j_{\mathcal{S}}, C^j_{\widehat{i}^j_{\mathcal{S}}}(m^j_{\mathcal{R}}) + i^j_{\mathcal{R}} \rangle$ on the even round and assumption that $m^j_{\mathcal{S}} \neq m^j_{\mathcal{R}}$ shows that the wanted probability $\Pr[D_j]$ can depend only on parameters $i^j_{\mathcal{S}}$, $\widehat{i}^j_{\mathcal{S}}$, $i^j_{\mathcal{R}}$ and $\widehat{i}^j_{\mathcal{R}}$. Adversary's act must be then targeted to $\widehat{i}^j_{\mathcal{S}}$ and $\widehat{i}^j_{\mathcal{R}}$. For probability calculation the thing that makes difference is then to know did adversary choose the values of $\widehat{i}^j_{\mathcal{S}}$ and $\widehat{i}^j_{\mathcal{R}}$ before or not before the sender or the receiver choosed values $i^j_{\mathcal{S}}$ and $i^j_{\mathcal{R}}$.

If j is odd then event D_j can occur only if $i^j_{\mathcal{R}} = \widehat{i}^j_{\mathcal{R}}$ and $C^j_{\widehat{i}^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i}^j_{\mathcal{S}}$. We have four possibilities to consider, either $\widehat{i}^j_{\mathcal{R}}$ was chosen before $i^j_{\mathcal{R}}$ or it was not chosen before and either $\widehat{i}^j_{\mathcal{S}}$ was chosen before $i^j_{\mathcal{S}}$ or it was not chosen before. Obviously these four cases gather the all possible cases and only one of them can actually occur. Closer analysis reveals that in the case $T(\widehat{i}^j_{\mathcal{R}}) < T(i^j_{\mathcal{R}})$ the probability $\Pr[D_j]$ is not depen-

dent on whether the $\widehat{i^j_{\mathcal{S}}}$ was chosen before $i^j_{\mathcal{S}}$ or not. From the protocol follows that $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}})$ and $T(i^j_{\mathcal{S}}) < T(\widehat{i^j_{\mathcal{R}}})$ and these together with $T(\widehat{i^j_{\mathcal{R}}}) < T(i^j_{\mathcal{R}})$ gives that $T(i^j_{\mathcal{S}}) < T(i^j_{\mathcal{R}})$, $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}})$ and $T(\widehat{i^j_{\mathcal{R}}}) < T(i^j_{\mathcal{R}})$. That means all other parameters are fixed at the time when $i^j_{\mathcal{R}}$ is chosen. Now we have three cases to analyse:

1. $T(\widehat{i^j_{\mathcal{R}}}) < T(i^j_{\mathcal{R}})$. The last event in time that sets $\Pr[D_j]$ is now the receiver choose $i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]$ and at that time $i^j_{\mathcal{S}}$, $\widehat{i^j_{\mathcal{S}}}$ and $\widehat{i^j_{\mathcal{R}}}$ are already set. Therefore we get,

$$\begin{aligned}\Pr[D_j] &= \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[m^{j+1}_{\mathcal{S}} = m^{j+1}_{\mathcal{R}}] \\ &= \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[i^j_{\mathcal{R}} = \widehat{i^j_{\mathcal{R}}} \wedge \\ &\quad C^j_{\widehat{i^j_{\mathcal{R}}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}}] \\ &\leq \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[i^j_{\mathcal{R}} = \widehat{i^j_{\mathcal{R}}}] \\ &= \frac{1}{Q_j} \leq \frac{\epsilon}{2^{k-j} \cdot n_j} \leq \frac{\epsilon}{2^{k-j}}, \end{aligned} \tag{3}$$

where the last row is get by using (1) and $n_j \geq 1$.

2. $T(\widehat{i^j_{\mathcal{R}}}) \geq T(i^j_{\mathcal{R}})$ and $T(\widehat{i^j_{\mathcal{S}}}) \geq T(i^j_{\mathcal{S}})$. Now the adversary chooses $\widehat{i^j_{\mathcal{R}}}$ not before the receiver chooses $i^j_{\mathcal{R}}$ and that is why we have to assume something about $\widehat{i^j_{\mathcal{R}}}$. As was mentioned earlier, D_j can occur only if $i^j_{\mathcal{R}} = \widehat{i^j_{\mathcal{R}}}$ when j is odd. Thus we assume that the adversary chooses $\widehat{i^j_{\mathcal{R}}} = i^j_{\mathcal{R}}$. From the protocol it follows that $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}})$ and $T(m^j_{\mathcal{S}}) < T(i^j_{\mathcal{S}})$ and $T(m^j_{\mathcal{R}}) < T(i^j_{\mathcal{R}})$. From this it follows that, $T(m^j_{\mathcal{S}}) < T(i^j_{\mathcal{S}}) \leq T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}})$. Now we know that $m^j_{\mathcal{R}}$, $m^j_{\mathcal{S}}$, $i^j_{\mathcal{S}}$ and $\widehat{i^j_{\mathcal{S}}}$ are fixed before $i^j_{\mathcal{R}}$ is chosen.

