TECHNICAL NOTE

Cryptanalysis and improvement of signcryption schemes

(Revised version)

H. Petersen
M.Michels

Indexing terms: Encryption, Signcryption, Cryptanalysis, Ciphers, Algorithms, Authenticity and confidentiality

Abstract: In 1997, two new schemes for authenticated encryption, called signcryption, have been proposed by Zheng. In this paper we point out a serious problem with these schemes. In fact, the way to gain nonrepudiation violates the confidentiality. Moreover, we compare the schemes to previously known authenticated encryption schemes, which were not mentioned by Zheng. Finally we outline a solution that overcomes the weakness.

1. Introduction

Authenticated encryption schemes should provide authenticity and confidentiality of sent messages. One way to implement such schemes is first to sign a message and then to encrypt it, called the *first-sign-then-encrypt* paradigm, the other is vice versa, called the *first-encrypt-then-sign* paradigm. Instances to both paradigms have been explicitly proposed [8,9,10], while [5] can be regarded as a mixture of both paradigms. The advantage of these approaches is that also nonrepudiation can be gained, as only the correct decryption must be proved. However, it must be taken care that the separation of the signature and the ciphertext is avoided.

Other schemes, which we call *combined* schemes in the following, try to reduce the amount of computation by gaining authenticity and confidentiality together [3,4,6]. However, these schemes do not gain nonrepudiation as pointed out in [9]. In practice, they are used to establish a session key and to authenticate a message, while the message is encrypted using the session key in a symmetric encryption scheme.

Recently, new combined schemes were proposed by Zheng [12], called *signcryption* schemes. It was claimed that authenticity, confidentiality and nonrepudiation was gained and the efficiency is superior to all schemes based on the paradigms mentioned above. In contrast to other combined schemes, the use of a symmetric cipher is included in the description explicitly.

In this paper, we describe the model, review Zheng's schemes and point out, why the confidentiality is lost under certain circumstances. As previous combined schemes are not mentioned in [12] we compare them and show their similarities. Finally, we outline how to overcome the weakness.

2. Model

An authenticated encryption scheme provides the following procedures:

- (probabilistic) *set-up algorithm SU*, that outputs the system parameters *P* used by all participants.
- (probabilistic) *key generation algorithm KG* which, on input the system parameters, returns a key pair (x, y) for a user.
- (probabilistic) *signature and encryption algorithm* $SE(m, x_S, y_R)$ which, on input the secret key x_S of the sender S, the public key y_B of the receiver R and a message m, returns an authenticated ciphertext c with respect to m.
- *decryption and verification algorithm* $DV(c, y_S, x_R)$ which on input x_R of the receiver, and the public inputs c and y_S outputs an 'alleged' message m', and convinces the receiver that m' is authenticated by the sender S and, if that is true, $m = m'$.
- *nonrepudiation protocol* $NR(m, c, y_S, y_R, x_R)$ which on secret input x_R of the receiver R, and on public inputs m, c, y_S, and y_R convinces a judge that m is the correctly decrypted message with respect to c, which is authenticated by the sender S.

To obtain a secure authenticated encryption scheme the following requirements must hold:

- *Authenticity*: There is no efficient algorithm that on input m, x_R, y_S and further public information returns a ciphertext c on an arbitrary message m with non-negligible probability, such that c is a ciphertext related to message m with respect to sender S and receiver R and m is authenticated by S.
- *Confidentiality*: There exists no efficient algorithm which, on input of the ciphertext c, the public keys y_S, y_R and further public information can decrypt the related cleartext m with non-negligible probability.

Additional *public information* is all information that is obtained by an attacker during previous protocol runs with different input parameters. Note, that the attacker is allowed to corrupt the receiver in order to

---

IEE Proceedings online no. 19981862

Paper first received 25th July and in revised form 22nd December 1997

H.Petersen is with r3 security engineering ag, Hofstrasse 98, CH-8620 Wetzikon, Switzerland

M.Michels is with Ubilab, UBS, Bahnhofstrasse 45, CH-8021 Zürich, Switzerland

destroy authenticity and the judge in order to destroy confidentiality for a message that is under dispute.

3. Review

We review the first system for authenticated encryption, called SCS1 [12].

