Cryptanalysis of publicly verifiable authenticated encryption

Zuhua Shao
Department of Computer and Electronic Engineering
Zhejiang University of Science and Technology
Hangzhou, Zhejiang, P. R. of China, 310012
Email: zhshao_98@yahoo.com

Abstract: Ma and Chen proposed a new authenticated encryption scheme with public verifiability. This scheme requires less computational costs and communication overheads than the conventional signature-then-encryption approaches. In this letter, we show that the Ma-Chen scheme does not satisfy three security properties: unforgeability, confidentiality and non-repudiation.

Introduction: For electronical commercial applications, evidence of possession of documents is especially important. A digital signature is analogous to an ordinary hand-written signature and establishes both of signer authenticity and data integrity assurance. However, it is necessary to keep commercial documents confident to protect the privacy of users in many applications.

One simple way to implement such authenticated encryption scheme is to sign and encrypt message separately, first-sign-then-encrypt or first-encrypt-then-sign. This way perhaps results in separation of signature and ciphertext. Other way is to combine signature and encryption together in order to reduce the amount of computational cost and communication overheads.

In 1997, Zheng proposed two new combined schemes [1], called signcryption scheme, in which message encryption and digital signature are simultaneously fulfilled in a logically single step. Besides some security shortcomings [2, 3], the Zheng schemes are not efficient as a zero-knowledge proof is required in its non-repudiation protocol.

Recently, Ma and Chen proposed a new authenticated encryption scheme with public verifiability [4]. They claimed that their scheme is as efficient as the Zheng signcryption schemes with respect to both computational costs and communication overheads. In addition, their scheme has an efficient non-repudiation procedure without using a zero-knowledge proof protocol. Ma and Chen further claimed that their scheme satisfy three security properties: unforgeability, confidentiality and non-repudiation.

In this letter, we would show the Ma-Chen scheme is not only erroneous but also insecure. The honest receiver cannot convince the judge that the valid signature is signed by the true signer, while the dishonest receiver can deceive the judge into believing the forged signature of any message. Moreover, if the scheme is adapted for the case of a long message, it cannot withstand the known plaintext-ciphertext attack.

Belief review of the Ma-Chen scheme:

Initially, two large primes p and q with $q|(p-1)$ and an element $g \in Z_p^*$ of order q are computed by a trusted third party (TTP for short) and are authenticated to each user. Each user $i \in \{A, B\}$ chooses a secret key $x_i \in Z_q^*$ and computes his public key $y_i = g^{x_i} \bmod p$. He publishes y_i which is

certified by the TTP and keeps x_i secret. In addition, the TTP chooses a public one way hash function H with $|H| < |p|$, where $|x|$ denotes the number of bits in x and $|H|$ denotes the number of bits in the output value of hash function H. To send a message $m \in Z_p^*$, Alice does the following:
(A-1) picks a random number $k \in Z_q^*$
(A-2) computes $v = (g \cdot y_B)^k \bmod p$ and $e = v \bmod q$
(A-3) computes $c = m \cdot (H(v))^{-1} \bmod p$
(A-4) computes $r = H(e, H(m))$
(A-5) computes $s = k - x_A \cdot r \bmod q$

Alice then sends (c, r, s) to Bob. After receiving (c, r, s), Bob does the following:

(B-1) computes $v' = (g \cdot y_B)^s \cdot y_A^{r(x_B+1)} \bmod p$ and $e' = v' \bmod q$

(B-2) recovers the message $m = c \cdot H(v) \bmod p$
(B-3) verifies $r = H(e', H(m))$

For public verification, Bob computes

$$K_1 = (y_B^{\ s} \cdot y_A^{\ r \cdot x_B} \bmod p) \bmod q = (y_B^{\ k} \bmod p) \bmod q$$

and forwards $(H(m), K_1, r, s)$ to an arbitrary TTP. To verify that Alice is the originator of the encryption and signature, the TTP does the following:
(TTP-1) computes $e' = (g^s \cdot y_A^r \cdot K_1 \bmod p) \bmod q$
(TTP-2) verifies $r = H(e', H(m))$

