基于签密技术的可认证密钥协商协议

张串绒[1,2]， 肖国镇[2]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077；
2. 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)

摘 要：对Zheng的可认证密钥协商协议进行改进，提出基于身份签密的可认证密钥协商协议。该协议具有签密技术的优点，在同一个逻辑步内同时实现了认证和加密两项密码功能，提高了协议的效率；基于身份的公钥密码系统的使用，降低了建立和管理公钥基础设施的代价，用户无需存储、管理和传输公钥及其证书；另外，椭圆曲线上双线性对使协议能以短的密钥和小的计算量实现同等安全要求。文中所提的可认证密钥协商协议具有计算量和传输量小，安全性高的特点。

关键词：密码学；可认证密钥协商；签密；基于身份的公钥系统；双线性对
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-3516(2006)06-0065-03

1999年，Zheng在文献[1]中指出了利用签密构建密钥协商协议的思想，给出了具体的基于签密技术的密钥协商协议。最近，文献[2]又重申了利用签密方法协商密钥的思想。本文对文献[1]中Zheng提出的密钥协商协议进行改进，提出一种基于身份签密的可认证密钥协商协议。

1 基于身份的公钥密码系统

1984年，Shamir提出了基于身份的公钥密码系统[3]，在基于身份的公钥密码系统中，用户的公钥就是用户的身份信息或由身份信息生成的信息，比如电子邮箱地址IP地址、电话号码等。用户不再需要管理公钥簿；消息的加密和签名过程也不再需要证书的传递和验证，只要接收者和签名者的身份信息和一些系统参数即可。与传统的公钥密码系统相比，基于身份的公钥密码系统有很大的优势。

不同于传统公钥密码系统，在基于身份的公钥密码系统中系统参数由可信第三方PKG(Private Key Generator)选取如下：选取两个q阶的循环群$(G_1,+)$和$(G_2,\cdot)$，G_1的生成元为P，G_1和G_2上的双线性变换为e。PKG随机选取自己的私钥(也叫主密钥)$s\in Z_q^*$，公钥$P_{pub}=sP\in G_1$。本文提出的协议中，PKG选取安全的对称密码算法(E_k,D_k)和散列函数$H_0:\{0,1\}^*\to G_1$，$H_1:\{0,1\}^*\to Z_q^*$及钥控的单向哈希函数$KH_K(\cdot)$。

这样本文基于身份公钥的密码系统的系统参数为$(G_1,G_2,e,P,P_{pub},E_k,D_k,H_0,H_1,\mathrm{KH}_k(\cdot))$。PKG为用户$U$生成公私钥对的过程为：给出用户的身份信息$\mathrm{ID}_U$，PKG计算$Q_U=H_0(\mathrm{ID}_U)$，$S_U=sQ_U$分别作为用户的私钥和公钥秘密发给用户$U$。

其中双线性变换e的定义如下：

设G_1、G_2是两个q阶的循环群，P是G_1的生成元。变换e是双线性变换，如果满足以下条件：

1)双线性：对任意P_1、P_2，$Q\in G_1$有：$e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$及$e(P+Q_1,Q_2)=e(P,Q_1)e(P,Q_2)$。

2)非退化性：存在$P\in G_1$，使$e(P,P)\neq 1$。

3)可计算性：对所有的P_1、$P_2\in G_1$，存在有效的算法计算$e(P_1,P_2)$。

收稿日期：2006-04-19
基金项目：国家自然科学基金资助项目(J60404290135)和"973"计划基金资助项目(G1999035800)
作者简介：张串绒(1965-)，女，陕西眉县人，博士生，副教授，主要从事密码学和信息安全技术研究；
肖国镇(1934-)，男，吉林四平人，教授，博士生导师，主要从事密码学、信息安全等技术研究.