The other requirement for D_j to occur was for polynomials over Galois field $C^j_{\widehat{i^j_{\mathcal{R}}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}}$ and we assumed in the beginning that $m^j_{\mathcal{S}} \neq m^j_{\mathcal{R}}$. Then no choice of $i^j_{\mathcal{R}}$ and $\widehat{i^j_{\mathcal{S}}}$ can make the polynomials as functions of $i^j_{\mathcal{R}}$ the same. In general polynomials over some field are defined to be the same if for all elements x in the field their values are the same. In this case the reader may check as an algebraic exercise that $m^j_{\mathcal{S}} \neq m^j_{\mathcal{R}}$ implies the fact that no choice of $i^j_{\mathcal{S}}$ and $\widehat{i^j_{\mathcal{S}}}$ can make the polynomials as functions of $i^j_{\mathcal{R}}$ the same. This gives now,

$$\begin{aligned}\Pr[D_j] &= \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[m^{j+1}_{\mathcal{S}} = m^{j+1}_{\mathcal{R}}] \\ &= \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[i^j_{\mathcal{R}} = \widehat{i^j_{\mathcal{R}}} \wedge \\ &\quad C^j_{\widehat{i^j_{\mathcal{R}}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}}] \\ &\leq \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[C^j_{\widehat{i^j_{\mathcal{R}}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = \\ &\qquad C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}} \,|\, \widehat{i^j_{\mathcal{R}}} = i^j_{\mathcal{R}}] \\ &= \Pr_{i^j_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[C^j_{\widehat{i^j_{\mathcal{R}}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = \\ &\qquad C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}}] \\ &\leq \frac{1}{Q_j}\left\lceil \frac{n_j}{\log Q_j} \right\rceil \leq \frac{\epsilon}{2^{k-j}}, \end{aligned} \tag{4}$$

where the last row follows from observation that,

$$\begin{aligned} C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} &= C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i^j_{\mathcal{S}}} \\ C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) - C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + i^j_{\mathcal{S}} - \widehat{i^j_{\mathcal{S}}} &= 0, \end{aligned} \tag{5}$$

which is the polynomial over $\mathrm{GF}[Q_j]$ and for that we know that the number of roots is at most degree of that polynomial. By calculating the degree we must remember that $m^j_{\mathcal{S}}$ and $m^j_{\mathcal{R}}$ are n_j-bit strings. Now the question is how many elements of the $\mathrm{GF}[Q_j]$ n_j long bit string can represent at most. Entropy of n_j-long bit string is n_j and entropy of a field element is $\log Q_j$ then the degree of the polynomial (5) is $\lceil n_j / \log Q_j \rceil$. Obviously $\lceil n_j / \log Q_j \rceil \leq n_j$ since $n_j \geq 1$ and then from (1) follows $Q_j \geq 2$.

3. $T(\widehat{i^j_{\mathcal{R}}}) \geq T(i^j_{\mathcal{R}})$ and $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{S}})$. Also in this case from the protocol follows that $T(m^j_{\mathcal{S}}) < T(i^j_{\mathcal{S}})$ and $T(m^j_{\mathcal{R}}) < T(i^j_{\mathcal{R}})$ and we can again assume that the adversary chooses $\widehat{i^j_{\mathcal{R}}} = i^j_{\mathcal{R}}$. Based on the protocol we know that $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}})$ and $T(i^j_{\mathcal{S}}) < T(\widehat{i^j_{\mathcal{R}}})$, and this case assumed that $T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{S}})$ and $T(i^j_{\mathcal{R}}) \leq T(\widehat{i^j_{\mathcal{R}}})$. These imply that,

$$\begin{aligned} T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{R}}) \leq T(\widehat{i^j_{\mathcal{R}}}), \\ T(\widehat{i^j_{\mathcal{S}}}) < T(i^j_{\mathcal{S}}) < T(\widehat{i^j_{\mathcal{R}}}). \end{aligned} \tag{6}$$

