# 群密钥协商协议的效率分析

王明辉[1,2],王建东[1]
(1. 南京航空航天大学 信息科学与技术学院,江苏 南京 210016;
2. 盐城工学院 现代教育技术中心,江苏 盐城 224051)

**摘要**:给出了两类群密钥协商协议的效率比较,它们分别是基于口令群密钥协商协议和基于双线性对群密钥协商协议。比较的结果为对密钥协商协议的安全性分析,形式化证明及设计更有效、更安全的群密钥协商协议提供了很大的帮助。

**关键词**:群密钥协商,双线性对,安全性分析
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1671-5322(2011)01-0059-03

密钥协商协议的目的是在参与通信的成员之间快速建立一个安全的通信信道。随着两方、三方密钥协商协议的发展,群密钥协商协议由于应用范围广,也越来越受到密钥管理研究者的重视,现有的应用领域有视频会议、安全数据复制等。

自从DH密钥交换协议[1]发表之后,研究者们很快把它推广到多方参与的密钥协商协议中来,1982年,在文献[2]中,Ingemarsson等人首次应用DH问题,提出了群密钥协商方案。标志着群密钥协商协议研究的开始。

群密钥协商协议允许群内的通讯方在一个不安全的,开放的网络环境下建立一个共有的会话密钥,这个会话密钥只能被有效的群内的成员所知,将被用于加密群成员之间的通信。由于群密钥协商协议的应用,可以不需要认证中心的参与,这就给用户带来很大的方便。

近年来,关于群密钥协商协议的研究也有了不同的方向,例如基于双线性对的群密钥协商协议,基于口令的群密钥协商协议,基于椭圆曲线的群密钥协商协议。还有人专门研究群密钥协商协议的设计,效率分析,安全性分析,形式化证明模型等等。

## 1 群密钥协商协议中涉及到的困难假设

CDH参数描述:$G_1$ 是一个 $q$ 阶循环加法群,$G_2$ 是一个和 $G_1$ 同阶的循环乘法群。

CDH问题(可计算Diffie-Hellman问题):在一个 $q$ 阶加法群 $G$ 中,当给定一个 $G$ 的生成器 $P$ 和 $aP,bP(a,b\in Z_q^*)$ 时,计算出 $abP$ 的值。准确地说,攻击者 $A$ 关于 $IG_{CDH}$ 的定义如下:

$$Pr[A(G,P,aP,bP) = abP \mid G\leftarrow IG_{CDH}(1^k);P\leftarrow G;a,b\leftarrow Z_q^*]$$

如果攻击者 $A$ 任何多项式时间(PPT)内解决CDH问题的优势是可忽略的,$IG_{CDH}$ 满足CDH假设。

DDH问题(判定Diffie-Hellman问题):$G$ 是一个 $q$ 阶有限循环群。DDH问题的定义如下:给定一个三元组$\langle U,V,W\rangle$,区分这个三元组是一个DH三原组$\langle g^a,g^b,g^{ab}\rangle$,还是一个随机三元组$\langle g^a,g^b,g^r\rangle$,如果:$|\Pr[a,b\leftarrow Z_q:A(g,g^a,g^b,g^{ab})=1]-\Pr[a,b,r\leftarrow Z_q:A(g,g^a,g^b,g^r)=1]|\geq\varepsilon$,那么在运行时间内,算法 $A$ 的优势 $Adv_{G,A}^{ddh}(t)$ 等于 $\varepsilon$。

当给定一个 $G$ 的生成器 $P$ 和 $aP,bP(a,b\in Z_q^*)$ 时,计算出 $abP$ 的值。准确地说,攻击者 $A$ 关于 $IG_{CDH}$ 的定义如下:

$$Pr[A(G,P,aP,bP) = abP \mid \leftarrow IG_{CDH}(1^k);P\leftarrow G;a,b\leftarrow Z^*q]$$

