On the Authentication of One Popular Signcryption Scheme

Zhengjun Cao

Department of Mathematics, Shanghai University,

Shanghai, China, 200444. caozhj@shu.edu.cn

Abstract Whether a recipient *can prove* a signature to others is of great importance. The function is just one reason that we call a signature "signature" rather than others. In this paper, we point out that one popular signcryption signature convinces *only* the designated document's recipient that the signer deliberately signed the document. The *designated recipient* can *check* the validity of a given signcryptext but *cannot prove* it to others. We also improve it using the efficient technique developed in Schnorr's signature instead of a zero-knowledge proof such that the receiver can *check* the validity of a given signcryptext and *can prove* it to a third party.

Keywords signcryption, universal authentication, restrictive authentication, designated authentication.

1 Introduction

Message authenticity (corroboration of the identity of an entity) is an important goal of cryptography, which was realized by the advent of digital signatures. Message confidentiality (keep information secret from all but those who are authorized to see it) is another important goal of cryptography. In 1997, Zheng [8] proposed a cryptographic scheme called signcryption which integrates the functionality of discrete log based public key encryption and digital signature schemes in a very efficient way without sacrificing each scheme's security. Although Zheng's signcryption scheme has been the focus of a number of research works, no reductionist-style security analysis of Zheng's signcryption has ever been given. In 2007, Baek et al [1] gave a formal proof for the security of signcryption. They showed that Zheng's signcryption scheme [8] is secure in their confidentiality model and is secure in their unforgeability model. Their model does not explicitly include support for non-repudiation, that is, the ability of a receiver of a valid signacryptext to convice a third party that a given sender has sent this signcryptext. They also pointed out that non-repudiation can always be achieved using a protocol run between the receiver and the third party, which convinces the third party of the validity of a signcryptext with respect to a given message and sender and receiver public keys. A generic solution which does not compromise the receiver's secret key to the third party, is to use a zero-knowledge proof of signcryptext validity.

In this paper, we classify signatures into three kinds according to the characteristics of the document's recipient. We then show that Zheng's signcryption scheme is designated-authentic. That means a signcryption signature convinces *only* the designated document's recipient that the signer deliberately signed the document. In the case, the *designated recipient* can *check* the validity of a given signcryptext but *cannot prove* it to others. We then improve it using the efficient technique developed in Schnorr's signature instead of using a zero-knowledge proof. The *designated recipient* can *check* the validity of a given signcryptext and *can prove* it to others in the improved scheme.

The rest of the paper is organized as follows. In Section 2, we classify signatures into three kinds according to the characteristics of the document's recipient. In Section 3, we review and analyze the Zheng's signcryption scheme. In Section 4, we improve the Zheng's signcryption such that the designated recipient can *check* the validity of a given signcryptext and *can prove* it to others. Some conclusion remarks are given in Section 5.

2 Different authentications of signatures

The essential security requirements for digital signatures can be described as follows [3].

1. Authentication. The signature convinces the document's recipient that the signer deliberately signed the document.
2. Unforgeability. The signature is proof that the signer, and no one else, deliberately signed the document.
3. Non-repudiation. The signature and the document are physical things. The signer cannot later claim that he or she didn't sign it.

Note that the requirement of authentication does not definitely point out the characteristics of the document's recipient. Practically, signatures can be classified into three kinds according to the characteristics of the document's recipient, i.e., universal authentication signature, restrictive authentication signature and designated authentication signature.

A universal authentication signature convinces any document's recipient that the signer deliberately signed the document. In the case, *any recipient* can *check* the validity of a given signature and *can prove* it to others.

A restrictive authentication signature convinces the designated document's recipient that the signer deliberately signed the document. In the case, the *designated recipient* can *check* the validity of a given signature and *can prove* it to others. The signature is usually called a nominative signature [4].

A designated authentication signature convinces *only* the designated document's recipient that the signer deliberately signed the document. In the case, the *designated recipient* can *check* the validity of a given signature but *cannot prove* it to others. The signature is usually called a designated-verifier signature [2].

