强安全两方认证密钥协商方案 *

刘文浩，许春香
（电子科技大学 计算机科学技术与工程学院，成都 611731）

摘　要：提出一个新的强安全认证密钥协商方案。新方案满足抗密钥泄露伪装、已知会话临时信息安全和抗哈希值泄露攻击等特性，只要每方至少有一个未泄露的秘密，那么新方案在 eCK 模型下就是安全的，而且新方案是已知同类方案中运算量最少的。

关键词：扩展 CK 安全模型；强安全；认证密钥协商；两方
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2011)03-1133-03
doi:10.3969/j.issn.1001-3695.2011.03.096

Strongly secure two party authenticated key agreement scheme

LIU Wen-hao, XU Chun-xiang
(*School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 611731, *China*)

Abstract: This paper proposed a new strongly secure AKA scheme. The new scheme satisfied many known desirable security properties for AKA including resistance to key-compromise impersonation(KCI) attacks, resilience to the leakage of known session-specific temporary information and the leakage of hash values. The new scheme was secure in the eCK model as long as each party had at least one uncompromised secret, what's more, the new scheme enhanced the computational efficiency.
Key words: eCK secure model; strongly secure; AKA; two party

1993 年，Bellare 等人[1]首次提出了认证密钥协商(authenticated key agreement，AKA)的形式化安全模型。2001 年，这种模型被 Canetti 等人[2]修改为 CK 模型。从此，CK 模型在 AKA 协议安全分析中被广泛认为是可以被接受的安全模型，但该安全模型不能阻挡密钥泄露伪装攻击或已知会话临时信息泄露产生的攻击，因此，CK 模型下被证明是安全的认证协议仍然可能是不安全的。在 2005 年的亚密会上，由 Kudla 等人[3]提出了密钥协商协议的模拟安全证据，但它是基于一种较强的安全假设(gap bilinear Diffie-Hellman，GBDH)。直到 2007 年，LaMacchia 等人[4]通过扩展 CK 模型对 AKA 协议提出了一种更强的安全模型(extended Canetti-Krawczyk model，eCK 模型)。这种模型允许攻击者显示一方测试会话时的静态私钥(长期私钥)或显示一方的临时私钥，能帮助敌手获得更强的攻击能力，但它不允许显示使用临时私钥和静态私钥来计算的秘密值。文献[4]中方案也存在一个致命安全问题，如果某用户临时私钥和其长期私钥共同作用而产生的哈希值(如 $H(a,D_A)$，$H(b,D_B)$)泄露，那么敌手能计算出最终的会话密钥，因此，该方案是不安全的。同年，Okamoto[5]提出了第一个在标准模型下基于 PKI 的 AKA 协议，该协议每方需要 8 次指数运算，计算量比较大，影响了通信效率。2008 年，Lee 等人[6,7]先后提出了在计算 Diffie-Hellman 假设下认证密钥交换安全和具有紧安全归约的一个有效的认证密钥交换协议。文献[6,7]中每方分别需要 5 次、3 次指数运算。同年，Huang 等人[8]提出了一个新的基于计算 Diffie-Hellman 假设下认证密钥交换协议。该方案中，每方需要 5 次指数运算，通信效率也不太理想，而且文献[6~8]中方案都不能抗哈希值泄露产生的攻击(哈希值泄露，敌手就能计算出最终的会话密钥)。2009 年，Cheng 等人[9]在修改 eCK 模型下提出了一个新的强安全认证密钥交换协议。该方案中，每方需要 5 次指数运算。同年，Moriyama 等人[10]提出了一个无随机谕示 eCK 模型下认证密钥交换协议，其实质是采用基于 PKI 的认证协议，每方需要 12 次指数运算，计算量更大，通信效率更低于上述方案。以上方案中，要么不能同时满足抗密钥泄露伪装、已知会话临时信息安全等安全特性和抗哈希值泄露攻击，要么使用了次数较多的指数操作，通信效率不理想。按照 Miracl[11]执行一个 512 位 Tate pairing(配对)需要花费 20 ms，而一个 1 024 位素数模指数操作却只需要 8.80 ms。运行一次双线性对操作的时间大约是椭圆曲线上点乘运算的 21 倍，运行一次指数操作的时间大约是椭圆曲线上点乘运算的 3 倍[12]，所以，使用双线性对操作和模指数操作越多的方案其通信效率越低。一个好的协议必须同时满足安全性好和效率高两个条件。而上述方案，要么存在安全漏洞，要么效率不理想。本文提出的新方案不仅能同时满足密钥安全协商的六种安全属性，能允许敌手显示临时私钥产生的哈希函数值，而且也消除了双线性对操作，大大降低了计算复杂度。只要每方保留一个未泄露的秘密值，那么新方案在 eCK 模型下就是安全的。

