基于身份的认证群密钥协商协议

李国民[1] 何大可[1,2]

(西南交通大学信息安全与国家计算网格实验室 成都 610031)[1] (现代通信国家重点实验室 成都 610041)[2]

摘 要 认证群密钥协商(AGKA)协议能为一群用户产生一个共享的会话密钥,使得群用户间能在公共数据网络进行安全通信。现有的大部分基于公钥技术的AGKA协议可分两类:第一类,认证部分是基于PKI/CA,会话密钥协商部分主要用模指数(或点乘)实现;第二类,认证部分是基于身份(ID)的公钥体制,会话密钥协商部分主要是用Weil对或Tate对实现。第一类AGKA协议存在一个较显著问题:公钥管理问题;第二类AGKA协议虽然有效地解决了公钥管理问题,但由于其会话密钥协商部分主要是用双线性对(即Weil对或Tate对)实现,与前者相比,计算量较大。针对这些不足,提出了一个新的AGKA协议,其认证部分是基于身份(ID)的公钥体制,会话密钥协商部分的运算主要用模指数实现;并在ROM,ECDH和BDH假设下证明了该AGKA协议的安全性。该协议与基于PKI/CA的相关AGKA协议相比,克服了后者在密钥管理上的困难;与其它基于身份的AGKA协议相比,在效率上具有一定的优势。

关键词 认证群密钥协商协议,会话密钥,双线性对

ID-based Authenticated Group Key Agreement Protocol

LI Guo-min[1] HE Da-ke[1,2]

(Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031, China)[1]

(National Laboratory for Modern Communications of China, Chengdu 610041, China)[2]

Abstract An authenticated group key agreement (AGKA) scheme allows a group of users in a public network to share a session key which may later be used to achieve desirable secure communication. According to various authentication flavors by using asymmetric techniques, the previous AGKA protocols are sorted PKI/CA-based ones that most cost of computation is modular exponentiation (or dot multiplication) and ID-based ones which are implemented by using pairing. Compared with PKI/CA-based AGKA, ID-based authenticated AGKA simplifis the key agreement (management) procedures. Whereas they require expensive computation cost than PKI/CA-based AGKA protocols. Aiming at the weaknesses of the two kinds of AGKA protocols, a novel ID-based AGKA protocol was proposed that was implemented by using dot multiplication.

Keywords Authenticated group key agreement protocol, Session key, Pairings

随着公共网络上群组通信业务的日益增长,一个至关重要的问题是如何保证群成员间通信的安全性,而该问题的核心是群组成员间如何安全高效地进行密钥协商(交换)。近几年来,Bresson等在Bellare等工作[1-3]的基础上建立了认证群密钥协商(AGKA)协议安全模型[4-6](简记为BCP模型)。在Steiner等工作[7]的基础上,Bresson等[4-6]提出一些可证安全的AGKA协议,但效率较低,具体为计算量和通信量较大、轮数与用户数呈线性关系,因此该协议不适合用户数较大的群组通信。Burmester等[8]提出了一个GKA协议(简记为BD方案)并于2005年在文献[9]中给出了该方案的安全性证明。BD方案是第一个具有常数轮(2轮)的群密钥协商协议,其计算量为每个用户需计算3次模指数和$(n^2+3n-6)/2$次模乘法运算。虽然该方案是不带认证的,但由于BD结构的高效性,所以近年来出现了许多在BD方案及其变形的基础上的AGKA协议[10-13]。

与以上基于PKI/CA系统的AGKA协议相比,由于基于身份(ID)的密码系统在密钥管理方面较简单,所以近几年来,基于身份的用双线对实现的群密钥协商的研究已成为一个热点。在2000年,Joux[14]通过Weil对和Tate对仅用一轮就实现了三方密钥协商协议,但该协议不带认证功能。在2002年,文献[15,16]提出用Weil对和Tate对且含认证的三方密钥协商协议;同年,Reddy等[17]首次用单向Hash函数树和Weil对实现了基于身份的认证群密钥协商协议,但该方案没有对其安全性进行证明。在2003年,Barua等[18]用三叉树和Weil对实现了基于身份的认证群密钥协商协议,并对该协议进行了安全性证明。这两个基于身份的认证群密钥协商协议效率较低,主要是群中每个用户完整执行一次该协议需要进行$O(\lg n)$轮交互。在2004年,Choi等[13]用BD结构实现了一个常数轮的基于身份的认证群密钥协商协议,并对其安全性进行了证明。但Zhang等[19]指出,Choi等的AGKA协议

