不使用 Hash和 Redundancy函数的认证加密方案

张串绒[1,2], 尹忠海[2,3], 肖国镇[1]
(1.西安电子科技大学综合业务网国家重点实验室,陕西西安 710071; 2.空军工程大学电讯工程学院,陕西西安 710077;
3.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071)

摘 要: 本文提出了一类新的认证加密方案,这类方案首次将消息可恢复签名和对称加密有机结合.它有两个特点,一个是签名中的承诺值只有预定的接收者才能算出,从而又可将该承诺值用作对称加密的密钥,取得一举两得之功效;另一个是用签名中恢复出的消息与对称解密得到的消息相比较,实现消息有效性的验证,改变了传统上使用 Hash函数或 Redundancy函数的验证方法.因此本文提出的新方案是一类不使用 Hash函数和 Redundancy函数的认证加密方案,

关键词: 密码学; 消息可恢复签名; 认证加密; 哈希函数; 冗余函数
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 05-0874-04

Authenticated Encryption Schemes Without Using Hash and Redundancy Functions

ZHANG Chuan-rong[1,2], YIN Zhong-hai[3], XIAO Guo-zhen[1]
(1. *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China;*
2. *Telecommunication Engineering Institute, Airforce Engineering University, Xi'an, Shaanxi 710077, China;*
3. *The Ministry of Education Key Laboratory of Computer Network and Information Security, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract A new type of authenticated encryption schemes is proposed. It first combines signature with message recovery schemes and symmetric encryption schemes together. This type of schemes has the following two characteristics: the commitment value of the signature is only recoverable by an intended receiver, so the value also can be used as a shared symmetric key of symmetric encryption and acts as "two birds one stone". The validity of the received message is verified by comparing the recovered message from the signature with the decrypted message instead of using Hash or Redundancy functions in traditional method. Therefore, the proposed scheme is an authenticated encryption without using Hash functions or Redundancy functions.

Key words cryptography; signature with message recovery; authenticated encryption; Hash function; Redundancy function

1 引言

随着网络的广泛应用,网上传输信息不仅仅要求机密性保证,而且要求认证性服务,在许多的应用,如电子邮件、电子商务、电子政务等中,往往还是同时需要机密性和认证性保护.作为信息安全主要技术的密码学是以加密技术保护消息的机密性,以数字签名实现认证性的.传统上同时实现认证和加密的方法是加密和签名的组合,通常采用"先签名再加密"的方法.这种组合的计算和传输代价是加密和签名的总和,且这种传统方法使用的是公钥加密和签名算法,计算速度慢,代价高.1994年, Horster, Michels和 Petersen在文献[1]中基于 Nyberg和 Rueppel文献[2]中的消息可恢复签名方案(N-R签名)提出了一种认证加密方案(authenticated encryption scheme),简称 HMP方案,能以较低的传输代价同时实现认证和加密功能.1995年, Lee和 Chang在文献[3]中给出 HMP方案的一个修改方案—LC方案,其特点是不需要 Hash函数,因此计算代价显著降低而且保持了与 HMP方案有相同的传输代价.1999年, Chen又进一步提出对 HMP方案和 LC方案的改进方案—Chen方案[4],该方案不使用 Hash函数,但与 LC

收稿日期: 2005-06-28; 修回日期: 2005-11-27
基金项目: 国家自然科学基金重大项目 (No. 90104005); "十五"通信预研基金 (No. 41001040102)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

方案一样要使用 Redundancy函数来验证消息的有效性. 1997年, Zheng提出了一种新的实现认证加密的思路, 称之为签密 (signcryption)[5], 它将对称加密和数字签名相结合, 在一个逻辑步骤里同时实现认证和加密的功能, 其代价远远低于传统方法. 但到目前为止提出的所有签密方案包括 Zheng的方案都要使用 Hash函数.

在密码方案中, Redundancy函数和 Hash函数的使用必然导致方案要承受由 Hash和 Redundancy函数带来的安全威胁。已有认证加密方案都使用 Hash或 Redundancy函数. 为此, 本文结合消息可恢复签名和签密的思想, 对已有方案进行改进, 提出了一类不使用 Hash 和 Redundancy函数的认证加密方案.

2 相关工作

N-R消息可恢复签名、HMP方案、LC方案和 Chen的认证加密方案以及 Zheng的签密方案都是本文所设计方案的重要基础, 鉴于这些方案之间的相互关联性, 这里主要对 N-R消息可恢复签名、LC认证加密和 Zheng的签密作一介绍.

