INFORMATION-THEORETIC BOUNDS FOR AUTHENTICATION FRAUDS

Andrea Sgarro

Dipartimento di Scienze Matematiche
Università di Trieste, 34100 TRIESTE (Italy)

Short version

Abstract. Several properties of authentication codes depend on a mathematical structure, called below a fraud scheme, which is much simpler than the one originally given. Relying on this fact, we present a powerful lower bound, which is a sort of mould to painlessly derive a whole range of information-theoretic bounds to fraud probabilities in authentication coding.

1. **Introduction.** A Shannon-theoretic frame for authentication theory has been put forward by G. Simmons ([1]). The main attacks to an authentication code are impersonation and substitution, but several variants of these can be considered. In the literature, information-theoretic bounds to fraud probabilities are provided which require a lot of boring computations to be repeated each time. We will show that one can dispose of all this drudgery.

An *authentication code* is a finite random triple XYZ (X: *source state* or *source message*, Y: *authenticated message* or *codeword*, Z: *encoding rule* or *key*). Under each key (encoding rule), decoding is assumed to be deterministic; instead probabilistic encoding (*splitting*) is allowed. Key and source state are independent random variables. In the *authentication matrix* χ of the code one has $\chi(z,y)=1$ iff key z authenticates codeword y, that is iff there exists a source state x which is encoded to y under key z. (Capital letters denote random variables, the corresponding small letters denote their values.)

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 467-471, 1993.

A deterministic code is completely described by giving the encoding matrix, the key probability distribution and the source state probability distribution. In the case of splitting, there are entries in the encoding matrix which contain several codewords, and so one must further specify the random "splitting strategy" for each such entry. Since a zero-error decoding scheme is prescribed, each codeword can appear at most once in each row of the encoding matrix. So, the number of ones in each row of χ is at least $|X|$ (exactly $|X|$ for codes without splitting, $s|X|$ for s-balanced codes, i.e. codes such that each entry of χ contains s codewords).

In the case of an *impersonation attack* the mischievous opposer chooses a codeword y hoping it to be authenticated by the current key Z. The probability of fraud for the opposer's optimal strategy is:

(1) $$P_I = \max_y \ \mathrm{Prob}\{\chi(Z,y)=1\}$$

In the case of *substitution* the opposer grabs the legal codeword c and replaces it by a fake codeword y hoping that y be decoded to a source state different from g(Z,c) (g denotes deterministic decoding and so g(z,c) represents the unique source state which is encoded to codeword c under key z). The relevant fraud probabilities are:

$$P_S(c) = \max_y \mathrm{Prob}\{\chi(Z,y)=1,\ g(Z,y)\neq g(Z,c) \mid Y=c\}$$

$$P_S = \Sigma_c \mathrm{Prob}\{Y=c\}\ P_S(c)$$

(The vertical bar denotes probabilistic conditioning.) In the case of codes without splitting, $P_S(c)$ can be written more simply as:

$$P_S(c) = \max_{y\neq c} \mathrm{Prob}\{\chi(Z,y)=1 \mid Y=c\}$$

The most popular lower bounds to P_I are *Simmons bound* which involves the mutual information I(Z;Y) (in terms of Shannon entropies I(Z;Y), which is a measure of stochastic dependence, is defined as H(Y)+H(Z)-H(YZ)):

$$P_I \geq 2^{-I(Y;Z)}$$

and the combinatorial bound for deterministic codes:

$$P_I \geq \frac{|X|}{|Y|}$$

2. **Fraud schemes**. We find it convenient to define a more abstract notion than authentication codes, namely *fraud schemes* (T,ρ). Let two finite (non-empty) sets be given, the set of *tokens* and the set of *fakes* (in the applications, tokens will stand

for keys, or conditional keys, fakes for fraudulently inserted codewords). Let T be a random token and let ρ be a binary matrix row-indexed in the set of tokens and column-indexed in the set of fakes; when $\rho(t,f)=1$ we say that token t is *deceived* by fake f. The only requirement we make on (T,ρ) is that for each token fraud is possible (in each row of ρ there is at least a one). We find it convenient to allow for "impossible" (zero-probability) tokens and "unusable" fakes (whose column is all-zero). A *row-balanced* scheme is one where the number of ones is the same for each positive-probability row of ρ, i.e. each "possible" token is deceived by the same number of fakes, k, say.

Further we define the *fraud probability* as:

(2) $$P = \max_f \ \mathrm{Prob}\{\rho(T,f)=1\}$$

Notice that each authentication code XYZ yields a fraud scheme by simply setting T=Z, $\rho=\chi$. If XYZ is s-balanced, (T,ρ) is row-balanced with k=s|X|. Of course different codes can yield the very same scheme, while, if one is given the scheme (T,ρ) to start with, it may well happen that this scheme *cannot* be embedded into any authentication code XYZ with Z=T, $\rho=\chi$, $|X|\geq 2$. So, in spite of the formal coincidence of (1) and (2), the notion of a fraude scheme is *strictly more general* than that of an authentication code. What one can always do, however, is to complete (T,ρ) to a random couple TF such that $\rho(t,f)=1$ iff $\mathrm{Prob}\{F=f|T=t\}\neq 0$. To do this, convert ρ into a stochastic matrix by replacing the ones in each row of ρ by positive numbers which sum to one. For any such completion TF one has