到稿日期:2008-02-28 本文受现代通信国家重点实验室基金(No. 151436050404QT2202)资助。

李国民(1974—),男,博士研究生,主要研究方向为群密钥协商协议的分析与设计、移动通信系统安全、信息系统安全工程,E-mail:li-gm95@163.com;**何大可**(1944—),男,教授,博士生导师,主要研究方向为密码学、信息安全、并行计算。

中的任何一个用户的两个邻居可以假冒该用户。针对这类攻击，在 2005 年，J. Katz 等[20]提出了一个将 GKA 协议转换成 AGKA 协议的编译器，其主要思想是在原有 AGKA 协议的基础上增加了一轮用数字签名来实现的密钥确认。

上述基于公钥的 AGKA 协议，其结构一般可分为两个部分：认证部分和会话密钥协商部分。认证部分根据其所基于的公钥系统又分两类：基于 PKI/CA 的认证方案、基于身份(ID)的认证方案；会话密钥协商部分根据其所基于的困难假设也可大致分两类：基于 CDH，DDH 或该困难问题的变形(ECDH 等)或扩展(如 GDH 等)的会话密钥协商(即这类会话密钥协商主要用模指数或点乘实现)，基于 BDH 或 DBDH 的会话密钥协商(即这类会话密钥协商主要是用 Weil 对或 Tate 对实现)。

组合认证部分和会话密钥协商部分，可得 4 类 AGKA 协议。根据已公开的文献，现有的大部分基于公钥的 AGKA 协议似乎仅属于其中的两类：第一类，认证部分是基于 PKI/CA，会话密钥协商部分主要用模指数(或点乘)实现；第二类，认证部分是基于身份(ID)的公钥体制，会话密钥协商部分主要是用 pairings(Weil 对或 Tate 对)实现。第一类 AGKA 协议存在一个较显著问题：公钥管理较困难；第二类 AGKA 协议虽然有效地解决了公钥管理问题，但由于其会话密钥协商部分主要是用双线性对(即 Weil 对或 Tate 对)实现，故其计算量较大，效率较低(有关双线性对与点乘或模指数之间计算量的详细比较见文献[30])。针对这些不足，一个很自然的问题是能否设计一个 AGKA 协议，其认证部分是基于身份(ID)的公钥体制，会话密钥协商部分的运算主要用点乘实现。本文正是在这方面进行了初步研究。

本文组织如下：第 1 节介绍有关困难假设；第 2 节介绍安全模型及相关概念；第 3 节介绍 Choi 等的基于身份的认证方案；第 4 节提出了一个新的基于身份(ID)的 AGKA；第 5 节对该协议的安全性进行了证明；第 6 节分析了该协议的效率；最后是结论。

1 椭圆曲线 Diffie-Hellman (ECDH)和双线性 Diffie-Hellman (BDH)[14]

设 G_1，G_2 分别是一个加法和乘法循环群，其阶均为 $q\geqslant 2^k$，其中 q 为素数，k 为安全参数，P 是 G_1 的一个生成元，且在群 G_1，G_2 中，离散对数问题(DLP)是困难问题。$e:G_1\times G_1\rightarrow G_2$ 为一有效的双线性映射。

椭圆曲线 Diffie-Hellman (ECDH)：挑战者随机选取 Z_q^* 中元素 a，b，计算 $P_a=aP$，$P_b=bP$。挑战者最后将$\{G_1,P,P_a,P_b\}$给攻击者。攻击者的目标是计算(或找到)值 abP。本文中的 ECDH 问题是超奇异椭圆曲线群上的 ECDH 问题。

双线 Diffie-Hellman 问题(BDH)：挑战者随机选取 Z_q^* 中元素 a，b，c，计算 $P_a=aP$，$P_b=bP$ 和 $P_c=cP$。挑战者最后将$\{G_1,G_2,e,P,P_a,P_b,P_c\}$给攻击者。攻击者的目标是计算(或找到)值 $e(P,P)^{abc}$。

2 安全模型[10,11,13]

由于 Bresson 等[4-6]提出的安全模型是非对称的，而本文的 AGKA 协议是对称结构，故本文的安全模型来自文献[10,11,13]。本文的攻击者 A 均为概率多项式时间(PPT)攻击者，通过用不同的询问模仿攻击者 A 的攻击能力，且攻击者 A 控制了用户实例间的所有通信，并能在任何时刻都可以要求一个实例泄露其会话密钥或私钥。

2.1 协议参与者(Protocol Participants)