This allows us to make assumption that $T(i^j_{\mathcal{R}}) < T(i^j_{\mathcal{S}})$. (We can see that when this assumption is made then from (6) follows stricter limit $T(i^j_{\mathcal{R}}) < T(\widehat{i^j_{\mathcal{R}}})$. This however can be accepted since we are anyways assuming that the adversary chooses $\widehat{i^j_{\mathcal{R}}} =$

$i^j_{\mathcal{R}}$ and then it is irrelevant when does that happen.) Now putting everything together we have $m^j_{\mathcal{S}}$, $m^j_{\mathcal{R}}$, $\widehat{i}^j_{\mathcal{S}}$ and $i^j_{\mathcal{R}}$ fixed before the sender chooses $i^j_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]$. Thus,

$$\begin{aligned}
\Pr[D_j] &= \Pr_{i^j_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[m^{j+1}_{\mathcal{S}} = m^{j+1}_{\mathcal{R}}] \\
&= \Pr_{i^j_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[i^j_{\mathcal{R}} = \widehat{i}^j_{\mathcal{R}} \wedge \\
&\quad C^j_{\widehat{i}^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) + i^j_{\mathcal{S}} = C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i}^j_{\mathcal{S}}] \\
&\leq \Pr_{i^j_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_j]}[i^j_{\mathcal{S}} = \\
&\quad C^j_{i^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{i}^j_{\mathcal{S}} - C^j_{\widehat{i}^j_{\mathcal{R}}}(m^j_{\mathcal{S}})] \\
&= \frac{1}{Q_j} \leq \frac{\epsilon}{2^{k-j}}. \qquad (7)
\end{aligned}$$

The case if j is even is identical to the case when j is odd if we interchange $\mathcal{S}$ and $\mathcal{R}$. Therefore we can consider that it is also covered now. To conclude this proof we sum the probability of event D_j for all j and get the adversary's cheating probability that is,

$$\sum_{j=1}^{k-1} \Pr[D_j] \leq \sum_{j=1}^{k-1} \frac{\epsilon}{2^{k-j}} < \epsilon. \qquad (8)$$

■

Next will be shown that the length n_{j+1} of $m^{j+1}_{\mathcal{S}}$ and $m^{j+1}_{\mathcal{R}}$ in round j is roughly logarithmic in the length n_j of $m^j_{\mathcal{S}}$ and $m^j_{\mathcal{R}}$ in round $j-1$. This fact is then used to upper bound the length n_k of the manually authenticated string.

Claim 1 *If* $n_j > \frac{2^{k-j}}{\epsilon}$ *for every* $1 \leq j \leq k-2$, *then* $n_{k-1} \leq \max\{4\log^{(k-2)} n_1 + 4\log 5 + 3,\ 27\}$.

Proof. This will be shown by induction on k. Assume for every j, $1 \leq j \leq k-2$, $n_j > \frac{2^{k-j}}{\epsilon}$ and by using (1) we get,

$$\begin{aligned}
Q_j &< \frac{2^{k-j+1} \cdot n_j}{2} \\
&= \frac{2 \cdot 2^{k-j} \cdot n_j}{\epsilon} \\
&< 2n_j^2, \qquad (9)
\end{aligned}$$

and thus,

$$\begin{aligned}
n_{j+1} &= \lceil 2\log Q_j \rceil \leq \lceil 2\log 2n_j^2 \rceil \\
&= \lceil 2(\log n_j^2 + \log 2) \rceil \\
&= \lceil 4\log n_j + 2 \rceil \\
&\leq 4\log n_j + 3. \qquad (10)
\end{aligned}$$

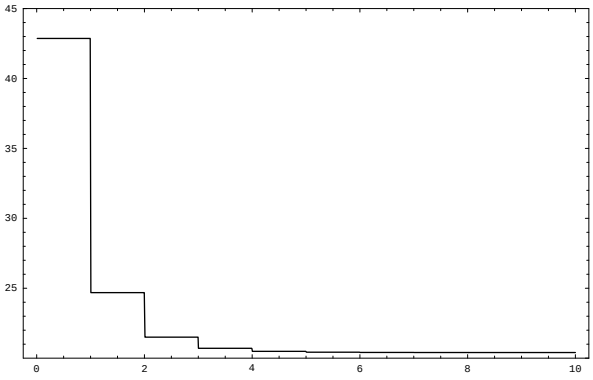

Figure 2: Saturation of $4\log x + 3$ as function of the number of nestings ($n_1 = 1000$).

