# AUTHENTICATION WITHOUT SECRECY

TERRY C. JONES AND JENNIFER SEBERRY

ABSTRACT. Recently, Seberry proposed a method for subliminal message transmission over an insecure channel in the case where authentication but not secrecy is required. Here we examine her ideas in some detail, and propose certain changes to the method that would be necessary for implementation.

## Introduction.

The most commonly cited example of a situation requiring authenticity without secrecy is that described by Simmons [4] wherein "Two mutually deceitful and distrusting parties" (countries) wish to place underground listening devices in each others territory to monitor compliance with a nuclear test ban treaty. In short, the host country requires that all outgoing messages be openly readable in order to check the accuracy of the device and ensure that no other information is transmitted, while the monitoring country requires strong authentication of the received messages to be convinced that innocuous reports have not been substituted for incriminating ones (or vice-versa).

Simmons [4] has discussed the general authentication without secrecy problem using two key cryptographic methods. It was also Simmons [3, 4] who suggested the possible transmission in an authentication system of a subliminal message. Imagine an authentication system such as that described above, where more than one choice of key could be used to (correctly) authenticate a given message. If the key that was used is recoverable by the receiver, then additional information may be conveyed by the choice of key. Simmons showed how this could be done in the simple case where two keys could be used to authenticate a message, and the recovery of the key used would provide one bit of subliminal message.

Seberry [2] has shown how these ideas could be incorporated into an authentication without secrecy environment employing Shamir's knapsack based signature method for authentication. In Shamir's method [7], for every message transmitted, a random binary vector $R$ is chosen to add to the security of the system, and Seberry shows a method by which the chosen $R$ may be recovered by the receiver.

ARS COMBINATORIA 21-A (1986), pp. 115-121

Under this system, to send a message $M$, $M$ is converted to a $k$-bit binary number, and the sender chooses a modulus $n$, and a random $k \times 2k$ matrix $H$. A $2k \times 1$ matrix $A$ is then computed such that

$$HA = \left[1, 2, 4, \ldots, 2^{k-1}\right]^T \pmod{n}.$$

To provide additional security, a random $1 \times 2k$ binary vector $R$ is also chosen for each message. An authentication vector $C_2$ is then formed for $M$ in the following way. The sender forms

$$\begin{aligned} M' &= M - RA \\ C' &= (\mathrm{REV}\,(M'))H \\ C_2 &= C' + R \end{aligned}$$

where $\mathrm{REV}\,(M')$ is the binary representation of $M'$ written backwards. The vector $C_2$ is the authenticator for $M$ and the pair $(M, C_2)$ is transmitted. Authentication by the receiver is performed by checking that $C_2A = M$, and recovery of $R$ is possible by solving $C_2B = RB \pmod{n}$ given $C_2$ and the superincreasing $B$.

This system, as proposed by Seberry has several shortcomings which we will now attempt to resolve.

### The value of the modulus ($n$).

We have found that the value of the modulus, $n$, cannot be chosen quite as arbitrarily as was thought. If $n$ is chosen to have more than $k$ bits, then there will be messages such that $M' \geq 2^k$, making the multiplication $M'H$ impossible, since $M'$ will have more than $k$ bits and hence $\mathrm{REV}\,(M')$ will be a vector with length greater than $k$.

We need to enforce the condition that $n < 2^k$. An instance of the method going wrong when this is not enforced occurs in Seberry's example where the message 1 is to be transmitted and $R$ is chosen as [0 1 0 0], since here, with $n = 5$ and $k = 2$, $M' = 1 - 2 = 4 \pmod{5}$, a number with $k + 1$ bits ($100_2$), and hence $\mathrm{REV}\,(M')$ is [0 0 1].

**The recovery of (the subliminal) $R$.**

Following message reception, the $R$ that was used to form the authenticator $C_2$ is recovered as the solution of $C_2B = RB \pmod{n}$. Seberry proposed that $B$ be chosen as a superincreasing $2k \times 1$ vector to facilitate simple recovery of $R$. We have since discovered that making $R$ superincreasing does not aid in this as much as was hoped.