We insist that whether a recipient *can prove* a signature to others is of great importance. The function (transferability) is just one reason that we call a signature "signature" rather than others.

3 Review and analysis of Zheng's signcryption scheme

3.1 Review

The Zheng's signcryption scheme can be described as follows.

```
Common parameter/oracle generation GC($k$)
  Choose at random primes $p$ and $q$ such that $|p| = k, q > 2^{l_q(k)}$, and $q \mid (p-1)$
  ($l_q : \mathbb{N} \to \mathbb{N}$ is a function determining the length of $q$)
  Choose a random $g \in \mathbb{Z}_p^*$ such that $\mathrm{Ord}_p(g) = q$
  Choose a hash function $\mathcal{G} : \{0,1\}^* \to \{0,1\}^{l_\mathcal{G}(k)}$
  ($l_\mathcal{G} : \mathbb{N} \to \mathbb{N}$ is a function determining the length of the output of $\mathcal{G}$)
  Choose a hash function $\mathscr{H} : \{0,1\}^* \to \mathbb{Z}_q$
  Choose a bijective one-time symmetric key encryption scheme $\mathcal{SKE} = (E, D)$
  with message/key/ciphertext spaces $SPm/\{0,1\}^{l_\mathcal{G}}/SP_c$
  $cp \leftarrow (k, p, q, g, \mathcal{G}, \mathscr{H}, \mathcal{SKE})$
```

```
        Return $cp$

    Sender key-pair generation $\mathrm{GK}_A(cp)$
        $x_A \leftarrow \mathbb{Z}_q^*; y_A \leftarrow g^{x_A}$
        $sk_A \leftarrow x_A; pk_A \leftarrow y_A$
        Return $(sk_A, pk_A)$

    Receiver key-pair generation $GK_B(cp)$
        $x_B \leftarrow \mathbb{Z}_q^*; y_B \leftarrow g^{x_B}, sk_B \leftarrow x; pk_B \leftarrow y_B$
        Return $(sk_B, pk_B)$

    Signcryption $\mathrm{SC}(cp, sk_A, pk_B, m)$
        $x \leftarrow \mathbb{Z}_q^*; K \leftarrow y_B^x; \tau \leftarrow \mathcal{G}(K)$
        $c \leftarrow E_\tau(m); r \leftarrow \mathscr{H}(m, y_A, y_B, K);$
        If $r + x_A = 0$ Return $Rej$
        Else $s \leftarrow x/(r + x_A), C \leftarrow (c, r, s)$
        Return $C$

    Unsigncryption USC $(cp, sk_B, pk_A, C)$
        Parse $C$ as $(c, r, s)$
        $\omega \leftarrow (y_A g^r)^s; K \leftarrow \omega^{x_B}; \tau \leftarrow \mathcal{G}(K), m \leftarrow D_\tau(c)$
        If $\mathscr{H}(m, y_A, y_B, K) = r$ Return $m$
        Else Return $Rej$
```

In the full version of the signcryption scheme [8], Y. Zheng definitely pointed out that

> The signcryption scheme requires a repudiation settlement procedure different from the one for a digital signature scheme is required. In particular, the judge would need Bob's cooperation in order to correctly decide the origin of the message.

He also gave four possible repudiation settlement procedures, each requiring a different level of trust on the judge's side [8].

1. **With a Trusted Tamper-Resistant Device.** The tamper-resistant device would follow essentially the same steps used by Bob in unsigncrypting (c, r, s). The judge would then take the output of the tamper-resistant device as her decision. Note that in this case, Bob puts his trust completely on the device, rather than on the judge.
2. **By a Trusted Judge.** In this case, Bob simply presents to the the judge x_B together with other data items.

3. **By a Less Trusted Judge.** In this case, Bob and the judge engage in a zero-knowledge interactive/non-interactive proof/argument protocol (with Bob as a prover and the judge as a verifier), so that Bob can convince the judge of the fact that $K = ((y_A \cdot g^r)^s)^{x_B} \bmod p$ does have the right form.

