叛逆者可追踪的非对称群组密钥协商协议

赵秀凤[1,2] 徐秋亮[2] 刘 伟[1]

(信息工程大学电子技术学院 郑州 450004)[1] (山东大学计算机科学与技术学院 济南 250101)[2]

摘 要 非对称群组密钥协商(Asymmetric Group Key Agreement,ASGKA)的概念在2009年欧密会上被首次提出,其协议结束时协商出来的只是一个共享的加密密钥。这个加密密钥可以被敌手访问,而且对应多个不同的解密密钥,每个群组用户都可以计算出一个对应该公钥的解密密钥。同时指出进一步研究的问题之一是如何实现叛逆者可追踪的ASGKA协议。设计了一个标准模型下可证安全的非对称密钥协商协议ASGKAwTT,该协议可以实现叛逆者追踪。

关键词 非对称密钥协商,双线性配对,多签名,叛逆者可追踪

中图法分类号 TP309.2 **文献标识码** A

Asymmetric Group Key Agreement with Traitor Traceability

ZHAO Xiu-feng[1,2] XU Qiu-liang[2] LIU wei[1]

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)[1]

(School of Computer Science and Technology, Shandong University, Jinan 250101, China)[2]

Abstract The notion of asymmetric group key agreement(ASGKA) was first introduced in EuroCrypt 2009, in which the group members merely negotiate a common encryption key which is accessible to attackers and corresponds to different decryption keys, each of which is only computable by one group member. One of the future works is to achieve asymmetric group key agreement with traitor traceability. In this paper, we proposed a provable security asymmetric group key agreement protocol ASGKAwTT in standard model, the new protocol provides traitor traceability.

Keywords Asymmetric group key agreement, Bilinear pairing, Multi-signature, Traitor traceability

1 引言

密钥协商是信息安全中的基础问题,是建立信息系统安全机制的关键。由于网络中群组活动的增多,比如远程会议、多方协作、网络资源服务等,使用群组密钥协商(Group Key Agreement,GKA)协议来保护通信的安全性的需求越来越广泛,群密钥协商协议的研究因而成为近来非常活跃的研究领域。研究群密钥协议对电子政务、电子商务等方面都有重要的理论意义和应用价值。

群组密钥协商作为一种基本的密码学任务,其目标在于允许多个用户在公开的网络环境中建立一个共享密钥。从应用的角度来看,群组密钥协商的最终目的在于为多个用户提供一个秘密的信道。2009年欧密会上,伍前红等人[1]首次提出了非对称群组密钥协商协议(Asymmetric Group Key Agreement,ASGKA)的概念。在非对称群组密钥协商协议中,群组用户协商出的不是一个共享的密钥,而是一个共享的公钥。这个公钥可以被敌手访问,而且对应多个不同的解密密钥,每个用户都可以计算出一个对应该公钥的解密密钥。其实,对非对称群组密钥协商的研究可以追溯到秦波的博士学位论文[2]。

伍前红、秦波等人首次定义了ASGKA的安全模型,给出了一个从零开始的(from scratch)一轮ASGKA协议的通用构造,并在标准模型下实例化了一个可证安全的ASGKA协议。所谓从零开始的GKA协议,即在协议执行之前,不需要假设任何保密信道。因此,所有基于PKI的群组密钥协商协议都不是从零开始的[3-5],原因在于PKI建立的过程其实就是执行一轮的协议。但是,从零开始的ASGKA协议无法实现认证,不能抵抗主动攻击。最近,Zhang等人[6]给出了一个在随机预言机模型下可证安全的基于身份的认证ASGKA协议。

ASGKA是一个全新的概念,它留下了很多开放性问题和继续研究的思路,例如叛逆者可追踪的ASGKA协议。本文的目标在于设计叛逆者可追踪的ASGKA协议。

在传统的GKA协议中,每个成员都共享相同的会话密钥。因此,追踪到底是哪个成员将会话密钥泄漏给外部攻击者是完全不可能的。而在ASGKA协议中,为了得到一个(等价的)解密钥,至少需要一个群成员的秘密输入。也就是说,ASGKA中的解密钥总是和某个或者某些群成员的秘密输入对应着的,这就为在ASGKA中追踪叛徒提供了可能。

研究ASGKA协议中的叛逆者追踪问题在电子商务和军事活动中具有十分重要的意义。在商业活动和军事行动中,经常发生协商的机密信息泄露的情况,从而需要追踪泄露机

到稿日期:2010-10-20 返修日期:2011-01-17 本文受国家自然科学基金(60873232),山东省自然科学基金(ZR2010FM045)资助。

赵秀凤(1977—),女,博士生,讲师,主要研究方向为信息安全与密码学;徐秋亮(1960—),男,教授,博士生导师,主要研究方向为信息安全与密码学;刘 伟(1963—),男,副教授。

密信息的群组成员，即叛逆者，并追究其法律责任。

利用 Lu 等人[7]的多签名(multisignature)方案，我们设计了一个标准模型下可证安全的非对称群组密钥协商协议。当恶意的群成员泄露解密密钥时，利用追踪算法可以恢复其身份信息。

