LOWER BOUNDS FOR AUTHENTICATION CODES WITH SPLITTING

Andrea Sgarro

Dept. of Mathematics and Computer Science
University of Udine, 33100 Udine, Italy

and: Dept. of Mathematical Sciences
University of Trieste, 34100 Trieste, Italy

Abstract. The role of non-deterministic authentication coding (coding with splitting) is discussed; a new substitution attack is put forward which is argued to be more relevant than usual substitution for codes with splitting. A reduction theorem is proved which allows to extend "abstract" bounds for impersonation (including the new JS-bound, which is shown to hold on the large class of "abstract" authentication codes) to the new substitution attack.

INTRODUCTION

In Simmons' model an authentication code is a finite random triple XYZ (random message, random codeword, random key; according to the original terminology: random source state, random authenticated message and random encoding rule). Further, the following is required: X and Z are independent; X = g(Y,Z) (decoding has to be deterministic). Instead, Y = f(X,Z) (deterministic encoding) is *not* required. If this happens the code is called deterministic, or *without splitting* . Below, as an example, we show an *encoding matrix* , the corresponding *decoding matrix*, and the binary matrix specifying *key-codeword admissibility;* this is obtained from the decoding

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 283-293, 1991.

matrix by writing ones instead of messages and zeroes instead of blanks, and tells which codewords are authenticated by which keys.

	x1	x2	x3
z1	y1	y2	y3
z2	y3	y4	y1

	y1	y2	y3	y4
z1	x1	x2	x3	
z2	x3		x1	x2

	y1	y2	y3	y4
z1	1	1	1	0
z2	1	0	1	1

To describe a code one may give the encoding matrix and specify the statistics of X and Z; however, in case of splitting many "homophones" can occupy the same entry; then one has also to specify the random selection rule of the homophones given the key and the message (for convenience, we rule out one-dimensional "objects", be they messages or keys, with zero probability; we assume $|X| \geq 2$). Decoding being deterministic, the same codeword appears *at most once* in each row of the encoding matrix.

Given a code XYZ we shall find it convenient to deal with the marginal couple YZ, forgetting about the random message X. We shall say that YZ is the *abstract code* derived from the *operational code* XYZ; actually we shall need all the abstract codes (random couples) YZ, even those which are not derivable from operational codes. In a way, we have the following inclusion: deterministic codes $\subseteq$ operational codes $\subseteq$ abstract codes.

THE JS-BOUND

So far our code might be a secrecy code, codewords being cryptograms, or even a source code, when only one key is there; we go now to authentication theory for good; cf /1,2/. In the *impersonation attack* a clever opponent, who ignores the key, chooses a codeword and sends it to the legal receiver in the hope that it will be accepted; the codeword is chosen so as to maximize the probability of fraud, P_I:

$$P_I = \max_y \ \text{Prob}(Z \in A_y), \qquad \text{with } Ay = \{z: \text{Prob}(Y=y,Z=z)\neq 0\}$$

A_y is the set of keys which authenticate y and corresponds to the ones below y in the binary matrix (similarly, one defines A_z, the set of codewords authenticated by z, which corresponds to the ones on the right of z).

For P_I several lower bounds are known (below I(Y;Z)=H(Y)+H(Z)-H(YZ) denotes mutual information in bits; H(.) is Shannon entropy; bars denote size):

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

$P_I \geq \frac{|X|}{|Y|}$ combinatorial bound Universal

The first is abtract, that is it holds over the larger class of abstract codes; the second is universal, that is it is independent of (robust w.r.t.) source statistics. Actually the combinatorial bound can be easily generalized to

$P_I \geq \frac{\min_z |A_z|}{|Y|}$, which is both abstract and universal.

For deterministic codes a standard manipulation of information quantities (cf /1/) shows that Simmons bound becomes: $P_I \geq 2^{H(X)-H(Y)}$; of course the combinatorial bound can be always written as $P_I \geq 2^{\log|X|-\log|Y|}$. Typically $|Y|>>|X|$, so Simmons bound is better; however, for this silly binary code below the combinatorial bound is better: $H(X)\cong 0$, $H(Z)=1$, $Y=X\oplus Z$ (then $H(Y)=1$). Simmons bound gives approximately $\frac{1}{2}$, the combinatorial bound gives correctly 1. Recently, Johannesson and this author /3/ have put forward a new bound, which is a sort of "universal strengthening" of Simmons bound; it improves also on the combinatorial bound. Below we shortly rederive the JS-bound, so as to show that it holds over the large class of abstract codes.

The starting point is this: P_I is defined through A_y, which is defined through joint probabilities codeword-key which differ from zero: it doesn't matter how much they differ from zero! Actually P_I depends *only* on distr(Z) and on the binary matrix for key-codeword admissibility, and so, in particular, P_I is itself "universal". (There is more to it, since P_I does not even depend on the possible correlation between X and Z; cf /3/).