1. *Initialization*: The trusted third party chooses two large primes $p, q \in \mathbf{P}$ with $q|(p-1)$, an element α of order q and a one-way function $h: Z_p^* \rightarrow Z_p^*$. These public parameters are authentic to all users.
2. *Key generation*: Each user $i \in \{A, B\}$ chooses a secret key $x_j \in Z_q^*$ and computes his public key $y_j := \alpha^{xj} \pmod p$. He publishes y_j which is certified by a trusted third party and keeps x_j secret. Let further denote E,D the encryption or decryption function, respectively, of a suitable symmetric encryption scheme.
3. *Signature generation and encryption*: The signer Alice chooses a random $k \in Z_q^*$ and computes $e := y_B^k \pmod p$. She splits e into K_1, K_2, e.g. using a hash function as $K_1||K_2:=h(e)$, and computes $r :=d(K_2,m)$, where d is a hash function, $s:=k\cdot(r+x_A)^{-1} \pmod q$, $c := E(K_1, m)$ and sends (c, r, s) to the receiver Bob.
4. *Decryption and signature verification*: Bob recovers e from r, s, α, p and x_B *as* $e := (y_A \cdot\alpha^r)^{s\cdot x_B} \pmod p$ and splits e into K_1, K_2, e.g. by $K_1||K_2:=h(e)$. Then he decrypts $m := D(K_1, c)$ and checks if $d(K_2, m) = r$.
5. *Non-repudiation*: Bob proves the correctness of a signature (c, r, s) on a message m by revealing e to a judge and proving that discrete logarithms of e to base $(y_A\cdot\alpha^r)^s$ and y_B to α are equal using the protocol in [1]. Additionally the judge computes $K_1||K_2:=h(e)$ and checks whether $r = d(K_2, m)$, $c = E(K_1, m)$ holds.

The second scheme, called SCS2, is very similar. It is claimed that both schemes are *unforgeable* and provide *nonrepudiatio*n as well as *confidentiality*.

4. Cryptanalysis

As mentioned in [12], Bob can choose a message himself and generate a corresponding tuple (c, r, s). Therefore, to gain nonrepudiation in case of a dispute, a judge must be convinced by the verifier Bob, that the signature was issued by the signer Alice. Bob can demonstrate this by proving that $e \equiv (y_A\cdot\alpha^r)^{s\cdot x_B} \pmod p$ holds. Therefore, he delivers e to the judge and gives a zero-knowledge proof that the discrete logarithm of y_B to base α is equal to the discrete logarithm of e to base $(y_A\cdot\alpha^r)^s$. Unfortunately, everybody knowing e, r, s and y_B can compute the value $K_{DH} := e^{s^{-1}}\cdot y_B^{-r} \equiv \alpha^{x_A\cdot x_B} \pmod p$. Then, for any ciphertext (c', r', s') this person is able to compute $e' := K_{DH}^{s'}\cdot y_B^{rs} \pmod p$, split it into K_1',K_2' and decrypt the message $m' := D(K_2', c')$.

Therefore, the judge can decrypt any further message after he was once convinced by Bob of the authenticity of a message sent by Alice. In other words, in order to gain nonrepudiation confidentiality is lost.

5. Previously known combined schemes

Several schemes for authenticated encryption are known, but not mentioned in [12]. We describe one scheme from the family of schemes proposed in section 7.1 of [4], and compare it to Zheng's scheme. It is obtained by substituting the general variables in [4] suitably (i.e. $A := rs$, $B := -r$, $C := 1$) and resembles in many points to the SCS1 scheme reviewed above. In order to simplify the comparison with SCS1 we add the encryption of the message with a symmetric cipher into the scheme, where $E(K,m)$ denotes the encryption of m and $D(K,c)$ denotes the decryption of c with respect to key K and $D(K,E(K,m))=m$ holds.

The initialization and key generation are the same as described above. To send a message m, sender Alice picks random $k \in Z_q^*$, $K \in Z_p^*$, and computes $c:= E(K, m||h(m))$, $e := h(y_B^k \pmod{p}, c))$, $r:=K\cdot e \pmod p$ and $s:= k\cdot(r + x_A)^{-1} \pmod q$. The values (c, r, s) are the signed ciphertext. They are sent to Bob, who can compute $e':=h(y_B^{r\cdot s}\cdot y_A^{s\cdot x_B} \pmod{p}, c)$, $K' := r\cdot e'^{-1} \pmod p$ and finally $m' := D(K', c)$. If $m'=m||h(m)$, he the signed ciphertext is considered as valid.[1]

Hence a combined scheme with communication overhead of $|p| + |q|$ bit is obtained. As the symmetric key K is usually smaller than $|q|$ bit, Alice can compute $r:=K\cdot e \pmod q$ (and hence Bob recovers $K := r\cdot e^{-1} \pmod q$) using the M mode according to the notion in [4]. This reduces the communication overhead to $2\,|q|$ bit. Another variant that leads to the same result was suggested in [6]. Compared to $|q| + |d(K_2, m)|$ bit communication overhead in SCS1 and using the parameter sizes suggested in [12] ($|q|=160$ bit and $|d(K_2, m)|=80$ bit), this leads to a difference of 10 byte (independent of the size of $|p|$) which is clearly negligible if m is large. The computational costs for the sender and the receiver is the same in both approaches. Hence we can conclude that Zheng's scheme offers *no advantages* compared to previous solutions.