2 预备知识

2.1 双线性映射及双线性群

假定 G、G_T 是两个阶为 n 的乘法循环群。称满足下面条件的映射 $e:G\times G\to G_T$ 为双线性映射，称 G 为双线性群，条件如下：

1) 双线性性：$\forall u,v\in G$ 和 $\forall a,b\in \mathbb{Z}$，有 $e(u^a,v^b)=e(u,v)^{ab}$ 成立。

2) 非退化性：若 g 为群 G 的生成元，则 $e(g,g)$ 是 G_T 的生成元。

3) 可计算性：$\forall u,v\in G$，$e(u,v)$ 在有效时间内可计算。

2.2 复杂性假设

令 G 是一个阶为 n 的双线性群，g,h 为两个独立的生成元。记 $\vec{y}_{g,\alpha,n}=(g_1,\cdots,g_{n-1},g_{n+1},\cdots,g_{2n})\in G^{2n-1}$，其中 $g_i=g^{\alpha^i}$，$\alpha\in \mathbb{Z}_n^*$ 未知。算法 $\mathcal{B}$ 输出 $b\in\{0,1\}$，如果有

$$|\Pr[\mathcal{B}(g,h,\vec{y}_{g,\alpha,n},e(g_{n+1},h))=0]-\Pr[\mathcal{B}(g,h,\vec{y}_{g,\alpha,n},Z)=0]|\geqslant\varepsilon$$

则称算法 $\mathcal{B}$ 以优势 ε 解决判定性 n-BDHE 问题，其中 g,h 为两个独立的随机生成元，$\alpha\in_R \mathbb{Z}_n^*$，$Z\in_R G_T$。

如果不存在 ε 时间算法至少以优势 ε 解决判定性 n-BDHE 问题，则称判定性 (τ,ε,n)-BDHE 假设在群 G 中成立。

2.3 非对称密钥协商(ASGKA)

非对称群组密钥协商包括 7 个多项式算法[1,2]。

1) 系统参数生成(System Parameters Generation)：输入安全参数，生成系统公共参数。

2) 群组用户建立(Group Setup)：确定参与密钥协商的群组用户 $\mathcal{U}=\{U_1,\cdots,U_n\}$。

3) 群组密钥协商(Agreement)：每个群组用户计算并广播消息。

4) 加密密钥生成(Encryption Key Generation)：每个群组成员利用接收到的广播消息计算共享的加密密钥 pk。

5) 解密密钥生成(Decryption Key Generation)：每个群组成员 U_i 利用接收到的广播消息计算自己的解密密钥 dk_i。

6) 加密算法(Encryption)：任何实体利用共享的加密密钥对明文消息加密。

7) 解密算法(Decryption)：每个群组成员 U_i 都可以利用计算出的解密密钥 dk_i 对密文进行解密。

2.4 ASGKA 安全模型

伍前红和秦波等人在传统密钥协商安全模型的基础上给出了非对称密钥协商的安全模型[1,2]。

2.4.1 协议变量和伙伴关系

假定一个多项式大小的固定集合 $\mathcal{U}=\{U_1,\cdots,U_l\}$ 为群成员集，这个集合的任意非空成员子集可以在任何时候发起协议，在它们之间建立一个保密的广播信道。但在这里假设这个成员子集在整个协议运行期间保持不变，将注意力集中在静态群上。当然每次发起协议的时候，成员子集可以不同。

当群成员变化时，将形成一个新群 $\mathcal{U}_v=\{U_1,\cdots,U_n\}$，通过执行协议 Σ 在这个群中建立一个秘密信道。$\mathcal{U}_0$ 表示初始群，每次成员变化时下标 v 加 1。$\Pi_{U_i}^{s_i}$ 表示群成员 U_i 的一个实例 s_i，实例 $\Pi_{U_i}^{s_i}$ 具有唯一的会话标识 $Sid_{U_i}^{s_i}$ 和一个伙伴关系标识 $Pid_{U_i}^{s_i}$。群组密钥协商协议 Σ 被成功执行后，$\Pi_{U_i}^{s_i}$ 具有唯一的解密标 $Dkid_{U_i}^{s_i}$，对应一个解密密钥 $dk_{U_i}^{s_i}$ 以及唯一的加密标识 $Ekid_{U_i}^{s_i}$ 对应一个加密密钥 $ek_{U_i}^{s_i}$。新鲜性标识 $Fid_{U_i}^{s_i}$ 表示 $dk_{U_i}^{s_i}$ 是否泄漏。如果没有泄漏，$Fid_{U_i}^{s_i}=1$；否则 $Fid_{U_i}^{s_i}=0$。最后，伙伴关系标识 $Pid_{U_i}^{s_i}$ 对应一个群成员子集 $P_{U_i}^{s_i}=\mathcal{U}_v\backslash\{U_i\}$。

定义 1(GKA 的成功终止) 我们说一个 GKA 协议 Σ 在实例 $\Pi_{U_i}^{s_i}$ 中成功终止了，如果对 $1\leqslant k\neq i\leqslant n$ 满足：

(1) $P_{U_i}^{s_i}$ 中的每一个 U_k 都有包含 $\{Sid_{U_i}^{s_i},Pid_{U_i}^{s_i},Dkid_{U_i}^{s_i},Ekid_{U_i}^{s_i}\}$ 的 $\Pi_{U_k}^{s_k}$；

