一个前向安全的基于签密的密钥协商协议 *

魏 靓, 张串绒, 郑连清
(空军工程大学 电讯工程学院, 西安 710077)

摘 要: 安全有效地传递信息是计算机安全通信研究领域的主要目标。借鉴 Zheng 和张串绒将签密技术运用到密钥协商协议中的思想,利用基于身份的签密方案,提出一种具有前向安全性的密钥协商协议。该协议在具有基于身份的公钥密码体制特点的同时,又拥有签密技术的优点。与已有的方案相比,该密钥协商协议除了具有机密性、认证性、还具有前向安全性的特点。

关键词: 签密; 基于身份的公钥系统; 双线性对; 前向安全; 密钥协商
中图分类号: TN918.1 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1871-02
doi:10.3969/j.issn.1001-3695.2010.05.075

Forward secure key agreement protocol based on signcryption

WEI Liang, ZHANG Chuan-rong, ZHENG Lian-qing
(*Telecommunication Engineering Institute, Air Force Engineering University, Xi'an* 710077, *China*)

Abstract: Secure and efficient message delivery is one of the major aims of computer and communication security research. Based on the key agreement protocols using signcryption proposed by Zheng and Zhang chuan-rong, this paper proposed a forward secure key agreement protocol based on identity-signcyption. It combined the advantages of the identity-based public key system and signcryption technique. As compared to the existing schemes, the protocol is not only confidential, authenticated, but also forward secure.

Key words: signcryption; identity-based public key cryptosystem; bilinear pairing; forward secure; key agreement

签密是公钥系统中的一种新的范例,它能够在一个合理的逻辑步骤内同时实现数字签名和公钥加密的功能,并且只需要付出比传统的加密后再签名更少的代价。因而它是实现既保密又认证的传输消息的较为理想的方法[1]。签密技术已经得到广泛的应用,如电子现金支付系统、防火墙、安全认证的密钥分配等。

1984 年,Shamir[2] 提出了基于身份的公钥密码体制。在基于身份的公钥密码体制中,用户的公钥是直接从其身份信息(如姓名、身份证号、e-mail 地址等)得到,而私钥则是由一个私钥生成中心(PKG)的可信方生成。这种机制消除了对用户证书的依赖,极大地简化了密钥管理工作。自此以后,很多种基于身份的密码系统和安全协议被先后提出。2002 年 Malone-Lee[3] 定义了基于身份的签密方案的安全模型,利用双线性对构造了第一个基于身份的签密方案。

Zheng 等人在文献[4]中指出利用签密构建密钥协商协议的思想,并给出了具体的基于签密的密钥协商协议。2006 年,张串绒教授等人在文献[5]中对文献[4]中的方案进行了改进,提出了一种可认证密钥协商协议,但该方案不满足前向安全性。本文在此基础上设计了一种具有前向安全性的基于身份签密的密钥协商协议。

1 预备知识

1.1 双线性对

令 G_1 为由 P 生成的循环加法群,阶为 q,G_2 为具有相同阶 q 的循环乘法群,a,b 是 Z_q^* 中的元素。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。双线性对是指满足下列性质的一个映射 $e: G_1 \times G_1 \rightarrow G_2$:

a)双线性性。$e(aP, bQ) = e(P,Q)^{ab}$。

b)非退化性。存在 $P, Q \in G_1$,使得 $e(P,Q) \neq 1$。

c)可计算性。对所有的 $P, Q \in G$,存在有效的算法计算 $e(P,Q)$。

双线性映射 e 可以通过有限域上的超椭圆曲线上的 Tate 对或 Weil 对来构造[6]。

1.2 基于身份的签密方案的组成

一个基于身份的签密方案由以下几种算法组成:

(a)Setup(系统初始化算法)。由 PKG 完成,输入安全参数 k,输出主密钥 s 和系统参数 params,PKG 保密 s,公开 params。

(b)Extract(密钥生成算法)。输入一个用户的身份 ID_U,PKG 计算用户私钥 S_U 并通过安全方式发给这个用户。

(c)Signcrypt(签密算法)。输入系统参数 params、明文 m、接收者的身份 ID_B 和发送者的私钥 S_A,输出密文 σ = signcrypt(m, S_A, ID_B)。

(d)Unsigncrypt(解签密算法)。输入密文 σ、系统参数 params,接收者的私钥 S_B 和发送者的身份 ID_A,输出明文 m 或"j"表示解签密失败。

这些算法必须满足基于身份的签密方案的一致性要求,即如果 σ = signcrypt(m, S_A, ID_B),则 m = unsigncrypt(σ, ID_A, S_B)。

收稿日期: 2009-09-03; **修回日期**: 2009-10-23 **基金项目**: 国家自然科学基金资助项目(60873233)

作者简介:魏靓(1980-),女,山东青岛人,博士研究生,主要研究方向为无线网络安全、密码学(weijing0619@163.com);张串绒(1965-),女,陕西眉县人,副教授,博士,主要研究方向为无线网络安全、密码学;郑连清(1963-),男,山西曲沃人,教授,博士,主要研究方向为网络安全、信息对抗.

