分布式密钥分发方案的安全性证明*

徐海霞+, 李 宝

(信息安全国家重点实验室(中国科学院研究生院),北京 100049)

Security Proof for Distributed Key Distribution Scheme

XU Hai-Xia+, LI Bao

(State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88256433, Fax: +86-10-88258713, E-mail: hxxu@gscas.ac.cn, http://www.gscas.ac.cn

Received 2003-07-29; Accepted 2003-11-17

Xu HX, Li B. Security proof for distributed key distribution scheme. *Journal of Software*, 2005,16(4):570−576.
DOI: 10.1360/jos160570

Abstract: Security for composition of protocols is hotspot of international scope. By using composition method, it is proved that the distributed key distribution scheme introduced by Daza *et al* is secure. The scheme appends verifiable secret sharing and zero-knowledge proofs to the basic one which fits in the case of passive adversary to prevent from the action of an active adversary.

Key words: key distribution; composition of protocol; multi-party secure computation

摘 要: 复合协议的安全性是当前国际上的热点问题.应用复合协议的观点证明了 Daza 等人提出的分布式密钥分发方案是安全的.该方案在抵抗被动敌手攻击方案的基础上添加了可验证秘密分享和零知识证明,以抵抗主动敌手的攻击,从而具有更高的安全性.

关键词: 密钥分发;复合协议;多方安全计算

中图法分类号: TP309 **文献标识码**: A

群组用户为了在不安全信道上实现安全通信,要应用对称或公钥密码系统加密传输的消息.应用对称密码算法时,一个重要的问题是如何构造有效协议给群组中每个用户发送共用密钥.Needham 和 Schroeder 在文献[1]中的解决方案是:设置一个服务器负责分发和管理共用密钥.文献[2]将这种密钥分发中心的思想形式化.在这种模型中,一个单独的服务器负责给群组用户分发密钥的模式有一些弱点,服务器可能成为瓶颈而且它必须可信.为了克服这些弱点,有很多解决方案被提出,其中分布式密钥分发中心是应用最多的方法之一.文献[3]最早介绍了分布式密钥分发中心模型,这个模型中把单个服务器的任务分配给一组服务器.适用于这种模型的方案称为分布式密钥分发方案.文献[4]提出一种新的分布式密钥分发方案,其基本方案只能抵抗被动敌手(或称为“偷听”

* Supported by the National Natural Science Foundation of China under Grant No.90304013, 60173016 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.863-317-01-04-99, 2003AA144151 (国家高技术研究发展计划(863))

作者简介: 徐海霞(1973－),女,河北乐亭人,博士,主要研究领域为理论密码学,安全多方计算;李宝(1962－),男,博士,研究员,主要研究领域为信息安全.

敌手,只是收集信息,并不改动各个参与方的行为)攻击.为了抵抗主动敌手(或称为“拜占庭”敌手,可以执行违犯协议的任意恶意行为)攻击,文献[4]中的新方案在其基本方案的基础上添加了一些工具,例如可验证秘密分享和知识的非交互零知识证明.该方案是协议复合的一个典型例子,不论方案本身还是作为复合协议研究都有重要意义.文献[4]中提出了新方案但是并没有证明方案的安全性,我们证明了这个分布式密钥分发方案是安全的.

本文讨论的分布式密钥分发方案是一种多阶段的复合协议.以前讨论的安全性是针对单个、独立协议考虑的,不能直接用来处理复合协议.关于复合协议的安全性,见文献[5−7]等.处理独立协议的模型是:要考虑的参与方只是实际参与协议执行的参与方,并且只需考虑独立单个协议的执行.这种模型针对具体的问题,简化了协议的设计和分析.实际上,这种相对简单的模型是研究协议问题初始阶段的自然选择.但是,这种“独立计算”的模型不能满足现代网络的安全性要求.在现代网络中,一个协议可能和不计数量的其他协议并发运行.其他协议的参与方可能与目标协议的参与方完全不同,只不过它们可能有相关的输入或消息传输.另外,一个协议的局部输出可以被其他任意协议应用,应用的方法不可预料.显然,独立模型不能满足上述要求.解决上述问题通行的方法是设计和分析协议时把它看作独立的,在不同环境中的安全性通过安全复合定理保证.这种方法给协议的安全性定义和复合定理分别赋予新的含义,针对不同的敌手模型,提出了相应的安全性定义和复合定理.