如果攻击者 $A$ 任何多项式时间(PPT)内解决CDH问题的优势是可忽略的,$IG_{CDH}$ 满足CDH假设。

BDH参数描述:$G_1$ 和 $G_2$ 是两个同阶 $q$ 的群。双线性映射:$G_1\times G_1\rightarrow G_2$

收稿日期:2010-10-19
作者简介:王明辉(1977-),男,黑龙江绥棱县人,讲师,硕士研究生,主要研究方向为信息安全。

DBDH 问题(判定双线性 Diffie - Hellman 问题)在$[G_1,G_2,e]$中:非正式地说,DBDH 问题就是区分$(P,aP,bP,cP,e(P,P)^{abc})$和$(P,aP,bP,cP,e(P,P)^{d})$$(P\in G_1;a,b,c,d\in Z_q^*)$准确地说,攻击者 $A$ 关于$IG_{CDH}$的定义如下:

$$\left|Pr\left[A(G_1,G_2,e,P,aP,bP,cP,e(P,P)^{abc})=1\left|\begin{matrix}(G_1,G_2,e)\leftarrow IG_{CDH}(1^k);\\P\leftarrow G;a,b,c\leftarrow Z_q^*\end{matrix}\right.\right]-\right.$$
$$\left.Pr\left[A(G_1,G_2,e,P,aP,bP,cP,e(P,P)^{abc})=1\left|\begin{matrix}(G_1,G_2,e)\leftarrow IG_{CDH}(1^k);\\P\leftarrow G;a,b,c\leftarrow Z_q^*\end{matrix}\right.\right]\right|$$

如果攻击者 $A$ 任何多项式时间(PPT)内解决 DBDH 问题的优势是可忽略的,$IG_{CDH}$满足 DBDH 假设。

**双线性映射**:我们称 $e:G_1\times G_1\rightarrow G_2$ 是一个可接受的双线性映射,如果映射满足下列属性:

(1)双线性:$e(aP,bQ)=(aP,bQ)^{ab}$$(P,Q\in G_1;a,b\in Z_q^*)$

(2)非退化性:存在一个 $P\in G_1$,使得 $e(P,P)\neq 1$

(3)可计算性:存在一个有效的算法能够计算出 $e(P,Q)$$(P,Q\in G_1)$

## 2 对于不同类型群密钥协商协议的效率分析

### 2.1 基于口令的群密钥协商协议

在文献[3]中提出了 PAGKE 协议,我们称之为协议 2.1.1,其描述如下:第 1 轮:每一个用户 $U_i$ 选一个随机整数 $r_i\in Z_q^*$,计算 $x_i=g_1^{r_i}$ 模 $p$,$X_i=x_i\cdot g_2^{H(pw\|U_i)}$ 模 $p$。用户 $U_i$ 广播 $U_i\|1\|X_i$。

第 2 轮:每个用户 $U_i$ 使用 $pw$ 和发送者的 ID $(U_{i-1},U_{i+1})$分别计算 $x_{i-1}$和 $x_{i+1}$,然后计算 $Y_i=(x_{i+1}/x_{i-1})^{ri}$,并且广播 $U_i\|2\|Y_i$。

密钥计算:每个用户 $U_i$ 为 $F$ 计算密钥 $k_i=(x_{i-1})^{nr_i}\cdot Y_i^{n-1}\cdot Y_{i+1}^{n-2}\cdots\cdot Y^{i-2}$模 $p$。会话密钥 $sk_i=F_{sk_i}(U\|sid)(U=U_1,\cdots U_n,sid=1\|X\|2\|Y,X=X_1,\cdots X_n,Y=Y_1,\cdots Y_n)$。

可以看出协议的 $n$ 个成员进行了 $2n$ 次广播、$4n$ 次求幂的计算和 2 轮的密钥协商。

在文献[4]中提出了 PGKEP 协议,我们称之为协议 2.1.2,其描述如下:

第 1 轮:每一个用户 $U_i$ 选一个随机整数 $x_i\in Z_p^*$,广播 $ID_i\|E_{pw}(g^{x_i})$。

第 2 轮:收到 $ID_j\|E_{pw}(g^{x_j})$以后,每个用户 $U_i$ 计算 $w_i=h(g^{x_i-1^{x_i}})\oplus h(g^{x_ix_{i+1}})$,并且广播 $ID_i\|w_i$。

