A weakness in authenticated encryption schemes based on Tseng et al.'s schemes

L. Hernández Encinas[1]*, A. Martín del Rey[2]
and J. Muñoz Masqué[1]

[1] *Dpt. Information Processing and Coding, Institute of Applied Physics, CSIC*

C/ Serrano 144, E28006-Madrid, Spain. Emails: {luis, jaime}@iec.csic.es

[2] *Dpt. of Applied Mathematics*, *University of Salamanca, E.P.S.*

C/ Hornos Caleros 50, E05003-Ávila, Spain. Email: delrey@usal.es

Abstract

Tseng *et al.* have introduced in 2003 an authenticated encryption scheme by using self-certified public keys. Based on this scheme several authors have proposed new signature schemes avoiding some attacks against the original proposal. In this paper we show that there is a weakness on all these schemes affecting both the authentication of the signer's public key and the own security of the system. We propose a slight but necessary modification to these schemes in order to avoid that weakness.

Keywords: Authenticated encryption, Cryptanalysis, Cryptography, Digital signature, Self-certified public key.

1 Statement of results and cryptanalysis

As is well known, in self-certified public keys (see [3]) the public key of an user is obtained from his identity and his private key, such that it is signed by the

*Corresponding author: luis@iec.csic.es, Tel: (+34) 915618806, Fax: (+34) 914117651.

system authority by means of system's private key. In this way, the authentication of the public key can be carried out with the signature verification and no certificate to authenticate the signer is necessary. Moreover, in authenticated encryption schemes (see [4, 6, 7]) the digital signature of a message is generated by the sender such that only a specified receiver can recover the message and verify the signature of the sender.

In [1, 5, 9, 10, 11, 12, 13], the authors have proposed some new signature schemes for self-certified public keys. We have detected a weakness on these schemes affecting both the authentication of the signer's public key and the own security of the system.

In fact, the hash function used in all these schemes $m \mapsto h(m)$ must satisfy the additional condition $\gcd(h(m), \phi(n)) = 1$, where $n = pq$ is the modulus of the scheme, $p = 2p' + 1$, $q = 2q' + 1$ are two secret 1-safe prime numbers, and $\phi(n)$ denotes totient Euler's function. This is necessary in order $h(m)$ to admit an inverse modulo $\phi(n)$, which is essential to generate and to verify the key public of each user. This condition does not hold with the only assumption imposed by the authors, namely $h(m) < \min(p', q')$ for every m, as it assures only that $\gcd(h(m), p'q') = 1$, but the hash may be an even number and then, $\gcd(h(m), \phi(n)) = \gcd(h(m), 4p'q')$ could be 2 or 4. In that case, the system can be broken as proved in the following

Proposition. *With the same notations and hypotheses as above, if*

$$\gcd(h(m), \phi(n)) \geq 2$$

for an input string m, then n can be factored efficiently.

Proof. From the assumption in the statement, we obtain $h(r) = 2^{\nu} l$ with $\nu \in \{1, 2\}$, l being an odd integer and $r = Mg^{-k} \bmod n$, where M is the message, k is a random integer, and g is an integer of order $p'q'$ in $\mathbb{Z}_n^*$.

Let

$$y_U \equiv (f_U - I_U)^{\frac{1}{h(I_U)} \bmod \phi(n)} \bmod n \qquad (1)$$

be the public key of the user U, where I_U is the identity of U, and $f_U = g^{x_U} \bmod n$, x_U being the private key of U.

By virtue of the hypothesis, the equation

$$u^{h(r)} - f_U^{h(r)} \equiv 0 \bmod n, \quad u, v \in \mathbb{Z},$$

has four different solutions: $u_i = y_i^{h(I_U)} + I_U$, $i = 1, \ldots, 4$, which correspond to the pairs

$$\begin{aligned} &(f_U \bmod 4, f_U \bmod p'q'), \quad (f_U \bmod 4, -f_U \bmod p'q'), \\ &(-f_U \bmod 4, f_U \bmod p'q'), \quad (-f_U \bmod 4, -f_U \bmod p'q'), \end{aligned}$$

