Cryptanalysis and improvement of Petersen–Michels signcryption scheme

W.-H. He and T.-C. Wu

Abstract: Petersen and Michels showed that Zheng's signcryption schemes lose confidentiality to gain nonrepudiation. They also proposed another signcryption scheme modified from a signature scheme giving message recovery. The authors show that the Petersen–Michels scheme still violates the unforgeability property, and propose an improvement that overcomes the security leak inherent in the scheme. The improvement is as efficient as previous signcryption schemes with respect to both the computational cost and the communication overhead.

1 Introduction

At the Crypto'97 conference, Zheng [1] introduced a new type of cryptographic primitive termed 'signcryption', in which message encryption and digital signature are simultaneously fulfilled in a logically single step. Therefore, it requires less computational cost and less communication overhead than conventional signature-then-encryption approaches. Zheng also presented two signcryption schemes, called SCS1 and SCS2, developed respectively, from a ElGamal-based signature scheme [2] and a symmetric encryption/decryption scheme. Let 'signcrypted text' denote the result of a signcryption, 'signcrypter' the one who invokes the signcryption, and 'recipient' the one who is specified to receive the signcrypted text. Basically, a secure signcryption scheme should satisfy the following properties.

Unforgeability: It is computationally infeasible for an adaptive attacker to masquerade as the signcrypter in creating a signcrypted text.

Confidentiality: It is computationally infeasible for an adaptive attacker to find out any secret information from a signcrypted text.

Nonrepudiation: It is computationally feasible for a judge (who may be the arbiter of the system) to settle a dispute between the signcrypter and the recipient in an event where the signcrypter denies the fact that he is the sender of the signcrypted text to the recipient.

Petersen and Michels [3] showed that any secure signcryption scheme achieves the same goals as those provided by the authenticated encryption schemes [4–6]. They also showed that Zheng's SCS1 and SCS2 schemes lose confidentiality to gain nonrepudiation, and proposed another signcryption scheme modified from a signature scheme giving message recovery.

In this paper, we will show that the Petersen–Michels scheme still violates the unforgeability property. We also propose an improvement that overcomes the security leak inherent in the Petersen–Michels scheme. Moreover, our improvement is as efficient as previous signcryption schemes with respect to both the computational cost and the communication overhead.

2 Petersen–Michels signcryption scheme and its weakness

The initialisation and key generation stage of the Petersen–Michels scheme works as follows. First of all, the trusted centre (TC) of the system selects two large primes p and q, where $q(p-1)$, an element g of order q in Z_p, and a one-way hash function f that accepts a variant-length input and produces a fixed-length output. Then, TC publishes p, q, g and f. After that, each user in the system selects a secret key $x \in Z_q$ and computes the corresponding public key $y = g^x \bmod p$, where x is kept secret and y certified by TC is made public.

Let E and D be the encryption and the decryption functions, respectively, defined by an available symmetric algorithm, and be previously known to the signcrypter and the recipient. Suppose that a signcrypter U_a wants to secretly send a message m to the recipient U_b. First of all, he/she randomly selects an integer $t \in Z_q$, computes $e = f(y_b{}^t \bmod p)$, and then sends a signcrypted text $(c = E(K, m),\ r = K \cdot e \bmod q,\ s = t \cdot (r + x_a)^{-1} \bmod q)$, where $K \in Z_q$ is an encryption key randomly chosen by himself/herself. Upon receiving the signcrypted text (c, r, s) sent from U_a, U_b first computes $e = f((g^f \cdot y_a))^{s \cdot x_b} \bmod p)$, then obtains $K = r \cdot e^{-1} \bmod q$, and finally recovers $m = D(K, c)$.

