Authentication Amplification by Synchronization

Ueli Maurer
Department of Computer Science
ETH Zurich
Switzerland
Email: maurer@inf.ethz.ch

***Abstract*—Information-theoretic message authentication is traditionally defined as the task of authenticating a message, transmitted over an insecure channel, using a secret key shared between sender and receiver. Previous results have investigated the trade-offs between key size, message size, and the adversary's cheating probability.**

In this paper we propose a new approach to information-theoretic authentication, without a secret key, but assuming that a short message (much shorter than the actual message) can be transmitted authentically, for example by speaker identification over the phone. By using such a scheme recursively one can authenticate arbitrarily long messages if one can authenticate a very short message whose length only depends on the desired cheating probability, and if it is guaranteed as a mild form of synchronization that every message arrives before the next one is sent.

This result has also implications for key-based authentication. If the short message is itself authenticated with a key-based scheme, this combined scheme yields an optimal key-based authentication scheme for arbitrarily long messages, provably beating the best traditional authentication code, i.e., the best scheme that transmits a single key-dependent message over an insecure channel. The required key size is independent of the message length, which is impossible to achieve for traditional authentication codes.

The proposed schemes are not only of theoretical interest but may well have practical applications in contexts where information-theoretic security is required, for example in quantum cryptography.

I. Introduction

Message authentication is concerned with providing assurance to the receiver of a message that it was sent by a specified sender, even in the presence of an adversary who can intercept messages sent by the legitimate sender and send a fraudulent message to the receiver. Authenticity, like confidentiality, can be achieved by cryptographic coding based on a secret key k shared by sender and receiver.

Definition 1. In a plain authentication system (without secrecy), also called an *authentication code*, the sender authenticates a message m by computing an authentication tag

$$t = f(m, k),$$

where f is an appropriate function, and sending the pair (m, t) over the insecure channel. The receiver accepts the received message (m', t') if the tag matches, i.e., if

$$f(m', k) = t'.$$

The standard model considered in authentication theory is that the adversary has full (read and write) access to the communication channel and can choose between two different types of attacks. In a so-called *impersonation attack*, the adversary generates a fraudulent message (m', t'), before seeing a correctly authenticated message, and sends it to the receiver. In a so-called *substitution attack*, the adversary waits until an authenticated message (m, t) is sent and replaces it by some fraudulent message (m', t') with $m \neq m'$. The adversary is considered successful (in either attack) if the fraudulent message is accepted by the receiver, and he can choose the better of the two strategies.

This paper is concerned with *information-theoretically secure* message authentication, i.e., security against an adversary with unlimited computing power knowing everything about the system, except for the secret key. We consider authentication schemes for message space $\{0,1\}^n$ and key space $\{0,1\}^s$ (assuming the key is uniform). The tag length v is not a main concern as it is generally much shorter than the message, and because minimizing the communication is not of primary interest. One is interested in achieving high security, i.e., a low cheating probability.[1]

Definition 2. For an authentication code

$$f : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^v,$$

let $\gamma(f)$ be the cheating probability for an optimal cheating strategy, for the worst choice of the message to be sent.

Definition 3. Let $\pi(n, s)$ be the cheating probability for the optimal authentication scheme f for n-bit messages using an s-bit key:

$$\pi(n, s) \;=\; \min_f \gamma(f),$$

where the minimum is over all functions $f : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^v$, for any v.

There exists a huge body of literature on information-theoretic authentication codes, beginning with [2] (see also [7], [8], [9], [3]). The papers are mostly concerned with designing schemes f for which $\gamma(f)$ is small, with proving lower bounds on $\pi(n, s)$ or, more generally, proving results relating the key space size, the message space size, and the best achievable cheating probability.

[1] In the literature the problem of authenticating a *sequence* of messages has also been considered (see for example [4]).