2 具有前向安全性的基于身份签密的密钥协商协议

在本文提出的协议中，设 G_1 为由 P 生成的循环加法群，阶为 q，G_2 为具有相同阶 q 的循环乘法群，$e: G_1 \times G_1 \to G_2$ 为一个双线性映射。定义三个安全的 hash 函数：$H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \times G_2 \to Z_q$ 以及 $H_3: G_2 \to \{0,1\}^n$。PKG 随机选择一个主密钥 $s \in Z_q^*$，计算 $P_{pub} = sP$ 并公开系统参数 params = $\{G_1, G_2, n, e, P, P_{pub}, H_1, H_2, H_3\}$，保密主秘密 s。

给定一个用户 U 的身份 ID_U，PKG 计算该用户的私钥 $S_U = sQ_U$。其中，$Q_U = H_1(ID_U)$ 为该用户的公钥。在这里，假设 Alice 的身份为 ID_A，公钥为 Q_A，私钥为 S_A；Bob 的身份为 ID_B，公钥为 Q_B，私钥为 S_B。

Alice 和 Bob 要协商秘密会话密钥，首先根据身份信息，分别计算出对方的 $Q_A = H_1(ID_A)$ 和 $Q_B = H_1(ID_B)$，然后执行以下过程。

Alice：任选 $x \in Z_q^*$，计算 $T_A = xP \bmod p$，$(k_1, k_2) = H_2(e(P_{pub}, Q_B)^x)$；取得当前时戳 TS，计算 $c = E_{k_2}(T_A, TS)$，$r = H_3(c, k_1)$，$S = xP_{pub} - rS_A \in G_1$，$R = rQ_A$。Alice 将签密密文 (c, R, S) 给 Bob。

Bob：收到 Alice 的签密密文 (c, R, S) 后，计算 $(k_1, k_2) = H_2(e(S, Q_B)e(R, S_B))$ 和 $(T_A, TS) = D_{k_2}(c)$。计算 $r = H_3(c, k_1)$，验证 $R = rQ_A$ 是否成立，成立则接收 T_A 是 Alice 给自己的密钥信息。随后任选 $y \in Z_q^*$，计算 $K_{BA} = e(T_A + Q_A, yP_{pub} + S_B)$。

然后计算 $T_B = yP \bmod p$，$(k_1^*, k_2^*) = H_2(e(P_{pub}, Q_A)^y)$；取得当前时戳 TS^*，计算 $c^* = E_{k_2^*}(T_B, TS^*)$，$r^* = H_3(c^*, k_1^*)$，$S^* = yP_{pub} - r^* S_B \in G_1$，$R^* = r^* Q_B$。Bob 将签密密文 (c^*, R^*, S^*) 给 Alice。

Alice：收到 Bob 的 (c^*, R^*, S^*) 后，计算 $(k_1^*, k_2^*) = H_2(e(S^*, Q_A)e(R^*, S_A))$ 和 $(T_B, TS^*) = D_{k_2^*}(c^*)$。计算 $r^* = H_3(c^*, k_1^*)$，验证 $R^* = r^* Q_B$ 是否成立，成立则接收 T_B 是 Bob 给自己的密钥信息，然后，计算 $K_{AB} = e(xP_{pub} + S_A, T_B + Q_B)$。因为

$$\begin{aligned} K_{BA} &= e(T_A + Q_A, yP_{pub} + S_B) = \\ & e(T_A, yP_{pub})e(T_A, S_B)e(Q_A, yP_{pub})e(Q_A, S_B) = \\ & e(P, P)^{xys}e(Q_B, P)^{xs}e(Q_A, P)^{ys}e(Q_A, Q_B)^s = \\ & e(xP_{pub}, T_B)e(xP_{pub}, Q_B)e(S_A, T_B)e(S_A, Q_B) = \\ & e(xP_{pub} + S_A, T_B + Q_B) = K_{BA} \end{aligned}$$