本文方案中考虑的敌手模型是非自适应的(或“静态”的,即被敌手控制的“被入侵(corrupted)”的参与方集合是协议执行前就固定的)被动敌手或主动敌手,敌手的计算能力假定是概率多项式时间的.关于这些敌手模型的安全协议定义和复合定理在第 1 节中具体介绍.

在此简单回顾一下本文要用到的计算不可区分的概念:

两个随机变量 $X=\{X_\omega\}_{\omega\in S}$ 和 $Y=\{Y_\omega\}_{\omega\in S}$ 称为计算不可区分,记为 $X\overset{c}{\equiv}Y$,如果对任意多项式尺寸电路族 $\{C_n\}_{n\in N}$,任意多项式 $p(\cdot)$,所有充分大 n 及 $\omega\in S\cap\{0,1\}^n$,有下式成立:

$$|\Pr[C_n(X_\omega)=1]-\Pr[C_n(Y_\omega)=1]|<\frac{1}{p(n)}.$$

本文第 1 节回顾 Canetti 关于协议复合安全性的讨论.第 2 节介绍 V.Daza 等人提出的分布式密钥分发方案.第 3 节给出该方案的安全性证明.

1 多方协议的复合安全性

1.1 安全协议

首先回顾非自适应情形的安全协议定义.定义方式类似于独立协议,第 1 步形式化实际模型,接下来描述理想过程,最后提出理想过程被实际模型模拟的概念.

1.1.1 实际模型

一个 n-方协议 π 是 n 个交互概率算法的集合.每个算法是一个交互图灵机,用参与方 P_i 表示第 i 个算法.每个参与方 P_i 有输入 $x_i\in\{0,1\}^*$,随机输入 $r_i\in\{0,1\}^*$和安全参数 k(输入长度).

所谓非自适应实际模型敌手 A,是另一个交互图灵机,描述被敌手入侵的参与方的行为.敌手 A 的输入包括被入侵参与方的身份及各自输入.用 z 表示 A 收到的附加辅助输入,A 的随机输入记为 r_0.称一个敌手是 t-有界的若它至多控制 t 个参与方.

在计算过程的每一轮中,诚实方首先根据协议生成这一轮的消息.敌手掌握所有发送给被入侵参与方的消息.接着敌手生成本轮被入侵参与方要发送的消息.如果敌手是被动的,那么这些消息由协议确定.主动敌手则以任意恶意的方式生成被入侵参与方发送的消息.最后,每个诚实方收到发送给它的消息.计算结果是所有参与方生成各自的局部输出.诚实方的输出完全遵循协议,被入侵参与方输出一个特殊符号“⊥”表示他们被入侵过.敌手输出它视图的某个任意函数.敌手的视图由以下部分组成:辅助输入、随机输入、被入侵参与方的输入和随机输入以及被入侵参与方在整个计算过程中发送和接收到的消息.不失一般性,假设敌手的输出由它的全部视图组成.

用 $ADVR_{\pi,A}(k,\vec{x},z,\vec{r})$ 表示实际模型中敌手 A 的输出,其中 z 是辅助输入,π 是运行的协

议, $\vec{x}=(x_1,...,x_n)$, $\vec{r}=(r_0,r_1,...,r_n)$ (其中 x_i 和 r_i 分别是参与方 P_i 的输入和随机输入, r_0 是敌手 A 的随机输入). $EXEC_{\pi,A}(k,\vec{x},z,\vec{r})_i$ 是参与方 P_i 的输出.若 P_i 是诚实的,那么它的输出遵循协议执行;若 P_i 被入侵,那么 $EXEC_{\pi,A}(k,\vec{x},z,\vec{r})_i=\perp$.实际模型中,协议完成后的输出结果为 $EXEC_{\pi,A}(k,\vec{x},z,\vec{r})$: =($ADVR_{\pi,A}(k,\vec{x},z,\vec{r})$, $EXEC_{\pi,A}(k,\vec{x},z,\vec{r})_1$,..., $EXEC_{\pi,A}(k,\vec{x},z,\vec{r})_n$)(此处理方法区别于独立协议,在独立协议的情况下,只要考虑敌手的局部输出,而此时要考虑全体输出(global output)).

