一种可认证的三方密钥协商协议

邓俊蕾,左黎明,汤鹏志
(华东交通大学 基础科学学院,江西 南昌 330013)

摘 要:新协议提出了一个安全高效的三方密钥交换协议方案,通过在CDH假设下运用椭圆曲线密码体制,将长期私钥和临时私钥混合的方法保证协议的安全,通过对该协议的安全性进行分析,表明该协议可以抵御多种攻击;另一方面,将参与方中的任意两方作为一组,生成一个共同密钥,然后两方中的任意一方再与第三方进行消息认证和密钥协商,这样仅需要五次信息交互就可以实现整个协议的相互认证和密钥的确认功能,同时通过协议的比较还表明该协议具有较高的效率。

关键词:密钥协商;无证书密码学;密钥交换;前向保密性
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2012)02-0156-03

A Tripartite Key Agreement Protocol of Authentication

DENG Jun-lei, ZUO Li-ming, TANG Peng-zhi
(School of Basic Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: The new agreement proposed a safe and effective tripartite key exchange protocol, through assumptions in CDH, using elliptic curve cryptosystem keystore and temporary long-term keystore mixed method to assure the security, through the agreement the safety of this agreement are analyzed, show that this agreement can resist many attack; On the other hand, any of the parties involved two sides as a group, generates a common key, then both sides of arbitrary party with third parties again authentication and key agreement, news that need only five times information interaction can achieve the whole agreement of mutual authentication and key confirmation function, but through the comparison also show that agreement has high efficiency.

Key words: key agreement; certificateless cryptograph; key exchange; forward secrecy

0 引 言

密钥协商是在公开、不具备安全性的通信系统信道上,实现两个或多个实体协商建立共享会话密钥的安全通信过程,它是信息安全的一个重要研究分支。密钥是由参与各方协商形成,任一参与实体的欺诈行为都能对协商结果产生影响。构建安全的高层密钥协商协议对保证密钥协商的安全性至关重要。1976年Diffie等人[1]提出双方密钥协商交换协议,从此密钥协商协议就深受信息安全研究者的青睐。但该协议的缺陷在于缺乏认证,很快便引来人侵攻击者的中间人攻击。2000年Joux[2]提出基于双线性对的三方密钥协商协议,该协议经一轮交换可达到三方密钥协商,提高了协议运行效率,但仍没有解决人侵攻击的威胁。2003年S. S. Al- Riyami和K. G. Paterson[3]在Joux的协议的基础上,构造了基于Pairings的可认证三方密钥协商协议,随后K. Shim[4]指出该协议不具备已知密钥安全和密钥泄漏伪装安全。

在无证书公钥密码系统[5]的基础上,依据刘文刚等人[6]的两方密钥协商协议,文中设计了一种可认证的无证书三方密钥协商协议。

1 预备知识

针对协议的不同攻击,假如认证密钥协商协议满足下列属性,就会被认为是安全的。安全属性[7]如下所示:(1)已知密钥安全;(2)前向保密性;(3)未知密钥共享安全;(4)密钥泄漏伪装安全;(5)临时密钥泄漏安全;(6)密钥不可控性。

在安全性证明过程中,协议和密码算法的安全性一般可以归约为一个困难问题的假设上去。

定义1 离散对数(DL)问题[1]:给定P和Q,假如有$Q=nP(n\in Z_q^*)$存在,求n。

定义2(计算Diffie - Hellman(CDH)问题)[8]:a,$b\in_{Z_q}^*$,输入三元组(g,g^a,g^b),求解g^{ab}(如若能求解出

收稿日期:2011-06-12;**修回日期**:2011-09-21
基金项目:国家自然科学基金项目(11061014);江西省教育青年科学基金项目(GJJ10129);江西省教育科研项目(GJJ10708)
作者简介:邓俊蕾(1987-),女,河南周口人,硕士研究生,研究方向为信息安全;汤鹏志,教授,硕士,研究方向为信息安全。

群 G 的 DL 问题,CDH 问题也可解决;但 DL 问题能否归约为 CDH 问题,仍是未知问题[9])。

定义 3[9](CDH 假设):假如 $Adv^{CDH}(C)=\Pr[C(F,f,A=f^a,B=f^b)=f^{ab}]\leqslant\varepsilon(t)$ 成立,对任意概率多项式时间算法 C,足够大的安全参数 t 来说,就称做群 G 满足 CDH 假设。$\varepsilon(t)$ 是可忽略的,$a,b\in Z_q^*$,$Adv^{CDH}(C)$ 表示 A 解决 CDH 问题的优势。

