2009 International Conference on Computational Intelligence and Security

Different Authentication Properties and A Signcryption Scheme Revisited

Zhengjun Cao

Department of Mathematics,
Shanghai University, China
Département d'informatique,
Université Libre de Bruxelles. Belgium.
caozhj@yahoo.cn (or zhencao@ulb.ac.be)

Olivier Markowitch

Département d'informatique,
Université Libre de Bruxelles. Belgium.
Olivier.Markowitch@ulb.ac.be

***Abstract*—We put forward the concepts of universal authentication, restrictive authentication and designated authentication. We then revisit a popular signcryption scheme using a technique similar to the one developed in Schnorr's signature, allowing it respects the restrictive authentication property. Comparing with the modification suggested by Baek et al in 2007, which uses a zero-knowledge proof run between the recipient and the third party, our scheme saves about 1/2 cost. Besides, the security of the revisited scheme can be reduced to that of Schnorr's signature.**

***Keywords*-cryptography; universal authentication; restrictive authentication; designated authentication**

I. Introduction

Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation. The signature is authentic: it convinces the document's recipient that the signer deliberately signed the document. It must be verifiable: if a dispute arises about the origin of a signed document (caused by either a lying signer trying to repudiate his signature, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information (private key) [7]. Roughly speaking, the authentication is just the reason that we call a signature "signature".

Authentication is used (and often abused) in a very broad sense. It is one of the most important of all information security objectives. Until the mid 1970s, it was generally believed that secrecy and authentication were intrinsically connected. With the discovery of hash functions and digital signatures, it was realized that secrecy and authentication were truly separate and independent information security objectives.

In 1997, Zheng [17] 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. In 2007, Baek et al [1] gave a formal proof for the security of the signcryption scheme. They showed that Zheng's signcryption scheme [17] is secure in their confidentiality model and is secure in their unforgeability model. However, their model does not explicitly include support for the transferability of the non-repudiation, that is, the ability of a recipient of a valid signcryptext to convince 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 recipient and the third party, which convinces the third party of the validity of a signcryptext with respect to a given message and sender's and recipient's public keys. A generic solution which does not compromise the recipient's secret key to the third party, is to use a zero-knowledge proof of signcryptext validity.

In 1989, Schnorr [15] had constructed a well-known challenge based on the intractability of discrete logarithm problem and that of a cryptographic hash function in 1989. Its security has been proved in [12], [13]. Schnorr's signature is so efficient that it can be used for smart cards.

Our contributions. In this paper, we put forward the concepts of universal authentication, restrictive authentication and designated authentication. We then point out that Zheng's signcryption scheme respects the designated authentication property. We will revisit Zheng's scheme using a technique similar to the one developed in Schnorr's signature such that the recipient can prove the resulting signcryptext to a third party in an efficient way. Comparing with the modification suggested by Baek et al in 2007, which uses a zero-knowledge proof run between the recipient and the third party, our scheme saves about 1/2 cost. Besides, the security of the revisited scheme can be reduced to that of Schnorr's signature.

II. Different authentication properties of signatures

Generally, the essential security requirements for digital signatures can be described as follows [7].

978-0-7695-3931-7/09 $26.00 © 2009 IEEE
DOI 10.1109/CIS.2009.61

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 objects. The signer cannot later claim that he or she didn't sign it.

Notice that the requirement for authentication does not explicitly specify the ability of the document's recipient. Now we consider the following two situations.

1. Bob submits his academic record signed by the president of his university to a company. In this case, the content of signature is concerned with the verifier's privacy.
2. A voting center wants only a voter himself to be convinced that the vote he casted was counted.

Practically, the abilities of the documents's recipients in these situations are different. Further analysis of the abilities shows us that almost all signatures can be classified into the following three kinds, i.e., universal authentication signature, restrictive authentication signature and designated authentication signature.

(I) A universal authentication signature convinces any document's recipient that the signer deliberately signed the document. The *arbitrary recipient* can *check* the validity of a given signature and *can prove* it to a third party.