1.1.2 理想过程

理想过程可描述为把输入向量映为输出向量的随机过程.这样的过程表示为函数功能 $f:N\times(\{0,1\}^*)^n\times\{0,1\}^*\to(\{0,1\}^*)^n$,其中第 1 个输入是安全参数,第 2 个输入是各个参与方的输入向量,最后一个是随机输入.所谓(非自适应)理想过程敌手 S 是描述被入侵参与方行为的交互图灵机.敌手 S 的输入包括:被入侵参与方的身份和输入、随机输入以及安全参数 k.除此之外,还有一个可信方,记为 T.理想过程如下:

输入替换阶段:理想过程敌手 S 看到所有被入侵参与方的输入.如果 S 是主动敌手,那么它能够根据当前所有信息修改这些输入.如果 S 是被动敌手,那么它对输入不做替换.

计算:每一方 P_i 将各自的输入(可能被修改) y_i 发送给可信方 T.T 选择 $r_f\leftarrow R_f$,给每个参与方发送 $f(k,\vec{y},r_f)_i$.

输出:每个诚实方 P_i 输出 $f(k,\vec{y},r_f)_i$,被入侵方输出 $\perp$.敌手输出理想过程中收到的所有消息的任意函数,这些消息包括敌手的随机输入、被入侵参与方的输入以及计算结果{ $f(k,\vec{y},r_f)_i:P_i$ 被入侵}.

令 $ADVR_{f,S}(k,\vec{x},z,\vec{r})$ (其中 $\vec{r}=(r_f,r)$),表示理想过程敌手 S 的输出,安全参数是 k,随机输入是 r,辅助输入 z, f 是可信方计算的函数(随机输入 r_f),各个参与方的输入 $\vec{x}=(x_1,...,x_n)$.用 $(n+1)$ 维向量 $IDEAL_{f,S}(k,\vec{x},z,\vec{r}):=ADVR_{f,S}(k,\vec{x},z,\vec{r}),IDEAL_{f,S}(k,\vec{x},z,\vec{r})_1,...,IDEAL_{f,S}(k,\vec{x},z,\vec{r})_n$ 表示理想过程中参与方的输出(诚实方 P_i 输出 $IDEAL_{f,S}(k,\vec{x},z,\vec{r})_i$,被入侵方输出 $\perp$).

1.1.3 两种模型中计算的比较

类似于独立协议的处理方法,对于非自适应敌手情况仍然考虑模拟,即协议 π 模拟计算函数 f 的理想过程.简单地说,对于任意实际模型,敌手 A 都存在一个理想过程敌手 S,使得 $IDEAL_{f,S}\overset{c}{\equiv}EXEC_{\pi,A}$.

定义(文献[5]定义 4 计算不可区分情形). 令 f 是一个 n-方函数, π 是 n-方协议.称 π 非自适应, t-安全计算 f,如果对于任意 t-有限敌手 A 都存在理想过程敌手 S (其运行时间是 A 运行时间的多项式),使得 $IDEAL_{f,S}\overset{c}{\equiv}EXEC_{\pi,A}$.

1.2 复合定理

如前所述,在处理非自适应敌手情况时,是将一项给定任务分成几部分子任务,设计完成每个子任务的协议,把这些协议作为解决给定任务的子程序来应用.其中,每一个协议安全完成子任务,通过复合定理保证整个任务安全完成.为了陈述复合定理,首先介绍混合计算模型.