2　新的三方无证书密钥协商方案

1)参数选择与密钥生成。

设 n 为安全参数,G 是椭圆曲线上阶为素数 q、生成元为 P 的加法循环群,Z_q 为模 q 的整数集。H_1,H_2,H 是 3 个抗强碰撞的哈希函数[10],$H_1:\{0,1\}^*\times\{0,1\}^*\times G\times G\rightarrow Z_q^*$,$H_2:G\rightarrow Z_q^*$,$H:\{0,1\}^*\times G\rightarrow Z_q^*$,其中 $Z_q^*=Z_q\backslash\{0\}$。(E_k,D_k) 是安全的对称密码算法,k 为安全对称密码算法的密钥,T_A、T_B、T_C 分别是 A、B 和 C 的时间戳,使用时戳 T 的目的是为了防止主动对手的延迟攻击。设 $x_A\in Z_q^*$ 为用户 A 的私钥,相应的公钥为 $Y_A=x_AP$;$x_B\in Z_q^*$ 为用户 B 的私钥,相应的公钥为 $Y_B=x_BP$;$x_C\in Z_q^*$ 为用户 C 的私钥,相应的公钥为 $Y_C=x_CP$。本协议把用户 A、B 作为一组,他们生成共同的密钥参数 $k'=k_A'=k_B'$,之后,再与用户 C 进行密钥协商,最终可得到共享密钥,该协议仅需要五次认证信息交互。

2)消息认证和密钥协商。

(1)用户 A 随机选择 $a\in Z_q^*$,计算 $Q_A=aP$,$D_A=aY_A$,$k_A=H_2(ax_AY_B)$,$\delta_A=H_1(T_A,D_A,Y_A,Q_A)$ 和 $S_A=(a+\delta_A)Y_A$,A 将消息 (c_A,δ_A,S_A) 发送给 B,其中,$c_A=(T_A,D_A,Y_A,Q_A)$。

(2)用户 B 收到 A 的消息后,计算 $D_A=S_A-\delta_AY_A$,$k_A=H_2(x_BD_A)$,验证 $H_1(T_A,D_A,Y_A,Q_A)=\delta_A$ 是否成立,若成立,计算 $k_B'=bx_BD_A$,否则终止协议。

(3)用户 B 随机选择 $b\in Z_q^*$,计算 $Q_B=bP$,$D_B=bY_B$,$k_B=H_2(bx_BY_A)$,$\delta_B=H_1(T_B,D_B,Y_B,Q_B)$,$S_B=(b+\delta_B)Y_B$,$B$ 将消息 (c_B,δ_B,S_B) 发送给 A,其中 $c_B=(T_B,D_B,Y_B,Q_B)$。

(4)用户 A 收到 B 的消息后,计算 $D_B=S_B-\delta_BY_B$,$k_B=H_2(x_AD_B)$,验证 $H_1(T_B,D_B,Y_B,Q_B)=\delta_B$ 是否成立,若成立,计算 $k_A'=ax_AD_B$,否则终止协议。协商完成后,用户 A 和 B 可建立统一共享会话密钥参数 $k=H_2(k')$,其中 $k'=k_A'=k_B'=abx_Ax_BP$。

(5)把 k 作为一个参数,用户 A 计算 $Q_A'=kP$,$D_A'=kkP$,$k_{A1}=H_2(kkY_C)$,$\delta_A'=H_1(T_A,D_A',Y_A,Q_A')$,$S_A'=(k+\delta_A')Q_A'$,$A$ 将消息 (c_A',δ_A',S_A') 发送给用户 C,其中 $c_A'=(T_A,D_A',Y_A,Q_A')$。

(6)用户 C 接收到 A 信息后,计算 $D_A'=S_A'-\delta_A'Q_A'$,验证 $k_{A1}=H_2(x_CD_A')$,$H_1(T_A,D_A',Y_A,Q_A')=\delta_A'$ 是否成立,成立则接收 A 发送的信息。