选取一个非空集合 $U=\{U_i\mid i=1,2,\cdots,n\}$，该集合是由 n 个将参与群 Diffie-Hellman 协议 P 的用户身份标识构成。用户数 n 是安全参数 k 的多项式。一个用户 $U_i\in U$ 可能有许多不同的实例(有时称预言机)同时在协议 P 中运行。Π_i^s 表示用户 U_i 的一个实例 s，其中 $s\in\mathbb{N}$，用不带下标的 U 表示群中的某一个不固定用户。同样，Π_U^s 表示 U 的实例，$s\in\mathbb{N}$。用 ID_i 表示用户 U_i 的身份标识，它是一比特串，其中 $ID=ID_1||\cdots||ID_n$)。

2.2 用户 U 的公私钥对

在基于身份的密码系统中，每个用户 $U_i\in U$ 按如下方式获得其公私钥对：

(1)密钥生成中心(KGC：Key Generate Central)运行算法 $Setup(1^k,l)$ 产生主私钥(s)和全局参数($params$)，其中 l 是用比特串表示的用户身份标识的长度。

(2)从 KGC 用算法 Ext (即 Ext：$S_i\leftarrow Ext_s(ID_i)$)计算出与其用户 U_i 身份对应的长期私钥 S_i 后，并通过安全信道将 S_i 秘密传送给 U_i。

2.3 会话标识(Session IDS：SIDS)和伙伴关系(Partnering)

在协议 P 的一次运行中，定义预言机 Π_i^s 的会话标识($SIDS$)为：$SIDS(\Pi_i^s)=\{SID_{ij}:j\in ID\}$，其中 SID_{ij} 是预言机 Π_i^s 和预言机 Π_j^t(也可能是攻击者 A)之间在协议 P 的一次运行中所交换全部信息的级联。$SIDS$ 是公开的，它不依赖于会话密钥，因此攻击者 A 可以使用；实际上，A 仅需监听预言机之间的通信，就可把 $SIDS$ 恢复出来。$PIDS(\Pi_j^t)$ 表示实例 Π_i^s 的伙伴，如果 $PIDS(\Pi_i^s)=PIDS(\Pi_j^t)$，而且 $SIDS(\Pi_i^s)=SIDS(\Pi_j^t)$，则实例 Π_i^s 和 Π_j^t 是伙伴关系。

2.4 新鲜性(Freshness)

如果一个实例 Π_U^s 是新鲜的(或实例 Π_i^s 有一个新鲜密钥 K)，则须下面 3 个条件同时成立：(1) Π_U^s 已接受一个会话密钥 K；(2)在 Π_U^s 接受密钥 K 前，没有对它进行 $Corrupt$ 询问，且在 Π_U^s 接受密钥 K 后，没有对它进行 $Reveal$ 询问；(3)没有对 Π_U^s 的伙伴 $PIDS(\Pi_U^s)$ 进行 $Reveal$ 询问。

2.5 预言机询问(Oracle Queries)

每类询问模仿攻者的一种能力。询问类型及相应回答如下：

$Extract(ID_U)$：这类询问允许攻击者获得与身份 ID_U 相应的私钥 S_{ID}，且 $ID_U\notin ID$。

$Execute(ID)$：这类询问模仿被动攻击。在群中用户完整运行该 AGKA 协议时，攻击者通过窃听等手段获得用户间交互数据的全部复本。而且，参与运行 AGKA 协议的群中成员数量由攻击者确定。

$Send(\Pi_U^s,m)$：这类询问模仿攻击者 A 向用户实例 Π_U^s 发送消息 m。用户实例 Π_U^s 在接收到消息 m 并处理完后，将处理结果作为与之相应的回答返回给攻击者 A。如果用户实例 Π_U^s 仍没终止，协议 P 的运行导致 Π_U^s 的接受，则变量 $SIDS$ 被更新。$Send(\Pi_U^s,\text{“}start\text{”})$ 表示对协议 P 进行初始化。

$Reveal(\Pi_U^s)$：这类询问模仿导致会话密钥泄露的攻击。

只有在用户实例$\prod_U^i$已接收的情况下，攻击者A才可以使用*Reveal*询问。*Reveal*询问要求用户实例$\prod_U^i$无条件泄露与之相应的会话密钥。

Corrupt(ID_i)：这类询问模仿导致用户U私钥(S_i)泄露的攻击。在这类攻击中，虽然攻击者A获得了用户U私钥，但它不能获得用户实例$\prod_U^i$在协议P运行过程中的任何内部数据。

Test($\prod_U^i$)：这类询问模仿会话密钥的语义安全性，即在协议P运行过程中，攻击者A只能使用一次*Test*询问，而且被询问的用户实例$\prod_U^i$必须是新鲜的(*Fresh*)。用户实例$\prod_U^i$随机抛一硬币b，如果$b=1$，则将SK作为*Test*询问结果返回给攻击者A。否则，将向攻击者A返回一个随机数。