6. Conclusion

Let us conclude with an outline how to gain nonrepudiation *without* loosing confidentiality. One simple approach is to prove the correct use of x_B in the decryption with a general zero-knowledge proof based on circuits without revealing e [7]. Another suggestion is that the judge is somehow trusted and therefore the attack does not work in that model. However, in both cases the benefits of the combined schemes over schemes based on the other paradigms are definitely lost. The first countermeasure is extremely inefficient and thus unacceptable even if we take into consideration that the dispute case happens quite rarely. The second countermeasure is unrealistic as well, as such a strong assumption is not necessary using the schemes on the first-sign-then-encrypt paradigm.

To overcome the problems in the SCS1 scheme we suggest an *alternative approach*: Let G be a finite group of order p and g be a generator of G of order p. We suggest to use $h(x) := g^x \in G$ to compute $K_1||K_2$, while the algorithms remain the same except for the nonrepudiation protocol. This works as follows: Given a signature (c, r, s), Bob computes and reveals

---

[1] In a previous version of this article the incorporation of a symmetric encryption scheme into the authenticated encryption scheme was done incorrectly, as e does not depend on c. The authors were made aware that this leads to some vulnerabilities, as the signature parameters r and s do not depend on the message m. Moreover, m instead of $m||h(m)$ is encrypted in the previous version, which causes problems if m does not satisfy a redundancy scheme.

$K=K_1||K_2$ as described above. In order to show that he computed K correctly he additionally gives a proof that $\log_z(\log_g(K))=\log_\alpha(y_B)\ (\mathrm{mod}\ q)$ with $z:=y_A^s\cdot\alpha^{r\cdot s}\ (\mathrm{mod}\ p)$ using a protocol in [11]. The other checks described above can be performed by the judge using this K.

Clearly, the price paid for the reasonable efficient nonrepudiation protocol is that the computational costs for signing/encrypting and verifying/decryption increases, as an additional exponentiation in G is needed to compute g^x .

References

1 CHAUM, D.: ‘Zero-knowledge undeniable signatures', LNCS 473, Advances in Cryptology - Eurocrypt '90, Springer, 1991, pp. 458-464.

3 HORSTER, P., MICHELS, M., PETERSEN, H.: ‘Authenticated encryption schemes with low communication costs', *Electronics Letters*, Vol. 30, No. 15, July, 1994, pp. 1230-1231.

4 HORSTER, P., MICHELS, M., PETERSEN, H.: ‘Meta-Message recovery and Meta-blind signature schemes based on the discrete logarithm problem and their applications', LNCS 917, Advances in Cryptology - Asiacrypt '94, Springer, 1995, pp. 224 - 237.

5 KOHNFELDER, L.M.: ‘On the signature reblocking problem in public key cryptosystems', *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 179.

6 LEE, W.-B., CHANG, C.-C.: ‘Authenticated encryption scheme without using a one way function', *Electronics Letters*, Vol. 31, No. 19, September, 1995, pp. 1656-1657.

7 GOLDREICH, O., MICALI, S., WIGDERSON, A.: ‘How to prove all NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design', LNCS 264, Advances in Cryptology - Crypto '86, Springer, 1987, pp. 171-185.

8 NYBERG, K., RUEPPEL, R.: ‘Message recovery for signature schemes based on the discrete logarithm problem', LNCS 950, Advances in Cryptology - Eurocrypt '94, Springer, 1994, pp. 182 - 193.

9 NYBERG, K., RUEPPEL, R.: ‘Message recovery for signature schemes based on the discrete logarithm problem', *Designs, Codes and Cryptography*, 7, 1996, pp. 61 - 81.

10 RIVEST, R.L., SHAMIR, A., ADLEMAN, L.: ‘A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.

11 STADLER, M.: ‘Publicly verifiable secret sharing', LNCS 1070, Advances in Cryptology - Eurocrypt'96, Springer, 1996, pp. 190-199.

12 ZHENG, Y.: ‘Digital Signcryption or How to achieve Cost(Signature + Encryption) « Cost(Signature) + Cost(Encryption)', LNCS 1294, Advances in Cryptology - Crypto'97, Springer, 1997, pp. 165-79.

13 ZHENG, Y.: ‘Signcryption and its application in efficient public key solutions', Proc. of 1997 Information Security Workshop (ISW'97), LNCS, Springer, 1997.