* 1

关于不使用 Hash 和 Redundancy 函数签密方案的分析与改进

柏　骏[1]，张串绒[1]，王　珏[2]
(1. 空军工程大学　电讯工程学院，陕西　西安　710077；2. 空军工程大学　工程学院，陕西　西安　710038)

摘　要：在实际应用中，前向安全性和公开验证性对密码系统来说是非常重要的。分析了不使用 Hash 和 Redundancy 函数的签密方案的前向安全性和公开验证性，分析表明该方案不具备前向安全性和公开验证性。分别就其前向安全性和公开验证性提出了相应的改进方案，并对方案进行了理论上的证明。改进方案克服了原方案中不具备前向安全性或公开验证性的缺陷；而且从效率上来分析，并没有明显增加计算量或传输量。

关键词：密码学；签密；Hash；Redundancy；前向安全性；公开验证性
DOI：10.3969/j.issn.1009－3516.2010.01.021
中图分类号：TP918.1　　**文献标识码**：A　　**文章编号**：1009－3516(2010)01－0091－04

自 Y. L. Zheng 于 1997 年提出签密方案 SCS[1-2] 以来，签密算法已取得了长足的发展。为解决 SCS 在实现不可否认性的过程中会造成消息机密性泄露的问题，Petersen 和 Michels 在 1998 年提出了 PM 方案[3]，2003 年，Seo 和 Lee 提出了多重签密方案 SL 方案[4]。同年，Libert，Quisquater 提出了基于身份的签密算法[5]。2009 年，张串绒等针对文献[5]不同时具备方向安全性和公开验证性而提出了方案[6]。这些签密方案的安全都是基于 Hash 函数的安全的，即必须保证 Hash 函数的单向性和无碰撞性。随着对 Hash 算法的研究，Hash 算法的安全性受到前所未有的挑战。目前应用的 Hash 算法主要是 MD5 和 SHA－1。王小云教授等学者先后提出 MD5 和 SHA－1 算法的杂凑碰撞[7-9]，从而使得相关的密码算法都不再安全。因此，研究设计一种不需要 Hash 的签密方案更具有现实的意义。2006 年，文献[10]提出了不使用 Hash 和 Redundancy 函数的签密方案，很好地解决了上述问题。但是该方案并不具备前向安全性和公开验证性，而前向安全和公开验证对于网络化时代的通信、电子商务、电子邮件系统等又是至关重要的。本文对该文献中签密方案的前向安全性和公开验证性进行了分析，并提出相应的改进方案。

1　不使用 Hash 和 Redundancy 函数的签密方案

设 p 是一个大素数，q 是 $p-1$ 的大素因子，$g \in Z_p^*$ 是 q 阶元素，x_a 和 $y_a = g^{x_a} \bmod p$ 分别是发送者 Alice 的私钥和公钥，同样，x_b 和 y_b 分别是接收者 Bob 的私钥和公钥，(E_K, D_K) 是安全的对称加解密算法对。假设 Alice 要签密消息 $m \in Z_p^*$ 给 Bob。则签密与解签密过程如下：

(A－1)随机选取 $k \in Z_p^*$；

(A－2)计算 $K = (y_b^k \bmod p) \bmod q$，$r = mg^{-K} \bmod p$，$c = E_K(m)$，$s = k/(r + x_a) \bmod q$；

Alice 将 (c, r, s) 发送给 Bob；

(B－1)计算：

* **收稿日期**：2009－07－02
基金项目：国家自然科学基金资助项目(60873233)；陕西省工业科技攻关基金资助项目(2008－k04－21)；西安市产学研合作基金资助项目(CXY08016)；中国博士后科学基金资助项目(20080440550)
作者简介：柏　骏(1985－)，男，四川南充人，硕士生，主要从事密码学与网络安全研究.
E－mail：peking1985－2005@163.com

$$K = ((y_b^r y_a^{x_b})^s \bmod p) \bmod q \tag{1}$$

(B-2)解密:

$$m = D_K(c)$$

(B-3)验证:

$$r = mg^{-K} \bmod p \tag{2}$$

若式(2)成立,Bob 接受(c,r,s)是 Alice 对 m 的有效签密;否则拒绝接受。

方案的安全性以及效率在文献[10]中已经论述,在此只讨论其前向安全性以及公开验证性。

2 方案的前向安全性分析及其改进方案

在方案的解签密过程中,对于式(1),有下式成立:

$$((y_b^r y_a^{x_b})^s \bmod p) \bmod q = (y_b^{(r+x_a)s} \bmod p) \bmod q \tag{3}$$

由此可知,虽然 Bob 可以用他的私钥 x_b 由上式左边求出 K,但同时对于任意知道 Alice 私钥 x_a 的人也都能由上式右边求出 K。也就是说,如果 Alice 的私钥泄露,将会造成先前以该私钥(x_a)通信的所有消息的泄露。因此,此方案无前向安全性。

