Information-Theoretic Bounds in Authentication Theory[1]

Ueli M. Maurer
Department of Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland

Abstract — **This paper gives a simplified treatment of, and new results on, information-theoretic lower bounds on an opponent's cheating probability in an authentication system with a given key entropy.**

I. Introduction

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

Compared to Shannon's theory of secrecy, authentication theory is more subtle and involved. After some purely combinatorial results on authentication theory had been derived [1], Simmons [4] initiated a sequence of research activities on information-theoretic lower bounds in authentication theory (e.g., see [2], [3], [5], [6]).

II. Description of the authentication model

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

An opponent can use either of two different strategies for cheating. In an *impersonation* attack at time i, the opponent waits until he has seen the encoded messages $Y_1, \ldots, Y_{i-1}$ (which he lets pass to the receiver) and then sends a fraudulent message $\tilde{Y}_i$ which he hopes to be accepted by the receiver as the ith message. In a *substitution* attack at time i, the opponent lets pass messages $Y_1, \ldots, Y_{i-1}$, intercepts Y_i and replaces it by a different message $\tilde{Y}_i$ which he hopes to be accepted by the receiver and decoded to a message different from the one sent by the sender. There are three possible goals an opponent might persue in either of these two attacks:

- The receiver accepts Y_i as a valid message.
- The receiver accepts Y_i and decodes it to a message $\hat{X}_i$ *known* to the opponent. In other words, an opponent is only considered successful if he also guesses the receiver's decoded message $\hat{X}_i$ correctly.
- The receiver accepts Y_i and decodes it to a particular message $\hat{X}_i = x$ *chosen* by the opponent. Hence this type of attack depends on a particular value x.

[1]This work was supported by the Swiss National Science Foundation.

We will denote the maximal possible probabilities of success, for the three described scenarios, by $\hat{P}_I(i)$, $\tilde{P}_I(i)$ and $\hat{P}_I(i,x)$, respectively, for an impersonation attack at time i, and by $\hat{P}_S(i)$, $\tilde{P}_S(i)$ and $\hat{P}_S(i,x)$, respectively, for a substitution attack at time i.

III. Information-theoretic bounds

The literature on information-theoretic bounds in authentication theory is quite diverse because various different models are considered. Generally, the proofs are quite complicated and valid only for a restricted model while the results could actually be proven for a general model. For instance, some proofs only hold for deterministic encoding, for single (rather than a sequence of) messages, for a sequence of messages but with the restrictions that the encoding rule be the same for each message and that consecutive messages be distinct, or that the encoding rules do not depend on previous messages.

The goal of this paper is to derive various bounds in a coherent, more general setting, but by a simpler proof technique than those used before. In particular, we consider all three scenarios described above and our results could be generalized to a scenario where, for the sake of a smaller cheating probability, also a specified maximal probability of a decoding error for a correct message can be tolerated.

Some of the derived bounds are stated below. The first two bounds were also derived in [5] in a slightly less general form.

$$\begin{aligned}
\hat{P}_I(i) &\geq 2^{-I(Y_i;Z|Y_1\ldots Y_{i-1})} \\
\hat{P}_S(i) &\geq 2^{-H(Z|Y_1\ldots Y_i)} \\
\tilde{P}_I(i) &\geq 2^{-I(Y_i;Z|Y_1\ldots Y_{i-1}X_i)} \\
\tilde{P}_S(i) &\geq 2^{-H(Z|Y_1\ldots Y_i X_i)} \\
\hat{P}_I(i,x) &\geq 2^{-I(Y_i;Z|Y_1\ldots Y_{i-1},X_i=x)} \\
\hat{P}_S(i,x) &\geq 2^{-H(Z|Y_1\ldots Y_i,X_i=x)}
\end{aligned}$$

References

[1] 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.

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

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

[4] 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. New York, NY: Springer, 1985, pp. 411–431.

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

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