(II) A restrictive authentication signature convinces the designated document's recipient that the signer deliberately signed the document. The *designated recipient* can *check* the validity of a given signature and *can prove* it to a third party. The signature is usually called a nominative signature [9].

(III) A designated authentication signature convinces the designated document's recipient that the signer deliberately signed the document. The *designated recipient* can *check* the validity of a given signature but *cannot prove* it to a third party. The signature is usually called a designated-verifier signature [4].

We refer to [5], [6], [10], [11], [14], [16] for these signature models, definitions, requirements, and their applications. But we should point out that they have not formally clarified these different authentication concepts.

III. A SIGNCRYPTION SCHEME REVISITED

Message authenticity (corroboration of the identity of an entity) is an important objective realized by the advent of digital signatures. Message confidentiality is another important goal realized by the means of encryption schemes. In 1997, Zheng [17] 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.

A. Review of the signcryption scheme

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 $q \,|\, (p-1)$

($l_q : \mathcal{NN} \to \mathcal{N}$ is a function determining the length of q)

Choose a random $g \in \mathcal{Z}_p^*$ such that $\text{Ord}_p(g) = q$

Choose a hash function $\mathcal{G} : \{0,1\}^* \to \{0,1\}^{l_{\mathcal{G}}(k)}$

($l_{\mathcal{G}} : \mathcal{N} \to \mathcal{N}$ is a function determining the length of the output of $\mathcal{G}$)

Choose a hash function $\mathcal{H} : \{0,1\}^* \to \mathcal{Z}_q$

Choose a bijective one-time symmetric key encryption scheme $\mathcal{SKE} = (E, D)$, with message/key/ciphertext spaces $SPm/\{0,1\}^{l_{\mathcal{G}}}/SP_c$

$cp \leftarrow (k, p, q, g, \mathcal{G}, \mathcal{H}, \mathcal{SKE})$. Return cp.

Sender key-pair generation $\text{GK}_A(cp)$

$x_A \leftarrow \mathcal{Z}_q^*; y_A \leftarrow g^{x_A}$. $sk_A \leftarrow x_A; pk_A \leftarrow y_A$. Return (sk_A, pk_A).

Recipient key-pair generation $GK_B(cp)$

$x_B \leftarrow \mathcal{Z}_q^*; y_B \leftarrow g^{x_B}, sk_B \leftarrow x_B; pk_B \leftarrow y_B$. Return (sk_B, pk_B).

Signcryption $\text{SC}(cp, sk_A, pk_B, m)$

$x \leftarrow \mathcal{Z}_q^*; K \leftarrow y_B^x; \tau \leftarrow \mathcal{G}(K)$. $c \leftarrow E_\tau(m); r \leftarrow \mathcal{H}(m, y_A, y_B, K)$.

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

If $\mathcal{H}(\hat{m}, y_A, y_B, \hat{K}) = r$, return $\hat{m}$. Else Return Rej.

In the full version of the signcryption scheme [17], Y. Zheng definitely pointed out that: the signcryption scheme requires a repudiation settlement procedure different from the one for a digital signature scheme. 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 [17].

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.

B. Analysis of the signcryption scheme

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 show that Zheng's signcryption scheme is secure in their confidentiality model and is secure in their unforgeability model. Their model does not explicitly include support for the transferability of the non-repudiation, that is, the ability of a recipient of a valid signcryptext to convince 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 recipient and the third party, which convinces the third party of the validity of a signcryptext with respect to a given message and sender's and recipient's public keys. A generic solution which does not compromise the recipient'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 $\mathcal{H}(m, y_A, y_B, (y_A g^r)^{s\,x_B}) = r$ does not construct a challenge with respect to Alice's secret key x_A. As mentioned before, Bob should provide a zero-knowledge proof to convince the third party of the fact that $K = ((y_A \cdot g^r)^s)^{x_B} \bmod p$ has the right form. That means the unsigncryption should be as follows

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

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

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

nor

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

instead

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

Since the ability of a recipient to *prove* a signature to a third party is of great importance in practice, we suggest here an efficient way to transform the Zheng's signcryption scheme into a restrictive authentication signature.