1　预备知识

1.1　密钥协商的六个安全目标

1)已知密钥安全　协议参与者间的共同会话密钥被泄露后，获得该泄露密钥的攻击者无法根据已获得的会话密钥求出其他的会话密钥。

2)抗未知密钥共享　实体 A 如果不知道实体 B 的身份，

收稿日期：2010-09-09；**修回日期**：2010-10-28　　**基金项目**：国家“863”计划资助项目(2009AA01Z415)
作者简介：刘文浩(1974-)，男，湖北孝感人，博士，主要研究方向为信息安全、密码学(whl819_819@163.com)；许春香(1965-)，女，湖南宁乡人，教授，博导，博士，主要研究方向为信息安全、密码学.

实体 A 不会与实体 B 共享会话密钥。

3)抗密钥泄露伪装　假如实体 A 和 B 是协议的参与者,当实体 A 的长期私钥泄露后,获得该泄露密钥攻击者能向实体 B 冒充实体 A,反之则不行。

4)完美前向安全　若协议参与者间的长期私钥被泄露,获得该泄露密钥的攻击者不能求出在这次长期私钥被泄露之前协商得到的其他会话密钥。

5)无密钥控制　无论谁都不能将实体间协商的会话密钥预先设置其控制的选定值。

6)临时私钥泄露安全　用户在会话过程中产生的临时私钥泄露也不会影响最终生成的会话密钥的安全。

除上述六个基本安全目标外,本文另增加了哈希值泄露安全。用户的临时私钥和其长期私钥共同产生的哈希值(如 $H(a,D_A)$, a 表示用户 A 的临时私钥, D_A 表示用户 A 的长期私钥)泄露,那么也不影响方案的安全(简称为哈希安全)。

哈希安全包括四种情形:a)单纯的两个用户的哈希值被泄露,不会影响方案的安全,本文提到的文献[4]中方案不能满足此安全特性;b)两个用户的哈希值以及它们的长期私钥被泄露,不会影响方案的安全,本文中提到的文献[6,7,13]中方案不能满足此安全特性;c)两个用户的哈希值以及它们的临时私钥被泄露,不会影响方案的安全;d)两个用户的哈希值、一个用户的长期私钥和另一用户的临时私钥被泄露,不会影响方案的安全。本文提出的新方案能满足哈希安全的四种安全情形。

1.2　有关困难问题及相应假设

计算性 Diffie-Hellman 问题(computational Diffie-Hellman problem,CDHP):设 $G=\langle P\rangle$,阶为 q 的一个加法循环群, $a,b\in Z_q^*$, $aP,bP\in G$,计算 abP。在概率多项式时间内(PPT),算法 A 在解决 CDH 问题的优势定义如下:

$$Adv^{\mathrm{CDH}}(A)=Pr[A(aP,bP)=abP\mid a,b\in Z_q^*]$$

CDH 假设:对任意 PPT 算法 A, $Adv^{\mathrm{CDH}}(A)$ 是可以忽略的。

2　安全模型

2007 年,LaMacchia 等人在文献[4]中为密钥协商方案提出了一个较强的安全模型(称为 eCK 模型)。详细介绍见文献[7]。在非无证书的认证密钥协商方案中,通信中的每方都有两个秘密值,分别为 KGC 生成用户的部分私钥(长期私钥)、会话时用户选择的随机临时值(临时私钥)。本文按这两种秘密值自定义了三种安全类型:

a)如果攻击者知道用户长期私钥,两用户的临时私钥和长期私钥产生的哈希值(如 $M=H_3(a,D_A)$ 和 $N=H_3(b,D_B)$),两用户只各自保留临时私钥,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜。

b)如果攻击者知道某用户长期私钥,另一用户的临时私钥, $M=H_3(a,D_A)$ 和 $N=H_3(b,D_B)$,两用户只各自保留另外一个密钥中的一个,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜。

c)如果攻击者知道两用户临时私钥, $M=H_3(a,D_A)$ 和 $N=H_3(b,D_B)$,两用户只各自保留自己的长期私钥,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜。

