SUBLIMINAL-FREE AUTHENTICATION AND SIGNATURE
(Extended Abstract)

Yvo Desmedt

Dept. EE & CS, Univ. of Wisconsin – Milwaukee
P.O. Box 784, WI 53201 Milwaukee, U.S.A.

ABSTRACT

Simmons [17] introduced the notion of subliminal channel in 1983, by demonstrating how to "hide" secret information inside an authenticated message. In this paper we propose a practical subliminal-free authentication system and extend our results to subliminal-free signatures. The subliminal-freeness of our systems can be proven. We discuss applications in the context of verification of treaty and international bank communications.

I. INTRODUCTION

In the process of peace keeping, the verification of international treaty plays an important role [1]. Discussions of arms reductions include that each party is able to have observation posts in the other country, which can send authenticated (or even signed) messages. This introduces however a major security problem. Indeed, will the observation post be used for spying activities? The problem of *message authentication without secrecy* was initialized and investigated by Simmons [16]. This problem was not solved until today, as a consequence of the possibility of a *subliminal channel.* Five years ago Simmons discovered that a secret message can be hidden inside the authenticator (for more details see [17]). He called this "hidden" communication channel, the *subliminal channel.* Other subliminal channels were introduced inside signature systems *e.g.*, [18,19]. The concept of subliminal channel can be formalized and generalized [4].

In our paper we come up with a *practical authentication* system which *eliminates almost completely the possibility to use a subliminal channel.* This result is explained in Section IV., after having introduced the main ideas in Section III.. We extend our results to subliminal-free signature systems (see Section V.). How-

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 23-33, 1988.

ever the last system is less practical. The reader not familiar with the terminology used in modern cryptology, will find a brief introduction to it in Section II..

II. TERMINOLOGY IN MODERN CRYPTOLOGY

In this section we explain briefly:

- subliminal channels,
- the role of a warden,
- message authentication without secrecy,
- the Goldwasser–Micali–Rivest signature scheme,
- commitment in modern cryptology.

To better understand the concept of subliminal channels, let us discuss Simmons' illustration [17]. Two prisoners are communicating authenticated messages in full view of a *warden*. The warden is able to read the messages. The subliminal consists in hiding a message *through* the authentication scheme, such that the warden cannot detect its use nor read the hidden part.

Solving the problem of subliminal channels is not sufficient to obtain authentication without secrecy, as is well known. Subliminal information can be sent in an analog way through modulation, time jitter and so on. For a solution to overcome this problem see [20, p. 65]. The techniques we use here are digital. By combining our results with [20, p. 65], the problem of message authentication without secrecy can be completely solved.

Let us briefly explain the basic ideas used in the Goldwasser–Micali–Rivest signature scheme [14,15]. Their scheme is based on:

- claw-free permutation pairs,
- prefix-free mapping,
- an authentication tree.

Informally, claw-free permutation pairs are permutations f_0 and f_1 over a common domain for which its is computationally infeasible to find a triple x, y and z such that $f_0(x) = f_1(y) = z$ [14, p. 290]. If factoring numbers of a special form are hard then such claw-free permutations exist [14, pp. 292–293]. These numbers have the form:

$$n = p \cdot q, \quad p \text{ and } q \text{ primes such that: } \; p \equiv 3 \pmod 8 \text{ and } q \equiv 7 \pmod 8.$$

Such numbers n are known as Williams integers, due to there first use in cryptology by Williams [21] and are also known as Blum integers. The functions $f_{0,n} = x^2 \pmod{n}$ and $f_{1,x} = 4x^2 \pmod{n}$ form *permutations* over the set of quadratic residues modulo n and are claw-free [15] (remark that these functions were slightly modified in [14]). It is essential to know that the Jacobi symbol $(2|n) = -1$ if n is a Williams (Blum) integer, so 2 is a quadratic nonresidue modulo n. If there is no doubt about n we will shortly say f_0 instead of $f_{0,n}$ and f_1 instead of $f_{1,n}$. For authenticity and signature one does not only need claw-freeness for two permutations but a family of permutations which are pairwise claw-free. Hereto f_i is defined as $f_i(x) = f_{i_d}(f_{i_{d-1}}(\cdots f_{i_1}(f_{i_0}(x))\cdots))$, where $i = i_d i_{d-1} \ldots i_1 i_0$ in binary. We *define* $|i| = d+1$. One has to read f_i^{-1} as $(f_i)^{-1}$ so that $f_i^{-1}(f_i(x)) = x$. In order to exclude that anyone else could compute $f_j^{-1}(y)$ from a given $f_i^{-1}(y)$ $(j \neq i)$ Goldwasser, Micali and Rivest use prefix-free mapping $\langle \cdot \rangle$. A prefix-free encoding satisfies the property that $\langle j \rangle$ is never a prefix of $\langle i \rangle$ $(j \neq i)$. Finally, to avoid chosen text attacks and forgery, an authentication tree is used [15]. Different authentication trees have been presented, but their differences are not important in this context. We will not discuss these trees in detail, because they are only partially important in order to understand this paper. The motivation for an authentication tree is to make random "signatures" that can be used later on to sign real messages. In order to obtain the security one uses f-claw-free permutations and g-claw-free permutations (for more details see [9,14,15]).

