认证群密钥协商协议的安全性分析与改进

汪小芬[1]，李胜强[2]，肖国镇[1]

(1. 西安电子科技大学ISN综合业务网国家重点实验室 西安 710071; 2. 电子科技大学计算科学与工程学院 成都 610054)

【摘要】对Tseng协议构造了一种有效的中间人伪造攻击，敌手可以成功获得群会话密钥，因此Tseng协议不满足密钥认证性。然后基于Tseng协议的安全缺陷，提出改进协议，并进行安全性分析和性能分析。改进协议实现了通信节点之间的双向认证，不但满足前向安全性、密钥认证性，还能有效抵抗被动攻击和中间人伪造攻击。改进协议中的低能量节点计算出会话密钥的时间只需2.03 s，高能量节点的计算时间仅为原协议的1/2，并且通信开销减小了40%，更适用于能量受限，带宽受限的移动通信系统。

关 键 词 群密钥协商; 前向安全性; 密钥认证; 中间人伪造攻击

中图分类号 TN918 **文献标识码** A

Analysis and Improvement of an Authenticated Group Key Agreement Protocol

WANG Xiao-fen[1], LI Sheng-qiang[2], and XIAO Guo-zhen[1]

(1. National Key Lab of Integrated Service Networks， Xidian University Xi'an 710071;

2. School of Computer Science and Engineering , University of Electronic Science and Technology of China Chengdu 610054)

Abstract An authenticated group key agreement protocol for resource-limited mobile devices was proposed by Tseng Y.M. It is demonstrated that this protocol has security vulnerabilities by mounting a man-in-middle attack against it. The protocol can not achieve key authentication in the presence of an active attacker. This paper presents an improved protocol which achieves mutual authentication. It provides not only the capability of forward secrecy and key authentication, but also the capability against passive attack and man-in-middle attack. The analysis shows that the presented protocol has lower computation cost and communication cost compared with Tseng's protocol.

Key words group key agreement; forward secrecy ; key authentication; man-in-middle attack

密钥协商是安全通信的重要环节，通过密钥协商协议，可在通信节点之间建立共享会话密钥，以便实现开放网络中的安全通信。文献[1]提出了第一个两方的密钥协商协议，即Diffie-Hellman协议。

基于Diffie-Hellman协议，相继又提出了很多群密钥协商协议，用于多方间建立共享密钥，实现群组通信的安全目标，如广播和多播的机密性和数据完整性等。文献[2]提出认证的群密钥协商协议，使得群成员能显式认证对方的身份，然而该协议没有给出严格的安全性证明。文献[3-4]首次给出了认证群密钥协商协议的正规安全模型，并提出了几个可证明安全的协议[3-4]。然而这类协议中，固定的环状通信结构和随节点数目增加而线性增长的通信轮数导致协议很不实用。文献[5]提出一个能抵抗恶意参与者的群密钥协商协议，该协议仅需两轮通信，满足前向安全性，并且在被动攻击下是可证明安全的。然而该协议需要较大的计算复杂度，不适用于无线通信。文献[6]提出了一个适用于能量和带宽受限的无线通信的群密钥协商(Tseng)协议，并认为该协议满足隐式密钥认证，能抵抗伪造攻击。然而，研究中发现Tseng协议[6]存在安全缺陷，中间敌手通过篡改高能量节点的通信信息，伪装成高能量节点，发送信息给各低能量节点，能得到群会话密钥。因此，它不能抵抗中间人伪造攻击，也不满足密钥认证性。针对Tseng协议中的安全缺陷，本文提出的改进后的协议不但满足前向安全性、密钥认证性[7-8]，还能有效抵抗被动攻击和中间人伪造攻击。改进协议中的低能量节点计算出会话密钥的时间只需2.03 s，高能量节点的计算时间仅为原协议的1/2，通信开销减小了40%，对于能量受限、带宽受限的移动通信更加高效实用。

收稿日期：2007 – 09 – 24；修回日期：2008 – 04 – 23
基金项目：国家自然科学基金(60773003, 60603010)
作者简介：汪小芬(1982 –)，女，博士生，主要从事密码学方面的研究.