3　新方案

1)系统参数建立　输入安全参数 k,产生两个大素数 p、q,且 $q\mid p-1$。P 为椭圆曲线上循环群 G 中任意一阶为 q 的生成元,KGC 选择安全 hash 函数: $H_1:\{0,1\}^*\times G\to Z_q^*$, $H_2:G\times Z_q^*\times\{0,1\}^*\to Z_q^*$, $H_3:Z_q^*\times Z_q^*\to Z_q^*$, $H_4:G\to\{0,1\}^*$, $H:\{0,1\}^*\to\{0,1\}^k$,KGC 随机选择主密钥 $x\in Z_q^*$,计算 $y=xP$,系统公开参数 $(p,q,P,y,H_1,H_2,H_3,H_4,H)$,保密主密钥 x。

2)用户密钥生成　给定用户身份 ID_i,KGC 随机选择 $r_i\in Z_q^*$,计算 $R_i=r_iP$, $D_i=r_i+xH_1(ID_i,R_i)$,通过安全渠道返回 D_i 给用户 i,并作为其长期私钥。$R_i=r_iP$ 作为用户 i 的部分公钥, D_iP 作为用户 i 的长期公钥。

用户 i 可以通过计算等式 $R_i+yH_1(ID_i,R_i)=D_iP$ 是否成立来判断 KGC 分配给自己的长期私钥是否有效。

3)身份认证和密钥协商　用户 A 随机选取 $a,N_A\in Z_q^*$ (N_A 为任意比特长),计算 $M=H_3(a,D_A)$, $T_A=aP,X_1=MP$, $h_1=H_1(ID_B,R_B)$, $h=H_2(T_A\parallel N_A\parallel ID_A)$, $s=a/(D_A+h)$, $V_A=a(R_B+h_1y)$, $C=H_4(V_A)\oplus N_A$,发送消息 (ID_A,h,s,C,X_1) 给用户 B。B 收到用户 A 发过来的消息 (ID_A,h,s,C,X_1) 后,计算 $h_2=H_1(ID_A,R_A)$, $V_B=sD_B(R_A+yh_2+hP)=(D_B)aP=a(R_B+h_1y)=V_A$,恢复消息 $N'_A=C\oplus H_4(V_B)$, $T'_A=s(R_A+h_2y+hP)=aP=T_A$。若 $H_2(T'_A\parallel N_A\parallel ID_A)=h$ 成立,则用户 B 通过了对用户 A 的身份验证。用户 B 随机选取 $b\in Z_q^*$,计算 $N=H_3(b,D_B)$, $T_B=bP,Y_1=NP$,并使用 V_B 作为对称加密密钥计算 $e=E_{V_B}(T_B\parallel ID_B)$,消息 (e,ID_B,Y_1) 发送给 A。当用户 A 收到消息后,利用 V_A 解密 e,得到 T_B。A 和 B 计算:

$$K_{A1}=D_BP(a+M)=(aP+MP)D_B=K_{B1}=K_1$$

$$K_{A2}=aT_B=abP=bT_A=K_{B2}=K_2$$

$$K_{A3}=(T_B+Y_1+D_BP)D_A=D_AP(b+D_B+N)=K_{B3}=K_3$$

最终的会话密钥 $SK=H(SID,K_1,K_2,K_3)$,其中 $SID=(A,B,X_1,Y_1,T_A,T_B)$。

4　安全分析

按照本文前面定义的安全类型,可分为三种情况来讨论其安全性。

类型 a)安全中, D_A,D_B, $M=H_3(a,D_A)$ 和 $N=H_3(b,D_B)$ 同时泄露给攻击者:

攻击者不知道 a,b。攻击者求不出 abP。因为在不知道 a,b 的情况下,无法计算出 abP,要计算 abP 就需要解决 CDH 问题在 (G,P) 上的一个具体实例,所以在这种情况下,新方案可以抗密钥泄露伪装攻击和哈希值泄露产生的攻击。