The main weakness of the Petersen–Michels scheme is that the signature and the encryption can be separated. Two possible forgery attacks against the Petersen–Michels scheme are demonstrated below. Suppose that U_b holds one valid signcrypted text (c, r, s) of a message m generated by U_a and attempts to forge a valid signcrypted text (c', r', s') for another message m' without having U_a's secret key x_a. It can be seen that, given r and s, U_b knows e and then can easily obtain K. Therefore, U_b can easily

IEE Proceedings online no. 19990198
DOI: 10.1049/ip-cdt:19990198

Paper first received 21st July1998, and in revised form 22nd December 1998

The authors are with Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan 106, ROC

forge a valid signcrypted text ($c' = E(K,m')$, $r' = r$, $s' = s$) for any m' by U_a without knowing x_a. In an alternative way, U_b randomly chooses $\omega \in Z_q$ and computes $e' = f((g^r \cdot y_a)^{s \cdot x_b \cdot \omega} \bmod p)$ and $K' = r \cdot (e)'^{-1} \bmod q$. Again the triple ($c' = E(K', m')$, $r' = r$, $s' = \omega \cdot s \bmod q$) is also a valid signcrypted text for any m' by U_a. Another existential forgery attack also exists in the Petersen–Michels scheme. This existential forgery attack can be done by anyone just by picking random numbers for c, r, s. In such an attack, a recipient can decrypt that signcrypted text and obtains a message which cannot be controlled by the attacker. However, this attack is valid only under the condition that the message does not satisfy a redundancy scheme. From the above analyses, we can conclude that the Petersen–Michels scheme still violates the unforgeability property.

3 Our improvement

In the following, we will present an improvement that can avoid the weaknesses inherent in the Petersen–Michels scheme. The initialisation and key generation stage of our improvement is the same as that in the Petersen–Michels scheme.

Suppose a signcrypter U_a wants to secretly send a message m to the recipient U_b. Instead of randomly selecting an encryption key, U_a first computes the encryption key as $K = z \| f(m, z)$, where '$\|$' is the concatenation operator, and computes $c = E(K, m)$. Then, he/she randomly selects an integer $t \in Z_q$ and computes $e = f(y_b^t \bmod p, c)$. After that, U_a constructs r and s as does the original Petersen–Michels scheme. Upon receiving the signcrypted text (c, r, s) sent from U_a, U_b first computes $e = f((g^r \cdot y_a)^{s \cdot x_b} \bmod p, c)$, then obtains $K = r \cdot e^{-1} \bmod q$, and finally recovers $m = D(K, c)$. The recovered m can be further verified by first extracting z and $f(m, z)$ from K and then checking if the extracted $f(m, z)$ is equivalent to the hash value of the recovered m and z.

Here, we only reconsider the forgery attacks against our improvement. Regarding how our improvement can gain nonrepudiation without losing confidentiality, the readers can refer to the repudiation settlement procedure presented by Petersen and Michels [3]. In our improvement, the immediate parameter e can be rewritten as:

$$\begin{aligned} e &= f((g^r \cdot y_a)^{s \cdot x_b} \bmod p, E(K, m)) \\ &= f((g^r \cdot y_a)^{s \cdot x_b} \bmod p, E(z \| f(m, z), m)) \end{aligned}$$

This implies that the attacker cannot separate the signature (r, s) and the encryption $c = E(K, m)$ due to plotting the forgery attacks. Furthermore, the recovered m can be verified by only using the obtained encryption key K, without employing a redundancy scheme.

4 Conclusions

We have shown that the signcryption scheme proposed by Petersen and Michels [3] still violates the unforgeability property. We also have proposed a countermeasure in which the forgery attacks can be avoided, without losing confidentiality and nonrepudiation. Our improvement is as efficient as previous signcryption schemes with respect to both the computational cost and the communication overhead.

7 Acknowledgments

The authors wish to thank the anonymous referees for their very useful comments that greatly improve the presentation of this paper.

8 References

1 ZHENG, Y.: 'Digital signcryption or how to achieve cost(signature and encryption) < cost(signature) + cost(encryption)', in: *Advances in Cryptology: CRYPTO'97'* (LNCS 1294, Springer-Verlag, 1997), pp. 165–179

2 EL GAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT–31**, (4), pp. 469–472

3 PETERSEN, H. and MICHELS, M.: 'Cryptanalysis and improvement of signcryption schemes', *IEE Proc., Comput. Digit. Tech.*, 1998, **145**, (2), pp. 149–151

4 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications', in: *Advances in cryptology: ASIACRYPT'94'* (LNCS 917, Springer-Verlag, 1994) pp. 224–237

5 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Authenticated encryption schemes with low communication costs', *Electron. Lett.*, 1994, **30**, (15), pp. 1212–1213