密钥计算:收到 $ID_j\|w_j(i\neq j)$以后,每个用户 $U_i$ 连续地计算 $h(g^{x_j-1^{x_j}})(1\leqslant j\leqslant n)$和群会话密钥 $SK$,具体如下:

$$h(g^{x_j-1^{x_j}})=w_j\oplus h(g^{x_jx_j})=h(g^{x_jx_j})\oplus h(g^{x_jx_{j+1}})\oplus h(g^{x_{j+1}x_{j+2}})$$
$$SK=H(h(g^{x_1x_2})\|\cdots\|h(g^{x_nx_n-1^{x_n}})\|h(g^{x_nx_1}))$$

可以看出协议的 $n$ 个成员进行了 $2n$ 次广播、$2n$ 次求幂的计算和 2 轮的密钥协商。

### 2.2 基于双线性对的群密钥协商协议

在文献[5]中提出了 AGKA 协议,我们称之为协议 2.2.1,其描述如下:

第 1 轮:每一个用户 $U_i$ 选一个随机整数 $a_i\in Z_q^*$,计算 $P_i=a_iP$。用户 $U_i$ 向其他用户广播 $P_i$。

第 2 轮:当收到 $P_{i-1}P_{i+1}P_{i+2}$后,每个用户 $U_i$ 计算:$D_i=e(a_i(P_{i+2}-P_{i-1}),P_{i+1})$,并且广播 $D_i$ 给所有其他用户。

密钥计算:每个用户计算 $K_i=e(a_iP_{i-1},P_{i+1})^nD_i^{n-1}D_{i+2}^{n-2}\cdots D_{i-2}$ 会话密钥 $K=e(P,P)^{a_1a_2a_3+\cdots+a_{n-1}a_na_1+a_na_1a_2}$

可以看出协议的 $n$ 个成员进行了 $2n$ 次广播、$3n$ 次求幂的计算和 2 轮的密钥协商。

在文献[6]中提出了 T - AGKA 协议,我们称之为协议 2.2.2,其描述如下:

参数描述:

$H_1:\{0,1\}^*\rightarrow G_1$; $H_2:G_2\rightarrow\{0,1\}^n$;

$H_3:\{0,1\}^n\rightarrow\{0,1\}^n$; $H_4:G_2\rightarrow\{0,1\}^n$;

$H_5:\{0,1\}^n\rightarrow Z_q^*$; $H_6:G_1\rightarrow\{0,1\}^n$

第 1 轮:每一个用户 $U_i$ 选一个随机整数 $\delta\overset{R}{\leftarrow}G_2,r\leftarrow\{0,1\}^n,k_1\leftarrow Z_p^*$,然后 $U_i$ 计算 $D_1=\langle R,P_2,\cdots\cdots,P_n,V,W,L\rangle$

$D_1=\langle\delta,r\oplus H_4(e(S_1,Q_2)\cdot\delta),\cdots\cdots,r\oplus H_4(e(S_1,Q_n)\cdot\delta),H_5(r)\cdot k_1P_{pub},L\rangle$,并且广播 $D_1$。

第 2 轮:当收到 $D_1$ 后,每个用户 $U_i(2\leqslant i\leqslant n)$计算:$r'=H_4(e(Q_1,S_i)\cdot R)\oplus P_i$,如果 $D_1$ 是有效的,显然 $r'=r$,然后 $U_i$ 选 $k_i\overset{R}{\leftarrow}Z_p^*$,并且计算和广播 $D_i=\langle H_5(r)\cdot k_iP,k_iP_{pub}\rangle$给所有其他用户。

密钥计算:收到 $D_i$ 以后,每个用户 $U_1$ 计算 $z_1=H_5(r)^{-1}\cdot V,z_j=H_5(r)^{-1}\cdot X_j(2\leqslant j\leqslant n)$确认 $\hat{e}(P,\sum_{j=1}^{n}Y_j)^?=\hat{e}(P_{pub},\sum_{j=1}^{n}z_j)$。如果成立,$U_i$ 就确