in the isomorphism $\mathbb{Z}_n = \mathbb{Z}_4 \times \mathbb{Z}_{p'q'}$ as follows from the Chinese Remainder Theorem. Let us assume that $u_1 = y_U^{h(I_U)} + I_U$ and $u_2 = -u_1$. Then, the following equations hold:

$$\begin{aligned} \gcd\left(\left(y_i^{h(I_i)} + I_U\right)^l - f_U^l, n\right) &= p, \\ \gcd\left(\left(y_i^{h(I_i)} + I_U\right)^l + f_U^l, n\right) &= q, \end{aligned}$$

for $i = 3, 4$. □

Furthermore, if $h(r)$ is even, then the authentication of the public key fails, as there are four candidates for it, precisely y_i, $i = 1, \ldots, 4$.

2 An Example

We can consider an example in order to illustrate this weakness.

Let $p = 503 = 2 \cdot 251 + 1$, $q = 227 = 2 \cdot 113 + 1$ be two 1-safe prime numbers. Then $n = p \cdot q = 114181$, and $\phi(n) = 113452$. We suppose that the identity of a user U is $I_U = 84314$, and let $g = 104$ be an element of order $p' \cdot q' = 28363$ in $\mathbb{Z}_{114181}^*$. If the private key of U is $x_U = 64170$, then $f_U = g^{x_U} \bmod n = 86289$. Moreover, suppose that $h(r) = 28$, $h(I_U) = 49$, and $h\left(I_U\right)^{-1} \bmod \phi(n) = 53253$.

The public key of U is computed by the system authority from equation (1):

$$y_U = (86289 - 84314)^{53253} \bmod 114181 = 19758.$$

The verification of this public key is immediate since

$$\begin{aligned}\left(y_U^{h(I_U)}+I_U\right) \bmod n &= \left(19758^{49}+84314\right) \bmod 114181 = 86289\\ &= g^{x_U} \bmod n = 104^{64170} \bmod 114181.\end{aligned}$$

Now, we suppose that the user U wants to sign the message $M = 48924$. Then U chooses $k = 96230$ at random and computes his signature for M as follows:

$$\begin{aligned} r &= M\cdot g^{-k} \bmod n = 48924\cdot 104^{-96230} \bmod 114181 = 106361,\\ s &= k - x_U\cdot h(r) = 96230 - 64170\cdot 28 = -1700530.\end{aligned}$$

From the signature $(r,s) = (106361, -1700530)$, any user can recover the original message by computing

$$\begin{aligned}&\left(r\cdot g^s\cdot\left(y_U^{h(I_U)}+I_U\right)^{h(r)}\right) \bmod n\\ &= \left(106361\cdot 104^{-1700530}\cdot\left(19758^{49}+84314\right)^{28}\right) \bmod 114181 = 48924 = M.\end{aligned}$$

Nevertheless, the equation

$$\left(y^{h(I_U)}+I_U\right)^{h(r)} \equiv f_U^{h(r)} \bmod n,$$

has more than one solution. In fact, the solutions to the equation

$$\left(y^{49}+84314\right)^{28} - 86289^{28} \equiv 0 \bmod 114181$$

are

$$y_1 = 19758,\quad y_2 = 33842,\quad y_3 = 51765,\quad y_4 = 65849,$$

and all of them permit to recover the original message, in spite of the fact that only the first solution, $y_1 = y_U$, is the true public key of the user U:

$$\left(106361\cdot 104^{-1700530}\cdot\left(y_i^{49}+84314\right)^{28}\right) \bmod 114181 = 48924,\quad i = 1,\dots,4.$$

Moreover, in this situation, it is possible to factor the modulus n efficiently:

$$\begin{aligned}\gcd\left(\left(\left(y_j^{49}+84314\right)^7 - 86289^7\right) \bmod 114181, 114181\right) &= 503 = p,\\ \gcd\left(\left(\left(y_j^{49}+84314\right)^7 + 86289^7\right) \bmod 114181, 114181\right) &= 227 = q,\end{aligned}$$

where $j = 2, 3$.

3 Analysis of the distinct proposals

Below, we analyse the different improvements and variants of the original scheme [11] introduced in [1, 5, 9, 10, 12, 13].

1. In [11, Theorems 1 and 2] and in the proof of [11, Theorem 3] the authors state that the public key y_i is verified indirectly, which is not correct if $h(r)$ is even.