2.6 AGKA协议的AKA安全性

通过攻击者A和用户实例$\prod_U^i$之间的游戏来定义协议的安全性：

(1) 在系统建立阶段，密钥生成器$IG(1^k)$产生与安全参数k相关的用户的公私钥对；

(2) 攻击者A向用户实例$\prod_U^i$发送询问，实例$\prod_U^i$根据协议向A返回相应回答；

(3) 在协议运行的某一阶段，攻击者A向某一新鲜的用户实例$\prod_U^i$发送*Test*询问，然后A可继续作其它询问，最后A输出*Test*询问中b的猜测值b'。

在这个游戏中，用攻击者A正确区分会话密钥和随机值的能力来衡量A的优势，即A猜测b的能力，用*Succ*表示A正确猜出b，则A的攻击协议P的优势定义为$Adv_{A,P}^{AGKA}(k)=|2\Pr[Succ]-1|$。

认证群密钥协商(AGKA)协议是*AKE*安全的，如果它满足下列两个条件：

(1) 正确性：群中成员计算出的会话密钥是相同的；

(2) 不可区分性：对任意关于安全参数k概率多项式时间(*PPT*: *probability polynomial time*)的攻击者A，其优势$Adv_{A,P}^{AGKA}(k)$是可忽略的。

2.7 AGKA协议的前向安全性

AGKA协议的前向安全性是指当用户私钥泄露后，攻击者A仍不能获得有关该用户在私钥泄露前建立的会话密钥的任何信息。

3 Choi等的认证方案

Choi等定义的认证方案[13]如下：

Generation. 设用户私钥$S_{ID}=sH_1(ID)$，计算$T=aP_{pub}+hS_{ID}$，其中$a\in_R Z_q^*$，$h=H(aP)$，用户身份信息为$ID\in\{0,1\}^*$；即$\langle aP,T\rangle\leftarrow\Gamma_{gen}(S_{ID})$。

Verification. 给定用户U_{ID}的公钥$Q_{ID}=H_1(ID)$和$\langle aP,T\rangle$，验证$e(T,P)=e(aP+hQ_{ID},P_{pub})$，其中$h=H(aP)$；*True*或$False\leftarrow\Gamma_{ver}(Q_{ID},\langle aP,T\rangle)$。

此认证方案的不可伪造性由文献[6]的定理3给予了详细证明。

4 本文建议的方案ID-AGKA

建议方案ID-AGKA的认证部分是利用基于身份的认证方法，且在验证时用Weil实现，而密钥协商部分采用点乘来实现。本协议详细描述如下：

系统参数为$\{G_1,G_2,e,q,P,H,H_1\}$，其中G_1是一个生成元为P、阶为素数q的循环加法群，G_2是一个阶为素数q的循环乘法群，$e:G_1\times G_1\rightarrow G_2$是一个双线性映射，$k$为系统的安全参数，$H$，$H_1$是*ROM*中的两个Hash函数，其中$H:\{0,1\}^*\rightarrow Z_q^*$，$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\rightarrow\{0,1\}^k$。设将参与群会话密钥协商的用户集为$U=\{U_i\mid i=1,2,\cdots,n\}$，群中用户$U_i$对应的身份标识为$ID_i$，下标$i$是模$n$后的值。

Setup. 密钥产生中心(*KGC*: *key generate center*)运行*BDH*参数生成器，选择随机数s和G_1的生成元P，并计算$P_{pub}=sP$。*KGC*将s作为其主私钥并秘密保存，公布系统参数$para=\{G_1,G_2,e,q,P,P_{pub},H,H_1\}$。

Extract. 当用户U_i向*KGC*提交其身份信息$ID_i\in\{0,1\}^*$申请注册时，经*KGC*检查通过后，*KGC*计算$Q_i=H_1(ID_i)$及其对应的私钥$S_i=sQ_i$，并将S_i安全传送给该注册用户，则U_i的公私钥对为$\langle Q_i=H_1(ID_i),S_i=sQ_i\rangle$。

*Round*1 每个用户U_i选择一随机数$r_i\in\{0,1\}^k$，广播消息$ID_i||r_i$；接收到群中其它成员相应的广播消息后，计算并存储$nonce_i=ID_1||r_1||\cdots||ID_n||r_n$；