(2) $Sid_{U_k}^{s_k}=Sid_{U_i}^{s_i}$；

(3) $P_{U_k}^{s_k}=\mathcal{U}_v\backslash\{U_i\}$。

2.4.2 敌手模型

在 ASGKA 模型中仅仅考虑被动攻击者，它只能窃听网络中的所有通信。攻击者 $\mathcal{A}$ 与各个主体或更准确地说它们的实例在网络中的交互模型化为下列预言机。

Parameter(1^λ)：对于 $\mathcal{A}$ 的询问 λ，该预言机用公共参数 π 作答，其中包括两个多项式时间算法 $E(\cdot,\cdot)$ 和 $D(\cdot,\cdot)$。

Setup($\mathcal{U}_0$)：$\mathcal{A}$ 输入询问 $\mathcal{U}_0$ 发起协议 Σ，该预言机输出初始群 $\mathcal{U}_0=\{U_1,\cdots,U_l\}$，并对 $1\leqslant k\leqslant l$ 初始化下列变量 $Sid_{U_k}^{s_k}\leftarrow 0$，$P_{U_k}^{s_k}\leftarrow\emptyset$，$Dkid_{U_k}^{s_k}\leftarrow\wedge$(空串)，$Ekid_{U_k}^{s_k}\leftarrow\wedge$，$Fid_{U_i}^{s_i}\leftarrow 1$，$S\leftarrow 0$。

Execute($U_1,\cdots,U_n$)：在群成员 $\{U_1,\cdots,U_n\}=\mathcal{U}_v\subseteq\mathcal{U}_0$ 未使用过的实例之间执行协议，该预言机输出协议执行的副本，其中群成员数目和它们的身份由攻击者决定。对 $1\leqslant k\leqslant n$，更新下列变量 $Sid_{U_k}^{s_k}\leftarrow Sid_{U_k}^{s_k}+1$，$P_{U_k}^{s_k}\leftarrow\mathcal{U}_v\backslash\{U_k\}$，$Dkid_{U_k}^{s_k}\leftarrow dk_{U_k}^{s_k}$，$Ekid_{U_k}^{s_k}\leftarrow ek_{U_k}^{s_k}$，$S\leftarrow S+1$。$S$ 是全局标识符记录协议执行的次数。

Reveal($\Pi_{U_i}^{s_i}$)：输出 $Ekid_{U_k}^{s_k}$。

Dk-Reveal($\Pi_{U_i}^{s_i}$)：输出 $Dkid_{U_k}^{s_k}$，更新 $Fid_{U_i}^{s_i}\leftarrow 0$。

Test($\Pi_{U_i}^{s_i}$)：这个询问用来定义攻击者的优势。$\mathcal{A}$ 对一个新鲜实例 $\Pi_{U_i}^{s_i}$ 可以随时发出这个询问，但是只能询问一次。$\mathcal{A}$ 询问后会收到一个挑战密文 $c^*=E(m_\rho,ek_{U_i}^{s_i})$，其中 ρ 是掷均匀硬币的结果。最后，$\mathcal{A}$ 输出一个猜测比特 ρ'。

2.4.3 安全性定义

定义 2(正确性) GKA 协议 Σ 是正确的，如果当协议成功终止时，对任意实例 $\Pi_{U_i}^{s_i}$ 及其伙伴 $\Pi_{U_k}^{s_k}$，$E(\cdot,\cdot)$ 消息空间中任意消息 m，下列关系成立：

(1) $D(E(m,ek_{U_i}^{s_i}),dk_{U_k}^{s_k})=m$；

(2) $E(D(m,ek_{U_k}^{s_k}),dk_{U_i}^{s_i})=m$。

定义 3(非对称群组密钥协商，ASGKA) 如果协议成功终止后 $dk_{U_i}^{s_i}=dk_{U_k}^{s_k}=sk$ 成立，则称 GKA 协议 Σ 是对称的；否则称 Σ 是非对称的群密钥协商协议。

定义 4(新鲜性) 称一个 ASGKA 协议实例 $\Pi_{U_i}^{s_i}$ 是新鲜的，如果在攻击者回答 Test 预言机之前，任何实例 $\Pi_{U_i}^{s_i}$ 以及它们的伙伴实例都没有收到过 Dk-Reveal 询问。

定义 5(ASGKA 的保密性) 设 $\mathcal{A}$ 为 ASGKA 协议 Σ 的被动攻击者，$\mathcal{A}$ 用 Test($\Pi_{U_i}^{s_i},m_0,m_1$)询问 Σ 中的一个新鲜性实例 $\Pi_{U_i}^{s_i}$ 后收到一个挑战密文 $c^*=E(m_\rho,ek_{U_i}^{s_i})$，最后 $\mathcal{A}$ 必须

输出一个猜测比特 ρ'，这里 ρ' 是投掷硬币的结果。在上述保密博弈中，$\mathcal{A}$ 的优势定义为

$$Adv_{A,\Sigma}^{ASGKA}=|\Pr[\rho'=\rho]-1/2|$$

我们称 Σ 是静态群中一个安全的 ASGKA 协议，如果对任何多项式时间的攻击者 $\mathcal{A}$ 允许询问所有的预言机，而 $\mathcal{A}$ 在上述保密博弈中的优势 $Adv_{A,\Sigma}^{ASGKA}$ 是可以忽略的。