以下是对该方案关于前向安全的改进,相关参数如上。

(A-1)随机选取 $k \in Z_p^*$;

(A-2)计算 $K = (y_b^k \bmod p) \bmod q$, $r = mg^{-K} \bmod p$, $c = E_K(m)$;

(A-3)以式子 $k = (rs + x_a) \bmod q$ 求得 s,计算 $S = g^s \bmod p$;

Alice 将(c,r,S)发送给 Bob;

(B-1)计算:

$$K = ((S^r y_a)^{x_b} \bmod p) \bmod q \tag{4}$$

(B-2)解密:

$$m = D_K(c)$$

(B-3)验证:

$$r = mg^{-K} \bmod p \tag{5}$$

若式(5)成立,Bob 接受(c,r,S)是 Alice 对 m 的有效签密;否则拒绝接受。

式(1)的正确性证明如下:

$$K = (y_b^k \bmod p) \bmod q = (y_b^{(rs+x_a)} \bmod p) \bmod q = (g^{x_b(rs+x_a)} \bmod p) \bmod q = ((S^r y_a)^{x_b} \bmod p) \bmod q$$

显然等式$((S^r y_a)^{x_b} \bmod p) \bmod q = (y_b^{(r+x_a)s} \bmod p) \bmod q$ 是成立的。对于知道 Alice 私钥 x_a 的任何用户,由于不知道 s,是无法根据(c,r,S)求出 K 的。因此,此改进方案具备了前向安全性。

在计算量上,改进方案要比原方案多一个模指数运算($S = g^s \bmod p$),但效率依旧高于传统的"先签名后加密"算法,而在传输量上则增加了$|p| - |q|$比特。

3 方案的公开验证性分析及其改进方案

原方案中,如果需要进行公开验证,Bob 需将他与 Alice 的通信消息 m 告知第 3 方才能进行,而这已经危及消息的机密性了。可见,方案公开验证性的实现是以机密性的丧失为代价的。因此,在要求保证消息机密性的情况下将无法实现第 3 方验证。

以下是对方案的公开验证性改进:

(A-1)随机选取 $k \in Z_p^*$;

(A-2)计算 $K_1 = (g^k \bmod p) \bmod q$, $K_2 = (y_b^k \bmod p) \bmod q$, $r = cg^{-K_1} \bmod p$, $c = E_{K_2}(m)$, $s = k/(r + x_a) \bmod q$;

Alice 将(c,r,s)发送给 Bob;

(B-1)计算:

$$K_1 = ((g^s y_a)^r \bmod p) \bmod q \tag{6}$$

$$K_2 = ((y_b^r y_a^{x_b})^s \bmod p) \bmod q \tag{7}$$

(B-2)验证:

$$r = mg^{-K_1} \bmod p \tag{8}$$

若式(8)成立,Bob 接受(c,r,s)是 Alice 对 m 的有效签密,解密密文;否则拒绝接受。

(B-3)解密:

$$m = D_{K_2}(c)$$

出现纠纷时,如果需要第 3 方验证,Bob 将(c,r,s)发送给第 3 方,则:

(C-1)计算:

$$K_1 = ((g^s y_a)^r \bmod p) \bmod q \tag{9}$$

(C-2)验证:

$$r = cg^{-K_1} \bmod p \tag{10}$$

如果上式成立,则(c,r,s)为 Alice 发给 Bob 的签密文件;否则不是。

此方案中接收方 Bob 对消息的验证在解密前进行,这样在验证不通过的情况下可以不用解密,从而省去了解密的计算量。

方案在传输量上不变,但在计算 K_1,K_2 时需要的运算量偏大,因此,为了不增加过多的运算量,可将原方案中的 $r = mg^{-K} \bmod p$ 改为 $r = cg^{-K} \bmod p$,在需要第 3 方验证时进行,Bob 只需将计算出的 K 和 c 发送给第 3 方,即可进行公开验证。这样不仅可以减小 Bob 发往第 3 方的信息传输量,同时也减小了第 3 方的运算量。

4　结束语

本文针对文献[10]中方案不具备前向安全性和公开验证性的问题,分别提出了相应的改进方案。改进方案具备了前向安全性或公开验证性,这使得不使用 Hash 和 Redundancy 函数的签密方案能够更广泛地应用于对前向安全和公开验证有特殊要求的现代通信、电子商务、电子邮件等系统中。然而改进方案前向安全性或公开验证性的具备是以牺牲高效性为代价的,因此,能够同时实现前向安全性、公开验证性和高效性的签密方案将是以后工作中的一个重要研究方向。

参考文献:

[1] Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) ≪ Cost (Signature) + Cost (Encryption) [C]//CRYPTO97, LNCS1294. Berlin:Springer-Verlag, 1997: 165-179.