*Round*2 每个用户U_i选择一随机数$a_i\in Z_q^*$，计算$P_i=a_iP$并秘密保存a_i后，向群中广播P_i；

*Round*3 每个用户U_i在接收到*Round*1中所有其他群成员广播数据后，计算$t_i^L=H_2(a_iP_{i-1}||nonce_i)$，$t_i^R=H_2(a_iP_{i+1}||nonce_i)$，$D_i=t_i^L\oplus t_i^R$，$T_i=a_iP_{pub}+h_iS_i$，其中$h_i=H(D_i||P_i||nonce_i||P_{ID})$，$P_{ID}=P_1||\cdots||P_n$；接着向群中广播$\langle D_i,T_i\rangle$；

Key Computation. 每个用户U_i在计算会话密钥前，对群中其它成员及其发送的数据进行互认证：

$$e(T_j,P)=e(P_j+h_jQ_j,P_{pub}),\ j\in\{1,\cdots,n\}\bigcap j\neq i$$

若不成立，则U_i终止协议的本次运行并广播“失败”；如果相等，又因为$t_i^R=t_{i+1}^L$，$t_{i+1}^R=D_{i+1}\oplus t_{i+1}^L$，所以$U_i$可恢复出$t_{i+1}^R$。类似地，$U_i$可恢复出$t_{i+2}^R,\cdots,t_{i+n-1}^R$等，则$U_i$计算会话密钥：$sk_i=H_2(t_1^R||\cdots||t_n^R||nonce_i)$。

易验证，对群中任意用户U_i有：$sk_i=H_2(t_1^R||\cdots||t_n^R||nonce_i)$，所以这是一个*GKA*协议。

5 安全性分析

在ROM，ECDH假设下，分析了本文提出的AGKA的安全性(为了分析方便，将本协议简记为ID-AGKA)。

定理1 设协议中H，H_1，H_2分别是*ROM*中互不相同的Hash函数，在ECDH困难假设和安全认证方案的前提下，协议ID-AGKA是一个安全的AGKA协议，且具有前向安全性。即对一攻击者A，其最大运行时间为t，并设q_{ex}，q_s分别表示允许A在时间t内向ID-AGKA发送*Excute*询问、*Send*询问的最大次数，n是群成员的数目，$Adv_A^{ID-AGKA-fs}(t,q_{ex},q_s)$是攻击者成功攻击协议ID-AGKA的优势，$Succ_\Gamma^{Forge}(t)$是攻击者成功攻击该认证方案$\Gamma$的概率，$Succ_{G1}^{ECDH}(t)$是攻击者成功解决ECDH问题的概率，则有如下结论：

$$Adv_A^{ID-AGKA-fs}(t,q_{ex},q_s)\leqslant 2nSucc_\Gamma^{Forge}(t)+2q_Hq_s^2Succ_{G1}^{ECDH}(t)$$

上述定理可看出，ID-AGKA协议的安全性是建立在安全认证方案和ECDH问题基础上。为使证明过程更清晰，本文采用Shoup[21,22]提出的游戏理论来证明，该理论现已大量

应用于公钥密码系统和 AGKA 协议的安全性证明[11,23-27]，本文的证明方法与文献[11,27]类似。

证明：本文采用一系列游戏$\{Game_0,\cdots,Game_3\}$来模拟 A 对协议的攻击。在每个游戏中，A 执行 *Test* 查询并得到一个类似投币游戏的值 b。以 $Succ_i$ 表示攻击者在 $Game_i$ 中输出结果 b' 和查询结果 b 一致。

$Game_0$：这个游戏与实际协议 ID-AGKA 相同。所有成员都从 KGC 获得与自己身份(即公钥)相对应的私钥，并随机选取 a_i。在这个攻击游戏中，攻击者 A 的优势与他在攻击实际协议中所取得的优势相等，即有

$$\Pr[Succ_0]=\frac{Adv_A^{ID-AGKA-fs}+1}{2} \tag{1}$$

$Game_1$：在这个游戏中，考虑事件 *Forge* 发生的情况下攻击者 A 所能取得的优势。首先定义事件 *Forge* 为攻击者 A 伪造用户 U_i 关于消息 m 的认证码，并通过执行 Send 询问发送消息 m，代替 U_i 进行密钥协商，并且 m 能被其他成员验证、接收；而且，m 是首次使用，U_i 也未被执行过 $Corrupt(U_i)$ 询问。当事件 *Forge* 发生时，游戏停止，A 随机输出 b'。$Game_0$ 和 $Game_1$ 的不同之处在于事件 *Forge* 是否发生。所以 $|\Pr[Succ_1]-\Pr[Succ_0]|\leqslant\Pr[Forge]$。如果能正确猜中群中哪个成员被攻击者 A 假冒并且该成员又发生了事件 *Forge*，就可以成功地对 Choi 等的认证方案进行存在性伪造攻击，因此有 $Succ_\Gamma^{Forge}(t)\geqslant\frac{1}{n}\Pr[Forge]$，则进一步有

$$|\Pr[Succ_1]-\Pr[Succ_0]|\leqslant\Pr[Forge]\leqslant n\cdot Succ_\Gamma^{Forge}(t) \tag{2}$$