978-1-4799-0446-4/13/$31.00 ©2013 IEEE

It is well-known (e.g., see [4]) that

$$\pi(n,s) \;\geq\; 2^{-s/2}, \tag{1}$$

i.e., that for any $n \geq 1$ no scheme can achieve a cheating probability lower than the inverse of the square root of the key space size. More generally, the bound is $2^{-H(K)/2}$, where K is the random variable corresponding to the key. The intuition behind this bound is that the correctly authenticated message must give as much information as possible about the secret key (to counter an impersonation attack) but at the same time hide as much as possible about K (to counter a substitution attack), the best trade-off being that it leaks half the key entropy. Indeed, consider the authentication of a single bit (i.e., $n = 1$). It is not difficult to see that an optimal scheme is to split the key into two halves of equal length and to send (as the tag t) the first [or second] half of the key if the bit is $m = 0$ [or $m = 1$]. Inequality (1) can also be stated as[2]

$$s \;\geq\; 2\log\frac{1}{q}, \tag{2}$$

where q is a given bound on the cheating probability, i.e., if $\pi(n,s) \leq q$ is required. Note that this bound is independent of the message length and holds even for $n = 1$.

It is also known [1] that for any authentication code achieving $\gamma(f) \leq q$, the key size satisfies

$$s \;\geq\; \log n + \log\frac{1}{q}, \tag{3}$$

i.e., the key size must grow logarithmically in n and logarithmically in $\frac{1}{q}$.

II. Polynomial-based Authentication

A well-known scheme for $n > 1$ is based on arithmetic in a finite field $GF(2^r)$. For $n = r$ and $s = 2r$ we can define $f(m,k)$ as follows. The key $k \in \{0,1\}^{2r}$ is interpreted as a pair $k = (k_1, k_0)$ of elements of $GF(2^r)$, and (using field arithmetic)

$$f(m,k) \;=\; k_1 m + k_0.$$

It is straight-forward to prove that this scheme is optimal in the sense that

$$\gamma(f) \;=\; 2^{-s/2} \;=\; 2^{-r},$$

which shows that the bound (1) holds with equality for $n \leq s/2$, i.e., for messages not longer than half the key length.

For longer messages, equality can not be achieved anymore. Many papers investigated the problem of extending the message space, for given key size, without sacrificing too much on the cheating probability. One of the best schemes is described below. We need the following definition.

Definition 4. For a given field $GF(2^r)$, the *message polynomial* for message $m \in \{0,1\}^*$ is the polynomial

$$p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0,$$

where

$$m = m_{b-1}||\cdots||m_1||m_0,$$

i.e., the message is parsed into $b = \lceil n/r \rceil$ r-bit blocks which constitute the coefficients of $p_m(x)$.

In this paper we assume, for simplicity and without much loss of generality, that the message length n is known. For variable n, certain simple modifications are needed to avoid a misinterpretation of leading 0's in the message.

Theorem 1. *For the authentication scheme for key $k = (k_1, k_0) \in GF(2^r)^2$, defined by*

$$f(m,k) \;=\; k_1 p_m(k_1) + k_0,$$

the cheating probability of any adversary is upper bounded by

$$\gamma(f) \;\leq\; \lceil n/r \rceil \cdot 2^{-r}.$$

Proof. Since the tag $t = f(m,k)$ is uniformly random in $GF(2^r)$, no impersonation attack has success probability more than 2^{-r}. To analyze substitution attacks, note that $f(m,k)$ is statistically independent of k_1 and hence, for the adversary, k_1 is still uniformly random after observing the correctly authenticated message. For a fraudulent message $m' \neq m$, the probability that a given tag t' matches is equal to the probability that

$$t - t' \;=\; k_1 p_m(k_1) - k_1 p_{m'}(k_1). \tag{4}$$

Since the polynomial

$$q(x) \;:=\; x p_m(x) - x p_{m'}(x) - t - t'$$

has degree at most $b = \lceil n/r \rceil$ (and is non-zero, as $m' \neq m$), it can have at most $\lceil n/r \rceil$ roots. Since k_1 is random, the probability that (4) is satisfied is at most $\lceil n/r \rceil \cdot 2^{-r}$. □

The theorem implies

$$\pi(n,s) \;\leq\; \lceil 2n/s \rceil \cdot 2^{-s/2}$$

for even s.