1.2.1 混合模型

所谓混合模型是指执行协议 π 的过程中需要可信方帮助计算函数功能 $f_1,...,f_m$.根据协议执行,在某些特定轮调用可信方.这些特定轮的计算模拟理想过程,即所有参与方将计算某个函数 f_j 的输入交给可信方 T,接着每个参与方得到相应的输出: P_i 得到 $f_j(k,x_1^{f_j},...,x_n^{f_j},r_{f_j})_i$.

令 $EXEC_{\pi,A}^{f_1,...,f_m}(k,\vec{x},z)$ 表示 $(f_1,...,f_m)$-混合模型协议 π 的输出.

1.2.2 替换理想计算过程为子协议

协议 π 在第 l 轮将理想计算过程替换为 n-方协议 ρ 是直接的过程,此处不再赘述.令 $\pi^{\rho_1,...,\rho_m}$ 表示协议 π 将每个计算函数 f_i 的理想过程替换为协议 ρ_i 的执行过程.

复合定理(文献[5]中推论 7). 令 $t<n$, $m\in N$, $f_1,...,f_m,g$ 是 n-方函数.令 π 是 $(f_1,...,f_m)$-混合模型中安全计算函数 g 的非自适应 t-安全协议. $\rho_1,...,\rho_m$ 是 n-方协议,其中 ρ_i 非自适应 t-安全计算 f_i.那么,协议 $\pi^{\rho_1,...,\rho_m}$ 非自适应 t-安全计算 g.

2 分布式密钥分配方案

文献[4]中提出的新的分布式密钥分配方案记为 π,分成 3 个阶段,具体结构如下.

(1) 初始阶段(秘密分享)

初始阶段是在服务器集合 P 的鲁棒子集中执行的(所谓鲁棒子集是指:任一个用户通过与服务器的某个子集通信而得到会话密钥,每个这样的服务器集合称为一个鲁棒子集),满足条件的服务器关于一个随机选择的秘密值 $\alpha \in Z_q^*$,根据接入结构(所有权限子集组成的结构)Γ(access structure),生成各自的分享值 $\{\alpha_i\}_{i\in P}$.分享方案要抵抗主动敌手的攻击,主动敌手能够入侵敌手结构 A 的某个子集.每个服务器都能够得到 α 的分享值 α_i,但是不在 Γ 中的服务器得不到关于 α 的任意信息.对任意鲁棒子集 R,要满足对任意 $B\in A$,有 $R-B\in\Gamma$. R 中服务器以分布式的方式生成 α 分享值的协议如下:

每个服务器 $P_i\in R$ 随机选择一个 $k_i\in Z_q$,应用可验证向量空间秘密分享方案在服务器集合 P 中分配 k_i 的碎片. 令 q 和 p 是大素数并且使得 $q\,|\,p-1$.令 $\tilde{g}$ 是 Z_p^* 的 q 阶乘法子群的生成元. P_i 选择一个随机向量 $\vec{V}_i=(v_i^{(1)},...,v_i^{(r)})\in(Z_q)^r$ 使得 $\vec{V}_i\cdot\psi(D)=k_i$ ($\psi: S\cup\{D\}\to(Z_q)^r$ 是一个函数,使得 $W\in\Gamma$ 当且仅当 $\psi(D)\in\langle\psi(P_i)\rangle_{P_i\in W}$),这里, D 表示集合 P 之外的一个实体. P_i 给 P 中的每一个服务器 P_j 发送碎片 $k_{ij}=\vec{V}_i\cdot\psi(S_j)$,它也广播对于 $v_i^{(l)}$ ($1\le l\le r$)的承诺值 $V_{il}=\tilde{g}^{v_i^{(l)}}$.每个参与方 $P_j\in P$ 通过计算等式 $\tilde{g}^{k_{ij}}=\prod_{l=1}^{r}(V_{il}^{\psi(P_j)^{(l)}})$ 是否成立来验证由 P_i 发送来的碎片 k_{ij} 的正确性.如果验证没有通过, P_j 公开对 P_i 的一个抱怨(complain).如果对 $P_i\in P$ 发出抱怨的参与方组成一个不属于 A 的子集,即有诚实方对 P_i 发出抱怨,那么 P_i 被拒绝(终止);不然,即 $P_i\in P$ 收到的抱怨只来自于敌手,那么 P_i 公开被抱怨的碎片 k_{ij},如果上述等式仍然不成立,那么 P_i 被拒绝(终止).用 $Qual\subset R$ 表示通过验证阶段的参与方的集合.所生成的随机秘密 $\alpha=\sum_{i\in Qual}k_i$.每个服务器 $P_j\in P$ 计算 α 的碎片,记为 $\alpha_j=\sum_{i\in Qual}k_{ij}$.注意 $D_j=\tilde{g}^{\sum_{i\in Qual}k_{ij}}=\prod_{i\in Qual}\tilde{g}^{k_{ij}}=\prod_{i\in Qual}\prod_{l=1}^{r}(V_{il})^{\psi(S_j)^{(l)}}$ 初始阶段计算功能定义为