$Game_2$：给定 ECDH 多元组 $(P,A=xP,B=yP,C=xyP)$，无论何时成员 U_i 和 U_{i+1} 随机选择 a_i 和 a_{i+1}，并且计算 $P_i=a_iP$ 和 $P_{i+1}=a_{i+1}P$，则我们可对该游戏做作如下仿真：首先选取 $c_i,c_{i+1}\in_R Z_q^*$，计算 $P_i=c_iA$ 和 $P_{i+1}=c_{i+1}B$；其次，用 $c_ic_{i+1}C$ 计算相应的 Hash 值 $t_i^R(=t_{i+1}^L)$。由上可得，只要 $c_i,c_{i+1}\in_R Z_q^*$，则 $Game_2$ 与 $Game_1$ 相同。因此有

$$\Pr[Succ_2]=\Pr[Succ_1] \tag{3}$$

$Game_3$ 与 $Game_2$ 类似，只是给定多元组为 $(P,A=xP,B=yP)$，而没有给出这个 Diffie-Hellman 值 $C=xyP$ 的任何信息。无论何时成员 U_i 和 U_{i+1} 随机选择 a_i 和 a_{i+1}，并且计算 $P_i=a_iP$ 和 $P_{i+1}=a_{i+1}P$，我们仍可以按照 $Game_2$ 中的方法来仿真 $Game_3$。但在 U_i 或 U_{i+1} 在 ID-AGKA 协议的 *Round*3 向群中广播$\langle D_i,T_i\rangle$或$\langle D_{i+1},T_{i+1}\rangle$时，因为 $D_i=t_i^L\oplus t_i^R$ 且 $t_i^R=H_2(a_iP_{i+1}||h_i||ID)$，故可用随机值 $r\in_R\{0,1\}^k$ 来代替 t_i^R(或 t_{i+1}^L)。此时，定义事件 Hash 为攻击者 A 通过用 *HashOracle* 询问检测出广播消息中的 Hash 值 t_i^R(或 t_{i+1}^L)是不正确的。当攻击者 A 能正确猜出这个 Diffie-Hellman 值 $c_ic_{i+1}C$，且用该值进行 HashOracle 询问并接收到相应的询问结果(即对应的 Hash 值)时，事件 Hash 是可能发生的，因为此时攻击者 A 就会发现这个 Hash 值与前面所用的随机值 r 不同。当事件 Hash 发生时，游戏停止，A 随机输出 b'，因此有 $|\Pr[Succ_3]-\Pr[Succ_2]|\leqslant\Pr[Hash]$。

如果给定 $(P,A=xP,B=yP)$，要得到有效的 Diffie-Hellman 值 $C=xyP$，则必须满足两个条件：(1)两个成员 U_i 和 U_{i+1} 计算 $P_i=c_iA$ 和 $P_{i+1}=c_{i+1}B$ 并用随机值 $r\in_R\{0,1\}^k$ 来代替 t_i^R；(2) 然后，攻击者 A 用成功猜出的 Diffie-Hellman 值 $c_ic_{i+1}C$ 去询问 HashOracle，则事件 Hash 发生，则有 $Succ_{G1}^{ECDH}(t)\geqslant\frac{1}{q_Hq_s^2}\cdot\Pr[Hash]$，进一步有

$$|\Pr[Succ_3]-\Pr[Succ_2]|\leqslant\Pr[Hash]\leqslant q_Hq_s^2Succ_{G1}^{ECDH}(t) \tag{4}$$