Given an abstract code YZ consider the stochastic matrix W=Y|Z of the conditional probabilities codeword-given-key. Observe that if one "binarizes" W by writing ones instead of its non-zero entries one re-obtains the binary matrix! Take Y*Z* s.t. Z* has the same distribution as Z, W*=Y*|Z* has the same zeroes as W. Then $A_y=A_y^*$. Then $P_I=P_I^*$. So, the following chain holds:

for any $W^*\sim W$ $\quad P_I \geq 2^{-I(Y^*,Z^*)}$

$P_I \geq 2^{-\inf I(Y^*,Z^*)}$ $\quad$ inf w.r.t. all $W^*\sim W$

$P_I \geq 2^{-\min I(Y^*,Z^*)}$ $\quad$ min w.r.t. all $W^*\leq W$

(W*~W means that the stochastic matrix W* has exactly the same zeroes as W; W*≤W means that W* has at least the same zeroes as W; in the last line we simply closed the open minimization set: there are examples where the minimizing W* has more zeroes than W, and so lies on the boundary; cf /3/). Observe that the minimum in the exponent of the JS-bound can be interpreted as a suitable rate-distortion function evaluated at zero: so, the very efficient algorithm available for the latter can be used to compute it. (An intriguing question: why did a rate-distortion function show up in this authentication-theoretic context?)

For W*~W with uniform rows:

$$I(Y^*,Z^*) = H(Y^*) - E_Z \log |A_Z| \leq \log|Y| - \min \log |A_z|$$

and one re-obtains the (abstract) combinatorial bound.

A GENERALIZED ATTACK

After this preliminary material on impersonation, we still have to pause on a boring insert devoted to a new "formal" attack: *conditional-constrained impersonation* . Let E and F be non-void sets of codewords and set:

$$P_{I(E,F)} = \max_{y \in F} \text{Prob}\{Z \in A_y | Y \in E\}$$

The opposer is constrained to choose his codeword inside F and can use the information Y∈E: this attack generalizes both impersonation and *substitution* of codeword c; in the latter case F={y:y≠c}, E={c}. We shall prove a "reduction theorem": from YZ a new *abstract* code Y*Z* will be constructed, such that, under mild regularity assumptions:

$$P_{I(E,F)}(YZ) = P_I(Y^*Z^*)$$

Once one is able to "reduce" the fraud probability for the new attack to the fraud probability in an impersonation attack, all the (abstract) lower bounds obtained for impersonation are usable for the new attack! The construction of the new code follows. For Z* take Z|Y∈E (throw away zero-probability keys); Y* takes its values in F; to obtain Y*|Z*=z pump up the probabilities for Y|Z=z so as to make them sum to 1 (provided this pumping is feasible: this is the regularity assumption, which however will turn out to be trivially met when we shall need it). In symbols

$$\Pr\{Z^*=z\} = \Pr\{Z=z|Y\in E\}, \quad z\in \cup_{y\in E} A_y$$

$$\Pr\{Y^*=y|Z^*=z\} = \alpha^{-1} \Pr\{Y=y|Z=z\}, \quad y\in F$$

$$\text{with} \quad \alpha = \alpha(F) = \Sigma_{y\in F} \Pr\{Y=y|Z=z\}$$

The regularity condition is simply that α should be strictly positive for all z's in the range of Z*; in other terms, any key which authenticates at least a codeword in E should authenticate at least a codeword in F. Since this reduction theorem is an unimaginative generalization of a result given in /4/ for the case of substitution attacks details of the proof are omitted.

CODES WITH SPLITTING

Let's turn to (operational) codes with splitting. In a pure impersonation model they are *useless* (if one throws away homophones, that is ones in the binary matrix, P_I does not increase). However, authentication codes with splitting cannot be disposed of for very serious reasons, two of which follow. First: homophony (splitting) is a brilliant idea for secrecy ciphers and so splitting can be good in a mixed authentication-secrecy model, even if authentication is restricted to impersonation. Second: as shown by Simmons,

splitting is essential in the mixed impersonation-substitution model which he has proposed, where the opposer is free to play either impersonation or substitution, according to which one pays better. Even so, however, a difficulty arises: we shall argue below that usual substitution is *not* a relevant attack to mount in the case of codes with splitting.

We shall make a distinction between two attacks: *codeword substitution* (substitution as defined usually) versus *message substitution*. These are genuinely different attacks when there is splitting. The point is the following. If the opposer substitutes the legal codeword by one of its homophones the system is safe: so, why declare his substitution successful? In the attack of message substitution we demand not only that the codeword is successfully substituted, but also that it is decoded to a message different from the legal message, so that havoc is brought about in the system. The probability of success is then:

$$P_{MS}(c) = \max_{y(\neq c)} \text{Prob}\{Z \in A_y - H_{y,c} | Y=c\}, \text{ with } H_{y,c}=\{z: g(y,z)=g(c,z)\}$$

By averaging with respect to $\Pr\{Y=c\}$ one has the overall probability of message substitution $P_{MS}=\Sigma_y \Pr\{Y=c\} P_{MS}(c)$; (the probabilities of codeword substitution are defined similarly, only omitting the conditions $Z \notin H_{y,c}$; observe that, unlike codeword substitution, message substitution does not make sense for abstract codes, since it explicitly involves messages).