$$(...,k_i,...,\perp,...)\to(\alpha_1,...,\alpha_n) \tag{a}$$

其中 k_i 是 R 中参与方的输入,敌手没有输入.

(2) 计算密钥阶段

联合生成秘密分享值 α 之后,所有服务器都能够知道关于 α_i 的公共承诺值 $D_i=g^{\alpha_i}$,其中 $1\le i\le n$.当前用户可以要求一个会话密钥 K_c .每个服务器 $P_i\in Qual$ 广播一个密文 (r_i,s_i) .本阶段的目标是得到密文 (r_i,s_i),是对明文 $h_C^{\alpha_i}$ 的加密.密钥询问和计算功能定义为

$$(...,(\alpha_i,\beta_i,h_C),...)\to(...,(r_i,s_i),...) \tag{b}$$

其中 α_i,β_i 是 Z_q^* 中的随机数, h_C 是作用在 C 上的 hash 值.

(3) 密钥生成和传递阶段

每个输出 (r_i,s_i) 的服务器 P_i (其他输出 $\perp$)能够形成 Γ 中的子集(注意 R 的定义).那么在权限集 $Q(\in\Gamma)$ 中的服务器可以计算会话密钥 $k_C=(h_C)^\alpha$ 的密文 (r,s):

$$r=\prod_{P_i\in Q}r_i^{\lambda_i^Q}=g^{\sum_{P_i\in Q_i}\lambda_i^Q\cdot\beta_i}\bmod p,\ s=\prod_{P_i\in Q}s_i^{\lambda_i^Q}=(h_C)^\alpha(y_j)^{\sum_{P_i\in Q}\lambda_i^Q\cdot\beta_i}\bmod p,$$

其中, λ_i^Q 是重建系数,使得 $\psi(D)=\sum_{P_i\in Q}\lambda_i^Q\psi(P_i)$,所以 $\alpha=\sum_{P_i\in Q}\lambda_i^Q\alpha_i \bmod q$,服务器 $P_i\in Q$ 将密文 $c=(r,s)$ 发送给用户 U_j.

3 方案安全性证明

为了节省篇幅,我们只对主动敌手的情况给出证明,至于被动敌手的情况可以从当前证明适当简化得到.根

据文献[5]中的复合定理,本文中的分布式密钥分发方案是顺序协议复合,根据非自适应敌手模型中协议复合的安全定义,我们只须分别证明每个阶段的协议是非自适应安全的即可.

(1) 关于初始阶段

为了证明方便,首先按步骤写出本阶段的协议.

输入:每个服务器 $P_i \in R$ 随机选择 $k_i \in Z_q$ 作为输入,不在 R 中的服务器没有输入.

Step C1: 每个服务器 $P_i \in R$ 选择随机向量 $\vec{V}_i = (v_i^{(1)},...,v_i^{(r)}) \in (Z_q)^r$ 使得 $\vec{V}_i \cdot \psi(D) = k_i$.发送 $k_{ij} = \vec{V}_i \cdot \psi(S_j)$ 给 P_j,广播 $V_{il} = \tilde{g}^{v_i^{(l)}}$,其中 $1 \le l \le r$.