C. The signcryption scheme revisited

Description. To achieve the restrictive authentication property in Zheng's scheme, it suffices to use the efficient technique developed in Schnorr's signature scheme. In 1989, Schnorr [15] constructed a challenge based on the intractability of discrete logarithm problem and that of a cryptographic hash function. Its security is credible [12], [13]. In addition, the cost of generating such a challenge is comparatively small [15].

We now describe the revisited signcryption scheme as follows.

Common parameter/oracle generation GC(k) (see the original description)

Sender key-pair generation $\text{GK}_A(cp)$ (see the original description)

Recipient key-pair generation $GK_B(cp)$ (see the original description)

Signcryption $\text{SC}(cp, sk_A, pk_B, m)$

$x \leftarrow \mathcal{Z}_q^*; \rho \leftarrow g^x; K \leftarrow y_B^x$. $\tau \leftarrow \mathcal{G}(K); c \leftarrow E_\tau(m)$. $r \leftarrow \mathcal{H}(m, y_A, \rho, K)$.

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

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

return $\hat{m}$. Else Return Rej.

Correctness.

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

Unforgeability. For simplicity, we make a comparative explanation.

(1) The change of replacing the y_A, y_B in the following equation

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

with any two public data z_A, z_B, such that it becomes

$$\mathcal{H}(m, z_A, z_B, (y_A g^r)^{s\,x_B}) = r$$

This does not alter the intractability of the challenge because y_A, y_B are simply viewed as padding.

(2) The revisited scheme replaces only the "padding" y_B with $(y_A g^r)^s$. Both y_B and $(y_A g^r)^s$ are reachable for an adversary. In addition, $(y_A g^r)^s$ binds (r, s) to the secret key x_A. However, the form $(y_A g^r)^{s\,x_B}$ indicates that only the recipient Bob can recover the last component of the hash function.

(3) In nature, for the designated verifier Bob, the following challenge

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

suffices to grantee the unforgeability. We refer to [1] for the further discussion.

Restrictive authentication. The restrictive authentication property of the revisited scheme is based on the universal authentication property of the Schnorr's signature [15].

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

[Setup] Public key. p : a large prime. q : a large prime factor of $p-1$. g : a base element of order q mod p. $y := g^x \bmod p$. The private key $x \in \mathcal{Z}_q^*$.

[Signing] (1) Select a random secret integer $k \in \mathcal{Z}_q^*$.

(2) Compute

$$e = g^k \bmod p,\ r = \mathcal{H}(m||e),\ s = xr + k \bmod q$$

(3) The signature for message m is the pair (r, s).

[Verifying] Accept it if and only if

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

Comparing the challenge in the revisited scheme, i.e.,

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

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

$$\mathcal{H}(m, g^s y^{-r}) = r \tag{1}$$

we know the challenge

$$\mathcal{H}(m, v_1, (y_A g^r)^s, v_2) = r \tag{2}$$

where v_1, v_2 are open data under the approvement of the designated recipient, is just a variation of Eq.(1) with respect to the secret key x_A, if we view v_1, v_2 as padding. There is no essential difference between them [12], [13]. The recipient can either check the validity of the signcryptext or prove it to a third party that the sender deliberately signed the document.

The thought behind the new construction can be depicted as below

$$\begin{aligned}&\mathcal{H}\,(m, y_A, (y_A g^r)^s, \Lambda) = r\\ &\qquad\longrightarrow \text{universal authentication}\\ &\mathcal{H}\,(m, y_A, (y_A g^r)^s, ((y_A g^r)^s)^{x_B}) = r\\ &\qquad\longrightarrow \text{restrictive authentication}\end{aligned}$$

where Λ is reachable for any recipient. The form $(y_A g^r)^s$ aims at binding (r, s) to the secret key x_A. If the signer Alice restricts the form of Λ such that it is of the form y_B^μ (where μ is randomly picked by Alice and is hidden in the pair (r, s)), then it cannot be verified without the approvement of the designated verifier Bob. Bob can recover y_B^μ by computing $((y_A g^r)^s)^{x_B}$. That is to say, the function of the form $((y_A g^r)^s)^{x_B}$ aims at designating a special verifier.