1 Tseng协议介绍

令$U_i(1\leqslant i\leqslant n)$表示低能量节点； S 表示高能量节点；G 表示阶为 p (p 为大素数)的群；g 为G 的生成元； $(\mathrm{PK}_i,\mathrm{SK}_i)$ 为U_i 的Shamir-Tauman签名[9]密钥对； SK_i 为从 Z_p 中随机选取的； $\mathrm{PK}_i=g^{\mathrm{SK}_i}$ ； $(\mathrm{PK}_s,\mathrm{SK}_s)$ 为S 的类似的签名密钥对，PK_s 公开；H 为Hash函数。

$U_i(1\leqslant i\leqslant n)$ 与 S 执行以下协议：

(1) Z_p 中随机选取 x_i ，并计算 x_i^{-1} 、$\alpha_i=(PK_s)^{x_i}$ 、$y_i=g^{x_i}$ 和 $\sigma_i=\mathrm{Sign}(\mathrm{SK}_i,y_i)$ ，U_i 对 y_i 的Shamir-Tauman签名， $(x_i,x_i^{-1},\alpha_i,y_i,\sigma_i)$ 由 U_i 预计算并保存。U_i 将 y_i 和 σ_i 发送给 S 。

(2) S 验证 U_i 的签名 σ_i 的正确性，若验证成功，S 在 Z_p 中随机选取 x ，计算 $X=g^x$ 、 $z_i=y_i^x$ 、$\alpha_i'=(y_i)^{\mathrm{SK}_s}$ 和 $C=H(X\oplus z_1\oplus z_2\oplus\cdots\oplus z_n)$ ， S 将消息 $M=[C,\alpha_i'(1\leqslant i\leqslant n),z_i(1\leqslant i\leqslant n)]$ 广播。

(3) U_i 计算 $X'=(z_i)^{x_i^{-1}}$ 、 $C'=H(X'\oplus z_1\oplus z_2\oplus\cdots\oplus z_n)$ ； U_i 检验 $\alpha_i'=\alpha_i$ 、 $C'=C$ 是否成立，且 $z_i\neq 1(1\leqslant i\leqslant n)$ 。如果检验成功， U_i 计算会话密钥 $K=X'\prod_{i=1}^{n}z_i$ 。

2 Tseng协议的一种有效的伪造攻击

主动攻击敌手 A 能实施中间人伪造攻击，通过截获和伪造通信双方 S 和 $U_i(1\leqslant i\leqslant n)$ 之间的信息，得到群会话密钥。敌手 A 实施的攻击如下：

(1) A 窃听到 U_i 发送给 S 的消息 (y_i,σ_i) ；

(2) A 随机选取 $r\in Z_p$ ，计算 $X^*=g^r$ 、$z_i^*=y_i^r$ 和 $C^*=H(X^*\oplus z_1^*\oplus\ldots\oplus z_n^*)$ ；

(3) A 截获 S 发送给 U_i 的消息 $M=[C,\alpha_i'(1\leqslant i\leqslant n),z_i(1\leqslant i\leqslant n)]$ ，将伪造的消息 $M^*=(C^*,\alpha_i'(1\leqslant i\leqslant n),z_i^*(1\leqslant i\leqslant n))$ 发送给节点 $U_i(1\leqslant i\leqslant n)$ ，其中 $\alpha_i'(1\leqslant i\leqslant n)$ 保持不变；

(4) 节点 $U_i(1\leqslant i\leqslant n)$ 接收到消息 M^* 后，计算 $X'=(z_i^*)^{x_i^{-1}}=g^r$ 和 $C'=H(X'\oplus z_1^*\oplus z_2^*\oplus\cdots\oplus z_n^*)$ ，显然， $C'=C^*$ 、 $\alpha_i=\alpha_i'$ 成立，于是 $U_i(1\leqslant i\leqslant n)$ 计算出 $K=X'\prod_{i=1}^{n}z_i^*=g^r\prod_{i=1}^{n}z_i^*$ ；