Step C2: P_j 根据收到的碎片 k_{ij} 验证等式 $\tilde{g}^{k_{ij}} = \prod_{l=1}^{r}\left(V_{il}^{\psi(P_j)^{(l)}}\right)$ 是否成立.如果验证没有通过, P_j 公开对 P_i 的一个抱怨(complain).

Step C3: $P_i \in P$ 收到的抱怨来自一个不属于 A 的子集,即有诚实方对 P_i 发出抱怨,那么 P_i 被拒绝(终止);否则,即 $P_i \in P$ 收到的抱怨只来自于敌手,那么 P_i 公开被抱怨的碎片 k_{ij},如果上述等式仍然不成立,那么 P_i 被拒绝(终止).

Step C4:用 $Qual \subset R$ 表示通过验证阶段的参与方的集合.每个服务器 $P_j \in Qual$ 计算 $\alpha = \sum_{i \in Qual} k_i$ 的碎片,记为 $\alpha_j = \sum_{i \in Qual} k_{ij}$.

定理 1. 上述协议安全计算功能(式(a)).

证明:根据第 1 节中的安全定义,我们需要证明 $IDEAL_{f,S} \overset{c}{\equiv} EXEC_{\pi,A}$,其中 $IDEAL_{f,S}$ 和 $EXEC_{\pi,A}$ 分别表示在理想模型和实际模型中各参与方的全部输出,此时 f 即为式(a)所定义的函数.为了比较敌手和参与方在两种模型中的输出,将敌手看作一个附加的实体 A,控制被入侵参与方的集合,其中敌手的输出是所有的视图.

我们如下构造理想模型敌手 S.首先, S 以被入侵方的输入 k_i 调用 P_i, P_i 选择随机向量 $\vec{V}_i = (v_i^{(1)},...,v_i^{(r)}) \in (Z_q)^r$ 使得 $\vec{V}_i \cdot \psi(D) = k_i$,计算 $k_{ij} = \vec{V}_i \cdot \psi(S_j)$, $V_{il} = \tilde{g}^{v_i^{(l)}}$,其中 $1 \le l \le r$. S 根据 P_i 的输出验证等式 $\tilde{g}^{k_{ij}} = \prod_{l=1}^{r}\left(V_{il}^{\psi(P_j)^{(l)}}\right)$ 是否成立,即此时 S 充当外部的验证者.如果等式不成立,那么 P_i 终止, P_i 将输出发送给 S(注意至此 S 没有调用可信方);如果等式成立,那么 S 将输入 k_i 发送给可信方,从可信方处得到 $\alpha_j = \sum_{i \in Qual} k_{ij}$,因为此时 S 是敌手, S 不属于接入结构,那么 S 中的服务器 P_i 得到的碎片是完全随机的,因此, S 可以随机地选取 $k_{ji} \in Z_q$ 作为诚实方 P_j 发送给它的碎片,所以 S 和 A 的视图是不可区分的.

根据协议,诚实方所得到的输出是通过验证的,没有通过验证的参与方被终止,因此被入侵方的碎片不计入最后计算结果,从而诚实方在理想模型和实际模型的输出是等分布的.因此,在本阶段协议是安全的.

(2) 关于密钥询问和计算阶段

为了证明方便,我们首先把原来协议改写成多方安全计算协议.

结构(密钥询问和计算协议):

输入:每个服务器有一个安全参数 1^k,对于 α_i 有承诺值 $D_i = g^{\alpha_i}$,所有的 $1 \le i \le n$,而且 $D_i = g^{\alpha_i}$ 对于所有服务器是公共的.

Step C1:每个服务器 $P_i \in R$ 对 C 应用 Hash 函数 H,得到 $h_C = H(C) \in Z_p^*$.

Step C2:服务器 P_i 随机选择 $\beta_i \in Z_q^*$.

Step C3: P_i 计算 $r_i = \tilde{g}^{\beta_i} \bmod p, s_i = h_C^{\alpha_i} y_j^{\beta_i} \bmod p$ 并且广播密文 $c_i = (r_i, s_i)$.