Examples. Beside the case of impersonation and codeword or message substitution, below we consider also two probabilities of *deception* : $P_d=\max(P_I,P_{CS})$, as defined by Massey /2/, and $P_\delta=\max(P_I,P_{MS})$, which is a natural analogue of P_d in the case of message substitution. In general $P_\delta \le P_d$; equality holds for deterministic codes (and for some probabilistic codes). (Deception as defined by Simmons is a more complicated game-theoretic notion; in his case the maximum is only a lower bound to P_d). The following examples /5/ show that, unlike in the case of pure impersonation, deleting homophones can be detrimental to the performance of the code in the case of substitution or deception.

Consider the three codes C_1, C_2 and C_3 specified by the encoding matrices below. The message is a fair coin, while the key probabilities are $\frac{3}{7}$, $\frac{3}{7}$ and $\frac{1}{7}$, top to bottom. C_2 and C_3 are obtained from C_1 by adding a codeword (by adding a one in the admissibility matrix). The homophones are equiprobable.

C1	
y1	y2
y3	y4
y5	y3

C2	
y1,y4	y2
y3	y4
y5	y3

C3	
y1	y2
y3,y5	y4
y5	y3

In the table below results are given in 56-ths to help comparisons; the easy computations are omitted.

	P_I	P_{CS}	P_d	P_{MS}	P_δ
C_1	32	52	52	52	52
C_2	48	51	51	51	51
C3	32	56	56	48	48

In the case of C_2 splitting helps whenever substitution is involved, but it is harmful for impersonation; there is no practical difference between codeword and message substitution. In the case of C_3 the proposed splitting is catastrophic for *codeword* substitution; however the same splitting is advantageous for *message* substitution; it does no harm even to impersonation taken by itself, and so C_3 should be definitely preferred to both C_1 and C_2.

These examples show that deterministic coding can be "pointwise" improved by splitting, but they do not answer a deeper question: are there cases when (asymptotically) optimal encoding is necessarily probabilistic? Actually, at the moment such a question is not even well-defined, since a Shannon-theoretic framework for authentication theory is still in the make (cf /6/).

A REDUCTION THEOREM FOR MESSAGE SUBSTITUTION

Now we prove a reduction theorem for message substitution, which reduces it to *abstract* impersonation. From XYZ construct a new operational code XY'Z (only the random codeword changes) with an extra codeword d which takes the place of the homophones of c in the encoding matrix. Set $E=\{c\}$, $F=\{y: y\neq c,d\}$. Then:

$$P_{MS}(c) = P_{I(E,F)}(XY'Z) = P_I(Y_cZ_c)$$

where Y_cZ_c is obtained from Y'Z in the same way as Y*Z* was obtained from YZ in the boring insert.

Proof. The first equality follows from the following obvious facts: Y'=c iff Y=c, $Z\in A'_y$ iff $Z\in A_y\text{-}H_{y,c}$. The second follows from the insert; $|X|\geq 2$

ensures that the regularity assumption is met (recall that d is a homophone of c and so occupies the same entry of the encoding matrix).

Consequently, abstract lower bounds for impersonation can be recycled to bounds for message substitution. From each of them, one learns (necessary but not sufficient) conditions a code should meet to be a good code. Simmons bound recycled tells that Y and Z should be strongly correlated given c, but correlation due to homophones does not count. The JS-bound recycled improves on this and tells that only "deterministic" correlation (as measured by the infimum mutual information) matters:

$$P_{MS}(c) \geq 2^{-\inf I(Y^*;Z_c)}$$

where Y^*Z_c is constrained to have the same admissibility matrix as Y_cZ_c.

The abstract combinatorial bound yields instead:

$$P_{MS}(c) \geq \frac{|X|-1}{|Y|-1}, \quad \text{and therefore} \quad P_{MS} \geq \frac{|X|-1}{|Y|-1}.$$

Proof. Going from XYZ to XY'Z the number of codewords increases at most by 1; going from Y'Z to Y_cZ_c it decreases at least by 2; so $|Y_c| \leq |Y|-1$. Assume that c decodes to x under key z in XYZ, or XY'Z; at least |X|-1 more codewords are needed for key z to decode to the remaining |X|-1 messages; none of these can be equal to d, since g(d,z)=g(c,z). So $|A^c{}_z| \leq |X|-1$ for any z.

A similar combinatorial bound was well-known for codeword substitution; it does not implies ours, though, as $P_{CS}(c)$ can be strictly greater than $P_{MS}(c)$.

We think that the foregoing vindicates the role of abstract codes in Simmons theory of authentication.

REFERENCES

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

/2/ J. Massey "An introduction to contemporary cryptology", Proceedings of the IEEE, may 1988, 533-549

/3/ R. Johannesson, A. Sgarro "Strengthening Simmons' bound on impersonation", submitted

/4/ A. Sgarro "Informational-divergence bounds for authentication codes", Proceedings of Eurocrypt 89, Houthalen, April 1989

/5/ M.-G. Croatto "Codifica probabilistica nei sistemi di segretezza e autenticazione", tesi di laurea, Università di Udine, marzo 1990

/6/ A. Sgarro "Towards a coding theorem in authentication theory", IEEE Information Theory Workshop, Eindhoven, June 1990