类型 b)安全中, (D_A,b,M,N) 或 (a,D_B,M,N) 泄露给攻击者:

若 (D_A,b,M,N) 泄露给攻击者。攻击者求不出 aD_BP。因为在不知道 (a,D_B) 的情况下,无法计算出 aD_BP,要计算 aD_BP 就需要解决 CDH 问题在 (G,P) 上的一个具体实例,所以在这种情况下,新方案可以抗中间人攻击,密钥泄露伪装攻击和哈希值泄露产生的攻击。若 (a,D_B,M,N) 泄露给攻击者。攻击者求不出 bD_AP。因为在不知道 (D_A,b) 的情况下,无法计算出 bD_AP,要计算 bD_AP 就需要解决 CDH 问题在 (G,P) 上的一个具体实例,所以,在这种情况下,新方案可以抗中间人攻击,密钥泄露伪装攻击和哈希值泄露产生的攻击。

类型 c)安全中, a,b,M,N 同时泄露给攻击者:

攻击者不知道 (D_A,D_B)。攻击者求不出 D_AD_BP。因为在不知道 (D_A,D_B) 的情况下,无法计算出 D_AD_BP,要计算 D_AD_BP 就需要解决 CDH 问题在 (G,P) 上的一个具体实例,所以,在这

种情况下,新方案可以抗因临时私钥泄露产生的中间人攻击和和哈希值泄露产生的攻击。

a)已知密钥安全。因为攻击者(包括 KGC)不知道 A 和 B 每次变化着的临时私钥(a,b),即使它知道某次的会话密钥,它们仍然无法求出 abP,要计算 abP 就需要解决 CDH 问题在(G,P)上的一个具体实例,所以新方案满足已知密钥安全。

b)前向安全。即使两用户的长期私钥(D_A,D_B)泄露给攻击者,但因为攻击者不知道 A 和 B 每次变化着的临时私钥(a,b),它就无法求出 abP。因为在不知道 a,b 的情况下,无法计算出 abP,要计算 abP 就需要解决 CDH 问题在(G,P)上的一个具体实例,所以新方案满足前向 KGC 安全。即使攻击者知道系统主私钥 s,但如果它不知道 KGC 为每个用户选择的临时信息 r_i,那么它也求不出(D_A,D_B),在这种情况下,即使攻击者还知道 A 和 B 每次变化着的临时私钥(a,b),它也求不出(D_A,D_B),要计算(D_A,D_B)就需要解决 CDH 问题在(G,P)上的一个具体实例,因此,新方案满足主私钥前向安全特性。

c)无密钥控制。因为计算最终的会话密钥与 a,b,D_A,D_B 相关联,(D_A,D_B)是由 KGC 产生的,所以无论是 A 还是 B 都无法预先计算出最终的会话密钥,所以新方案满足无密钥控制特性。

d)抗未知密钥共享。因为新方案使用了签密技术,验正签名时认证了对方的身份,所以新方案满足抗未知密钥共享安全特性。

e)抗密钥泄露伪装攻击。详细分析见类型一和二安全分析。因此,新方案满足抗密钥泄露伪装攻击。

f)已知会话临时信息安全。详细分析见类型三安全分析。因此,新方案满足已知会话临时信息安全特性。

g)哈希安全。根据上面类型一、二和三安全分析,可知新方案满足哈希安全。

5　协议效率与安全性能比较

大多数认证密钥协商方案之所以不安全,主要是由于这些方案不能同时满足密钥生成中心前向安全、抗密钥泄露伪装和已知会话临时私钥安全等安全特性以及哈希值泄露安全。而效率之所以较低,主要是它们采用了双线性对运算和过多指数运算。一个好的认证协议既要消除昂贵的对操作,选择最强安全模型和使用最弱的困难假设,更要同时满足密钥协商的六种基本安全属性。下列协议安全性方面主要考虑:密钥生成中心前向安全性(KGC-FS)、是否抗密钥泄露伪装攻击(KCIR)、是否满足已知会话临时信息安全(KSTS)等几个主要安全属性方面以及哈希值泄露安全。表 1 为效率与安全性能的比较。表中√表示满足该属性,×表示不满足该属性。效率方面主要考虑三种运算:P 表示双线性配对操作,E 表示指数操作,M 表示椭圆曲线上点乘操作。