3 Lu 等人的多签名方案回顾

首先，方案中被签名的消息表示为 $\{0,1\}^k$ 上的比特串，其中 k 是一个固定的值。G、G_T 是两个阶为素数 p 的循环群。g 为群 G 的生成元。映射 $e:G\times G\to G_T$ 为一个双线性配对映射。$u'\in_R G, U=(u_i)$ 为一个长度 n 的向量，$u_i\in_R G$。

多签名方案由 5 个算法组成，$\mathcal{WM}=\{Kg,Sig,Vf,Comb,Mvf\}$，分别描述如下。

Kg：该算法为每个群组用户 U_i 随机选择 $\alpha_i\in_R \mathbb{Z}_p$，计算公钥为 $pk_i=e(g,g)^{\alpha_i}$，私钥为 $sk_i=\alpha_i$。

$Sig(sk_i,M)$：假如被签名的消息 M 表示为 $\{m_1,m_2,\cdots,m_k\}\in\{0,1\}^k$，随机选择 $r_i\in_R\mathbb{Z}_p$，计算签名为 $\sigma_i=(\sigma_1^{(i)},\sigma_2^{(i)})\in G^2$，其中

$$\sigma_1^{(i)}=g^{\alpha_i}\cdot\left(u'\prod_{l=1}^{k}u_l^{m_l}\right)^{r_i},\sigma_2^{(i)}=g^{-r_i}$$

$Vf(pk_i,M,\sigma_i)$：验证下面的等式是否成立：

$$e(\sigma_1^{(i)},g)e\left(\sigma_2^{(i)},\left(u'\prod_{l=1}^{k}u_l^{m_l}\right)\right)=pk_i$$

如果成立，则 σ_i 是有效的签名，否则 σ_i 是无效的签名。

$Comb((pk_i,\sigma_i)_{i=1}^n,M)$：如果存在一个用户的签名是无效的，则退出，否则计算

$$\sigma_1=\prod_{i=1}^{n}\sigma_1^{(i)}=g^{\sum_{i=1}^{n}\alpha_i}\cdot\left(u'\prod_{l=1}^{k}u_l^{m_l}\right)^{\sum_{i=1}^{n}r_i}$$

$$\sigma_2=\prod_{i=1}^{n}\sigma_2^{(i)}=g^{-\sum_{i=1}^{n}r_i}$$

多签名为 $\sigma=(\sigma_1,\sigma_2)$。

$MVf((pk_i)_{i=1}^n,M,\sigma)$：验证下面的等式是否成立：

$$e(\sigma_1,g)e\left(\sigma_2,\left(u'\prod_{l=1}^{k}u_l^{m_l}\right)\right)=\prod_{i=1}^{n}pk_i$$

如果成立，则 σ 是有效的签名，否则 σ 是无效的签名。

这个多签名方案是不可伪造的，其不可伪造性可以规约到 Waters 签名方案[4]的不可伪造性。

4 ASGKAwTT 协议

4.1 基本思想

文献[1]中 ASGKA 通用构造使用了基于可累加签名的广播(Aggregatable Signature-Based Broadcast, ASBB)。ASBB 具体方案的签名算法中使用了哈希函数 $H:\{0,1\}^*\to G$，其作用是将字符串映射为群 G 中的元素，并在证明中视为 Random Oracle。同时，文献[1]中指出，可以通过随机选择 $h_i\in G$ 替代 $h_i=H(ID_i)$ 来实现用户 U_i 和 h_i 的绑定，从而得到一个标准模型下可证安全的 ASGKA 协议。

2005 年欧密会上，Waters[8]提出了著名的标准模型下可证安全的基于身份的加密方案，同时给出了一个签名方案。2006 年欧密会上 Lu 等人[7]将 Waters 签名方案扩展为一个多签名方案，签名方案中使用了一个标准的函数 $f(ID_i)$ 将用户的身份信息映射到群 G 中。我们借助 Lu 等人的多签名方案设计叛逆者可追踪的非对称密钥协商(ASGKA with Traitor Traceability, ASGKAwTT)协议，该协议在标准模型下是可证安全的，同时可以实现叛逆者可追踪。

4.2 协议描述

我们在双线性群中设计 ASGKAwTT 协议。协议具体描述如下：

1) 系统参数生成 ParaGen(1^λ)

令 PairGen 是这样一个算法：输入安全参数 λ，输出元组 $\gamma=\{p,G,G_T,e\}$，其中 G、G_T 为两个阶为素数 p 的循环群，映射 $e:G\times G\to G_T$ 为一个双线性配对映射。g 为群 G 的生成元，随机选择一个元素 $u'\in G$，并随机选择一个长度 n 的向量 $U=(u_i)$，$u_i\in_R G$。系统公开参数为 $\pi=\{\gamma,g,u',U\}$。

2) 群组建立(Group Setup)

建立参与密钥协商的群组 $\mathcal{U}=\{U_1,\cdots,U_n\}$。令 ID_i 为用户 U_i 的身份索引信息，用 $\{0,1\}^k$ 上的比特串表示，记为 $ID_i=(s_1^{(i)},s_2^{(i)},\cdots,s_k^{(i)})(i=1,2,\cdots,n)$，其中 k 是一个固定的值。