2. The same happens in the proposal of [12], since the authors do not modified this point in the Tseng-Jan-Chien original schemes.

3. The previous analysis also applies the the item 3 in the message recovery phase in [9, Section].

4. Similarly, in the Properties 1, 2, and 3 in [1, Section 4] the equation $p_i = (y_i - d_i)^{h(d_i)^{-1}} \bmod n$ has no meaning if $h(d_i)$ is even. The same happens in the improved scheme of [1] proposed in [13] because both systems have the same initialization phase.

5. Finally, in [5, 10] the authors do not explain how the public key is verified explicitly, but the equation to solve is the same as above and hence the same reasoning can be applied.

4 Conclusions

We have seen that if the hash function $h(\cdot)$ is not relatively prime to $\phi(n)$, then the modulus n can be factored. The condition $h(m) < \min(p', q')$ does not suffice to assure that $\gcd(h(m), \phi(n)) = 1$. It is also necessary $h(m)$ to be an odd integer for all m. If $h(m)$ is not odd, then the security of the self-certified public keys schemes proposed in the references, is compromised. Moreover, the authentication of the public key can be checked with probability 0.25 only.

The solution is simple: one must consider the hash function $h(m) = 2H(m)+1$, where $H(\cdot)$ is either SHA1 ([2]) or MD5 ([8]) hash functions, which increases the number of bits of $h(\cdot)$ by one at most.

Acknowledgements

This work has been partially supported by Ministerio de Educación y Ciencia (Spain) under grant SEG2004-02418.

References

[1] Y.F. Chang, C.C. Chang, and H.F. Huang, Digital signature with message recovery using self-certified public keys without trustworthy system authority, *Appl. Math. Comput.*, vol. 161, pp. 211–227, 2005.

[2] Federal Information Processing Standard Publication 180-1, *Secure hash standard*, US Department of Commerce/NIST, National Technical Information Service, Springfield, VI, April 17, 1995.

[3] M. Girault, "Self-certified public keys, in Advances in Cryptology—EUROCRYPT'91, Lecture Notes in Comput. Sci. 547, D.W. Davies (Ed.), Springer, Berlin, pp. 490–497, 1991.

[4] P. Hoster, M. Michels, and H. Petersen, Authenticated encryption schemes with low commuincation costs, *Elect. Lett.*, vol. 30, pp. 1212–1213, 1994.

[5] S.J. Hwang, Improvement of Tseng et al's authenticated encryption scheme, *Appl. Math. Comput.*, vol. 165, pp 1–4, 2005.

[6] M.S. Hwang, and C.Y. Liu, Authenticated encryption schemes: Current status and key issues, *Inter. J. Network Security*, vol. 1, no. 2, pp. 61–73, 2005.

[7] K. Nyberg, and R.A. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem, in Advances in Cryptology—EUROCRYPT'94, Lecture Notes in Comput. Sci. 950, A. de Santis (Ed.), Springer, Berlin, pp. 182–193, 1995.

[8] R.L. Rivest, RFC 1321: The MD5 message-digest algorithm, Internet Request for Comments 1321, Rump session of Crypto'91, April, 1992.

[9] Z. Shao, Improvement of digital signature with message recovery using self-certified public keys and its variants, *Appl. Math. Comput.*, vol. 159, pp. 391–399, 2004.

[10] C.S. Tsai, S.C. Lin, and M.S. Hwang, Cryptanalisis of an authenticated encryption scheme using self-certified public keys, *Appl. Math. Comput.*, vol. 166, pp. 118-122, 2005.

[11] Y.M. Tseng, J.K. Jan, and H.Y. Chien, Digital signature with message recovery using self-certified public keys and its variants, *Appl. Math. Comput.*, vol. 136, pp. 203–214, 2003.

[12] Q. Xie, and X.Y. Yu, Cryptanalysis of Tseng et al.'s authenticated encryption schemes, *Appl. Math. Comput.*, vol. 158, pp. 1–5, 2004.

[13] J. Zhang, W. Zou, D. Chen, and Y. Wang, On the security of a digital signature with message recovery using self-certified public key, *Informatica*, vol. 29, pp. 343–346, 2005.