2.1 N-R消息可恢复签名

消息可恢复签名是指消息可以在签名中传递并在接收者处被恢复出来. 也就是说, 消息不需要 Hash或者和签名一同传输, 这样可以节省存储空间和传输带宽[6].

在最著名的签名方案, 基于大数分解的 RSA和基于离散对数的 ElGamal和 DSA签名方案中, RSA签名自身具有消息可恢复功能, 而基于离散对数的 ElGamal签名和 DSA签名都没有. 文献[6]给出了一种方法, 使得基于离散对数的签名方案也可具有消息可恢复功能, 由此可得到一批基于离散对数的消息可恢复签名方案, 下面是其中一例.

设 p是一个大素数, q是 $p-1$的一个大的素因子, $g\in Z_p^*$ 是 q阶元素, x_a 和 $y_a=g^{x_a}\pmod p$分别是 Alice的私钥和公钥, 类似地, x_b 和 y_b 分别是 Bob的私钥和公钥.

假设 Alice要发送签名的消息 $m\in Z_p^*$ 给 Bob, Alice首先随机选取 $k\in Z_q^*$, 计算 $r=mg^k \bmod p$, $r'=r \bmod q$ 和 $s=k^{-1}(1+r'x_a)\bmod q$, 并将签名 (r, s)发送给 Bob. Bob由 (r, s)恢复消息 $m=g^{-s^{-1}}y_a^{-r's^{-1}}r \bmod p$, 然后再用 Redundancy函数验证消息 m 的签名的有效性.

文献[6]给出的消息可恢复签名方案中有一些不需要求逆, 这在本文提出的这类方案中也会发挥其特有的作用.

2.2 LC认证加密方案

基于 N-R消息可恢复签名, HMP给出的认证加密方案尽管有较低的传输代价, 但 HMP方案需要 Hash函数. 而 Hash函数的安全性是依赖于迭代函数计算复杂性分析的, 它会在一些特殊的攻击下变得不再安全. 为此, Lee和 Chang修改了 HMP方案, 在 HMP方案基础上给出了一种不使用 hash函数的认证加密方案-LC认证加密方案. 具体方案为: Alice随机选取 $k\in Z_q^*$, 计算 $K=(y_b^k \pmod p)\cdot \pmod q$, $r=mK \pmod p$和 $s=(k-x_a r)\pmod q$, 并将 (r, s)给 Bob. Bob接收到 (r, s), 先计算出 $y_{ab}=g^{x_a x_b}\pmod p=y_a^{x_b}\pmod p$和 $K=(y_b^s y_{ab}^r \pmod p)\pmod q$, 然后恢复消息 $m=rK^{-1}\pmod p$, 最后再用预先选好的Redundancy函数验证消息的有效性.

与 HMP方案相比, LC方案没有使用 Hash函数, 但文献[3]称 LC方案与 HMP方案一样可抗击已知消息-密文对攻击 (本文认为 LC方案抗击已知消息-密文对攻击的强度与 HMP方案所能达到的强度不同). 在 HMP方案中, 如果不使用 Hash函数, 攻击者由 (m, r, s)便可计算出收发双方的 Diffie-Hellman共享密钥 y_{ab}. 在 LC方案中攻击者由 (m, r, s)计算收发双方的 Diffie-Hellman共享密钥 y_{ab}的途径有两个, 一个是通过 $K=(y_b^k \pmod p)\pmod p$, 计算出 $y_b^k \pmod p$, 再由 $y_{ab}=[y_b^k(y_b^s)^{-1}]^{r^{-1}}\pmod p$, 计算 y_{ab}; 另一个是由 $K=(y_b^s y_{ab}^r \pmod p)\pmod q$直接计算 y_{ab}. 而这两种途径无论哪一种都要遇到双重模难题 (关于此问题的困难性见文献[3]).