3)群组密钥协商(Group key agreement)

群组中的每个成员 U_i 按照如下步骤执行：

Step1　随机选择 $a_i,r_i\in_R\mathbb{Z}_p^*$，计算

$R_i=g^{-r_i}$，$A_i=e(g,g)^{a_i}$

公钥为 $pk_i=(R_i,A_i)$，私钥为 $sk_i=(r_i,a_i)$。

Step2　计算 $f(ID_j)=u'\prod_{l=1}^{k}u_l^{s_l^{(j)}}$，$j=1,2,\cdots,n$。

Step3　计算签名 $\sigma_{i,j}=g^{a_i}\cdot f^{r_i}(ID_j)$，$j=1,2,\cdots,n$。

Step4　广播消息 $(R_i,A_i,\{\sigma_{i,j}\}_{j=\{1,2,\cdots,n\},j\neq i})$，即矩阵(1)中相应行的消息，其中 $\sigma_{i,i}$ 不进行广播，由用户 U_i 秘密保存在本地。矩阵(1)中 $\prec$ 表示广播，$\downarrow$ 表示解密密钥的计算，$\Downarrow$ 表示加密密钥计算。

$$\begin{array}{cccccc}
 & U_1 & U_2 & \cdots & U_n & TPK \\
U_1 \prec & \phi & \sigma_{1,2} & \cdots & \sigma_{1,n} & (R_1,A_1) \\
U_2 \prec & \sigma_{2,1} & \phi & \cdots & \sigma_{2,n} & (R_2,A_2) \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
U_n \prec & \sigma_{n,1} & \sigma_{n,2} & \cdots & \phi & (R_n,A_n) \\
 & \downarrow & \downarrow & \cdots & \downarrow & \Downarrow \\
\text{example} & dk_1 & dk_2 & \cdots & dk_n & (R,A)
\end{array} \tag{1}$$

4) 群组加密密钥生成(Group encryption key derivation)

为了生成群组成员共享的加密密钥，每个用户 U_i 验证 n 个消息-签名对 $(ID_i,\sigma_{j,i})$：

$$e(\sigma_{j,i},g)\cdot e(R_j,f(ID_i))=A_j$$

对所有 $j=1,2,\cdots,n$，如果所有的签名都是有效的，则计算

$$R=\prod_{j=1}^{n}R_j=g^{-\sum_{i=1}^{n}r_j},A=\prod_{j=1}^{n}A_j=e(g,g)^{\sum_{j=1}^{n}a_j}$$

5) 群组解密密钥生成(Group decryption key derivation)

用户 U_i 利用收到的广播消息计算秘密的解密密钥 $dk_i=\prod_{j=1}^{n}\sigma_{ji}$，并验证：

$$e(dk_i,g)\cdot e(R,f(ID_i))=A$$

如果等式成立，则 U_i 接受 dk_i 为解密密钥，否则退出。

6) 加密(Encryption)

对于明文消息 m，任何实体都可以随机选择 $t\in_R\mathbb{Z}_p^*$，计算密文 $c=(c_1,c_2,c_3)$，这里 $c_1=g^t$，$c_2=R^t$，$c_3=m\cdot A^t$。

7) 解密(Decryption)

对于密文 c，任何拥有有效消息-签名对 (ID_i,dk_i) 的群组成员都可以解密获得明文

$$m=\frac{c_3}{e(dk_i,c_1)e(f(ID_i),c_2)}$$

8) 追踪(Trace)

对于恶意参与者泄露给外部敌手的解密密钥 dk_l，群组中的每个成员 U_i 按照如下步骤可以恢复出恶意参与者的身份信息。

Step1　用户 U_i 利用收到的广播消息计算 $dk_j'=\prod_{k=1,k\neq j}^{n}\sigma_{k,j}$，$j=1,2,\cdots,n$ 且 $j\neq i$。

Step2　计算 $\sigma_j'=\dfrac{dk_l}{dk_j'}$，即验证下式是否成立：

$e(\sigma_j',g)\cdot e(R_j,f(ID_j))=A_j$，$j=1,2,\cdots,n$ 且 $j\neq i$

如果存在 j 使得上式成立，则 dk_l 为用户 U_j 泄露的解密密钥，即叛逆者为 U_j，其身份为 ID_j。

4.3　安全性证明

采用文献[1,2]中提出的敌手模型和 ASGKA 安全定义，我们有如下定理。

定理 1　假设存在敌手 $\mathcal{A}$ 以优势 ε 在时间 τ 内赢得 ASGKA 安全游戏，则存在一个算法 $\mathcal{B}$ 以相同的优势 ε 在时间 $\tau'=\tau+O(n^2\tau_{exp})$ 内解决判定性 n-BDHE 问题。