双线性变换是基于身份密码协议的重要工具,文献[4-5]等给出了双线性变换的实例。

2 Zheng 的基于签密的密钥协商协议

文献[6]提出了一种新的密码技术:签密,它能在一个逻辑步里同时实现认证和加密两项密码功能,且其效率远远高于传统的"先签名再加密"的认证加密方法。本文对文献[1]中用签密构造可认证密钥协商协议进行改进,给出了一种基于身份签密的高效安全可认证密钥协商协议。为此,首先对文献[1]中 Zheng 的基于一般签密的密钥密钥协商协议作以回顾。

公钥系统参数:p 是一个大素数; q 是 $p-1$ 的一个大的素因子, $q \in Z_p$ 是模 p 的 q 阶元素, Hash 是一个单向哈希函数,输出至少为 128 bit, $KH_k(\cdot)$是钥控的单向哈希函数, (E_k, D_k)是安全的对称密码的加解密算法对。

Alice 的公私钥对是$(x_a, y_a = g^{x_a} \bmod p)$,其中 x_a随机选自 Z_q,是 Alice 的私有密钥;相应地, $(x_b, y_b = g^{x_b} \bmod p)$是 Bob 的公私钥对。TS 是当前时戳, Other 是通信双方共同知道的有关双方身份的信息,如公钥,公钥证书等。

假设 Alice 要与 Bob 协商秘密的会话密钥, Key 和 Key* 分别是双方要提供给对方的会话密钥的秘密信息,他们执行以下过程。

Alice :任选 $x \in Z_q^*$,计算 $k = \mathrm{Hash}(y_b^x \bmod p)$,且将 k 分成长度相当的 k_1、k_2;取得当前的时戳 TS ,计算

$$c = E_{k_1}(\mathrm{Key}, TS)\ , r = \mathrm{KH}_{k_2}(\mathrm{Key}, TS, \mathrm{Other})\ , s = x/(r + x_a) \mod q$$

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 $k = (k_1, k_2) = \mathrm{Hash}((y_a g^r)^{sx_b} \bmod p)$,$(\mathrm{Key}, \mathrm{TS}) = D_{k_1}(c)$;

验证 $r = \mathrm{KH}_{k_2}(\mathrm{Key}, \mathrm{TS}, \mathrm{Other})$是否成立,成立则接受 Key 是 Alice 发给自己的密钥信息。

然后,任选 $y \in Z_q^*$,计算 $k^* = \mathrm{Hash}(y_a^y \bmod p)$,且将 k^*分成长度相当的 k_1^*、k_2^*;取得当前的时戳 TS*,计算 $c^* = E_{k_1^*}(\mathrm{Key}^*, \mathrm{TS}^*)$,$r^* = \mathrm{KH}_{k_2^*}(\mathrm{Key}^*, \mathrm{TS}^*, \mathrm{Other})$,$s^* = y/(r^* + x_a) \bmod q$

Bob 将签密密文(c^*, r^*, s^*) 给 Alice

Alice : 收到 Bob 的(c^*, r^*, s^*)后,计算 $k^* = (k_1^*, k_2^*) = \mathrm{Hash}((y_a g^r)^{sx_b} \bmod p)$,$(\mathrm{Key}^*, \mathrm{TS}^*) = D_{k_1^*}(c^*)$;

验证 $r^* = \mathrm{KH}_{k_1^*}(\mathrm{Key}^*, \mathrm{TS}^*, \mathrm{Other})$是否成立,成立则接受 Key* 是 Bob 发给自己的密钥信息。

最后,Alice 计算 $\mathrm{Tag} = \mathrm{MAC}_{\mathrm{key}\oplus\mathrm{key}^*}(\mathrm{TS})$,并发送 Tag 给 Bob,Bob 验证 $\mathrm{Tag} = \mathrm{MAC}_{\mathrm{key}\oplus\mathrm{key}^*}(\mathrm{TS})$,以确认 Alice 与他共享着同一会话密钥 Key⊕Key* 。

该协议是基于传统公钥密码系统的,在协议的执行过程中用户面临着公钥及其证书的管理、传递和验证的繁杂问题。本文提出一种新的密钥协商协议,它是基于身份和椭圆曲线上双线性对的,能大大降低建立和管理公钥基础设施的代价和用户所需计算、传输代价。