Commitment originates from Blum's ideas [2]. It allows A to randomly choose a number R and to commit herself to this number, *e.g.*, to B. Hereto A encrypts R and sends the result $C = h_k(R)$ to B. If a good encryption system, *e.g.*, a probabilistic encryption system as [12], has been used no information is revealed about R. Later on A is able to reveal R. As a consequence of her commitment A is unable to lie or pretend that her choice was R' instead of R. B is able to verify if R is correct when A reveals it together with k. A sufficient condition for commitment is that:

$$h_k(x) = h_{k'}(y) \qquad \text{implies} \qquad x = y. \tag{1}$$

Let us briefly discuss a practical commitment algorithm, which is however not guaranteed secure. To commit herself to the bit 0, A sends $h_k(0, 0, \ldots, 0)$ where h is the DES and key k is chosen randomly; to commit to 1, A sends $h_k(1, 1, \ldots, 1)$.

III. MAIN IDEA

The main idea to obtain subliminal-freeness is to use an *active warden.* We call a warden *active*, if he does not only listen to catch up subliminal channel users, but he also ***interacts*** in the communication in a special way to better enforce the subliminal-freeness. Remember that a warden is allowed to send fake messages trying to convince the receiver that they are authentic [17]. So the only trust in the active warden consists in believing he will not help to set-up a subliminal-channel.

The idea of an active warden is not 100% new. Simmons already used a similar idea (without calling it active warden) to exclude the use of analog covert channels [20, p. 65]. Our active warden is however digital.

Let us now explain in more detail how to realize the subliminal-freeness. Let us call A the sender of the message M, B the receiver of M and W the active warden. A first sends the message to W, who sends it to B. A then convinces B that the message is indeed authentic, by answering (random) questions from B. The warden's role is to guarantee that these answers and questions can not be abused to send secret information in an hidden way. Hereto he will modify the questions and answers. Nevertheless the fact that these questions and answers have been modified, B must be still convincible that indeed A has sent the message and nobody else, the warden included.

Let us now present the technical results.

IV. SUBLIMINAL-FREE AUTHENTICATION

To simplify the presentation, we first reduce the task of the warden to guarantee that A (the sender of the message M) can not use a subliminal channel; however B (the receiver of the message M) is allowed to send information in a subliminal way. At the end of this section we will also eliminate the possibility that B can use subliminal channels.

The authentication mechanism we propose is a one-time-valid authentication scheme [5, p. 154]. A one-time-valid authenticated message looses his validity once the authenticity of the message has been checked by the legitimate receiver of the message, or after a certain time. The concept of one-time-validity itself is certainly not new. It can be obtained by adding the actual date and time to the message. It can also be obtained using zero-knowledge [11,13]. This approach is now used.

Our system is partially based on the Goldwasser–Micali–Rivest signature scheme, which was briefly explained in Section II.. We also use some methods which were developed in [7]. From now on we assume that the message M and i are encoded with a prefix-free encoding [15]. Remark that no authentication tree is necessary, because the scheme is not a signature system and because our protocol is zero-knowledge. The need to use two different claw-free pairs (f and g) also disappears. The authentication mainly consists in proving that A knows $f_M^{-1}(R)$, where f is based on claw-free permutations, as explained in Section II.. Let us explain the details of the protocol.

$n = p \cdot q$ a Williams (Blum) integer together with $R_1, R_2, \ldots, R_k$ form the public key of the sender (A). The R_j are chosen randomly such that the Jacobi symbol of $(R_j \mid n) = 1$. p and q are secret.

Before that A uses the system, W (the active warden) *asks A to "prove" that n is indeed the product of* two *primes, which satisfy the above conditions*. This can be done using a zero-knowledge protocol (see *e.g.*, [10]). This zero-knowledge protocol has only to be used once, because W can store n and label it as being verified.