If the system were implemented as it stands, the message receiver would have to solve $RB = s \pmod{n}$ for $s = C_2B$. Were there no considerations of modulus, the superincreasingness of $B$ would make the solution trivial. Given the existence of the modulus, and the condition $n < 2^k$, our problem is to find solutions to the system of equations

$$RB = s + an \quad (a = 1,2,3,\ldots,p) \qquad \text{where}$$

$$s + pn \leq \Sigma b_i < s(p+1)n \quad (b_i \text{ in } B) \qquad \text{and}$$

$$p = \text{floor}((\Sigma b_i - s)/n).$$

floor($x$) represents the integer part of the number $x$. The maximum number of solutions for $R$ satisfying $RB = s \pmod{n}$ is $p$. Not all of these equations need have a solution. An example will make this clearer. Consider the system with the following parameters

$$k = 3 \quad n = 5$$

$$A = [2\ 2\ 2\ 2\ 4\ 1]^T, \quad B = [1\ 2\ 4\ 9\ 18\ 40]$$

$$H = \begin{bmatrix} 2 & 2 & 4 & 1 & 3 & 1 \\ 4 & 4 & 1 & 1 & 0 & 2 \\ 4 & 3 & 4 & 2 & 2 & 0 \end{bmatrix} \quad M = 3 \quad R = [0\ 1\ 1\ 0\ 1\ 1]$$

then,

$$\begin{aligned} M' &= M - RA \\ &= 4 \pmod{5} \\ C' &= (\text{REV}(M'))H \\ &= [0\ 0\ 1]\begin{bmatrix} 2 & 2 & 4 & 1 & 3 & 1 \\ 4 & 4 & 1 & 1 & 0 & 2 \\ 4 & 3 & 4 & 2 & 2 & 0 \end{bmatrix} \\ &= [4\ 3\ 4\ 2\ 2\ 0] \\ C_2 &= C' + R \\ &= [4\ 4\ 0\ 2\ 3\ 1] \end{aligned}$$

Then, on reception of $(3, [4\ 4\ 0\ 2\ 3\ 1])$, to authenticate $M = 3$, the receiver computes $C_2 A = 33 \pmod 5 = 3 \pmod 5 = M$, and to recover $R$, solves $C_2 B = RB \bmod 5 = 4 \pmod 5$.

So, the receiver must solve each of

$$\begin{aligned} RB &= 4 \\ RB &= 4 + 5 \\ RB &= 4 + (2 \times 5) \\ &\vdots \\ RB &= 4 + (14 \times 5). \end{aligned}$$

In this case, the solution set is found to be

$$\begin{aligned} R = \{&001000,\ 000100,\ 101100,\ 100010,\ 011010,\ 010110,\ 111110, \\ &001001,\ 000101,\ 101101,\ 100011,\ 011011,\ 010111,\ 111111\} \end{aligned}$$

note that we get 14 solutions to our 15 equations, $RB = 39$ having no solution.

The solutions for $R$ such that $RB = s$ will form a class. Let the class corresponding to the solutions for $RB = s$ be named $S$ (where $S = s \pmod n$).

Seberry suggests reauthentication to resolve which of the elements of the class was the one used for the generation of the received $C_2$. That is, reauthenticate the received message with each $R$ in class $S$ until the authenticator $C_2$ is obtained. Clearly this procedure will be unacceptable in terms of time taken to recover $R$ if there happen to be a large number of elements in $S$.

### A solution.

Ideally we would like to preserve the structure of the system as far as possible, since it allows for the sending of such a large subliminal message (twice the size as the message $M$). There are two approaches that spring to mind that could be taken to achieve this. Both are aimed at reducing the number of elements in classes.

The first approach is to try to minimise the average number of elements in each class, and thus make the system as fast as it could be (on average). How fast would this be? We have $2^{2k}$ elements to distribute among $n$ classes. The average number in a class will therefore be $2^{2k}/n$. To minimise this number we must maximise $n$, (i.e., $n = 2^k - 1$) giving $2^k$ classes, or an average of $2^k$ elements per class in the best case.

From this we see immediately that the system is unacceptable, as was hinted at in the previous section, since the time taken to recover $R$ rises exponentially with the length of the message.

A second approach would be to try to choose the parameters ($B$ and $n$) for the system in such a way that a large number of classes contained only a small number ($> 0$) of elements, and allow the bulk of the elements to be spread among the remaining few classes. That this cannot be done we have been unable to prove, but simulations run on a VAX 11/780 have not provided examples where it is possible. It has been suggested that the proof of this follow some group theoretical or Central Limit Theorem approach. If it were possible, then it may prove preferable to the solution we now propose.

Given that we cannot restrict the number of elements falling into the classes in either of the above ways, it is suggested that the class into which the authenticator $C_2$ falls constitute the subliminal message. Although this reduces the amount of subliminal information that is conveyed by a $k$-bit message from $2k$-bits to $k$-bits (in the case where $n = 2^k - 1$), we feel that this is still ample. However, we now have the important advantage that the recovery of the subliminal message has been made as fast as the authentication procedure itself.