3 基于身份签密的可认证密钥协商协议

在本文提出的协议中, G_1、G_2 是两个 q 阶的循环群,其中 G_1是基于有限域的椭圆曲线 $E(E_p)$ 上的加法子群, G_2 为有限域 F_p上的乘法子群, p 是 G_1的生成元,随机选自椭圆曲线 $E(F_p)$ 上; e 是椭圆曲线 $E(E_p)$ 上的双线性变换。又设 Alice 的公私钥分别是 $Q_A = H_0(\mathrm{ID}_A)$和 $S_A = sQ_A$,Bob 的是 $Q_B = H_0(\mathrm{ID}_B)$和 $S_B = sQ_B$;

假设 Alice 和 Bob 要协商秘密会话密钥首先根据身份信息,分别计算出对方的公钥 $Q_A = H_0(\mathrm{ID}_A) \in G_1$、$Q_B = H_0(\mathrm{ID}_B) \in G_1$,然后执行以下过程。

Alice :任选 $x \in Z_q^*$,计算 $\mathrm{Key} = xP \bmod p$,$(k_1, k_2) = \mathrm{Hash}(e(P_{\mathrm{pub}}, Q_B)^x)$;取得当前的时戳 TS,计算

$$c = E_{k_1}(\mathrm{Key}, \mathrm{TS}),\quad r = \mathrm{KH}_{k_2}(\mathrm{Key}, \mathrm{TS})\ ,\quad S = xP_{\mathrm{pub}} - rS_A \in G_1$$

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$(k_1, k_2) = \mathrm{Hash}(e(S, Q_B)e(Q_A, S_B)^r)$和$(\mathrm{Key}, \mathrm{TS}) = D_{k_1}(c)$。

验证 $r = \mathrm{KH}_{k_2}(\mathrm{Key}, \mathrm{TS})$是否成立,成立则接受 Key 是 Alice 给自己的密钥信息。

然后,任选 $y \in Z_q^*$,计算 $\mathrm{Key}^* = yP \bmod p$,$(k_1^*, k_2^*) = \mathrm{Hash}(e(P_{\mathrm{pub}}, Q_A)^y)$;取得当前的时戳 TS*,计算

$$c^* = E_{k_1^*}(\mathrm{Key}^*, \mathrm{TS}^*) \quad , \quad r^* = \mathrm{KH}_{k_2^*}(\mathrm{Key}, \mathrm{TS}^*), S^* = xP_{\mathrm{pub}} - r^* S_B \in G_1,$$

Bob 将签密密文(c^*, r^*, S^*)给 Alice。

Alice：收到 Bob 的(c^*, r^*, S^*)后，计算$(k_1^*, k_2^*) = \mathrm{Hash}(e(S^*, Q_A)E(Q_B, S_A)^{r^*})$

解密出$(\mathrm{Key}^*, \mathrm{TS}^*) = D_{k_1^*}(c^*)$；验证$r^* = \mathrm{KH}_{k_2^*}(\mathrm{Key}, \mathrm{TS}^*)$是否成立，成立，则接受 Key* 是由 Bob 给自己的密钥信息。

这样，Alice 与 Bob 共享密钥共享会话密钥 $K = e(\mathrm{Key}, \mathrm{Key}^*) = e(xP, yP) = e(P, P)^{xy}$。

协议的正确性：

$(k_1, k_2) = \mathrm{Hash}(e(P_{\mathrm{pub}}, Q_B)^x) = \mathrm{Hash}(e(P_{pub}, Q_B) = \mathrm{Hash}(e(S + rS_A, Q_B)) = \mathrm{Hash}(e(S, Q_B)e(rS_A, Q_B)$
$= \mathrm{Hash}(e(S, Q_B)e(rsQ_A, Q_B)) = \mathrm{Hash}(e(S, Q_B)e(rQ_A, Q_B)) = \mathrm{Hash}(e(S, Q_B)e(rQ_A, sQ_B)) = \mathrm{Hash}(e(S, Q_B)$
$e(rQ_A, S_B)^r)$

同理可证：$(k_1^*, k_2^*) = \mathrm{Hash}(e(P_{\mathrm{pub}}, Q_A)^y) = \mathrm{Hash}(e(S^*, Q_A)e(Q_B, S_A)^{r^*})$