As mentioned, this scheme is essentially optimal. Nevertheless, we want to raise the question whether one can do better. This question was addressed by Gemmell and Naor [1] who showed that by an *interactive* protocol between sender and receiver one can reduce and even eliminate the dependence of the cheating probability on the message length. Here we take a different approach, without requiring interaction. Instead, we make use of a weak form of synchronization naturally given in practical applications.

III. Authentication Amplification by Synchronization

In the following we assume a very mild form of time synchronization between sender and receiver, namely that when the sender sends two consecutive messages sufficiently separated in time, then the adversary can not modify the first message after seeing the second message. In other words, the receiver knows that if the first message comes too late, then he

[2] All logarithms in this paper are to the base 2.

should not accept it. And, conversely, he knows that when the message arrived on time, then, while it might come from the adversary, it can not depend on a subsequent message from the honest sender.

From now on, assume such synchronization and consider a setting where the sender can send, once, an authenticated message of length ℓ to the receiver. For example, the receiver might be able to recognize the sender's voice and hence the sender can read the (short) message to the receiver over an insecure but authenticated voice channel.

Definition 5. The authentication scheme $SyncAut(m)$ for message $m \in \{0,1\}^n$ (and field $GF(2^r)$) is defined as follows. First, m is sent over an insecure channel. Then (after the message is received by the receiver), the pair $(z, p_m(z))$ is sent over the authenticated channel to the receiver, where $z \in GF(2^r)$ is chosen uniformly at random by the sender.

Note that $\ell = 2r$ in this scheme.

Theorem 2. *If scheme SyncAut is used to transmit an n-bit message, the cheating probability of any adversary is upper bounded by* $(\lceil n/r \rceil - 1) \cdot 2^{-r}$.

Proof. The adversary must replace m by some $m' \neq m$ before seeing $(z, p_m(z))$, hoping that $p_m(z) = p_{m'}(z)$. (Note that he can not change z.) The polynomial $p_m(x) - p_{m'}(x)$ has degree $(\lceil n/r \rceil - 1)$; hence it has at most $(\lceil n/r \rceil - 1)$ roots. Since z is uniformly random, the probability that $p_m(z) = p_{m'}(z)$, i.e., that

$$p_m(z) - p_{m'}(z) = 0,$$

is at most $(\lceil n/r \rceil - 1) \cdot 2^{-r}$. □

Note that for very short messages ($n \leq r$) the scheme simply sends the message over the authenticated channel (and also over the insecure channel), and the cheating probability is therefore 0. Indeed, the bound in Theorem 2 becomes 0.

What this scheme achieves is that the problem of sending a long authenticated message is reduced to the problem of sending only a much shorter authenticated message (plus, of course, sending a long message insecurely, which is considered cheap). The scheme is actually practically relevant, for example in quantum cryptography, where the parties agreeing on a secret key must communicate large amounts of data *authentically*. Instead of using a secret key one could use a physical authentication mechanism for short messages, as described.

We observe that the assumption that the second channel be authenticated can be dropped if we use a secret key for the authentication of that message (see Section V). We also observe that the above approach can be used recursively, as discussed below.

IV. Recursive Application of the Scheme $SyncAut$

As mentioned, the scheme $SyncAut$ allows to authenticate a long message by sending it over an insecure channel and sending only a much shorter message authentically. In the terminology of constructive cryptography [6], [5], one constructs an n-bit authenticated channel from an n-bit insecure channel and an ℓ-bit authenticated channel, for $\ell < n$.

We note that ℓ depends on n and on the desired bound q on the cheating probability p. For the field $GF(2^r)$ we have

$$\ell = 2r \qquad \text{and} \qquad p = (\lceil n/r \rceil - 1) \cdot 2^{-r}.$$

For fixed q and n we have

$$\ell \; = \; O(\log n) + O(\log \frac{1}{q}).$$

To improve on this, we now consider a model, called the synchronous communication model, in which one can use, consecutively, a few synchronized insecure communication channels and an ℓ-bit authenticated channel at the end. Our goal is to minimize ℓ for given message length n and bound q on the cheating probability.