To authenticate a message M our public key authentication system follows the following protocol, where Steps 2–7 are repeated l times:

Step 1 A sends the message M to W, who sends it to B.

Step 2 A generates a t (not necessarily random) such that $\gcd(t, n) = 1$ and squares it $|M|$ times and multiplies it with (random) ±1 to obtain $X = \pm t^{(2^{|M|})} \pmod{n}$ and sends X to W.

Step 3 W checks that the Jacobi symbol $(X \mid n) = 1$. *If it is not, then* W stops the protocol, *else* W does similar as A did in Step 2 starting from a *truly* random t' to obtain X' and sends $\alpha = X \cdot X' \pmod{n}$ to B.

Step 4 B sends a (random) Boolean vector $(E_1, \ldots, E_k)$ to A (through the active warden).

Step 5 A sends $Y = t \cdot \prod_{E_j=1} f_M^{-1}(\pm R_j) \pmod{n}$ to W, where $+1$ is used if R_j is a quadratic residue, else -1 is used.

Step 6 W verifies (by squaring and multiplications) if Y is correct. *If* it is *not, then* W halts the protocol, *else* W sends $\beta = t' \cdot Y \pmod{n}$ to B.

Step 7 B verifies β by using square operations, multiplications, α and A's public key. The last multiplication is by ±1.

Remark that A would be able to send one bit of information (the fact that the protocol could be halted) in Step 3 or in Step 6, however the warden is then able to arrest A (if appropriated). The fact that this one bit of information, that A could send, is detectable by the warden implies that it is not a subliminal bit. Indeed subliminal as defined by Simmons implies undetectability by the warden. If necessary the warden can ask A to sign all her messages, so that the warden is able to prove later on that A tried to use a subliminal channel. However it is also possible that the warden (or an active eavesdropper) has tried to inject a fake message M and is unable to answer B's questions, and therefore stops the protocol. *So B has no guarantee about the authenticity of this bit.*

To discuss the security of the above protocol we need to remind what the mafia fraud is [6]. Suppose that A proves statement S to B using zero-knowledge for example, then A will answer questions from B. If C is able to claim to D that she is proving S, using B as dishonest verifier of A's proof, then the proof system is not secure against the mafia fraud. Several zero-knowledge protocols allow this fraud in *real-time.* Hereto B and C have to communicate questions and answers respectively from D to A and vice-versa. The mafia fraud is important to evaluate the security of authentication, signature and identification. Let us now discuss the security of our subliminal-free authentication system.

Theorem 1 *If one excludes the mafia fraud, the real sender will convince the prover and a fake prover will fail. This protocol is a zero-knowledge proof.*

Proof (sketch): Consider that the warden is not active, so $t' = X' = 1$, then the proof is similar as in [7, pp. 214–215]. □

Theorem 2 *Using the assumptions of [15], the protocol cannot be defrauded by the mafia fraud. To be more precise if A authenticates M an active eavesdropper can not modify the proof to authenticate M', unless the Goldwasser–Micali–Rivest system can be broken.*

Proof (sketch): Drop the effect of the active warden. The effect of the mafia fraud corresponds with an active eavesdropper who modifies M into M' and tries to convince B about the authenticity of M'. Hereto he can multiply X with X'', exor E_j with E_j'' and multiply Y with Y'', such that if B checks Y'', he is convinced that A has sent M'. The proof consists in demonstrating that if the active eavesdropper succeeds then he can break the Goldwasser–Micali–Rivest [15] signature system. □

Theorem 3 *If n is of the appropriated form, then A is not able to send subliminal information (a more formal theorem will be given in the final paper).*

Proof (sketch): The proof is based on perfect secrecy. □

In the previous protocol, B is able to send a secret message to A, by letting $(E_1, \ldots, E_k)$ correspond with a part of the hidden (encrypted) message. This can be avoided by modifying Step 4 and Step 5 using the concept of *commitment*. The modifications are:

Step 4.a W chooses a random Boolean vector $(F_1, \ldots, F_k)$ and random K and sends $h_K(F_1, \ldots, F_k)$ to B, where h satisfies condition (1).

Step 4.b B sends a (random) Boolean vector $(E_1, \ldots, E_k)$ to W.

Step 4.c W sends $(G_1, \ldots, G_k) = (E_1 \oplus F_1, \ldots, E_k \oplus F_k)$ to A, and reveals $(F_1, \ldots, F_k)$ and K to B.

Step 4.d B verifies $(F_1, \ldots, F_k)$ and the protocol continues if correct.