这样，Alice 和 Bob 共享会话密钥 $K = K_{AB} = K_{BA}$。协议的正确性：

$$\begin{aligned} (k_1, k_2) &= H_2(e(P_{pub}, Q_B)^x) = H_2(e(xP_{pub}, Q_B)) = \\ & H_2(e(S + rS_A, Q_B)) = H_2(e(S, Q_B)e(rS_A, Q_B)) = \\ & H_2(e(S, Q_B)e(rQ_A, sQ_B)) = H_2(e(S, Q_B)e(R, S_B)) \end{aligned} \quad (1)$$

同理可证

$$(k_1^*, k_2^*) = H_2(e(P_{pub}, Q_A)^y) = H_2(e(S^*, Q_A)e(R^*, S_A))。$$

3 安全性分析及性能评价

3.1 安全性分析

1）机密性　机密性保证了协商的密钥只有参与双方才知道。例如如果没有 Bob 的私钥，任何人不能从 (c, R, S) 中解密出 T_A，进而也得不到共享会话密钥 K。

2）前向安全性　所谓前向安全性是指如果某个用户的私钥被意外泄露或偷走，第三方也不能恢复出他过去所签密消息的明文。本文一方面在签密过程中用 $R = rQ_A$ 代替了 r，因此即使 Alice 泄露了 S_A，根据 $(k_1, k_2) = H_2(e(P_{pub}, Q_B)^x) = H_2(e(xP_{pub}, Q_B)) = H_2(e(S + rS_A, Q_B)) = H_2(e(S, Q_B)e(rS_A, Q_B))$，由于攻击者不知道 r，仍然得不到 T_A。

另一方面，在求会话密钥 K_{BA} 时，将 y 引入计算中，这样即使 S_B 泄露了，根据式(1)可以得到 T_A，但由于攻击者不知道 y，进而也求不出 $K_{BA} = e(T_A + Q_A, yP_{pub} + S_B)$ 的值。同时，若 S_A 和 S_B 同时泄露了，攻击者可以得到 T_A 和 T_B，但是得不到 x 或者 y，因而，不会造成共享会话密钥的泄露。总之，签密方案的改进和会话密钥生成方式两方面确保了协议的前向安全性。

3）可认证性　参与双方是可相互认证的，确保了通信双方实体的真实性。

3.2 性能评价

首先，由于采用基于身份的密码体制，用户的公钥就是用户的身份信息，用户不再需要管理公钥簿，无疑将大大提高整个协议的性能，省去了传统体制中公钥证书管理所带来的巨大额外开销。消息的签密过程也不再需要证书的传递和验证，只要接收者和签密者的身份信息和一些系统参数即可。双线性对的使用，使协议以较短的密钥得到同等安全强度。

其次，协议采用签密技术可以同时完成安全加密且恢复原消息和数字签名的功能，但是却只需付出远小于签名再加密方案所需的代价。在同样的参数条件下，无论是通信成本还是计算时间，签密技术更具有优势。

本协议为保证前向安全性，在签密过程中多了 $R = rS_A$ 的计算，在生成会话密钥时比文献[5]中多了两个加法和一个数乘运算，但对于计算能力较高的加密方来说，以较小的计算量增加换取安全性的增加是可以接受的。

4 结束语

本文基于身份的签密技术提出了一种密钥协商协议，并进行了安全性和性能分析。与其他方案相比，该协议最大的特点是前向安全性。与基于传统公钥密码系统的协议相比，具有更高的有效性。下一步的工作是解决该协议的公开验证性，使其更加完善。

参考文献：

[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]// Proc of Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1997: 165-179.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proc of Advances in Cryptology-CRYPTO'84, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1984: 47-53.

[3] MALONE-LEE J. 2002/098, IACR, Identity based signcryption [M]. Berlin: Springer, 2002: 362-379.

[4] ZHENG Y, IMAI H. Compact and unforgeable key establishment over an ATM network[C]// Proc of IEEE INFOCOM'98. San Francisco, CA: [s.n], 1998: 411-418.

[5] 张串绒，肖国镇. 基于签密技术的可认证密钥协商协议[J]. 空军工程大学学报：自然科学版, 2006, 7(6): 65-68.

[6] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]// Proc of Advances in Cryptology 2001. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001: 213-229.

[7] LIBERT B, QUISQUATER J-J. New identity based signcryption schemes from pairings[C]// Proc of IEEE Information Theory Workshop. Paris: [s.n], 2003: 155-158.