(5) A 计算出各节点的会话密钥 $K=g^r\prod_{i}^{n}z_i^*$ ，因此敌手 A 成功掌握了各节点的会话密钥 K 。

由以上的攻击可发现，高能量节点 S 与各低能量节点 $U_i(1\leqslant i\leqslant n)$ 没有实现相互认证，低能量节点 U_i 不能确定收到的消息 M 是否来自节点 S 。于是敌手可成功获得节点间的会话密钥。因此，在主动攻击敌手存在的情况下，Tseng协议不满足密钥认证的性质。

3 一种改进的认证群密钥协商协议

Tseng协议不能抵抗中间人伪造攻击，原因在于通信方没有对发送的消息提供认证，造成接收方不能确定消息来自真正的发送方还是中间敌手。虽然在Tseng协议中，U_i 计算并发送 $\alpha_i=(\mathrm{PK}_s)^{x_i}$ 给 S ， S 计算并发送 $\alpha_i'=(y_i)^{\mathrm{SK}_s}$ 给 U_i ，U_i 通过验证 $\alpha_i'=\alpha_i$ 认证 S 的身份，然而对于主动攻击的敌手，因为不能提供 S 所发送信息的完整性保护，而使得 U_i 无法真正认证消息发送方。本文基于Tseng协议的安全缺陷，提出一个改进协议.在改进协议中省略对 $\alpha_i=(\mathrm{PK}_s)^{x_i}$ 和 $\alpha_i'=(y_i)^{\mathrm{SK}_s}(1\leqslant i\leqslant n)$ 的计算及发送。

选择两个保密的大素数 p 和 q (长度为1 024 bit，且 $N=p\times q$ 、 $g\in Z_p$)； 节点 S 的签名密钥对为 (e,d) ， $e\times d\equiv 1\bmod\ \psi(N)$ ， e 和 d 的长度均为17 bit， e 公开， d 保密； I_s 为节点 S 的身份信息；节点 U_i 的签名密钥对为 $(\mathrm{PK}_i,\mathrm{SK}_i)$ ， $\mathrm{PK}_i=g^{\mathrm{SK}_i}$ 公开， $\mathrm{SK}_i\in Z_p^*$ 保密； $H:\{0,1\}^*\rightarrow Z_p^*$ 为Hash函数。

S 与 $U_i(1\leqslant i\leqslant n)$ 执行如下协议：

(1) U_i 随机选取 $x_i\in Z_p^*$ ，预计算并保存 $(x_i,x_i^{-1},y_i,\sigma_i)$ ，其中 $y_i=g^{x_i}$ ； $\sigma_i=\mathrm{Sign}(\mathrm{SK}_i,y_i)$ 是 U_i 对 y_i 的Shamir-Tauman在线/离线签名， U_i 将 (y_i,σ_i) 发送给 S 。

(2) S 验证 U_i 签名 σ_i 的正确性，若检验成功， S 随机选取 $x\in Z_p$ ，计算 $X=g^x$ 、 $z_i=y_i^x$ 、 $C=H(X\oplus z_1\oplus z_2\oplus z_2\oplus\cdots\oplus z_n)$ 和 $\sigma=(C-I_s)^d\mod N$ ， S 将 $(C,z_i(1\leqslant i\leqslant n),\sigma)$ 发送给 $U_i(1\leqslant i\leqslant n)$ 。

(3) $U_i(1\leqslant i\leqslant n)$ 收到消息后，计算 $X'=z_i^{x_i^{-1}}$ ，$C'=H(X'\oplus z_1\oplus z_2\oplus\cdots\oplus z_n)$.验证 $\sigma^e+I_s=C'\bmod N$ 是否成立。若成立，则 U_i 计算出会话密钥 $K=X'\prod_{i=1}^{n}z_i=g^{x(1+x_1+\cdots+x_n)}$ 。

4 协议的安全性证明与性能分析

4.1 安全性证明

假设1 判定Diffie-Hellman假设(DDH)[10]：

参数 p 和 q 是大素数, $p=2q+1$, g 是 q 阶子群 G_q 的生成元。给定 $y_a=g^{x_a}\bmod p$ 和 $y_b=g^{x_b}\bmod p$ ，x_a 和 x_b 是在 Z_q 中随机选取的，则三元组