2.3 Zheng的用短签名的签密方案

HMP方案、LC方案和 Chen方案都是基于消息可恢复签名的, 与之不同, Zheng开辟了一条新的实现认证加密的途径, 即将一般签名和对称加密有机结合的模式-签密. Zheng提出了两个非常类似的签密方案, 分别称为 SCS1和 SCS2[5,7]. 这两个方案分别用到 ElGamal族签名中 DSS的两个非常类似的短签名方案, 简称 SDSS1和 SDSS2. 与 DSS相比, 短签名 SDSS有以下好处: (1)签名较短, DSS为 $|2q|$比特, SDSS为 $|hash(\cdot)|+|q|$比特 (一般 $|q|\approx 2|hash(\cdot)|$); (2)在签名验证阶段不需要模逆运算或除法运算; (3)在随机预言机模型下是可证明安全的. 文献[6]给出了将一般签名方案转化为短签名的通用方法, 由此可得到一批有效的短签名方案.

下面给出 Zheng的签密方案, 以 SCS1为例. 该方案中 $hash$表示单向 Hash函数, KH 是钥控的单向 Hash函数, (E, D)是安全的对称加解密算法对, 其它参数同前面所述. 假设 Alice要签密消息 m 给 Bob. Alice首先随机选取 $k\in Z_q^*$, 计算 $K=hash(y_b^k \bmod p)$, 将 K 分成适当长度的 K_1 和 K_2; 并计算 $r=KH_{K_2}(m)$, $c=E_{K_1}(m)$和 $s=k/(r+x_a)\cdot \bmod q$. Alice将签密密文 (c, r, s)发送给 Bob. Bob执行解签密, 计算 $K=hash(y_a\cdot g^r)^{s\cdot x_b}\bmod p$, 并将 K 分成 K_1 和 K_2, 解密出消息 $m=D_{K_1}(c)$, 验证 $r=KH_{K_2}(m)$是否成立, 以决定接受 m 还是拒绝接受.

Zheng签密方案的巧妙之处在于以一种特殊的方式计算签名中的承诺值 K, 使得只有预定的接收者才可以恢复它, 那么该承诺值就可以用作发送方和接收方之间共享的对称密钥, 从而可应用于对称加密提供消息的保密性, 取得一举两得的功效.

© 1994-2016 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

3 不使用 Hash和 Redundancy函数的认证加密方案

N-R方案具有较小的签名长度和消息可恢复特性, LC方案用一个以上模运算难题取代了 HMP方案中的 Hash函数, Zheng的签密方案则利用了对称加密高效高速的优点. 尽管如此, 现有这些认证加密方案都毫不例外的需要使用 Hash函数或者 Redundancy函数. 本文结合 N-R消息可恢复签名、LC认证加密和签密的思想, 构造了一种不使用 Hash函数也不需要 Redundancy函数的新型认证加密方案. 下面给出这类新型方案的一个具体方案. 各参数如前所述.

假设 Alice要认证加密的发送消息 $m \in Z_p^*$ 给 Bob, 那么, Alice执行签名加密和 Bob解密验证的过程如下.

Alice签名加密: 随机选取 $k \in Z_q^*$, 计算

$$K = (y_b^k \pmod p) \pmod q$$
$$r = mg^{-K} \pmod p \quad c = E_K(m)$$
$$s = k/(r + x_a) \pmod q \qquad (1)$$

Alice将 (c, r, s)发送给 Bob

Bob解密验证:

计算 $K = ((y_b^r y_a^{x_b})^s \pmod p) \pmod q$ (2)

解密 $m = D_K(c)$

验证 $r = mg^{-K} \pmod p$ (3)

若式(3)成立, Bob接受 m 是 Alice发送给他的有效消息; 否则拒绝接受.

该方案的正确性推导如下:

$$\begin{aligned} K &= ((y_b^r y_b^{x_b})^s \pmod p) \pmod q \\ &= ((g^{x_b r} g^{x_a x_b})^s \pmod p) \pmod q \\ &= ((g^{(r+x_a)s})^{x_b} \pmod p) \pmod q \\ &= ((g^{x_b})^{s(r+x_a)} \pmod p) \pmod q \\ &= ((y_b^k) \pmod p) \pmod q = K \end{aligned}$$

由于消息可恢复签名的多样性和短签名的多样性, 用以上方法可以得到一类这样的认证加密方案.

4 讨论上述方案的安全性和有效性

该方案是基于 LC认证加密方案和 Zheng的签密方案的, 所以其安全性也是以 LC认证加密方案和 Zheng的签密方案的安全性为基础的. 以下具体通过可能存在的攻击来考察所给新方案的安全性.