Now for $k = 3$ we have $n_2 \leq 4\log n_1 + 3$ and the claim holds. Figure 2. shows the evolution of the upper bound in the equation (10) as j grows. Quickly it saturates to the value which is approximately 20.4. Therefore, it is guaranteed that if k is large enough the claim holds since clearly $20 < 27$. For smaller values of k the other option of the upper bound guarantees that the claim holds.

Let us now assume that the claim holds for k' then we have two cases to consider either $n_{k'-1} \leq 27$ or $n_{k'-1} \leq 4\log^{(k'-2)} n_1 + 4\log 5 + 3$. In addition for this induction step we have to assume that $n_{k'-1} > \frac{2^{(k'+1)-(k'-1)}}{\epsilon} = \frac{4}{\epsilon}$ which justifies the use of equation (10) for $j = k' - 1$. Then if $n_{k'-1} \leq 27$,

$$n_{k'} \leq 4\log n_{k'-1} + 3 \leq 4\log 27 + 3 \approx 22.02 < 27. \qquad (11)$$

If $n_{k'-1} \leq 4\log^{(k'-2)} n_1 + 4\log 5 + 3$, then

$$\begin{aligned}
n_{k'} &\leq 4\log n_{k'-1} + 3 \qquad (12) \\
&\leq 4\log(4\log^{(k'-2)} n_1 + 4\log 5 + 3) + 3,
\end{aligned}$$

and this leaves us with two cases to check, either $\log^{(k'-2)} n_1 \leq 4\log 5 + 3$ or $\log^{(k'-2)} n_1 > 4\log 5 + 3$. The first condition implies that

$$n_{k'} \leq 4\log(20\log 5 + 15) + 3 \approx 26.76 < 27 \qquad (13)$$

and the second condition that

$$\begin{aligned}
n_{k'} &< 4\log(5\log^{(k'-2)} n_1) + 3 \\
&= 4\log^{(k'-1)} n_1 + 4\log 5 + 3. \qquad (14)
\end{aligned}$$

That is the claim holds also for $k = k' + 1$. ■

With the help of the Claim 1 can be proved [1] the following claim.

Claim 2 *In protocol P_k the sender manually authenticates at most $2\log(1/\epsilon) + 2\log^{(k-1)} n + O(1)$ bits.*

From the Claim 2 follows the result which was mentioned in the beginning that for any integer $k \geq 3$, and any integer n and $0 < \epsilon < 1$, the protocol P_k enables the sender to authenticate an n-bit input message to the receiver, while manually authenticating at most $2\log(1/\epsilon) + 2\log^{(k-1)} n + \mathrm{O}(1)$ bits. If $k = \log^* n$ ($*$ refers to that when nesting of logarithm is done enough many times then the term $2\log^{(k-1)} n = \mathrm{O}(1)$) then manually authenticated bits are at most $2\log(1/\epsilon) + \mathrm{O}(1)$ which was mentioned in the abstract.

4 Conclusions

In this survey was introduced a protocol in manual channel model for which any adversary has probability of at most ϵ to cheat the receiver into accepting a fraudulent message. For this protocol with any $0 < \epsilon < 1$ there exists a $\log^* n$-round protocol for authenticating n-bit messages, in which only $2\log(1/\epsilon) + O(1)$ bits are manually authenticated [1]. The related work is done by S. Laur and K. Nyberg in [4] and A. Mashatan and D. Stinson in [5]. For example in [4] can be found an interesting and important theoretical result that two round message authentication protocols are inherently less secure than the message authentication protocols with three or more rounds.

References

[1] M. Naor, G. Segev and A. Smith, Tight Bounds for Unconditional Protocols in the Manual Channel and Shared Key Models, presented at CRYPTO '06.

[2] S. Vaudenay, Secure communications over insecure channels based on short authentication strings, In Advances in Cryptology - CRYPTO '05, pages 309-326, 2005.

[3] S. Vaudenau, Digital signature schemes with domain parameters: Yet another parameter issue in ECDSA, In Proceedings of the 9th Australasian Conference on Information Security and Privacy, pages 188-199, 2004.

[4] S. Laur and K. Nyberg, Efficient Mutual Data Authentication Using Manually Authenticated Strings, volume 4301 of Lecture Notes in Computer Science, Springer, 2006. To appear.

[5] A. Mashatan and D. Stinson, Noninteractive Two-channel Message Authentication Based on Hybrid-collision resistant Hash Functions, Cryptology ePrint Archive, Report 2006/302.