4　安全性和有效性

本文所提出的密钥协商协议是基于签密技术的，从安全性的角度讲，签密可同时提供消息的机密性和可认证性，即由该协议建立的共享密钥一方面具有机密性，保证协商的密钥只有参与双方才知道，另一方面具有可认证性，参与双方是可相互认证的，确保了通信双方实体的真实性。从效率的角度来说，签密的计算和传输代价远远低于传统的“先签名再验证”。

与 Zheng 的基于传统公钥密码系统的密钥协商协议相比，本文基于身份的公钥密码系统的特点，使协议的实施避免了传统公钥系统中复杂公钥管理难题。用户的公钥就是用户的身份信息或由身份信息生成的信息，用户不需要管理公钥簿；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。这样就降低了对用户终端计算、存储能力的需求和系统密钥管理的通信开销。

椭圆曲线上双线性对的使用，能使协议以较短的密钥得到同等安全强度。另外，目前普遍认为，非超奇异椭圆曲线离散对数问题的难度远远超过有限域 F_p 上离散对数问题（DLP）的难度，这使得椭圆曲线密码可以使用长度小得多的密钥，例如在同等安全前提下，160 bit 的椭圆曲线密码相当于 1 024 bit 的 RSA，而签名和解密速度比 RSA 快很多。这样可使我们的协议以更少的计算和传输量达到高的安全要求。

参考文献：

[1] Zheng Y, Imai H. Compact and Unforgeable Key Establishment over an ATM Network[A]. Proceedings of IEEE Ineocom [C]. San Francisco: 1998.

[2] Tor E Bjrstad, Alexander W. Dent. Building Better Signcryption Schemes with Tag - KEMs[A]. Appear in the 9th International Workshop on Practice and Theory[C]. 2006.

[3] Shamir A. Identity - based Cryptosystems and Signature Schemes[A]. Advances in Cryptology, Crypto84[C]. 1984.

[4] Boneh D, Franklin M. Identity Based Encryption From the Weil Pairing[A]. Advances in Cryptology - Crypto01, LNCS 2139 [C]. Springer: 2001.

[5] Joux A. A one Round Protocol for Tripartite Diffie - Hellman[A]. Algorithmic Number Theory Symposium, ANTS - IV [C]. 2000.

（编辑：门向生）

Sign - cryptic Technique Based on Authenticated Key Agreement Protocol

ZHANG Chuan - rong[1,2], XIAO Guo - zhen[2]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 71077, Shaanxi, China; 2. State Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, Shaanxi, China)

（下转第 71 页）

GAO Xiang[1], WANG Min[2], GUO Ying[1]
(1. Northwestern Polytechnical University, Xi'an 710072, Shaanxi, China; 2. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, Shaanxi, China)

Abstract: Intrusion detection system is a newly emerging and promising security measure. Data mining methods have been used to build automatic intrusion detection systems based on anomaly detection. The goal is to characterize the normal system activities with a profile by applying mining algorithms to audit data so that abnormal intrusive activities can be detected by comparing the current activities with the profile. This paper provides a new Intrusion Detection method based on data mining technology and combines fuzzy logic with apriori mining method. By grouping the quantitative attributes in network traffic according to fuzzy set, and by using genetic algorithm to construct the membership functions that state the fuzzy set, the existing "sharp boundary" problem can be avoided if the classic set theory is adopted. The experiment result shows that this combining fuzzy logic data mining method is an effective anomaly detection way.

Key words: data mining; intrusion detection; fuzzy logic; genetic algorithm; association analysis

(上接第67页)

Abstract: By improvement of Zheng's authenticated key agreement protocol, an identity sign - cryptic technique - based authenticated key agreement protocol is proposed. This protocol has the advantage of sign - cryptic technique and achieves the two functions of authentication and encryption in a single logical step. Therefore, it is of high efficiency. Moreover, due to using ID - based public key system, the expense of building and managing public key infrastructure is decreased and the users need not store or transfer public keys and certificate. And again, in our proposed protocol the bilinear pairing on elliptic curve is employed to reach the equivalent security levels with short length key and small computation cost. As a result, the remarkable properties of our authenticated key agreement protocol are low computation cost, narrow bandwidth requirement, and high security level.

Key words: cryptography; authenticated key agreement protocol; sign - cryptograph; ID - based public key system; bilinear pairing