证明：假设算法 $\mathcal{B}$ 接受到一个随机的判定性 n-BDHE 问题实例 $(g,h,g_1,\cdots,g_n,g_{n+2},\cdots,g_{2n},Z)$，其中，$g_i=g^{a^i}$，$i\in\{1,\cdots,n,n+2,\cdots,2n\}$，$\alpha\in\mathbb{Z}_p^*$ 未知。算法 $\mathcal{B}$ 的目标在于判断 $Z=e(g_{n+1},h)$ 是否成立。下面 $\mathcal{B}$ 将扮演敌手 $\mathcal{A}$ 在 ASGKA 安全游戏中的挑战者，并利用 $\mathcal{A}$ 的输出比特 b 来判断 $Z=e(g_{n+1},h)$ 是否成立。

1）系统参数生成模拟

首先，$\mathcal{B}$ 选择随机指数向量 $X=(x_1,x_2,\cdots,x_n)$，其中 $x_i\in_R\mathbb{Z}_p$。令 $g=g$，$u'=g_n$，$U=(u_i)$，$u_i=g^{x_i}$，并将系统参数 $\{g,u',U\}$ 发送给敌手 $\mathcal{A}$。

然后，$\mathcal{B}$ 为每个用户计算公钥。对于 $j=1,2,\cdots,n$，$\mathcal{B}$ 令 $v_j=\sum_{l=1}^{k}x_l s_l^{(j)}$ 并计算

$$f(ID_j)=u'\prod_{l=1}^{k}u_l^{s_l^{(j)}}=g_n\cdot\prod_{l=1}^{k}g^{x_l\cdot s_l^{(j)}}=g_n\cdot g^{\sum_{l=1}^{k}x_l\cdot s_l^{(j)}}=g_n g^{v_j}$$

$\mathcal{B}$ 随机选择 $i^*\in\{1,2,\cdots,n\}$，$a_i,r_i\in_R\mathbb{Z}_p^*$。记 $S_{i^*}=(1,\cdots,i^*-1,i^*+1,\cdots,n)$。计算

$$R_{i^*}=g^{-r_{i^*}}\Big(\prod_{k\in S_{i^*}}g_{n+1-k}\Big)$$

$$\sigma_{i^*,j}=g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big)R_{i^*}^{-v_j}\ (j\neq i^*)$$

我们有

$$\begin{aligned}
&e(\sigma_{i^*,j},g)e(R_{i^*},f(ID_j))\\
&=e\Big(g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big)R_{i^*}^{-v_j},g\Big)e(R_{i^*},g_n g^{v_j})\\
&=e\Big(g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big),g\Big)e(R_{i^*},g_n)\\
&=e\Big(g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big),g\Big)e\Big(g^{-r_{i^*}}\Big(\prod_{k\in S_{i^*}}g_{n+1-k}\Big),g_n\Big)\\
&=e\Big(g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big),g\Big)e\Big(g_n^{-r_{i^*}}\Big(\prod_{k\in S_{i^*}}g_{n+1-k+n}\Big),g\Big)\\
&=e(g^{a_{i^*}},g)e(g_{n+1},g)=e(g,g)^{a_{i^*}}e(g,g)^{a^{n+1}}\triangleq A_{i^*}
\end{aligned}$$

对于 $i\neq i^*$，计算

$$R_i=g^{-r_i}g_{n+1-i}$$

$$\sigma_{i,j}=g^{a_i}g_n^{r_i}g_{n+1-k+n}R_i^{-v_j}\ (j\neq i)$$

我们有

$$\begin{aligned}
&e(\sigma_{i,j},g)e(R_i,f(ID_j))\\
&=e(g^{a_i}g_n^{r_i}g_{n+1-k+n}^{-1}R_i^{-v_j},g)e(R_i,g_n g^{v_j})\\
&=e(g^{a_i}g_n^{r_i}g_{n+1-k+n}^{-1},g)e(R_i,g_n)\\
&=e(g^{a_i}g_n^{r_i}g_{n+1-k+n}^{-1},g)e(g^{-r_i}g_{n+1-i},g_n)\\
&=e(g^{a_i}g_n^{r_i}g_{n+1-k+n}^{-1},g)e(g_n^{-r_i}g_{n+1-i+n},g)\\
&=e(g,g)^{a_i}\triangleq A_i
\end{aligned}$$

因此，对于所有的 $j\neq i(i\in\{1,\cdots,n\})$，都有下式成立：

$$e(\sigma_{i,j},g)e(R_i,f(ID_j))=A_i$$

2）Setup 模拟

需要为敌手 $\mathcal{A}$ 生成 n 个群组用户的公钥 $\{pk_1,\cdots,pk_n\}$。$\mathcal{B}$ 令 $pk_i=(R_i,A_i)$ 并将 $\{pk_1,\cdots,pk_n\}$ 发送给敌手。由于 a_i，r_i 在 $\mathbb{Z}_p^*$ 上均匀分布，因此模拟的公钥和真实世界的公钥分布是相同的。