Theorem 3. *In the synchronous communication model, for* $q \leq 1/4$ *there exists a scheme with*

$$\ell \; = \; 2\lceil \log \frac{1}{q} \rceil + 4.$$

Proof. We only sketch the proof. By recursive use of scheme $SyncAut$, with adequate field sizes at each level, the message lengths transmitted over the insecure channels drop exponentially. The overall cheating probability is bounded by the sum of the cheating probabilities at each level. (This is quite obvious and also follows from the composition theorem of constructive cryptography [6], [5].)

Let us investigate the performance of the scheme where at the i-th level the message length is ℓ_i and the message consists of two elements of $GF(2^{r_i})$, where $r_i = \lfloor l_i/2 \rfloor$, used to authenticate a message of length $\ell_{i+1} = b_{i+1} r_i$ at the next higher level. The parameters b_i can be chosen arbitrarily, but $b_i \geq 3$ is required to boost the message size in increasing levels. When the recursion ends (at the lowest level, i.e., level 0), the length of the message that actually needs to be transmitted authentically is $\ell = \ell_0$. Let k be the number of levels. Then the cheating probability of the overall scheme is bounded by

$$\sum_{i=1}^{k} b_i 2^{-r_{i-1}}.$$

It is easy to verify that for the choice $r = r_0 \geq 4$. and $b_i = 3$ for all i, the above sum is smaller than $4 \cdot 2^{-r}$ for any k.[3] This means that one can authenticate a message of any length n by sending only $\ell = 2r$ bits authentically, and with cheating probability

$$p < 4 \cdot 2^{-r}.$$

Hence, if one chooses

$$r \; = \; \lceil \log \frac{1}{q} \rceil + 2,$$

then $p < q$ (if $r \geq 4$, i.e., if $q \leq 1/4$). □

[3] In an actual implementation, one would choose $b_2, b_3, \ldots$ much larger to have only two or three recursion levels.

V. Key-based Authentication with Optimal Key Size

As mentioned before, if no authenticated ℓ-bit channel is available, but instead a secret key is available, then one can use the key to authenticate the ℓ-bit message. Since ℓ is small, we can achieve key-based message authentication for arbitrarily long messages where the cheating probability is minimal, i.e., where the bound (2) is met essentially with equality. This beats the best schemes where a single insecure message (consisting of the message and the tag) is sent.

The proof of the following theorem is omitted. It should be contrasted with (3) which states that the key size must depend on the message length if no synchronization assumption is made, i.e., if the entire message can be replaced as a whole by the adversary.

Theorem 4. *In the synchronous communication model there exists a scheme with*

$$s \;=\; 2\log\frac{1}{q} + c.$$

for a given bound q on the cheating probability, where c is a (small) constant.

VI. Conclusions

We have demonstrated that a very weak assumption, namely a mild form of synchronization, which in practice is easily satisfied, can lead to a significant improvement in information-theoretically secure authentication schemes.

This leads on one hand to an authentication amplification scheme by which the capability of sending a *short* message authentically can be boosted to send an arbitrarily long message authentically. The scheme is practical and is a viable choice for being used in quantum cryptography instead of a key-based authentication scheme, at least for the establishment of a first key.

On the other hand, the described idea also leads to the optimal key-based authentication scheme which is superior to all previously proposed schemes. This scheme might be the preferred choice in practice for information-theoretically secure authentication, for example in quantum cryptography (if key-based schemes are used).

Acknowledgment

This research was supported by the Swiss National Science Foundation.

References

[1] P. Gemmell and M. Naor, Codes for interactive authentication, *Advances in Cryptology – CRYPTO' 93*, Lecture Notes in Computer Science, Springer-Verlag, pp. 355–367, 1993.

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

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

[4] U. Maurer, Authentication theory and hypothesis testing, *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1350–1356, July 2000.

[5] U. Maurer, Constructive cryptography – A new paradigm for security definitions and proofs, *Theory of Security and Applications (TOSCA 2011)*, Lecture Notes in Computer Science, Springer-Verlag, vol. 6993, pp. 33–56, 2011.

[6] U. Maurer and R. Renner, Abstract Cryptography, *The Second Symposium in Innovations in Computer Science, ICS 2011*, Tsinghua University Press, pp. 1–21, Jan. 2011.

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

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

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