因此在游戏 $Game_3$ 中，攻击者 A 在猜出结果 b 时并没有任何优势，因为我们假设是 Hash 函数 H,H_1,H_2 为 randomoracle，又因为 $t_i^R=H_2(a_iP_{i+1}||nonce_i)$，$h_i=H(D_i||P_i||nonce_i||P_{ID})$，$P_{ID}=P_1||\cdots||P_n$；故有每次 HashOracle 询问的输入均不同，因此

$$\Pr[Succ_3]=\frac{1}{2} \tag{5}$$

由式(1)－(5)，可得定理 1 中的结论。　　证毕。

6 ID-AGKA 协议效率分析

对一个 AGKA 协议效率的分析和比较，主要是对其轮数、通信量、计算量这 3 个方面进行分析和比较。由于 Choi. 等[13]的基于身份的 AGKA 协议后来在文献[19]被发现是不安全的，因此将本文的 ID-AGKA 协议仅与 Barua 等[18]的基于身份的 AGKA 协议比较。设群中用户数为 n，以 AGKA 协议完整运行一次(即从协议的初始化到群中所有成员都接受一个共享密钥)为一基本单位。在本文的 ID-AGKA 协议中，(1) 共需 3 轮，均为广播；(2) 每个用户发送的消息长度为 $2|G_1|+|k|$。计算量由以下几个部分组成：(1) n 次 *pairing* 计算；(2)$n+5$ 次点乘；(3) 每个用户需数 n 次模加法运算。

从表 1 中可看出，虽然本文的 ID-AGKA 协议在点乘上要比 Barua 等的多 n 次，但是在轮数上，Barua 等的却要比本文的多($\lceil\log_3 n\rceil-2$)轮；在每个用户发送消息长度上，本文方案中每个用户比 Barua 等的方案中的每个用户少发送的是 $(5n-2)(|G_1|+|k|)$ 比特；在计算 pairings 和模乘(加)的次数上，Barua 等的 AGKA 是本文的 AGKA 的($5\lceil\log_3 n\rceil$)倍和 9 倍，而一次 pairings 计算量相当于在相应超奇异椭圆曲线群上进行 24 次点乘运算[30]。因此，由以上比较可知，本文的方案与表 1 中 Barua 等的方案相比，在效率上有一定优势。

表 1　AGKA 协议的效率比较

协议	轮数	通信量(每个用户)	计算量(每个用户)		
		发送消息长度	pairings	点乘	模乘(加)法
Barua et. al[17]	$\lceil\log_3 n\rceil$	$5n\|G_1\|$	$5n\lceil\log_3 n\rceil+3$	5	$9(n-1)$
本文的 ID-AGKA 协议	3	$2(\|G_1\|+\|k\|)$	n	n+5	n

结束语　本文在总结现有相关 AGKA 协议结构特点的基础上，提出了一个新的基于身份的 AGKA 协议。该协议的认证部分是基于身份(ID)的，而会话密钥协商部分的运算主要用点乘实现。该协议与基于 PKI/CA 的 AGKA 协议相比，克服了后者在密钥管理上的困难；而与其它基于身份的 AGKA 协议相比，在效率上仍具有一定的优势，这主要是因为后者的会话密钥协商部分的计算主要用双线性对实现，而前者是主要用点乘实现。其次，本文对新提出的 AGKA 协议的安全性进行了证明。由于本文提出的 AGKA 协议是静态的，即没有考虑群成员加入和离去的开销，因此本文的下一步工作是在标准模型下研究该协议的动态情况。

参 考 文 献

[1] Bellare M, Rogaway P. Entity authentication and key distribution// Proc. of Crypto'93, LNCS773. Berlin, Heidelberg: SpringerVerlag, 1994: 232-249

[2] Bellare M, Rogaway P. Provable - secure Session Key Distribution: The Three Party Case// Proc. of the 27th Annual Symposium on the Theroy of Computing. ACM Press, 1995: 57-66

[3] Bellare M, Pointcheaval D, Rogaway P. Authenticated key exchange secure against dictionary attacks// Proc. of Eurocrypt'00, LNCS 1807. Berlin, Heidelberg: Springer-Verlag, 2000: 139-155

[4] Bresson E, Chevassut O, Pointcheval D. Dynamic Group Diffie-Hellman Key Exchange under Standard Assumption (Full version)// Proc. of Eurocrypt'02, LNCS 2332. Berlin, Heidelberg: Springer-Verlag, 2002: 321-336

[5] Bresson E, Chevassut O, Pointcheval D, et al. Provably Authenticated Group Diffie-Hellman Key Exchange// Proc. of 8th ACM CCS. ACM Press, 2001: 255-264

[6] Bresson E, Catalano D. Constant Round Authenticated Group Key Agreement via Distributed Computation// Proc. of Public-Key Cryptgraphy, LNCS 2947. Berlin, Heidelberg: Springer-Verlag, 2004: 115-129

[7] Steiner M, Tsudik G, Waidner M. Key Agreement in Dynamic Peer Groups. IEEE Trans. on Parallel and Distributed Systems, 2000, 11(8): 769-780

[8] Burmester M, Desmedt Y. A Secure and Efficient Conference Key Distribution System// Proceedings of Eurocrypt'94, LNCS 950. Berlin, Heidelberg: Springer-Verlag, 1995: 275-286