3）Ek-Reveal 模拟

首先记 $a=a_1+\cdots,a_n$，$r=r_1+\cdots+r_n$。$\mathcal{B}$ 计算

$$\begin{aligned}
R&=\prod_{j=1}^{n}R_j=R_{i^*}\cdot\prod_{k\in S_{i^*}}R_i\\
&=g^{-r_{i^*}}\Big(\prod_{k\in S_{i^*}}g_{n+1-k}\Big)\cdot\Big(\prod_{k\in S_{i^*}}g^{-r_i}g_{n+1-i}\Big)\\
&=g^{-r_{i^*}}\cdot\Big(\prod_{k\in S_{i^*}}g^{-r_i}\Big)=g^{-\sum_{k=1}^{n}r_k}=g^{-r}
\end{aligned}$$

$$\begin{aligned}
A&=\prod_{j=1}^{n}A_j=A_{i^*}\cdot\prod_{k\in S_{i^*}}A_k\\
&=e(g,g)^{a_{i^*}}e(g,g)^{a^{n+1}}\cdot\prod_{k\in S_{i^*}}e(g,g)^{a_k}\\
&=e(g,g)^{a^{n+1}}\cdot\prod_{k=1}^{n}e(g,g)^{a_k}\\
&=e(g,g)^{a^{n+1}+\sum_{k=1}^{n}a_k}=e(g,g)^{a^{n+1}+a}
\end{aligned}$$

然后，将公钥 (R,A) 返回敌手 $\mathcal{A}$。

4）Dk-Reveal 模拟

假如敌手 $\mathcal{A}$ 对用户 U_j 进行 Dk-Reveal 查询，则 $\mathcal{B}$ 计算

$$\begin{aligned}
dk_j&=\prod_{i=1}^{n}\sigma_{ij}=\sigma_{i^*,j}\cdot\prod_{k\in S_{i^*}}\sigma_{k,j}\\
&=g^{a_{i^*}}g_n^{r_{i^*}}\Big(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\Big)R_{i^*}^{-v_j}\cdot\prod_{k\in S_{i^*}}g^{a_k}g_n^{r_k}g_{n+1-k+n}R_k^{-v_j}\\
&=g^{a}g_n^{r}g_{n+1}R^{-v_j}
\end{aligned}$$

然后将 dk_j 返回给敌手 $\mathcal{A}$。dk_j 满足

$$\begin{aligned}
&e(dk_j,g)\cdot e(R,f(ID_j))\\
&=e(g^{a}g_n^{r}g_{n+1}R^{-v_j},g)e(R,g_n g^{v_j})\\
&=e(g,g)^{a}e(g_{n+1},g)\\
&=e(g,g)^{a^{n+1}+a}=A
\end{aligned}$$

5）Test 模拟

在某一时刻，敌手 $\mathcal{A}$ 选择明文 $m_0,m_1\in G_T$ 和新鲜的用户 U_i 进行 test 查询。$\mathcal{B}$ 随机选择一个比特 $b\in\{0,1\}$ 并计算挑战密文 (c_1^*,c_2^*,c_3^*)，其中

$$c_1^*=h,c_2^*=h^r,c_3^*=m_b Ze(g,h)^a$$

6）Response

敌手 $\mathcal{A}$ 输出猜测比特 b'。$\mathcal{B}$ 断定如果 $b'=1$，则有 $Z=e(g_{n+1},h)$。

成功概率分析：由于 g,h 是 G 的生成元，不妨设 $h=g^t$（t 未知）。如果 $Z=e(g_{n+1},h)$ 成立，则

（下转第 49 页）

全保障工程的投资决策;(3)建立信息安全保障工程的长效机制。系统化信息安全评价的方法适用于所有形式的信息安全保障工程,涵盖信息安全保障工程的3个方面:安全状态改善、防护能力评估和保障效果评价。

建立健全的信息系统的信息安全保障评估方法体系,是实施中国信息安全战略的重要保证。借助信息安全保障评价体系对我国的重点信息系统和核心业务系统进行统一分析和纵横比较,将有助于对我国信息安全防御态势做出量化的结论,为国家提供决策支持,对我国重点信息安全建设的规划、信息安全建设的投入,乃至信息安全管理政策的制定、信息安全技术的研究与发展都具有重要意义。因此,建立健全的国家信息安全保障评价体系是一项带有战略意义的任务。

参 考 文 献

[1] 国务院办公厅. 2006-2020年国家信息化发展战略[R]. 中共中央办公厅,2006:1-28

[2] 国家信息化领导小组. 加强信息安全保障工作的意见[R]. 2003:1-17

[3] 杨晨. 六大要素支撑我国信息安全保障体系—访信息安全专家曲成义[J]. 信息网络安全,2005,(3):11-12

[4] 曲成义,构建国家信息安全保障体系的思考[J]. 信息安全与通信保密,2004(5):20-21

[5] Systems Security Engineering Capability Maturity Model(SSE-CMM®): Model Description Document Version 3.0[R]. Carnegie Mellon University. June 2003

[6] 美国国家安全局信息保障解决方案技术处. 信息保障技术框架[M]. 北京:北京中软电子出版社,ISBN:7900057099,2002

[7] 李雄伟,杨义先,等. Fuzzy-AHP法在网络攻击效果评估中的应用[J]. 北京邮电大学学报,2006,29(1)

[8] 段海新,吴建平. 计算机网络的一种实体安全体系结构[J]. 计算机学报,2001(8)

[9] 黄遵国,卢锡城,王怀民. 可生存技术及其实现框架研究[J]. 国防科技大学学报,2002(2)

[10] Lu Xin, Ma Zhi. Information Assurance Evaluation for Network Information Systems[C]// 2006 International Conference on Computational Intelligence and Security. 2006,2:1528-1531