(7)用户 C 随机选择 $c\in Z_q^*$,计算 $Q_C=cP$,$D_C=cY_C$,$k_C=H_2(cx_CQ_A')$ 和 $\delta_C=H_1(T_C,D_C,Y_C,Q_C)$ 和 $S_C=(c+\delta_C)Y_C$。最后 C 计算 $K_C=cx_CD_A'$ 和 $tag=H_2(K_C)$。C 将 tag、(c_C,δ_C,S_C) 发送给 A 和 B,其中 $c_C=(T_C,D_C,Y_C,Q_C)$。

(8)A、B 收到 C 的消息,分别计算 $D_C=S_C-\delta_CY_C$,$k_{C_A}=H_2(kD_C)$,$k_{C_B}=H_2(kD_C)$,若 $H_1(T_C,D_C,Y_C,Q_C)=\delta_C$ 成立,则计算 $K_A=K_B=kkD_C$,并验证 $H_2(K_A)=H_2(K_B)=\text{tag}$ 是否成立,若成立则 A、B 接收 C 发送的消息,否则终止协议。

协商成功后,A、B、C 三方将对密钥进行 hash 处理,生成共享会话密钥 $K_S=H(K\|Y_A\|Y_B\|Y_C)$,其中,$K=K_A=K_B=K_C$。

3　安全性分析

3.1　已知密钥安全

1)假设攻击者获得了第一次的会话密钥 K_{S1},其中 $K_{S1}=kkD_C$,$k=H_2(abx_Ax_BP)$,$D_C=cx_CP$;由于会话的临时密钥 a、b 和 c 在每一次形成会话密钥过程中都会更新,用户 A、B 和 C 之间的攻击者若想由 K_{S1} 获得到下一次的会话密钥 K_{S2},其中 $K_{S2}=k_1k_1D_C'$,$k_1=H_2(a'b'x_Ax_BP)$,$D_C'=c'x_CP$,则他必须获得 a'、x_A、b' 和 x_B 或者 c' 和 x_C。攻击者要想从 (D_A')、(D_B')、Y_A、Y_B 中分别解出 a'、x_A、b' 和 x_B,或者从 (D_C') 和 Y_C 中解出 c' 和 x_C,都将面临 ECDLP 难题。

2)由于 A、B 作为一组,生成共同的会话密钥 K_1',假设 A、B 之间的攻击者获得了 A、B 之间的一个会话密钥 $K_1'=abx_Ax_BP$,而会话的临时密钥 a 和 b 在每次形成新的会话密钥过程中都在更新,攻击者想根据 K_1' 计算出下一个会话密钥 $K_2'=a'b'x_Ax_BP$,则他必须获得 a' 和 x_A 或者 b' 和 x_B。即攻击者要从 (D_A')、Y_A 解出 a'、x_A,或者从 (D_B')、Y_B 中解出 b' 和 x_B,同样将面临 ECDLP 难题。

3.2　前向保密性

假设攻击者获得了用户的长期私钥 (x_A,x_B,x_C),那么攻击者就可以对截获的密文进行解密,然后通过计算,就可得到 $(D_A,D_B,D_C,k_A,k_B,k_C)$。攻击者有以下 2 种途径可以计算出 K:

(1)从 $Q_A=aP$,$D_A=aY_A$ 中计算出 a,或者从 $Q_B=bP$,$D_B=bY_B$ 中计算出 b,或者从 $Q_C=cP$,$D_C=cY_C$ 中计算出 c,攻击者将面临 ECDLP 难题。

(2)通过 $aY_A=ax_AP$,$bY_B=bx_BP$ 和 $cY_C=cx_CP$ 计

算出 kkD_C，攻击者将面临 ECDH 难题。

3.3 未知密钥共享安全

Y_A、Y_B、Y_C 是由可信中心为 A、B 和 C 所颁发的证书中得到的，δ_A、δ_B 与 δ_C 又包含了各用户的身份信息、时戳等，可知消息被用户所绑定；C 若认为会和 F 共享同一会话密钥，还需从 D_C 中解出 c 和 Y_C 中解出 x_C，即攻击者能求解 ECDLP 难题。

3.4 临时密钥泄漏安全

当 x_A 和 x_B 泄漏给敌手后，敌手就可伪装为用户 C，然后对截获的密文解密算出 k_C、Q_C、D_A、D_B、D_C，敌手不能计算密钥 K，因为 a 和 b 未知；反之敌手能从 Q_A、D_A 求 a 和从 Q_B、D_B 求 b。同样地，攻击者将面临 ECDLP 难题。