认了参与方是组的有效成员。$U_i$ 计算会话密钥 $K=K_i=H_6(z_1)\oplus\cdots\oplus H_6(z_n)$。

可以看出协议的 $n$ 个成员进行了 $2n$ 次广播、$3n$ 次求幂的计算和2轮的密钥协商。

## 3 不同类型协议之间的效率比较

我们给出了两类群密钥协议,每种协议中我们分别给出了两个具体的协议,它们的具体比较细节如表1、表2所示。

两类协议都是基于离散对数困难性问题的。在困难性假设上,公认的是CDH假设弱于DDH假设。双线性对应用于DH假设就形成了BDH问题。由于椭圆曲线有一些独特的特性,所以,双线性对往往取自椭圆曲线,这样,BDH问题的困难性取决于双线性对的难度和具体的椭圆曲线方程。

表1　基于口令群密钥协议效率比较

Table 1　Efficient comparation of password based on group PKE

| 协议 | 轮数 | 求幂 | 广播次数 | 难题假设 |
|---|---|---|---|---|
| 协议2.1.1 | 2 | 4n | 2n | DDH |
| 协议2.1.2 | 2 | 2n | 2n | CDH |

表2　基于双线性对的群密钥协议效率比较

Table 2　Efficient comparation of bilinear pairings based group PKE

| 协议 | 轮数 | 消息 | 双线性对运算 | 难题假设 |
|---|---|---|---|---|
| 协议2.2.1 | 2 | 2n | 3n | DBDH和CDH |
| 协议2.2.2 | 2 | n+1 | 4n | DBDH |

## 4 结论

同类型的群密钥协商协议,由于协议的设计方法不同,它们之间的效率有可比性,不同类型的协议,由于适用的环境不同,在上述比较结果中不具有可比性。

我们从轮数、求幂计算次数、发送广播次数、难题假设等几个方面比较了不同类型的群密钥协商协议的效率,有利于我们更深入地理解协议的运行过程,为我们设计更加安全的密钥协商协议提供了材料,并且为我们对协议进行安全性分析和形式化证明打下了坚实的基础。

**参考文献:**


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

[2] Ingemarsson I, Tang D T, Wong C K. A Conference Key Distribution System[J]. IEEE Transactions on Information Theory, 1982,28(5):714-720.

[3] Jeong Ok Kwon, Ik Rae Jeong, Dong Hoon Lee. Provably-Secure Two-Round Password Authenticated Group Key Exchange in the Standard Model[C]. H. Yoshiura et al. (Eds.)2006:322-336.

[4] Su Mi Lee, Jung Yeon Hwang, Dong Hoon Lee. Efficient Password-Based Group Key Exchange[C]. S. Katsikas, J. Lopez, and G. Pernul (Eds.): TrustBus 2004:191-199.

[5] K Y C, J Y H, D H L. Efficient ID-based Group Key Agreement with Bilinear Maps[C]. F. Bao et al. (Eds.):PKC 2004:130-144.

[6] Lan Zhou, Willy Susilo, Yi Mu. Efficient ID-Based Authenticated Group Key Agreement from Bilinear Pairings[C]. J. Cao et al. (Eds.): MSN 2006:521-532.


# Efficient Analysis of Group Key Exchange Protocol


WANG Ming-hui[1,2], WANG Jian-dong[1]

(1. Nanjing University of Aeronautics and Astronautics, College of Information Sience and Technology, Jiangsu Nanjing 201106, China;
2. Modern Educational Technology Center, Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)



**Abstract**: In this paper, the compare about efficiency of two group key exchange protocols is given, in which one is password-based group key exchange protocol, the other is bilinear pairings-based on group key exchange protocol. The result for the comparison is helpful for security analysis, design and formal proof of group key exchange protocols.



**Keywords**: group key exchange, bilinear pairings, security analysis　(责任编辑:沈建新; 校对:张英健)