Step 5 A sends $Y = t \cdot \prod_{G_j=1} f_M(\pm R_j) \pmod{n}$ to W, where $+1$ is used if R_j is a quadratic residue, else -1 is used.

Remark that B will use the G_i at the moment that he checks β. The use of the concept of *commitment* was extremely important to avoid that the warden could cheat or that B could send subliminal information. The role of the active warden differs from before. Indeed to avoid that A can use a subliminal channel, the warden does not have to interact with A, he has to act similarly as an active eavesdropper. So the warden could interact in such a way that A and B are not conscious that he is intervening. However, to prevent B from sending subliminal information, the warden and B must contact each other. The proofs of security of these protocols will be fully discussed in the final paper. To prove them a more formal definition of subliminal-freeness will be given. Remark that if B is able to break the security of the encryption E then B is able to cheat and the subliminal-freeness disappears. When one wants stronger guarantees that the protocol is subliminal-free the following adaptation can be used:

Step 4.a B chooses a (random) Boolean vector $(E_1, \ldots, E_k)$ and random K and sends $h_K(E_1, \ldots, E_k)$ to W, where h satisfies condition (1).

Step 4.b W sends a random Boolean vector $(F_1, \ldots, F_k)$ to B.

Step 4.c B reveals $(E_1, \ldots, E_k)$ and K to W.

Step 4.d first W verifies $(E_1, \ldots, E_k)$ and if correct then W sends $(G_1, \ldots, G_k) = (E_1 \oplus F_1, \ldots, E_k \oplus F_k)$ to A and the protocol continues.

However, if W is able to break the security of E this time, then W can impersonate A by sending messages M and B will believe they originate from A. So, depending of how the protocol is used, the assumption that E is secure has different consequences.

The reader could correctly remark that A is able to send subliminal information at the moment of publication of n, R_j (her public key) by choosing them specially . However these keys are constant, so the subliminal information that they can contain is strongly limited. In case the warden nevertheless worries about it, he is able to eliminate this danger in a similar way as we proceed in Section V. (for more details see [4]).

V. SUBLIMINAL-FREE SIGNATURES

The idea is to make the Goldwasser–Micali–Rivest signature system subliminal-free. We use the same notations as in [15].

To make the signature subliminal free the warden has to guarantee that *all* the R_j, which are used in [15], are truly random. This can be obtained using the commitment idea. Before A starts to use her signature system, W has to be convinced (using zero-knowledge) that n has the appropriated form. To sign the j^{th} message M, the following protocol is used:

Step 1 A chooses a (random) quadratic residue R'_j (mod n) and random K and sends $h_K(R'_j)$ as commitment to W, together with the message M.

Step 2 W chooses a truly random quadratic residue R''_j (mod n) and sends it to A.

Step 3 A calculates $R_j = R'_j \times R''_j \pmod{n}$ and uses this R_j in the same way as in [15]. Then A reveals her R'_j and K and sends the signature α_j and the necessary authenticator (L_j) to the warden.

Step 4 W (the warden) checks R'_j, the authenticator(s) and the signature. He also checks if the Jacobi symbols $(\alpha_j \mid n) = (L_j \mid n) = 1$. *If* one of these does not correspond, *then* the warden halts the protocol, *else* he sends (or publishes) M, the authenticator(s) multiplied by ± 1 and the signature multiplied by ± 1. The warden stores the updated authentication tree, with the ± 1 that he used.

The same idea can be used to guarantee that R_0, which is a part of the public key of A, is subliminal-free. A is still able to send subliminal information in her public key n, by publishing a special n. It is theoretical possible to avoid this problem, however the implementation is involved (see [4]).

VI. PRACTICAL ASPECTS

The first protocol discussed in Section IV. is easy to set-up. In case of verification of treaty or international bank communications, the host country can be the warden. The example of international bank communications is important from a commercial point of view. Indeed several banking organizations with international activities frequently face the problem that they are not allowed to use encryption to protect the privacy of their messages. Subliminal-free authentication would make their communications more secure without security objections from the corresponding countries where the banks operate. Subliminal-free authentication can be used in identification systems. By authenticating messages as: "I, A, am at the moment in Town, Street, House Number, Floor, ...", describing the exact location of A and B, more secure identification systems can be made [5, pp. 154–155]. Making authentication systems subliminal-free, makes the use of it for identification more attractive. Many other applications exist.

It is easy to adapt the first protocol in order to work with *two* wardens, not trusting each other. This allows the phone companies to act as warden in national and in international communications. The other protocols can also be adapted to have two wardens, but the protocols become then more involved.