3.5 临时密钥泄漏安全

假设敌手获得了 a,b,c，攻击者就能计算出 Q_A，Q_B,Q_C,D_A,D_B,D_C，然后得到 (P,x_AP,x_BP,x_CP)，但是得不到 kkD_C，即共享密钥 K。反之，攻击者将面临 ECDH 问题。

3.6 密钥不可控性

(1)参数 a、b 和 c 都被共享密钥所包含，协议未开始三方用户不能确定会话密钥；

(2) 用户 A 和 B 进行信息交互得到双方共享的密钥参数 k，用户 A 或 B 再把 k 作为一个参数与用户 C 进行信息交互，得到三方共享密钥，任何一方都不能单独得到会话密钥。

4 结束语

在现代社会中，三方密钥协商的地位越来越高，且在商业活动中运用越来越广泛。文中提出了一个可以认证的三方密钥协商协议，能够抵抗各种攻击，与无证书密码学的可认证三方密钥协议[11]相比具有较高的安全系数；此外，通过分析该协议仅仅使用了倍点运算和哈希运算，各用户之间仅需要五次信息交互，与新的三方密钥交换协议[12]相比具有较高的效率。通过分析比较，该协议能够很好地应用到当代社会的各种实践当中。

参考文献：

[1] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Trans. on Information Theory, 1976, 22(6): 644-654.

[2] Joux A. A One-round protocol for tripartite Diffie-Hellman [C]//Proc of Algorithmic Number Theory Symposium. [s. l.]:Springer-Verlag, 2000.

[3] Al-Riyami S S, Paterson K G. Tripartite authenticated key agreement protocols from pairings[M]. [s. l.]: Springer2-Verlag,2003.

[4] Shim K. Efficient one-round tripartite authenticated key agreement protocol form the Weil pairing[J]. Electronics Letters,2003(39):208-209.

[5] Al-Riyami S S, Patersoni K G. Certificateless public key cryptography[C]// Proc of Advances in Cryptology2-Asiacrypt. [s. l.]:[s. n.],2003.

[6] 刘文刚，李 娓，何文星. 基于签密的高效可认证密钥协商协议[J]. 计算机工程，2011，37(2)：123-125.

[7] 师鸣若，姜中华. 一种无线认证密钥协商协议[J]. 计算机工程，2009，35(7)：142-143.

[8] Abdalla M, Pointcheval D. Interactive Diffie-Hellman assumptions with applications to password-based authentication [C]//The 9th International Conference on Financial Cryptography. Berlin: Springer-Verlag, 2005:341-356.

[9] 王元元. 三方认证密钥交换协议研究[D]. 上海：上海交通大学，2009.

[10] Stallings W. Cryptography and network security: principles and practices[M]. 3rd ed. London: Prentice Hall, Pearson Education International, 2000.

[11] 陈家琪，冯 俊，郝 妍. 基于无证书密码学的可认证三方密钥协商协议[J]. 计算机应用研究，2010，27(5)：1902-1904.

[12] 柳秀梅，周福才，刘广伟. 新的三方密钥交换协议[J]. 东北大学学报，2009，30(7)：976-979.

(上接第 155 页)

Proceeding of 29th Int Conference on Software Engineering. Minneapolis:[s. n.],2007.

[4] Huang Chin-Yu. An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees[J]. Reliability Engineering and System Safety, 2007,92(10):1403-1412.

[5] 覃志东，雷 航，桑 楠，等. 安全关键软件可靠性验证测试方法研究[J]. 航空学报，2005，26(3)：334-339.

[6] Seija K S. Models for Dependability Assessment and Estimation[R]. [s. l.]:[s. n.],2003:100-110.

[7] 陈火旺，王 戟，董 威. 高可信软件工程技术[J]. 电子学报，2003，3(1)：1933-1938.

[8] 颜 炯，王 戟，陈火旺. 基于模型的软件测试综述[J]. 计算机科学，2004，31(2)：121-127.

[9] 王儒敬，白石磊，毛雪岷. 大型知识库存储结构的研究[J]. 计算机工程，2003，29(21)：25-27.

[10] 黄燕敏. 计算机技术[J]. 苏州工学院学报，2000，20(2)：78-80.

[11] 於晓棣，李 青. 基于数据仓库的决策支持系统的研究与应用[J]. 计算机与现代化，2002(10)：32-34.