Step C4:服务器 P_i 调用 $|R|-1$ 次知识的零知识证明使得 P_i 是证明者,其他 $|R|-1$ 个服务器充当验证者.证明系统的公共输入是 $D_i, r_i, s_i, \tilde{g}, y^j, h_C$.证明者的辅助输入是 (α_i, β_i),证明者的目的是知道 α_i', β_i' 使得

$$D_i = \tilde{g}^{\alpha_i'} \wedge r_i = \tilde{g}^{\beta_i'} \wedge s_i = (h_C)^{\alpha_i'} (y_j)^{\beta_i'} \quad (1)$$

强调一点,$|R|-1$个证明系统都是在广播信道上发生,因此所有参与方都能够确定验证者的输出是接受还是拒绝.如果证明被拒绝,那么 P_j 广播对 P_i 的抱怨.一旦 P_i 收到抱怨的那些参与方形成一个不在 A 中的子集,那么 P_i 被拒绝并输出 $\perp$.不然,P_i 继续执行下一轮.如果 P_i 通过所有的验证,那么 P_i 输出 (r_i,s_i).

定理 2. 上述协议安全计算功能(式(b)).

证明:将敌手看作一个附加的实体 A,控制被入侵参与方的集合 $\{P_{i_1},P_{i_2},...,P_{i_k}\}$.分两种情况讨论,第 1 种情况是某个被入侵参与方 $P_{i_j}(1\le j\le k)$ 充当证明者;第 2 种情况是被入侵参与方充当验证者(此时诚实方是证明者).

首先考虑某个被入侵参与方 $P_{i_j}(1\le j\le k)$ 充当证明者的情况.这种情况下,我们把实际模型敌手 P_{i_j} 变换成理想模型敌手 B_{i_j},后者把 P_{i_j} 作为一个子程序. B_{i_j} 的输入是 $(\alpha_{i_j},\beta_{i_j})\in Z_q^*\times Z_q^*$.

1. B_{i_j} 调用 P_{i_j},输入是 $(\alpha_{i_j},\beta_{i_j},h_C)$.一旦 P_{i_j} 在 Step C1 时终止(或没有正确执行协议),就令 B_{i_j} 在调用可信方之前终止.否则,假设 P_{i_j} 计算出 r_{i_j},s_{i_j} 且广播密文 $c_{i_j}=(r_{i_j},s_{i_j})$.

2. B_{i_j} 试图得到(r_{i_j},s_{i_j})的原像.为此目的,B_{i_j} 应用 Step C4 中证明系统的知识抽取器.特别地,应用强知识抽取器,B_{i_j} 试图从 P_{i_j} 中抽取 $(\alpha'_{i_j},\beta'_{i_j})$ 满足式(1).一旦抽取器成功,B_{i_j} 置 $\alpha_{i_j}=\alpha'_{i_j}$ 和 $\beta_{i_j}=\beta'_{i_j}$.如果抽取器失败,那么 B_{i_j} 终止(在调用可信方之前).否则,执行下列步骤.

3. B_{i_j} 模拟 Step C4 的执行.即 B_{i_j} 模拟验证者和充当证明者的 P_{i_j} 交互.一旦被模拟的验证者被拒绝,机器 B_{i_j} 终止(在调用可信方之前).否则,它发送 $\alpha'_{i_j},\beta'_{i_j}$ 给可信方并且允许可信方回答参与方 B_{i_j}.

4. B_{i_j} 将执行过程的视图给 P_{i_j},输出 P_{i_j} 输出的结果.

因为协议没有交互,对于诚实方在实际模型的输出与理想模型的输出是一致的.根据第 1 节中非自适应敌手模型中协议安全性定义,全部输出(global output)只需考虑敌手的情形.我们需要证明对于上述功能以及协议 π,有

$$\{IDEAL_{f,B}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\}\overset{c}{\equiv}\{REAL_{\pi,A}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\} \tag{2}$$

而当前情况 $\{IDEAL_{f,B}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\}$ 和 $\{REAL_{\pi,A}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\}$ 的区别在于,P_{i_j} 成功地执行强知识验证得到 r_{i_j},s_{i_j} 的原像或者知识抽取器失败没有找到这样的一个原像.根据强知识验证者的定义,这样一个事件只能以可忽略的概率发生.因此,分布 $\{IDEAL_{f,B}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\}$ 和 $\{REAL_{\pi,A}(...,(\alpha_{i_j},\beta_{i_j},h_C),...)\}$ 是计算不可区分的.