The Ma-Chen scheme is best used for small message transmission, but it can be adapted for the case of a long message as follows. Alice partitions message m into $(|p| - 1)$-bit blocks $m_1, \ldots, m_t$ (uses padding if necessary), and she computes the ciphertext blocks $c_1, \ldots, c_t$ by $c_i = (m_i \oplus c^l{}_{i-1}) \cdot (H(v))^{-1} \bmod p$ (where $c^l{}_i$ denotes the most left $(|p| - 1)$ bits of c_i and $c_0 = v$) and r, s by (A-4) and (A-5), respectively. Alice then sends $(c_1, \ldots, c_t, r, s)$ to Bob. The rest of the scheme can be modified correspondingly.

Security considerations: Ma and Chen claimed that their scheme satisfies three security requirements: unforgeability, confidentiability and non-repudiation. But we would like to show that their claim is not correct.

Unforgeability: As Ma and Chen said, a dishonest receiver Bob is in the best position to forge signatures. Though we does not find ways for Bob to forge Alice's signature satisfying the verification procedure operated by Bob, we find that Bob can deceive any Trusted Third Party TTP into believing forged signatures. To forge the signature for any message m, Bob does the following:
(A'-1) picks two random numbers $e, s \in Z_q^*$
(A'-2) computes $r = H(e, H(m))$
(A'-3) computes $K_1 = e \cdot g^{-s} \cdot y_A^{-r} \bmod p$
and forwards $(H(m), K_1, r, s)$ to an arbitrary TTP. Obviously, the TTP cannot find this kind of

swindle.

Non-repudiation: Suppose that (*c, r, s*) is a valid signature of a message *m* sent from the signer Alice. After the honest receiver Bob validates it, Bob wants to convince any TTP in case of a dispute.

According to the non-repudiation procedure, for public verification, Bob computes

$$K_1 = ({y_B}^s \cdot {y_A}^{r \cdot x_B} \bmod p) \bmod q = ({y_B}^k \bmod p) \bmod q$$

and forwards ($H(m)$, K_1, *r, s*) to an arbitrary TTP. The TTP then computes $e' = (g^s \cdot {y_A}^r \cdot K_1 \bmod p) \bmod q$ and verifies $r = H(e', H(m))$.

We show that $e' \neq e$ by the following proof:

The triple (*c, r, s*) satisfies the equation:

$$v = (g \cdot y_B)^s \cdot {y_A}^{r(x_B+1)} \bmod p = (g^s \cdot {y_A}^r) \cdot ({y_B}^s \cdot {y_A}^{rx_B}) \bmod p$$

Let $a = (g^s \cdot {y_A}^r) \bmod p = u \cdot q + a_1$, $b = ({y_B}^s \cdot {y_A}^{rx_B}) \bmod p = v \cdot q + b_1$. $0 \le a_1, b_1 < q$.

Because $q|(p-1)$, $p = 1 \bmod q$

$$e = e' \Leftrightarrow (a \cdot b \bmod p) \bmod q = (a \cdot (b \bmod q) \bmod p) \bmod q$$

$$(a \cdot b \bmod p) \bmod q = ((u \cdot q + a_1)(v \cdot q + b_1) - w_1 \cdot p) \bmod q = (a_1 \cdot b_1 - w_1) \bmod q$$

where $w_1 = \lfloor (u \cdot q + a_1) \cdot (v \cdot q + b_1) / p \rfloor$, $\lfloor x \rfloor$ denotes the integer party of a real x.

$$(a \cdot (b \bmod q) \bmod p) \bmod q = ((u \cdot q + a_1) \cdot b_1 - w_2 \cdot p) \bmod q = (a_1 \cdot b_1 - w_2) \bmod q$$

where $w_2 = \lfloor (u \cdot q + a_1) \cdot b_1 / p \rfloor$.