The speed of the protocols can be compared with the speed of RSA, if several tricks are used. Ideas as described in [9] can be used. Remark in this context that the R_j are constants, so A can significantly speed up the calculations of $f_M^{-1}(\pm R_j)$, nevertheless that M is not constant. Hereto she has to store some values (more details will be given in the final paper). A also can speed up the calculation of X using her knowledge of $\phi(n)$.

Much faster subliminal-free authentication and signature systems can be made partially based on [7,8]. However these schemes have also disadvantages. Full details will be given in final paper.

VII. CONCLUSION

The problem of making subliminal-free authentication and signature systems, which was open for five years, is now solved. The applications of subliminal-free authentication go from verification of treaty to international banking communications. One can expect that in the near future more practical subliminal-free authentication and signature schemes will be presented using less interactions. The impact that non-interactive zero-knowledge [3] can have on such improvements has to be investigated.

REFERENCES

[1] J. A. Adam. Ways to verify the U.S.-Soviet arms pact. *IEEE Spectrum*, pp. 30–34, February 1988.

[2] M. Blum. Coin flipping by telephone – a protocol for solving impossible problems. In *digest of papers COMPCON82*, pp. 133–137, IEEE Computer Society, February 1982.

[3] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth ACM Symp. Theory of Computing, STOC*, pp. 103 – 112, May 2–4, 1988.

[4] Y. Desmedt. Abuses in cryptography and how to fight them. August 1988. To be presented at Crypto'88.

[5] Y. Desmedt. Major security problems with the "unforgeable" (Feige–)Fiat–Shamir proofs of identity and how to overcome them. In *Securicom 88, 6th worldwide congress on computer and communications security and protection*, pp. 147–159, SEDEP Paris France, March 15–17, 1988.

[6] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat–Shamir passport protocol. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto'87 (Lecture Notes in Computer Science 293)*, pp. 21–39, Springer–Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.

[7] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *Proceedings of the Nineteenth ACM Symp. Theory of Computing, STOC*, pp. 210 – 217, May 25–27, 1987.

[8] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 186–194, Springer–Verlag, 1987. Santa Barbara, California, U. S. A., August 11–15.

[9] O. Goldreich. Two remarks concerning the Goldwasser–Micali–Rivest signature scheme. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 104–110, Springer–Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15, 1986.

[10] O. Goldreich, S. Micali, and A. Wigderson. How to prove all NP statements in zero-knowledge and a methodolgy of cryptographic protocol design. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 171–185, Springer–Verlag, 1987. Santa Barbara, California, U. S. A., August 11–15.

[11] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In *The Computer Society of IEEE, 27th Annual Symp. on Foundations of Computer Science (FOCS)*, pp. 174–187, IEEE Computer Society Press, 1986. Toronto, Ontario, Canada, October 27–29, 1986.

[12] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2), pp. 270–299, April 1984.

[13] S. Goldwasser, S. Micali, and C. Rackoff. Knowledge complexity of interactive proofs. In *Proc. 17th STOC*, pp. 291–304, 1985.

[14] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *Siam J. Comput.*, 17(2), pp. 281–308, April 1988.

[15] S. Goldwasser, S. Micali, and R. Rivest. A paradoxical solution to the signature problem. In *Proceedings of 25th Symp. on Foundation of Computer Science*, pp. 441–448, 1984.

[16] G. J. Simmons. *Message Authentication Without Secrecy*, pp. 105–139. AAAS Selected Symposia Series 69, Westview Press, 1982.

[17] G. J. Simmons. The prisoners' problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology. Proc. of Crypto 83*, pp. 51–67, Plenum Press N.Y., 1984. Santa Barbara, California, August 1983.

[18] G. J. Simmons. The secure subliminal channel (?). In H. C. Williams, editor, *Advances in Cryptology. Proc. of Crypto 85 (Lecture Notes in Computer Science 218)*, pp. 33–41, Springer–Verlag, 1986. Santa Barbara, California, August 18–22, 1985.

[19] G. J. Simmons. The subliminal channel and digital signatures. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology. Proc. of Eurocrypt 84 (Lecture Notes in Computer Science 209)*, pp. 364–378, Springer–Verlag, Berlin, 1985. Paris, France, April 9–11, 1984.

[20] G. J. Simmons. Verification of treaty compliance–revisited. In *Proc. of the 1983 IEEE Symposium on Security and Privacy*, pp. 61–66, IEEE Computer Society Press, April 25–27 1983. Oakland, California.

[21] H. C. Williams. A modification of the RSA public–key encryption procedure. *IEEE Trans. Inform. Theory*, 26(6), pp. 726 - 729, November 1980.