$(y_a, y_b, g^{x_a x_b} \bmod p)$ 和 (y_a, y_b, R) 是多项式不可区分的，其中 R 在 Z_q 中随机选取，即不存在有效的多项式时间算法 A，在 x_a, x_b，R 随机选取时，对任意多项式 Q 满足：

$$\left|\Pr[A(g^{x_a}, g^{x_b}, g^{x_a x_b}) = \text{true}] - \Pr[A(g^{x_a}, g^{x_b}, R) = \text{true}]\right| > \frac{1}{Q|q|}$$

假设2　RSA困难假设[11]：

N 是两个大素数的乘积；e 是一个整数，满足 $\gcd(e, \psi(N)) = 1$。给定任意的 $c \in Z_N^*$，计算出 $m \in Z_N^*$ 满足 $m^e = c \bmod N$ 是困难问题。

定理1　在假设1成立的前提下，改进协议在被动攻击下是安全的。

证明　被动攻击敌手 A 窃听到 y_i 和 z_i，即 (g^{x_i}, g^{xx_i})，将证明敌手不能由 (y_i, z_i) 计算得 $K = X\prod_{i=1}^{n} z_i \bmod p$。本文用反证法证明。

假设敌手由 (y_i, z_i) 可得 $K = X\prod_{i=1}^{n} z_i \bmod p$，则存在有效的多项式时间算法 P，以不可忽略的概率区分 (y_i, z_i, K) 与 (y_i, z_i, R)，即能区分 $(g, g^{x_i}, g^{xx_i}, g^x g^{xx_i})$ 与 $(g, g^{x_i}, g^{xx_i}, R)$，$R$ 是随机数，于是敌手可区分 $(g, g^{x_i}, g^{xx_i}, g^x g^{xx_i})$ 与 $(g, g^{x_i}, g^{xx_i}, R' g^{xx_i})$，等价于可区分 $(g, g^{x_i}, g^{xx_i}, g^x)$ 与 $(g, g^{x_i}, g^{xx_i}, R')$，$R'$ 为随机数.设 $h = g^{x_i}$，则 $g = h^{y_i}$、$g^{xx_i} = h^x$、$g^x = h^{xy_i}$，存在多项式时间算法 P' 以不可忽略的概率区分 $(h, h^{y_i}, h^x, h^{xy_i})$ 与 (h, h^{y_i}, h^x, R')，与假设1矛盾。因此，改进协议在判定Diffie-Hellman假设成立的条件下，能抵抗敌手的被动攻击。

定理 2　在假设2成立的前提下，改进协议能抵抗中间人伪造攻击。

证明　改进协议提供了高能量节点与低能量节点之间的互相认证。$\sigma_i = \text{Sign}(\text{SK}_i, y_i)$ 是Shamir-Tauman签名[9]，它提供了高能量节点 S 对低能量节点 $U_i (1 \leqslant i \leqslant n)$ 的认证。$(C, z_i (1 \leqslant i \leqslant n), \sigma)$ 中 σ 是节点 S 的RSA签名，使得节点 $U_i (1 \leqslant i \leqslant n)$ 能验证消息的发送方 S 及所发送的消息。若敌手要得到会话密钥 K 必须伪造 z_i^*、Hash函数值 C^* 和RSA签名 σ^*，满足 $(\sigma^*)^e + I_s = c^* \bmod N$。然而，由RSA困难问题假设和hash函数的性质可知，敌手要伪造能通过验证的消息组 $(C^*, z_i^* (1 \leqslant i \leqslant n), \sigma^*)$ 是不可行的。

假设敌手可伪造能通过验证的消息组 $(C^*, z_i^* (1 \leqslant i \leqslant n), \sigma^*)$，则敌手可随机选取 $r \in Z_p$，计算 $X^* = g^r$、$z_i^* = y_i^r$ 和 $C^* = H(X^* \oplus z_1^* \oplus z_2^* \oplus \cdots \oplus z_n^*)$，伪造 σ^* 满足 $(\sigma^*)^e = c^* - I_s \bmod N$，与假设2矛盾。因此，改进协议能抵抗中间人伪造攻击。