Hence

$$e = e' \Leftrightarrow w_1 = w_2 \bmod q$$

$$\Leftrightarrow \lfloor (u \cdot q + a_1) \cdot v \cdot q / p + (u \cdot q + a_1) \cdot b_1 / p \rfloor = \lfloor (u \cdot q + a_1) \cdot b_1 / p \rfloor$$

In general, $(u \cdot q + a_1) \cdot vq = a \cdot (b - (b \bmod q)) > p$. If $p \mid (u \cdot q + a_1) \cdot v$, $w_1 = w_2 \bmod q$. However, it is impossible, since $(u \cdot q + a_1) < p$ and $v < p$.

Therefore, the honest receiver Bob cannot convince any TTP into believe a valid signature, since $e' \neq e$ in general.

The reason of inequality is (b mod q). One direct amendment is that $K_1 = ({y_B}^s \cdot {y_A}^{r \cdot x_B} \bmod p) \bmod q = ({y_B}^k \bmod p) \bmod q$ is replaced by

$$K_1 = ({y_B}^s \cdot {y_A}^{r \cdot x_B} \bmod p) = {y_B}^k \bmod p$$

However, this results in a new security problem. Any intruder can derive the Diffie –Hellman key K_{AB} from ($H(m)$, K_1, *r, s*) by computing:

$$K_{AB} = {y_A}^{x_B} = (K_1 \cdot {y_B}^{-s})^{r^{-1}} \bmod p$$

Then the intruder can compute session keys for all communications between Alice and Bob:

$$v = (g \cdot y_B)^s \cdot {y_A}^{r(x_B+1)} \bmod p = (g^s \cdot {y_A}^r) \cdot ({y_B}^s \cdot {k_{AB}}^r) \bmod p$$

Confidentiality: If the scheme is adapted for the case of a long message, it cannot withstand the known plaintext-ciphertext attack. Suppose that an intruder is given block plaintext m_i and the c_i and c_{i-1} are the corresponding ciphertext blocks. Thus he can compute $H(v) = (m_i \oplus c^l{}_{i-1}) \cdot c_i^{-1}$ mod p and further compute $m_j = (H(v) \cdot c_j) \oplus c^l{}_{j-1}$ mod p, $j = 2, \ldots, t$. Hence the intruder can decrypt all plaintext blocks except for the first block m_1.

If the first block m_1 is also given, the intruder can furthermore derive

$$v = c_0 = m_1 \oplus (H(v) \cdot c_1) \mod p$$

$$K_{AB} = v^{r^{-1}} \cdot (g \cdot y_B)^{-s \cdot r^{-1}} \cdot y_A{}^{-1} \mod p$$

If so, the intruder can derive all session keys between Alice and Bob only if signatures (*c, r, s*) are given.

Conclusion: Though Ma and Chen analysis the security properties of their scheme, we do not think so. We have showed that their scheme does not satisfy three security properties: unforgeability, confidentiality and non-repudiation. The honest receiver cannot convince the judge that the valid signature is signed by the true signer, while the dishonest receiver can deceive the judge into believing the forged signature of any message. Moreover, if the scheme is adapted for the case of a long message, it cannot withstand the known plaintext-ciphertext attack.

Acknowledgement: This work is A Project Supported by Scientific Research Fund of Zhejiang Provincial Education Department.

Reference

1. Y. Zheng: ‘Digital signcryption or how to achieve cost(signature + encryption) << cost(signature) + cost(encryption)’, LNCS 1294, *Advances in Cryptology – Crypto’97* (Springer, 1997), pp.165-179
2. H. Petersen and M. Michels: ‘Cryptanalysis and improvement of signcryption schemes’, *IEE Proc., Comput. Digi. Tech.*, 1998, Vol.145, (2), pp.149 –151
3. W. –H. He and T. –C. Wu: ‘Cryptanalysis and improvement of Petersen-Michels signcryption schemes’, *IEE Proc., Comput. Digi. Tech*., 1999, Vol.146, (2), pp.123 –124
4. C. Ma and K. Chen: ‘Public verifiable authenticated encryption’, *Electronics Letters,* 2003, Vol. 39, no.3, pp.281-282