A SUBLIMINAL CHANNEL IN CODES FOR AUTHENTICATION WITHOUT SECRECY

Jennifer Seberry*
Department of Computer Science
University of Sydney
N.S.W. 2006

Abstract

G.J. Simmons has advanced the concept of using authentication in an open channel to actually convey information. We review the use of the knapsack problem for public codes and explore the use of Shamir's method for a signature only knapsack to convey messages.

Introduction

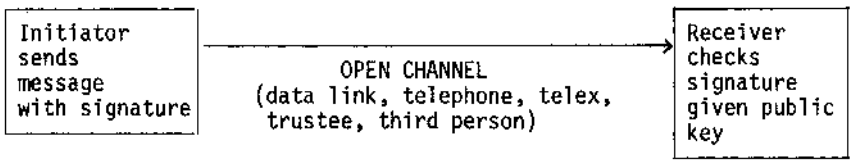
Simmons describes subverting authentication to carry secret information when the message-signature pair (M, C) is transported by a neutral or hostile medium on an open channel. Simmons describes how a warden might permit a trustee (or say the Red Cross) to carry an open communication between X and Y in the hope that he can deceive at least one into accepting as a genuine communication

(a) a fraudulent message created by the warden, or

(b) a modification of a genuine message.

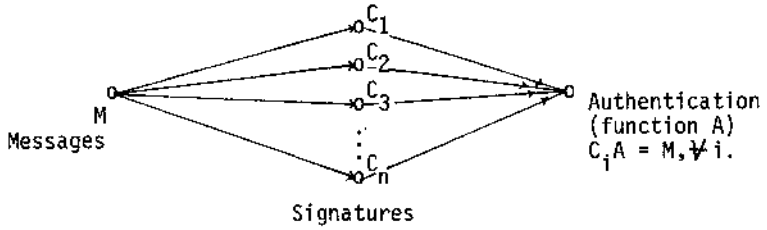
X and Y accept the use of an open channel and a potentially hostile transporter in order to have any communication at all but insist on a signature or authentication attached to the communication.

The model can be described by the following diagram.



As Simmons notes, there can be many valid signatures for one message, and if the signature space can be partitioned, information can be conveyed by the choice of signature.

*This research was supported by grants from the ACRB and the ARGS.



Shamir's Method

We first review Shamir's knapsack code for authentication without secrecy.

H is k x 2k random (0, 1) matrix,

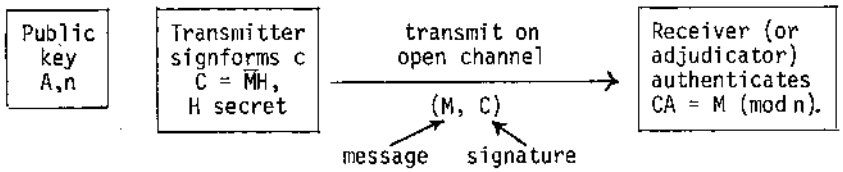
M is the message,

$\overline{M}$ is M written in binary with digits reversed to form a k-bit number; the method solves

$$HA = \begin{bmatrix} 1 \\ 2 \\ 4 \\ \vdots \\ 2^{k-1} \end{bmatrix} \pmod{n}$$

to form $A = (a_1,\ldots,a_{2k})^T$ (since H is k x 2k, HA gives k equations in 2k unknowns and so there is freedom to arbitrarily choose k of the coordinates of A).

The transmission procedure can be represented diagramatically as



The method works because

$$CA = \overline{M}HA = \overline{M}\begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^{k-1} \end{bmatrix} = M \pmod{n},$$

but to thwart the system it is necessary to solve $CA = M \pmod{n}$, where A and M are known, which is precisely the knapsack problem.

Added Security in Shamir's Method

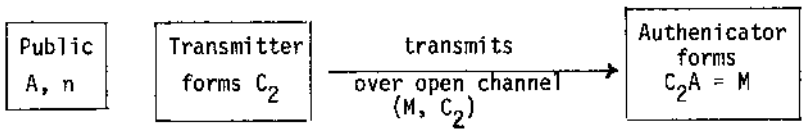
Nevertheless, security may be lessened if an observer obtains many sets of (A, n, M_i, C_i) and can deduce H. So Shamir suggested choosing a 1 x 2k random binary vector and forming

$M^1 = M - RA$ or $M = M^1 + RA$

$C^1 = \overline{M}^1 H$ giving $C^1 A = \overline{M}^1 HA = M^1$

$C_2 = C^1 + R.$

Diagramatically we now have



This method works because

$$C_2A = (C^1 + R)A = C^1A + RA = \overline{M}^1HA + RA$$
$$= M^1 + RA \pmod n$$
$$= M.$$

A Subliminal Message?

We note there are at least 2^{2k} C_i such that $C_iA = M$. Hence if we can recover R or part of R we can send a subliminal message in our transmitted pair (M, C_2).