定理 3　改进协议满足密钥认证性。

证明　由定理2可知，消息 (y_i, σ_i) 认证了低能量节点 U_i 发送的信息和身份信息；消息 $(C, z_i (1 \leqslant i \leqslant n), \sigma)$ 认证了高能量节点 S 发送的信息和 S 的身份信息。因为仅有 U_i 掌握 $(x_i, x_i^{-1}, y_i, \sigma_i)$，然后由 z_i 计算得 g^x，最后计算出 K。敌手通过被动攻击或中间人伪造攻击都不能得到 K。协议执行结束后，各节点能确信仅有合法节点才能得到会话密钥，因此改进协议满足密钥认证性。

定理 4　在随机预言机模型和假设1条件下，改进协议满足完善前向安全性。

证明　完善前向安全性指敌手即使获得合法节点的长期私钥，也不能得到以前的群会话密钥。假设敌手在时刻 $\tau + 1$ 获得高能量节点 S 的私钥 d 和低能量节点 $U_i (1 \leqslant i \leqslant n)$ 的私钥 SK_i，要获得 τ 时刻之前的群会话密钥 $K = X' \prod_{i=1}^{n} z_i = g^{x(1 + x_1 + \cdots + x_n)}$。敌手窃听到消息 $(y_i, \sigma_i)_{(1 \leqslant i \leqslant n)}$ 和 $(C, z_i (1 \leqslant i \leqslant n), \sigma)$，计算关于会话密钥 K 的信息，敌手需要根据 $y_i = g^{x_i}$、$z_i = y_i^x$ 和 $C = H(X \oplus z_1 \oplus z_2 \oplus \cdots \oplus z_n)$，得到 x 或 $X = g^x$ 的信息，或直接得到 K。证明分以下4种情形：

(1) 敌手由 $C = H(X \oplus z_1 \oplus z_2 \oplus \cdots \oplus z_n)$ 得到 $X = g^x$。将Hash函数看成随机预言机模型，敌手通过询问ROM，在 q_H 次询问后，敌手由 $C = H(X \oplus z_1 \oplus z_2 \oplus \cdots \oplus z_n)$ 成功获得 $X = g^x$ 的概率 $q_H / 2^k$ (k 为hash函数的输出长度)是可忽略的。

(2) 敌手由 $z_i = y_i^x$ 得到 x，其难度相当于计算离散对数模大素数问题。

(3) 敌手由 $y_i = g^{x_i}$ 得到 x_i，然后计算 $X' = z_i^{x_i^{-1}} = g^x$。由 $y_i = g^{x_i}$ 计算 x_i 也是求离散对数模大素数问题的困难性。

(4) 敌手由 $(y_i, z_i)_{1 \leqslant i \leqslant n}$ 得到 K。根据定理1的证明，$(g^{x_i}, g^{xx_i}, g^{x + \sum_{i=1}^{n} xx_i})$ 与 (g^{x_i}, g^{xx_i}, R) 是多项式不可区分的(R 为随机数)，因此敌手不能由 $(y_i, z_i)_{1 \leqslant i \leqslant n}$ 计算出 K。

由以上4种情形可知，即使敌手得到各节点的长期私钥也不能得到关于群会话密钥 K 的任何信息，因此满足完善前向安全性。

根据以上4个定理，改进协议满足密钥认证性、完善前向安全性，也能抵抗被动攻击和中间人伪造

攻击，与原协议比较，安全性更强。

4.2 性能分析

以下分析改进协议的计算开销和通信开销。

T_{VER} 为验证Shamir-Tauman在线/离线签名需要的时间；T_{EXP} 为指数为256 bit的模指数运算需要的时间；T_{exp} 为指数为17 bit的模指数运算需要的时间；T_H 为计算hash值需要的时间；T_{MUL} 为模乘运算需要的时间；n 为参与会话的低能量节点数。Tseng协议与改进协议计算开销的比较如表1所示。

表1 两个协议计算开销的比较

	Tseng协议	改进协议
U_i	$T_{\mathrm{EXP}}+T_H+(n+1)T_{\mathrm{MUL}}$	$T_{\mathrm{EXP}}+T_{\mathrm{exp}}+T_H+(n+1)T_{\mathrm{MUL}}$
S	$nT_{\mathrm{VER}}+(2n+1)T_{\mathrm{EXP}}+T_H+(n+1)T_{\mathrm{MUL}}$	$nT_{\mathrm{VER}}+(n+1)T_{\mathrm{EXP}}+T_{\mathrm{exp}}+T_H+(n+1)T_{\mathrm{MUL}}$