Efficiency. As for the efficiency of the new scheme, it definitely saves much costs of the original Zheng's signcryption scheme with an additional zero-knowledge proof, because it only adds an inputting component of the cryptographic hash function. In this case, the entire cost of the additional zero-knowledge proof is saved. As a whole, about 1/2 cost is saved if the cost of the additional zero-knowledge proof is equivalently viewed as that of the signcryption.

IV. Conclusion

In this paper, we classify cryptographic signatures into three kinds according to the recipient's ability, instead of the signer's ability. That means the result does not relate to proxy signature [8], blind signature [2], group signature [3] and so on. We suggest a signcryption scheme should satisfy *Encryption+Restrictive authentication signature*, and revisit the Zheng's signcryption scheme using the technique developed in Schnorr's signature.

Acknowledgment

National Natural Science Foundation of China (Project 60873227), Innovation Program of Shanghai Municipal Education Commission, Shanghai Leading Academic Discipline Project (S30104).

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] D.Chaum. Blind signatures for untraceable payments, In: *Advances in Cryptology-Crypto'82*, Springer-Verlag, 1983, 199-203.

[3] D.Chaum, E.van Heyst. Group signatures. In: *Advances in Cryptology‡EUROCRYPT'91*, vol. 547 of Lecture Notes in Computer Science, Springer, pp.257-265

[4] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated Verifier Proofs and Their Applications. In: *Advances in Cryptology-Eurocrypt'96*, vol. 1070 of Lecture Notes in Computer Science, Springer, 1996, pp.143-154

[5] D.Y. Liu, D.Wong, et al: Formal Definition and Construction of Nominative Signature. In: *Pro. Third International Conference on Information and Communications Security*, ICICS 2007, vol.4861 of Lecture Notes in Computer Science, Springer, pp.57-68

[6] H. Lipmaa, G. Wang, F. Bao: Designated Verifier Signature Schemes: Attacks, New Security Notions and a New Construction. In: *Proceedings of 32th International Colloquium on Automata, Languages and Programming (ICALP 2005)*, pp. 459-471

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

[8] M. Mambo, K. Usuda, E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. Fundamentals*, Sep. 1996, Vol. E79-A, No. 9, pp. 1338-1353

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

[10] E.Olio, O. Markowitch. Voting with Designated Verifier Signature-Like Protocol. In: *Pro. of the IADIS International Conference WWW/Internet 2004*, ICWI 2004, pp.295-301

[11] H. Park, I. Lee. A Digital Nominative Proxy Signature Scheme for Mobile Communication. *ICICS 2001*. vol.2229 of Lecture Notes in Computer Science, Springer, 2001, pp. 451-455

[12] D. Pointcheval and J. Stern. Security proofs for signature schemes. In: *Advances in Cryptology-Eurocrypt'96*, vol.1070 of Lecture Notes in Computer Science, Springer, 1996, pp. 387-398

[13] P. Paillier and D. Vergnaud, Discrete-log-based signatures may not be equivalent to discrete log. In: *Advances in Cryptology-Asiacrypt 2005*, vol.3788 of Lecture Notes in Computer Science, Springer, 2005, pp. 1-20

[14] S. Saeednia, S. Kremer, O. Markowitch. An Efficient Strong Designated Verifier Signature Scheme. In: *Pro. Third International Conference on Information and Communications Security*, ICISC 2003, vol.2971 of Lecture Notes in Computer Science, Springer, 2003, pp. 40-54

[15] C. Schnorr. Efficient signature generation for smart cards. In: *Advances in Cryptology-CRYPTO'89*, Springer, 1990, pp. 239-252

[16] G. Wang: Designated-Verifier Proxy Signature Schemes. In: *20th IFIP International Information Security Conference (SEC 2005)*. Kluwer, 2005, pp. 409-423

[17] Y. Zheng. Digital Signcryption or How to Achieve Cost(Signature & Encryption) $<<$ Cost(Signature) $+$ Cost(Encryption). In: *Advances in Cryptology-Crypto'97*, vol.1294 of Lecture Notes in Computer Science, Springer, 1997, pp.165-179.