接下来考虑被入侵参与方充当验证者(此时诚实方是证明者)的情况,为表述清楚,下文以某个被入侵参与方 $P_{i_j}(1\le j\le k)$ 为例说明.

1. B_{i_j} 发送 1^n 给可信方并且获得密文 (r_i,s_i) 是由可信方计算的证明者 P_i 发来的 $D_i,r_i,s_i,\tilde{g},y^j,h_C$ 的密文.

2. B_{i_j} 调用零知识证明系统模拟器,输入是 $D_i,r_i,s_i,\tilde{g},y^j,h_C$,应用 P_{i_j} 作为验证者.模拟器的视图记为 $View=S(D_i,r_i,s_i,\tilde{g},y^j,h_C)$.

3. B_{i_j} 将执行视图 $D_i,r_i,s_i,\tilde{g},y^j,h_C,View$ 给 P_{i_j}.

令 $R(...,(\alpha_i,\beta_i,h_C),...)$ 表示实际交互过程中验证者的视图,共同的输入是 $D_i,r_i,s_i,\tilde{g},y^j,h_C$.证明者的辅助输入是 (α_i,β_i),验证者记为 B_{i_j}.那么

$$\{REAL_{\pi,\bar{A}}(...,(\alpha_i,\beta_i,h_C),...)\}=(...,(r_i,s_i),...,P_{i_j}(R(...,(\alpha_i,\beta_i,h_C),...))),$$

$$\{IDEAL_{f,\bar{B}}(...,(\alpha_i,\beta_i,h_C),...)\}=(...,(r_i,s_i),...,B_{i_j}(S(D_i,r_i,s_i,\tilde{g},y^j,h_C))).$$

根据零知识的标准表示,带有辅助输入的模拟器也能够保证计算不可区分,我们有 $R(...,(\alpha_i,\beta_i,h_C),...)$ 和 $S(D_i,r_i,s_i,\tilde{g},y^j,h_C)$ 是计算不可区分的,所以等式(2)成立.

(3) 关于密钥生成和传递相位

我们讨论的模型是非自适应的(敌手所控制的参与方在协议执行之前已经确定). Q 中的服务器,即通过检验的参与方所组成的权限集合中至少有一方是诚实的,服务器将密钥发送给用户,因此用户能够得到关于会话

密钥的正确加密.显然,本阶段的协议是安全的.

综上,根据 Canetti 在文献[5]中关于协议复合的讨论,文献[4]中提出的新的分布式密钥分配方案是安全的.

References:

[1] Needham RM, Schroeder MD. Using encryption for authentication in large networks of computers. Communications of the ACM, 1978,21:993−999.

[2] Bellare M, Rogaway P. Provably secure session key distribution: The three party case. In: Proc. of the 27th Annual Symp. on the Theory of Computing. ACM, 1995. 57−66.

[3] Naor M, Pinkas B, Reingold O. Distributed pseudo-random functions and KDCs. Advances in Cryptology: Eurocrypt'99. LNCS 1592, Springer-Verlag, 1999. 327−346.

[4] Daza V, Herranz J, Padró C, Sáze G. A distributed and computationally secure key distribution scheme. 2002. http://eprint.iacr.org/2002/069

[5] Canetti R. Security and composition of multi-party cryptographic protocols. Journal of Cryptology, 2000,13(1):143−202.

[6] Goldreich O. Secure multi-party computation. 1998. http://philby.ucsd.edu

[7] Canetti R. Universal composable security: A new paradigm for cryptographic protocols. 2001. http://eprint.iacr.org/2000/067

[8] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31:469−472.

[9] Gennaro R. Theory and practice of verifiable secret sharing [Ph.D thesis]. Cambridge: Massachusetts Institute of Technology, 1996.