假设 $n=100$，低能量节点 U_i 每次计算会话密钥的时间仅需2.03 s，这对低能量节点是可以承受的。在改进协议中，高能量节点 S 减少了 n 个256 bit的模指数运算，假设节点 S 的计算能力是节点 U_i 的100倍，在改进协议中，S 需要的计算时间为0.8 s，而原协议中 S 需要的计算时间为1.56 s，因此运行时间大约缩短为原协议的一半。低能量节点基本密码操作的运行时间如表2所示。

表2 低能量节点基本密码操作的运行时间

	T_{MUL}	T_H	T_{EXP}	T_{exp}
运算时间(ms)	12	3	780	40

$|M|$ 表示消息 M 的长度，其中 $|p|$；$|H|$ 为1 024 bit；$|N|$ 为2×1 024 bit。两个协议通信量的比较如表3所示。

表3 两个协议通信量的比较

U_i	Tseng协议	改进协议
的通信量	$3\|p\|$	$2\|p\|$
S 的通信量	$\|H\|+2n\|p\|$	$\|H\|+n\|p\|+\|N\|$

原协议中总通信量为 $1\,024(5n+1)$ bit，改进协议中总通信量为 $1\,024(3n+3)$ bit。经比较可发现，当n很大时，改进协议中总通信开销减少40%。

5 结束语

认证群密钥协商协议对安全的群通信至关重要。对于文献[6]，本文给出一种有效的中间人伪造攻击，敌手通过伪造成功获取群会话密钥，并指出原协议不满足密钥认证的性质。针对文献[6]的安全缺陷，本文提出一种改进的认证群密钥协商协议，该协议不但满足前向安全性、密钥认证性，还能抵抗被动攻击和中间人伪造攻击。改进协议中高能量节点的计算开销为原协议的一半，通信开销减少了40%，更适用于能量受限、带宽受限的移动通信。

参 考 文 献

[1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transaction on Information Theory, 1976, 22(6): 44-654.

[2] ATENIESE G, STEINER M, TSUDIK G. New multiparty authentication services and key agreement protocols[J]. IEEE Journal of Selected Areas in Communications, 2000, 18(4): 628-639.

[3] BRESSON E, CHEVASSUT O, POINTCHEVAL D et al. Provably authenticated group diffie-Hellman key exchange[C]//8th Annual ACM Conference on Computer and Communications Security. New York: ACM Press, 2001: 255-264.

[4] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Dynamic group diffie-hellman key exchange under standard Assumptions[C]//Eurocrypt 2002. Berlin: Springer-Verlag, 2002: 321-336.

[5] TSENG Y M. A robust multi-party key agreement protocol resistant to malicious participants[J]. Computer Journal, 2005, 48(4): 480-487.

[6] TSENG Y M. A secure authenticated group key agreement protocol for resource-limited mobile devices[J]. Computer Journal, 2007, 50(1): 41-52.

[7] MANULIS M. Survey on security requirements and model for group key exchange[DB/OL]. [2007-08-18]. http://eprint.iacr.org/2006/388.pdf.

[8] DIFFIE W, OORSCHOT P C, WIENER M J. Authentication and authenticated key exchange[J]. Designs, Codes and Cryptography, 1992, 2: 107-125.

[9] SHAMIR A, TAUMAN Y. Improved on-line/off-line signature schemes[C]//Advances in Cryptology- Crypto '01. Berlin: Springer-Verlag, 2001: 355-367.

[10] BONEH D. The decision Diffie-Hellman problem[C]//3rd Algorithmic Number Theory Symposium. Berlin: Springer-Verlag, 1998: 48-63.

[11] RIVEST R L, KALISKI B. RSA problem[DB/OL]. [2007-08-18]. http//people.csail.mit.edu/rivest/RivestKaliski-RSAProblem.pdf.

编 辑 熊思亮