Now we suppose the message has been transmitted over an open channel using Shamir's signature scheme. The hostile or neutral transporter can check $C_2A = M$, but we assume the receiver knows everything the transmitter knows except the random 1 x 2k binary vector R. Thus the receiver knows M, H, C_2, A, n. Hence the receiver can form

$C_1 = \overline{M}H$

and knows

$$C_2 = C^1 + R = \overline{M}^1 H + R. \qquad (1)$$

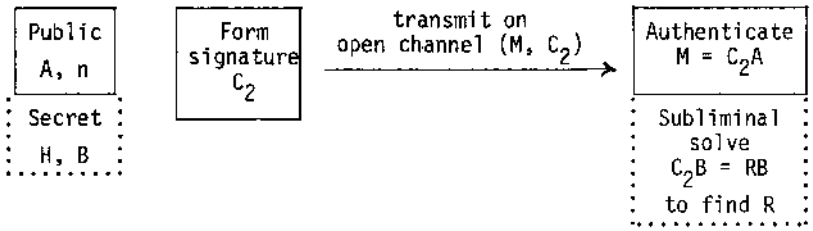
The receiver must solve this equation to find R, and this is equivalent to solving the knapsack problem.

A Trapdoor to Recover the Message

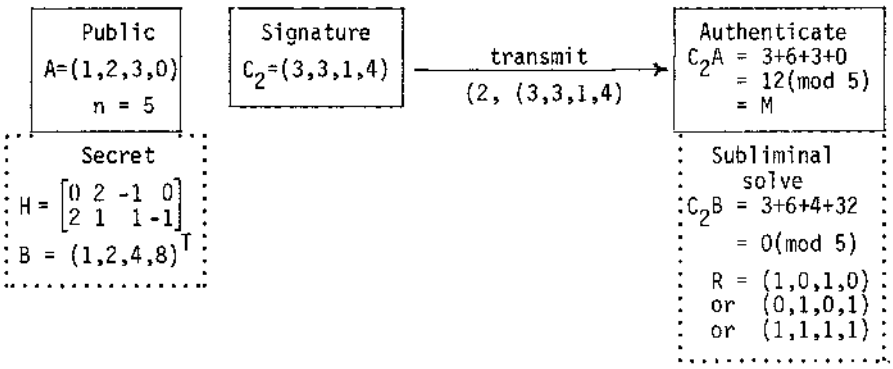
To solve for R we need a trapdoor. Suppose there exists a (1x2k) vector B such that $HB = 0$; then equation (1) becomes on multiplying by B

$C_2B = \overline{M}^1 HB + RB = RB \pmod n$.

Hence, if in addition B is superincreasing we can solve for R.
Diagramatically



Example: $M = 2$, $\overline{M} = 01$, $M^1 = 3 \pmod 5$, $C_2 = (3, 3, 1, 4)$



To be precise $R = (0,1,0,1)$, $R_2 = (1,0,1,0)$, $R_3 = (1,1,1,1)$ correspond to the signatures $C_1 = (0,1,0,1)$, $C_2 = (3,3,1,4)$ and $C_3 = (1,3,0,1)$ of the message $M = 2$ and we need to re-encipher to establish which solution for R corresponds to the subliminal message R.

For added security, the elements of H and B can be permuted, or B could be modified using modular arithmetic, as proposed by Merkle and Hellman [2].

Conclusion

If a suitable secret matrix H, not necessarily binary, and a secret easy to solve knapsack vector B such that $HB = 0$ exists, then Shamir's signature only knapsack authentication scheme can be modified to carry secret messages. This method appears to be more secure than the original knapsack encoding schemes as the third party is presumably unaware that any secret information is being conveyed. Furthermore, both the secret encipherment matrix H and solving knapsack B are not made public.

Acknowledgement

I wish to thank Gus Simmons for awakening my interest in authentication by his enthusiastic, careful explanation of current knowledge and his own work and his regular supply of preprints to an isolated research worker.

References

[1] Dorothy E.R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, Mass. - Sydney, 1982.

[2] R.C. Merkle and M.E. Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE Trans. on Info. Theory, Vol. IT-24(5), (1978), 525-530 (quoted in D.E.R. Denning, op.cit.).

[3] R.M. Karp, Reducibility among combinatorial problems, in Complexity of Computer Computations, ed. R.E. Miller and J.W. Thatcher, Plenum, New York (1972), 85-104 (quoted in D.E.R. Denning, op.cit.).

[4] A. Shamir, A fast signature scheme, MIT/LCS/TM-107, MIT Lab. for Computer Science, Cambridge, Mass. (July 1978) (quoted in D.E.R. Denning, op.cit.).

[5] Gustavus J. Simmons, The prisoners' problem and the subliminal channel, in Advances in Cryptology, ed. David Chaum, Plenum, New York, 1984.