4. **By any (Trusted/Untrusted) Judge.** The procedure uses techniques in zero-knowledge proofs/arguments and guarantees that the judge can make a correct decision, with no useful information on Bob's private key x_B being leaked out to the judge.

3.2 Analysis

In 2007, Baek et al [1] shew that Zheng's signcryption scheme [8] is secure in their confidentiality model and is secure in their unforgeability model. Their model does not explicitly include support for non-repudiation, that is, the ability of a receiver of a valid signacryptext to convice a third party that a given sender has sent this signcryptext. They also pointed out that non-repudiation can always be achieved using a protocol run between the receiver and the third party, which convinces the third party of the validity of a signcryptext with respect to a given message and sender and receiver public keys. A generic solution which does not compromise the receiver's secret key to the third party, is to use a zero-knowledge proof of signcryptext validity.

By the unsigncryption of Zheng's scheme, we know Bob cannot directly prove the signcryptext to a third party because the form

$$\mathscr{H}(m, y_A, y_B, (y_A g^r)^{s x_B}) = r$$

does not construct a challenge with respect to Alice's secret key x_A. As above mentioned, Bob should provide a zero-knowledge proof to convince the third party of the fact that

$$K = ((y_A \cdot g^r)^s)^{x_B} \bmod p$$

does have the right form. That means the unsigncryption should be fixed as follows

$$\begin{cases} \mathscr{H}(m, y_A, y_B, K) = r \\ \log_{(y_A \cdot g^r)^s} K = \log_g y_B \end{cases}$$

Precisely speaking, the original Zheng's signcryption scheme is neither

$$\text{Encryption} + \text{Universal authentication signature}$$

nor

$$\text{Encryption} + \text{Restrictive authentication signature}$$

instead

$$\text{Encryption} + \text{Designated authentication signature}$$

We know that whether a recipient *can prove* a signature to others is of great importance. The function (transferability) is just one reason that we call a signature “signature” rather than others. In view of this, a signcryption scheme should just be a restrictive authentication signature. Thus

$$\text{Signcryption} = \text{Encryption} + \text{Restrictive authentication signature}$$

4 Zheng's signcryption scheme revisited

4.1 Description of the improved scheme

To achieve the restrictive authentication in Zheng's scheme, it suffices to adopt the efficient technique developed in Schnorr's signature scheme. We now describe the improved scheme as follows.

```
Common parameter/oracle generation GC($k$) (See the original scheme)
Sender key-pair generation GK$_A$($cp$) (See the original scheme)
Receiver key-pair generation $GK_B(cp)$ (See the original scheme)
Signcryption SC($cp, sk_A, pk_B, m$)
  $x \leftarrow \mathbb{Z}_q^*; \rho \leftarrow g^x; K \leftarrow y_B^x$
  $\tau \leftarrow \mathcal{G}(K); c \leftarrow E_\tau(m)$
  $r \leftarrow \mathscr{H}(m, y_A, \rho, K)$
   If $r + x_A = 0$ Return $Rej$
  Else $s \leftarrow x/(r + x_A), C \leftarrow (c, r, s)$
   Return $C$

Unsigncryption USC ($cp, sk_B, pk_A, C$)
   Parse $C$ as $(c, r, s)$
   $\hat{\rho} \leftarrow (y_A g^r)^s; \hat{K} \leftarrow \hat{\rho}^{x_B}; \hat{\tau} \leftarrow \mathcal{G}(\hat{K}), \hat{m} \leftarrow D_{\hat{\tau}}(c)$
   If $\mathscr{H}(\hat{m}, y_A, \hat{\rho}, \hat{K}) = r$ Return $\hat{m}$
   Else Return $Rej$
```

Correctness.

$$\hat{\rho} = (y_A g^r)^s = g^{(x_A+r)s} = g^x = \rho$$
$$\hat{K} = \hat{\rho}^{x_B} = g^{x\,x_B} = y_B^x = K$$

4.2 Security

The proofs of confidentiality and unforgeability of the revisited scheme are the same as that of [1] As for the proof of the restrictive authentication of the presented scheme, it can be directly reduced to that of the Schnorr's signature [7].