[2] Zheng Y. Signcryption and Its Application in Efficient Public Key Solutions [C]//Information Security Workshop (ISW 97), LNCS 1396. Berlin:Springer-Verlag,1997:291-312.

[3] Petersen H, Michels M. Cryptanalysis and Improvement of Signcryption Schemes [J]. IEEE Computers and Digital Techniques, 1998,145(2):149-151.

[4] Seo S H, Lee S H. A Secure and Flexible Multi-signcryption Scheme[C]//ICCSA 2004, LNCS 3046. Berlin: Springer-Verlag,2004:689-697.

[5] Libert B, Quisquater J J. A New Identity Based Signcryption Scheme from Pairings[C]//2003 IEEE Information Theory Workshop. Paris, France:IEEE Press,2003:155-158.

[6] 张串绒,张玉清. 基于身份的前向安全和可公开验证签密方案[J]. 空军工程大学学报:自然科学版,2009,10(3):78-81.
ZHANG Chuanrong, ZHANG Yuqing. Identity Based Signcrytion Scheme with Forward Security and Public Verifiability [J]. Journal of Air Force Engineering University,2009,10(3):78-81. (in Chinese)

[7] Wang Xiaoyun, Feng Dengguo, Yu Xiuyuan, etc. Cryptandlysis of the Hash Functions MD4 and RIPEMD[C]//Eurocrypt 2005. Berlin:Springer-Verlag,2005:1-18.

[8] Wang Xiaoyun, Yu Hongbo. How to Break MD5 and Other Hash Functions[C]//Eurocrypt 2005. Berlin:Springer-Verlag, 2005:1-8.

[9] Wang Xiaoyun, Yin Yiqun Lisa, Yu Hongbo. Finding Collisions in the Full SHA-1 [C]//Cryptology CRYPTO'05. Berlin:

Springer – Verlag,2005:17 – 36.
[10] 张串绒,尹忠海,肖国镇. 不使用 Hash 和 Redundancy 函数的认证加密方案[J]. 电子学报,2006,45(5):108 – 111.
ZHANG Chuanrong,YIN Zhonghai,XIAO Guozhen. Authenticated Encryption Schemes Without Using Hash and Redundancy Functions[J]. Acta Electronica Sinica,2006,45(5):108 – 111. (in Chinese)

(编辑:徐楠楠)

The Analysis and Improvement of A Signcryption Scheme without Using Hash and Redundancy Functions

BAI Jun[1], ZHANG Chuan – rong[1], WANG Jue[2]
(1. Telecommunication Engineering Institute, Air force Engineering University, Xi′an 710077, China;2, Engineering Institute, Air Force Engineering University, Xi′an 710038, China)

Abstract: In practical applications, the forward security and public verifiability are very important to cryptography. An authenticated signcryption without using Hash and Redundancy functions is analyzed in this paper, and the result indicates that the scheme does not possess the characters of forward security and public verifiability. Modified schemes are proposed respectively according to each character mentioned above, and theoretically proved. By adopting the modified schemes, the original scheme's defects of non – forward – security or non – public – verifiability are overcome, and the computational cost and communication overhead are not increased.
Key words: cryptography; signcrytion; Hash; Redundancy; forward security; public verifiability

(上接第 43 页)

Analysis and Simulation for Micro – Doppler Information of Micro – Motion Target Based on Gabor Transformation

LI Kai – ming[1], LI Chang – dong[2], LI Song[3], LI Hong – jing[4], ZHANG Qun[1]
(1. Telecommunication Engineering Institute, Air Force Engineering University, Xi′an, 710077, China;. 2. Department of Aviation Theory, Air Force Aviation University, Changchun 130022, Jilin, China;3. Missile Institute, Air Force Engineering University, Sanyuan 713800, Shaanxi, China;4. College of Geographical Science, Southwest University, Chongqing, 400715, China;)

Abstract: The micro – Doppler signature is referred to as the unique signature of micro – motion target, which is significant for classification, recognition and imaging of special target. Because of the non – linear and non – stable characteristics of the special signal generated by micro – motion, in order to extract the micro – motion signature and provide a basis for target classification and identification, this thesis takes the object with rotating parts for example, under the single frequency system, to extract the micro – Doppler information based on the time – frequency analysis method. Then the micro – Doppler signature of micro – motion is obtained by simulation and verification, the transformation results and the differences of performance by using common time – frequency analysis tools are compared. The simulation testified that Gabor Transformation is feasible and stable in the aspect of extraction of micro – Doppler information, the remarkable potential of Gabor Transformation will provide a new approach of signature recognition for micro – motion target.
Key words: micro – motion; micro – Doppler; Gabor transformation; signature recognition