Here, since we know $C_2B = RB \pmod n$, the sender just chooses $R$ such that $RB = s \pmod n$ for a subliminal transfer of $S$. The receiver then simply forms $C_2B \pmod n$ to retrieve $S$. As well as the tremendous advantage gained in terms of speed, there is now no longer any need for $B$ to be superincreasing. $B$ could simply be some random permutation of $\{0, 1, 2, \ldots, 2k - 1\}$, or perhaps with some repeated elements. This also represents a saving in storage space and requires marginally less computation to be done in the multiplication of $C_2B \pmod n$.

### Obtaining additional security.

It is more than likely that a transmitter may never want to send more than one of a set of prearranged subliminal messages, or no subliminal message at all. This is especially relevant in the case of treaty compliance outlined in the introduction, where the listening device might have only a few possible states. If the number of acceptable subliminal messages is small compared with $n$, then detection of (correctly authenticated) forgeries inserted by some intruder can be accomplished with high probability.

Suppose there are $v$ valid subliminal messages at some point in time, then (pre)assign to each of these $v$ a distinct class. Now, if an intruder, unaware of any subliminal transmission, is able to compromise the au-

thentication system, then an inserted message will be detected with a probability of approximately $1-v/n$ (given that the number of elements in each class has been made approximately equal). Detection will occur in exactly those cases where the class into which the received authenticator falls does not match one of the (pre)arranged subliminal message classes. When such a message is received, a change of key is requested of the transmitter. There is no need to change the valid subliminal classes or their meanings–although (if feasible) this might be preferred.

It should be noted that the number of elements in each class is (in our experience) very uniform, and proving uniformity would be equivalent to proving the impossibility of constructing classes with a small number of elements. There exist choices of $B$ and $n$ which result in each of the classes containing exactly $2^k$ elements, and in these cases, if there was a strict protocol between sender and receiver, such that only one subliminal response was acceptable at any one time, then we have a 'perfect' authentication system as defined by Simmons [5]. That is, the probability of successful deception falls to its minimum, 1/n.

## Conclusion.

Modified as above, Seberry's method for subliminal message transfer in an authentication without secrecy environment becomes feasible and much faster. If additional authentication is implemented using valid subliminal classes, then security can also be greatly increased.

## 1. Addendum.

Concurrent with the work of Seberry [2] and received following the completion of this work, was that of Odlyzko [1] which breaks the basic Shamir Fast Signature Scheme. Odlyzko shows how to break Shamir's basic system (without the random vector $R$), and this carries directly over to the system with the random vector. Basically he solves $\sum_{i=1}^{2n} \in i^a i \equiv m(\mathrm{mod}\, n)$ without the need for knowledge of the secret matrix $H$.

In either case, some vector, say $C$, is received with the message $M$. Odlyzko's method provides some $C'$ such that $C'A = M$. Not surprisingly, some damage is done to our work on the subliminal channel. Something may be salvageable, but at the price of restricted operation. It is possible to use the subliminal message class for further authentication, or keep $A$ private. If the subliminal class is used for authentication, then the system takes on a contrived appearance, whilst if $A$ is

kept private we no longer have authentication without secrecy, but just authentication. This would not be suitable for the example concerning two countries and listening devices since the authenticator could not be shown to be so, unless $A$ were revealed following every message. This would probably not be acceptable to either country. The system could however still be used for authentication between two parties who kept $A$ secret, but in this case some stronger authentication would probably be chosen.

## REFERENCES


1. Odlyzko, A.M., *Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's Fast Signature Scheme*, IEEE Transactions on Information Theory **IT30 No. 4** (July 1984), 594-601.
2. Seberry, J., *A subliminal channel in codes for authentication without secrecy*, Ars Combinatoria **19A** (1985), 337-342.
3. Simmons, G.J., *Message authentication without secrecy*, in "Secure Communications and Asymmetric Cryptosystems", ed. by G.J. Simmons, AAAS Selected Symposia series, Westview Press, Boulder Co., 1982, pp. 105-139.
4. Simmons, G.J., *The prisoner's problem and the subliminal channel*, in "Advances in Cryptology", ed. by D. Chaum, Plenum Press, New York, 1984.
5. Simmons, G.J., *Verification of treaty compliance revisited*, in "IEEE Proceedings of the 1983 Symposium on Security and Privacy", IEEE Computer Society Press, Silver Spring, Md., 1983.
6. Simmons, G.J., *A game theory model of digital message authentication*, Congressus Numerantium **34** (June 1982).
7. Shamir, A., *A fast signature scheme*, MIT/LCS/TM-197 (1978), MIT Laboratory for Computer Science, Cambridge, Mass..



Basser Department of Computer Science
University of Sydney
Sydney, N.S.W., 2006
Australia