The Schnorr's signature scheme employs a subgroup of order q in $\mathbb{Z}_p^*$, where p is some large prime number. The method also requires a hash function $\mathcal{H} : \{0,1\}^* \longrightarrow \mathbb{Z}_q$.

Public key p : a large prime. q : a large prime factor of $p-1$. g : a base element of order q mod p. $y :\ = \ g^x$ mod p.

Private Key $x \in \mathbb{Z}_q^*$.

Signing (1) Select a random secret integer $k \in \mathbb{Z}_q^*$. (2) Compute $e = g^k$ mod p, $r = \mathcal{H}(m||e)$, $s = xr + k$ mod q. (3) The signature for message m is the pair (r, s).

Verifying Accept it if and only if

$$\mathcal{H}(m||g^s y^{-r} \bmod p) = r$$

By the unsigncryption of the improved scheme, i.e.,

Parse C as (c, r, s)

$\hat{\rho} \leftarrow (y_A g^r)^s; \hat{K} \leftarrow \hat{\rho}^{x_B}; \hat{\tau} \leftarrow \mathcal{G}(\hat{K}), \hat{m} \leftarrow D_{\hat{\tau}}(c)$

Check $\mathscr{H}(\hat{m}, y_A, \hat{\rho}, \hat{K}) = r$

we know there is a true challenge with respect to the sender's secret key x_A.

In fact, compared the challenge

$$\mathscr{H}(\hat{m}, y_A, (y_A g^r)^s, \hat{K}) = r$$

with the challenge in the Schnorr's signature scheme, i.e.,

$$\mathcal{H}(m, g^s y^{-r}) = r$$

it's easy to find that there is no essential difference [5, 6]. Bob can either check the validity of the signcryptext or prove it to others that the sender deliberately signed the document.

5 Conclusion

In this paper, we point out that a signcryption is naturally equivalent to

Encryption + Restrictive authentication signature

This result is derived according to the characteristics of the document's recipient. Note that the original cryptographic primitive proposed by Y. Zheng is not fully interpreted. We also improve the Zheng's signcryption scheme by using the technique developed in Schnorr's signature. We stress that one reason we call a signature "signature" rather than others is that the recipient can prove it to a third party.

References

[1] J. Baek, R. Steinfeld and Y. Zheng, Formal Proofs for the Security of Signcryption, Journal of Cryptology, Vol. 20, Issue 2, pp.203-235.

[2] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated Verifier Proofs and Their Applications. Advances in Cryptology-Eurocrypt'96, LNCS 1070, Springer, pp.143-154.

[3] A. Menezes, P. Oorschot, S. Vanstone. Handbook of Applied Cryptography, CRC Press, 1996.

[4] S.J.Kim, S.J.Park and D.H. Won, Zero-knowledge nominative signatures, Proc. of PragoCrypt'96, International Conference on the Theory and Applications of Cryptology, pp.380-392.

[5] D. Pointcheval and J. Stern, Security proofs for signature schemes, Eurocrypt'96, LNCS 1070, Springer-Verlag, pp. 387-398.

[6] P. Paillier and D. Vergnaud, Discrete-log-based signatures may not be equivalent to discrete log, Asiacrypt 2005, LNCS 3788, Springer-Verlag, pp. 1-20.

[7] C. Schnorr. Efficient signature generation for smart cards, CRYPTO'89, Springer-Verlag, pp. 239-252.

[8] Y. Zheng, Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption), Advances in Cryptology – Crypto'97, LNCS 1294, Springer, pp.165-179. (full version, available at http://www.sis.uncc.edu/ yzheng/papers/.)