表 1　效率与安全性能比较

协议	KGC-FS	KCIR	KSTS	哈希安全	P	E	M
LaMacchia[4]	√	√	√	×	0	4	0
Lee[6]	√	√	√	×	0	5	0
Lee[7]	√	√	√	×	0	3	0
Cheng[9]	√	√	√	√	0	5	0
Huang[8]	√	√	√	×	0	5	0
新方案	√	√	√	√	0	0	5

由表 1 可以看出,文献[4,6~8]协议不能抗哈希值泄露产生的攻击,而本文的新方案和文献[9]方案都能抗此种攻击。文献[4~9]协议分别使用了 4、8、5、3、5、5 次指数运算,而新方案中没有此种运算。在通信过程中,新方案中每个合法用户只需要进行 5 次椭圆曲线上的点乘运算就能完成安全的共同会话密钥协商,到目前为止,它是已知强安全认证协议中效率最高的协议,显然,新方案比本文提到的其他密钥协商方案有明显的优势。

6　结束语

新方案能同时满足:a)无用户密钥被托管,KGC 具有前向安全性;b)无密钥泄露伪装攻击(抗 KCI 攻击);c)会话时用户临时私钥泄露也不会产生中间人攻击。新方案无须配对操作和模指数运算,它比同类其他安全认证密钥协商方案具有更高的效率,特别适合移动通信和无线传感器网络中密钥协商。只要 CDH 假设成立,且每方至少有一个未泄露的秘密值,那么新方案就是安全的。如何设计出在标准模型下无配对操作和无模指数操作的强安全认证密钥协商方案将是一个值得研究的新课题。

参考文献:

[1] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]//Proc of the 13th Annual International Cryptology Conference on Advances in Cryptology. 1994:232-249.

[2] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]//Proc of EUROCRYPT 2001. London: Springer, 2001:453-474.

[3] KUDLA C, PATERSON K. Modular security proofs for key agreement protocols[C]//Lecture Notes in Computer Science, vol 3778. [S.l.]: Springer-Verlag, 2005:549-565.

[4] LaMACCHIA B A, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]//Proc of LNCS, vol 4784. 2007:1-16.

[5] OKAMOTO T. Authenticated key exchange and key encapsulation in the standard model[C]//Proc of ASIACRYPT 2007. Heidelberg: Springer, 2007:474-484.

[6] LEE J, PARK J H. Authenticated key exchange secure under the computational Diffie-Hellman assumption, Report 2008/344[R]. [S.l.]: Cryptology ePrint Archive, 2008.

[7] LEE J, PARK C S. An efficient authenticated key exchange protocol with a tight security reduction, Report 2008/345[R]. [S.l.]: Cryptology ePrint Archive, 2008.

[8] HUANG Hai, CAO Zhen-fu. Strongly secure authenticated key exchange protocol based on computational Diffie-Hellman problem[EB/OL]. (2008). http://eprint.iacr.org/2008/500.

[9] CHENG Qing-feng, MA Chuan-gui, HU Xue-xian. A new strongly secure authenticated key exchange protocol[C]//Proc of ISA 2009. Berlin: Springer-Verlag, 2009:135-144.

[10] MORIYAMA D, OKAMOTO T. An eCK-secure authenticated key exchange protocol without random oracles[C]//Proc of the 3rd International Conference on Provable Security. Berlin: Springer-Verlag, 2009:154-167.

[11] MIRACL. Multiprecision integer and rational arithmetic C/C++ library[EB/OL]. http://indigo.ie/mscott/.

[12] CHEN L, CHENG Z, SMART N P, *et al*. Identity-based key agreement protocols from pairings[J]. International JournalInformation Security, 2007, 6(4):213-241.

[13] KRAWCZYK H H. A high-performance secure Diffie-Hellman protocol[C]//Proc of CRYPTO 2005. Heidelberg: Springer, 2005:546-566.

[14] WU Jiang, USTAOGLU B. Efficient key exchange with tight security reduction, Report 2009/288[R]. [S.l.]: Cryptology ePrint Archive, 2009.