(3) $$P \geq 2^{-I(T;F)}$$

To prove this inequality one can literally repeat any of the standard proofs of Simmons bound to impersonation, e.g. those in [2,3]. As the "Simmons bound" (3) holds for any admissible completion TF, one soon obtains a result formally identical with the strengthened Simmons bound for impersonation given in [2]:

(4) $$P \geq 2^{-\inf I(T;F)}$$

the infimum being taken w.r. to all random couples TF yielding the given fraud scheme (T,ρ). The information theorist might appreciate the fact that inf I(T;F) as in the exponent of (4) is the *rate-distortion function* for source (*sic*) Z, distortion

matrix equal to the binary complement of ρ, and distortion level equal to zero, $R(Z,\mathcal{C}(\rho),0)$. Conditions for equality in this bound will be discussed in the full version of this paper. We shall be contented here with the following fact:

Equality criterium. For row-balanced authentication schemes, bound (4) holds with equality iff $\text{Prob}\{\rho(Z,f)=1\}$ does not depend on f, where f spans the set of usable fakes. In this case $P = \frac{k}{|F|}$ ($|F|$ is the number of usable fakes).

(The fact that $\text{Prob}\{\rho(Z,f)=1\}$ does not depend on f means that any usable fake f, and consequently any *fraud strategy,* is equally good, or equally bad, from the point of view of the opposer.)

Inequality (3) gives actually a whole class of bounds, out of which (4) is the best. Even weak bounds can be, however, meaningful. For example, in the case of row-balanced schemes, one can take (3) with the stochastic matrix obtained from ρ by filling the free entries with the constant $\frac{1}{k}$. A simple computation shows that in this case: $I(T;F) = H(F) - \log k \leq \log |F| - \log k$. So, *for row-balanced fraud schemes* one gets the following counterpart of the combinatorial bound for deterministic codes:

(5) $$P \geq \frac{k}{|F|}$$

Comparing with the equality criterium, we see that, rather surprisingly, this naive combinatorial bound is a *tight* bound for *good* row-balanced schemes (for schemes which attain the severe bound (4) with equality).

Up to now, the reader can have the unpleasant impression that we are just changing names: instead of *key, codeword, impersonation,* we say *token, fake, fraud.* In a way, this is it: old material used to a higher degree of abstraction. It is precisely this higher degree of abstraction, however, which will allow us to appreciate the real bearing of the result: in a way, *impersonation is a much more general notion than usually realized.* The next section 3 is meant to convince the reader of this fact.

3. Applications.

The most obvious application is impersonation; for a *meaningful* application, however, we go directly to substitution. Take T with the distribution of $Z|Y=c$. Construct $\rho=\chi_c$ from χ by specifying which codewords do cause a fraud when used

by the opposer. To this end set to zero the entries in χ for which $g(z,y)=g(z,c)$, including the column corresponding to c. Then

$$P_S(c) = \max_y \text{Prob}\{\chi(Z,y)=1,\ g(Z,y)\neq g(Z,c) \mid Y=c\} =$$
$$= \max_y \text{Prob}\{\chi_c(Z,y)=1 \mid Y=c\} = \max_y \text{Prob}\{\rho(T,y)=1\}$$

and so one obtains the powerful bound which was first given in [3]:

$$P_S(c) \geq 2^{-R(Z,\mathcal{C}(\chi_c),0 \mid Y=c)}$$

For s-balanced codes XYZ, χ_c is clearly row-balanced, and so (5) becomes:

$$P_S(c) \geq \frac{s(|X|-1)}{|Y|-1}$$

Assume XYZ is deterministic and set $\text{Prob}\{Y^*=y \mid Z=z, Y=c\} = \text{Prob}\{Y=y \mid Z=z, Y\neq c\}$; as the authentication matrix derived from the conditional distribution of ZY* given Y=c is precisely χ_c, (3) and Jensen's inequality give:

$$P_S(c) \geq 2^{-I(Y^*;Z \mid Y=c)}, \quad P_S \geq 2^{-I(Y^*;Z \mid Y)}$$

the latter being "Simmons bound for substitution".

We could multiply our examples, by taking into account the various attacks introduced in literature. By now, however, our point should be clear. In all cases *what one has to do is to resort to the fraud scheme* (T,ρ), *where* T *gives the distribution of the key conditional to the information possessed by the opposer, and* ρ *specifies, for each value* t *of* T, *which are the codewords that can be used successfully as "fakes", that is which are the codewords that do cause a fraud against the system.* Once this is done, the abstract bounds of Section 2 are painlessly converted into bounds for the attack under consideration.

References.

[1] G. Simmons, "A survey of information authentication", Proceedings of the IEEE, may 1988, 603-620

[2] R. Johannesson, A. Sgarro, "Strengthening Simmons' bound on impersonation", IEEE Transactions on Information Theory, vol.IT-37, n.4 (1991) 1182-1185

[3] A. Sgarro, "Lower bounds for authentication codes with splitting", in "Advances in Cryptology - Eurocrypt '90", ed. by I. B. Damgård, Springer Verlag, Lecture Notes in Computer Science 473 (1991) 283-293