[11] 徐辉,冯晋雯,叶志远. 基于动态贝耶斯规划图的状态安全报警关联[J]. 北京大学学报:自然科学版,2006(1)

[12] 付钰,吴晓平,严承华. 基于贝叶斯网络的信息安全风险评估方法[J]. 武汉大学学报:理学版,2006(5)

[13] 肖道举,杨素娟. 网络安全评估模型研究[J]. 华中科技大学学报,2002,30(4)

[14] 魏忠. 从定性到定量的系统性信息安全综合集成评估体系[J]. 系统工程理论方法应用,2004(10)

[15] 黄丽民,王华. 网络安全多级模糊综合评价方法[J]. 辽宁工程技术大学学报,2004,23(4)

[16] 孙旋,牛秦洲,等. 基于贝叶斯网络的人因可靠性评价[J]. 中国安全科学学报,2006(8)

[17] 赵文. 信息安全保障综合度量及综合评价研究[D]. 成都:四川大学数学学院,2000

[18] 吴志军,杨义先. 信息安全保障评价指标体系的研究[J]. 计算机科学,2010,37(7)

[19] 虞晓芬,傅玳. 多指标综合评价方法综述[J]. 统计与决策,2004(11):76-79

[20] 高伟. 基于状态观测的信息系统安全保障体系[D]. 中国民航大学,2010

[21] 方滨兴. 五个层面解读国家信息安全保障体系[EB/OL]. http://news.cnfol.com/090601/101,1587,5959421,00.shtml

[22] 国家信息中心. 信息安全保障评价指标体系[R]. 2005

(上接第44页)

$$c_1^* = h = g^t$$

$$c_2^* = h^r = (g^t)^r = (g^r)^t = R^t$$

$$c_3^* = m_b Z e(g,h)^a = m_b e(g_{n+1},h) e(g,h)^a$$

$$= m_b e(g^{a^{i+1}}, g^t) e(g,g^t)^a$$

$$= m_b e(g,g^t)^{a+a^{i+1}} = m_b A^t$$

因此,(c_1^*, c_2^*, c_3^*)是良定义的密文。从而$\mathcal{B}$以与$\mathcal{A}$相同的优势解决了判定性n-BDHE问题。

时间复杂度分析:在模拟过程中,$\mathcal{B}$的负担主要是计算$f(ID_j)$和$(\sigma_{i,j}, R_i, A_i)$。计算$f(ID_j)$需要$O(n)$个G中的指数运算,计算R_i需要$O(n)$个G中的指数运算,计算$\sigma_{i,j}$需要$O(n^2)$个G中的指数运算,计算A_i需要$O(n)$个G_T中的指数运算。因此算法$\mathcal{B}$的时间复杂度为$\tau' = \tau + O(n^2\tau_{exp})$,其中$\tau_{exp}$为$G$或$G_T$中的一个指数运算的时间复杂度。

结束语 基于多签名体制,提出了一个叛逆者可追踪的非对称密钥协商协议ASGKAwTT,从可证明安全性角度给出了协议在数学上的严格证明,从而保证了协议的安全性。本协议除了能满足基本的安全性要求外,还能有效实现叛逆者的追踪,有效解决了伍前红等人在2009年欧密会上提出的问题。ASGKAwTT协议只能抵抗被动攻击,可以利用KY编译器[9]将它们转换为抗主动攻击的密钥协商协议。

参 考 文 献

[1] Wu Qian-hong, Mu Yi, Susilo W, et al. Asymmetric Group Key Agreement[C]// Proc. of EUROCRYPT 2009. LNCS 5479, Berlin: Springer-Heidelberg, 2009:153-170

[2] 秦波. 基于对的群体密码学研究[D]. 西安:西安电子科技大学,2008

[3] Colin B, Manuel G N J. Round-optimal Contributory Conference Key Agreement[C]// Proc. of PKC 2003. LNCS 2567. Berlin: Springer-Verlag, 2002:161-174

[4] Mchoudary G, Colin B, Manuel G N J, et al. Generic One Round Group Key Exchange in the Standard Model[EB/OL]. http://eprint.iacr.org/2009/514

[5] Mchoudary G, Boyd C, Manuel G N J. One Round Group Key Exchange with Forward Security in the Standard Model[EB/OL]. http://eprint.iacr.org/2010/083

[6] Zhang Lei, Wu Qian-hong, Qin Bo, et al. Identity-based Authenticated Asymmetric Group Key Agreement Protocol[EB/OL]. http://eprint.iacr.org/2010/209.pdf, 2010

[7] Lu S, Ostrovsky R, Sahai A, et al. Sequential Aggregate Signatures and Multisignatures Without Random Oracles[C]// Proc. of EUROCRYPT 2006. LNCS 4004. Berlin: Springer-Heidelberg, 2006:465-585

[8] Brent W. Efficient Identity-based Ecnryption without Random Oracles[C]// Proc. of EUROCRYPT 2005. LNCS 3493. Berlin: Springer-Heidelberg, 2005:114-127

[9] Jonathan K, Yung M. Scalable Protocols for Authenticated Group Key Exchange[J]. Journal of Cryptology, 2007, 20:85-113