[9] Burmester M, Desmedt Y. A Secure and Scalable Group Key Exchange System. Information Processing Letters, 2005, 94(3): 137-143

[10] Katz J, Yung M. Scalable Protocols for Authenticated Group Key Exchange// Proceedings of Crypto'03, LNCS 2729. Berlin, Heidelberg: Springer-Verlag, 2003: 110-125

[11] Kim Hyun-Jeong, Lee Su-Mi, Lee Dong Hoon. Constant-round Authenticated Group Key Exchange for Dynamic Groups// Proceedings of Asiacrypt'04, LNCS 3329. Heidelberg: Springer-Verlag, 2004: 245-259

[12] Dutta R, Barua R. Constant Round Dynamic Group Key Agreement // Proceedings of ISC'2005, LNCS. Berlin, Heidelberg: Springer-Verlag, http://eprint.iacr.org/2005/221, 2005

[13] Choi Kyu Young, Hwang Jung Yeon, Lee Dong Hoon. Efficient ID-based Group Key Agreement with Bilinear Maps// Proc. of Public-Key Cryptography, LNCS 2947. Springer-Verlag, 2004: 130-144

[14] Joux A. One round protocol for tripartite Diffie-Hellman// Bosma W, ed. Proceedings of Algorithmic Number Theory Symposium (ANTS)IV, LNCS 1838. Springer-Verlag, 2000: 385-394

[15] Al - Riyami S, Paterson K G. Tripartite Authenticated Key Agreement Protocols from Pairings. Cryptology eprint Archive, 2002. http://eprint.iacr.org/

[16] Zhang F, Liu S, Kim K. ID-based One Round Authenticated Tripartite Key Agreement Protocols with Pairings. Cryptology ePrint Archive, Report 2002/035. 2002. http://eprint.iacr.org/

[17] Nalla D, Reddy K C. Identity - based Authenticated Group Key Agreement Protocol // Proc. of Indocrypt'02, LNCS 2551. Springer-Verlag, 2002: 110-125

[18] Barua R, Dutta R, Sarker P. Extending Joux's Protocol to Multi Party Key Agreement// Proc. of Indocrypt'03. LNCS 2947. Berlin, Heidelberg: Springer-Verlag, 2004: 130-144

[19] Zhang Fangguo, Chen Xiaofeng. Attack on an ID-based authenticated group key agreement scheme from PKC 2004. Information Processing Letters, 2004(91): 191-193

[20] Katz J, Shin J S. Modeling Insider Attacks on Group Key-Exchange Protocols// Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05). ACM Press, 2005: 180-189

[21] Cramer R, Shoup R. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003, 33(1): 167-226

[22] Shoup V. equences of games: a tool for taming complexity in security proofs, manuscript. Nov. 30, 2004. Revised, May 27, 2005; Jan. 18, 2006. http://shoup.net/papers/

[23] Bresson E, Chevassut O, Pointcheval D. Security proofs for an efficient password-based key exchange // Proc. of ACM-CCS'03. ACM Press, October 2003

[24] Abdalla M, Bresson E, Chevassut O, et al. Password - based Group Key Exchange in a Constant Number of Rounds// Yung M, Dodis Y, Kiayias A, et al., eds. Public Key Cryptography-PKC 2006. LNCS 3958. Springer-Verlag, April 2006: 427-442

[25] Abdalla M, Pointcheval D. A Scalable Password - based Group Key Exchange Protocol in the Standard Model// Lai X, Chen K, eds. Advances in Cryptology - Proceedings of ASIACRYPT '06 (december 2 - 6, 2006, Shanghai, China). LNCS 4284. Springer-Verlag, 2006: 332-347

[26] Abdalla M, Bohli J-M, Isabel M, et al. (Password) Authenticated Key Establishment: From 2-Party To Group// Vadhan S P, ed. Theory of Cryptography Conference--TCC 2007, LNCS 4392. IACR, February 2007: 499-514

[27] Bresson E, Chevassut O, Essiari A, et al. Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices // The Fifth IEEE International Conference on Mobile and Wireless Communications Networks. 2003

[28] 卿斯汉. 安全协议 20 年研究进展. 软件学报, 2003, 14(10): 1740-1752

[29] 冯登国. 可证明安全性理论与方法研究. 软件学报, 2005, 16(10): 1743-1756

[30] Boyen X. The BB1 Identity-based cryptosystem: A standard for Encryption and Key Encapsulation. http://grouper.ieee.org/groups/1363/IBC/submissions/index.html, Submitted 2006-08-14