6 NYBERG, K. and RUEPPEL, R. A.: 'Message recovery for signature scheme based on the discrete logarithm problem', *Des. Codes, Cryptog.*, 1996, **7**, (1/2), pp. 61–81

7 ZHENG, Y.: 'Signcryption and its applications in efficient public key solutions', in: 'Proceedings of 1997 information security workshop' (LNCS 1396, Springer–Verlag, 1997), pp. 291–312

Guide to authors of papers for *IEE Proceedings Computers and Digital Techniques*

1 Language
To ensure the widest possible readership, papers must be written in English.

2 Typescript
The complete typescript, i.e. Abstract, text of the paper, References and Figure captions, should be typed with double line spacing on one side of the paper only.

3 Number of copies
For the purpose of refereeing and editing, the IEE requires five copies of a paper, and where authors can supply this number without undue inconvenience or expense, they are asked to do so.

4 Affiliations of authors
The affiliation and full postal address of each author should be typed on a separate sheet and submitted with the paper.

5 Abstracts
Each paper should be accompanied by an abstract suitable for publication, of no more than 200 words.

6 Photographs and illustrations
Illustrations enclosed when a paper is first submitted need not be suitable for reproduction, but they must be clear for the purpose of refereeing. The authors should obtain from the owners of the copyright written permission to reproduce any illustration for which the copyright is not their own. The source of the illustration must be given in full and the words 'Reproduced by permission of . . . ' included with the illustration where necessary.

7 References
Other publications referred to in the text should be indicated by a number. Details of the References should be given in a list at the end of the paper in order of citation.

Each reference should include:
(a) names of all the authors (i.e. not '*et al.*')
(b) title of the paper
(c) full title of the journal
(d) year of publication and volume number
(e) first and last page numbers.
For a book, the author, book title, publisher and year of publication should be stated.

8 Length
Papers should not exceed six or seven printed pages [approximately 12–16 double spaced A4 pages (or 3000 words) plus 10–14 illustrations].

9 Peer review
All papers are rigorously refereed, and action may be taken against authors who have submitted the same work to other journals. Multiple submissions are strongly discouraged. It is our policy to ensure that a decision to publish or not is made within six months for no less than 90% of the papers submitted. Only in very exceptional circumstances does a paper remain under consideration for more than twelve months. It is our usual practice that authors are informed of the progress of their paper within six months.

Scope of *IEE Proceedings-Computers and Digital Techniques*
The journal is devoted to computers and information systems in the broadest sense, covering digital techniques, processor architectures, networks, parallel and distributed systems. Topics include formal and other design methodologies including CAD for both software and hardware (or both), computer architecture and networks (including protocols and cryptography). Papers may focus on theory, design, simulation or modelling, although theoretical papers will only be accepted where application or potential application of that theory is evident from the manuscript submitted.

Papers in logic design, synthesis and dsign methods, the traditional backbone of this journal, will still be welcomed but increasingly it is expected that issues such as hardware/software co-design, software engineering, computer architecture and higher level issues such as those found in distributed information systems, multimedia applications and the networks which support them will become more predominant

Paper must present original work, from either industrial or academic laboratories. Applications papers need not necessarily involve new theory, but may describe applications of existing techniques in new or novel situations. Review papers or tutorial expositions will also be accepted but only where such papers are of the highest standard.

The editors place great emphasis on rapid publication of substantial work and aim to have first decsions made on 95% of all papers within 6 months of submission. Publication delay will of course depend on the nature and extent of revisions asked for by the referees. Through this policy the aim of this journal is to provide a rapid and effective means of communication between engineers working in all aspects of computer and information systems gathering.

E.L. DAGLESS G. BREBNER

Related titles are
Vision, Image and Signal Processing – encompassed signal processing in the widest context
Software – practice, research and management aspects of software engineering
Disbritubed Systems Engineering – architecture, realisation and management of distributed computing systems
Please note that all papers submitted to the above publications are rigorously refereed.

Papers should be addressed to: The Managing Editor, *IEE Proceedings-Computer and Digital Techniques*, Publishing Department, Institution of Electrical Engineers, Michael Faraday House, Six Hills Way, Stevenage, Herts, SG1 2AY, United Kingdom

March 1999 Volume 146 Number 2

UK ISSN 1350–2387 ICDTEA 146 (2) 77–124

Contents