(1)除 Alice和 Bob外的第三者想从 (c, r, s)得到 x_a、x_b、K 和 $y_{ab} = y_a^{x_b} \bmod p = y_b^{x_a} \bmod p$. 求解秘密参数 k 和 y_{ab}要同时遇到离散对数难题和双重模难题; 想从式(1)解出 x_a 或从式(2)解出 x_b 和 K 也是不可能的; 通过式(3)求 K 必然遇到离散对数难题. 因此从公开参数及 (c, r, s)解出 x_a, x_b 和 K 都是不可能的.

(2)Bob想得到发送者的秘密 x_a 和 k. 与①中原因相同, 由于求解秘密参数要遇到离散对数难题和双重模运算的保护, Bob不知道 k 的值, 也就不能从式(1)解出 x_a. 尽管 Bob知道 y_{ab}和 K, 但要从式(2)解出 x_a 要面临离散对数难题.

(3)除了 Alice, 其他人包括 Bob想要伪造认证加密密文 (c, r, s). 如果 Bob想伪造 Alice的满足式(3)的认证加密密文, 那么他可以随机选一些参数, 再试图由方程解出其余参数, 在求其余参数的过程中他必然遇到离散对数或双重模运算难题, 因此这种方法是不可行的. 其他人伪造合法密文更不可能, 因为他们并不比 Bob拥有更强的能力.

(4)除了 Alice和 Bob, 任何第三者想得到消息 m. 这是不可能的, 因为他不知道秘密参数 K.

(5)新方案同 HMP和 LC一样是可抗击已知消息-密文对攻击的, 因为攻击者从 (m, c, r, s)得不到 K, 也得不到 y_{ab}、x_a 和 k.

新方案以一种特殊的方式计算消息可恢复签名中的承诺值 K, 使得只有预定的接收者才可以恢复它, 将该承诺值用作发送方和接收方之间共享的对称密钥, 从而使对称加密得以应用, 提供消息的保密性, 很好得将消息可恢复签名与对称加密结合在一起, 既利用了对称加密快速高效的特点又利用了消息可恢复签名可恢复消息及不需要 Hash函数的优点, 最终实现了不使用 Hash和 Redundancy函数的目的. 另外短签名的使用也减小了在解密认证阶段的模逆运算和除法运算.

5 结论

本文给出的新型认证加密方案将消息可恢复签名与对称加密相结合, 将由签名恢复出的消息和对称解密解出的消息相比较, 实现消息的有效性验证, 从而避免了 Hash函数和 Redundancy函数, 这样也就避免了使用这些函数所要面临的相应安全威胁. 因此, 设计这样的密码方案不仅有理论价值还有着实际意义.

参考文献:

[1] P Horster, M Michels, H Petersen. Authenticated encryption schemes with low communication costs[J]. Electronics Letters, 1994, 30(15): 1212-1213

[2] K Nyberg, R A Rueppel. A new signature scheme based on the DSA giving message recovery[A]. 1st ACM Conference on Computer and Communications security[C]. New York: ACM Press, 1993. 58-61

[3] W Lee, C Chang. Authenticated encryption scheme without using a one-way function[J]. Electronics Letters, 1995, 31(19): 1656-1657.

[4] K Chen. Signature with message recovery[J]. Electronics Letters, 1998, 34(20): 1934

[5] Y Zheng. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryp-

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

tion) [A]. CRYPTO′97, LNCS 1294[C]. Berlin Springer-Verlag 1997. 165- 179

[6] K Nyberg R A Rneppel Message recovery for signature schemes based on the discrete logarithm problem[A]. In Advances in Cryptography-Proceedings of EUROCRYPT′94[C]. Berlin Springer-Verlag 1995. 175- 190

[7] Y Zheng Signcryption and its application in efficient public key solutions[A]. In Information Security Workshop (ISW′97), LNCS 1396[C]. Berlin Springer-Verlag 1997. 291- 312

作者简介:

张串绒　女, 1965年生于陕西眉县, 博士生, 副教授, 现于空军工程大学电讯工程学院任教; 主要研究方向为密码学和信息安全.
E-mail: crzhang@126.com; crzhang@mail.xidian.edu.cn

尹忠海　男, 1964年生于河北沧州, 博士生, 副教授, 现于空军工程大学电讯工程学院任教, 主要研究方向为网络通信与安全.

肖国镇　男, 1934年生于吉林四平, 教授, 博士生导师; 主要从事密码学、信息安全等方面的教学与研究.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net