·安全技术· 文章编号:1000-3428(2018)09-0141-08 文献标志码:A 中图分类号:TP309

一种安全两群体认证协议

刘 卓[1a,1b],马敏耀[1a,1b],邱克娥[1a],冯 君[2]

(1. 贵州师范学院 a. 数学与计算机科学学院; b. 网络空间安全重点实验室,贵阳 550018;
2. 华中科技大学 计算机科学与技术学院,武汉 430000)

摘 要: 针对传统 1-to-1 和 m-to-1 认证模式中认证密码容易泄露的安全隐患,提出一种 m-to-n 认证模式。系统认证时,由 m 个客户端同时向 n 个认证服务器发起认证请求,将该认证模式抽象为安全两群体计算模型,并定义其在半诚实模型下的安全性。构造一个安全多方求和协议,并以该协议为基本构建模块,将健忘传输协议作为基本密码工具,设计安全两群体认证协议。分析结果表明,该协议安全性和效率较高,能够解决两群体群体内及群体间的安全认证问题。

关键词: 安全多方计算;安全两群体计算;m-to-n 认证模式;半诚实模型;健忘传输协议

中文引用格式: 刘 卓,马敏耀,邱克娥,等. 一种安全两群体认证协议[J]. 计算机工程,2018,44(9):141-148.

英文引用格式: LIU Zhuo, MA Minyao, QIU Ke'e, et al. A secure two-group authentication protocol[J]. Computer Engineering, 2018, 44(9): 141-148.

A Secure Two-group Authentication Protocol

LIU Zhuo[1a,1b], MA Minyao[1a,1b], QIU Ke'e[1a], FENG Jun[2]

(1a. School of Mathematics and Computer Science; 1b. Key Laboratory of Cyberspace Security, Guizhou Education University, Guiyang 550018, China;
2. School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430000, China)

【Abstract】 In order to solve the problem that the authentication cipher security risk of the traditional 1-to-1 and m-to-1 authentication mode is easier to leak, the paper proposes a m-to-n authentication mode, which includes m clients and n authentication servers. m clients request to n servers at the same time. In this mode, m clients and n servers are abstracted as the secure two-group computation model. It defines the model security under the semi-honest model, puts forward a security multi-party summation protocol. Taking the security multi-party summation protocol as the basic building block and the forgetfulness transfer protocol as the basic cryptographic tool, this paper designs a secure two-group authentication protocol. Analysis results show that this protocol has higher security and efficiency, it can solve the problem of security authentication between intra group and inter group .

【Key words】 secure multi-party computation; secure two-group computation; m-to-n authentication mode; semi-honest model; forgetfulness transfer protocol

DOI: 10.19678/j.issn.1000-3428.0049696

0 概述

安全多方计算的思想[1]自提出以来,受到了研究者广泛关注,主要包括半诚实和恶意 2 种攻击者模型。记参与方数目为 b,不诚实参与方数目为 t。文献[2]得到以下结论:在点对点网络模型下,假设攻击者计算能力是有限的,当 $t<b$ 时,在半诚实攻击者模型下存在安全的多方计算协议;当 $t<b/2$ 时,在恶意攻击者模型下存在安全的多方计算协议。文献[3-4]得到以下结论:在点对点网络模型下,假设攻击者计算能力是无限的,当 $t<b/2$ 时,在半诚实攻击者模型下存在安全的多方计算协议;当 $t<b/3$ 时,在恶意攻击者模型下存在安全的多方计算协议。文献[5-6]得到以下结论:在广播网络模型下,假设攻击者计算能力是无限的,当 $t<b/2$ 时,在半诚实攻击者模型下存在安全的多方计算协议;当 $t<b/2$ 时,在

基金项目: 贵州省教育厅青年科技人才成长项目(黔教 KY 字[2017]210,黔教 KY 字[2017]205);贵州省科学技术基金(黔科合基础[2016]1115);贵州省省级重点支持学科项目"计算机应用技术"(ZDXK201620);贵州省教育厅科技拔尖人才支持项目(黔教 KY 字[2017]081)。

作者简介: 刘 卓(1987—),女,讲师、硕士研究生,主研方向为信息安全;马敏耀,副教授、博士研究生;邱克娥,副教授;冯 君,博士研究生。

收稿日期: 2017-12-13 **修回日期:** 2018-02-05 **E-mail:** 994588536@qq.com

恶意攻击者模型下存在安全的多方计算协议。

在目前的信息系统认证协议中,主要有 2 种认证模式:1-to-1 和 m-to-1。在 1-to-1 认证模式中主要的安全风险是:黑客闯入或者服务器管理员被腐败都会危及服务器中数据的安全。在 m-to-1 认证模式中主要的安全风险是:用户端认证时每个参与人的份额都需要亮出来,得到这些份额的任何人都能够恢复出完整的认证密码,危及系统的安全。

本文提出一种 m-to-n 认证模式,其中包含 m 个客户端和 n 个认证服务器,认证密钥被独立随机地分成 m 份,认证密钥被独立随机地分成 n 份。系统认证时,由 m 个客户端和 n 个认证服务器以自己的秘密份额为输入,联合执行某种协议后,认证服务器端判断认证是否通过。m-to-n 模式可抽象为安全两群体模型,属于安全多方计算问题的扩展,其研究的是在 2 个群体之间进行隐私保护的计算问题,从保护两方个体的隐私扩展为保护两方群体的隐私。

1 知识准备

1.1 茫然传输协议

茫然传输协议(OT_n^1)是一种两方协议,其中,发送方 S 以 $y_1,y_2,\cdots,y_n$ 为输入,接收方 R 以整数 $k\in\{1,2,\cdots,n\}$为输入。协议结束时,R 输出 y_k,S 没有输出,并且满足:1)接收者 R 的隐私性,即 S 不知道 k 的任何信息;2)发送者 S 的隐私性,即 R 不知道 y_i $(i\neq k)$的任何信息[7-8]。

1.2 安全两群体计算模型

本文将 m 个客户端和 n 个认证服务器抽象为安全两群体计算模型,如图 1 所示,其中有 2 个群体 A_1、A_2,群体 A_1 中有 k_1个参与者 $A_{1\_1},A_{1\_2},\cdots,A_{1\_k_1}$,群体 A_2 中有 k_2个参与者 $A_{2\_1},A_{2\_2},\cdots,A_{2\_k_2}$,$A_1$、$A_2$ 安全两群体计算模型满足隐私性、正确性、安全性。

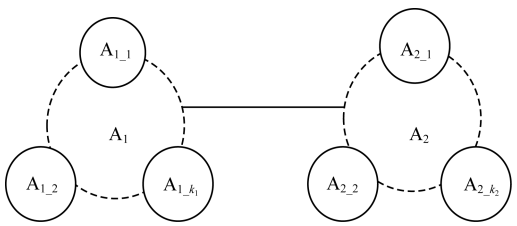

图 1 安全两群体计算模型

1.2.1 隐私性

对安全两群体计算模型的隐私性分析如下:

1)对于群体 A_1 内部多方参与者 $A_{1_1},A_{1_2},\cdots,A_{1_k_1}$和群体 A_2 多方参与者 $A_{2_1},A_{2_2},\cdots,A_{2_k_2}$而言,每个参与者的密钥不能被泄露给其他任何人(包括群体内部成员),在密钥恢复过程中,避免多个参与者共谋恢复出密钥。

2)对于群体 A_1、A_2之间而言,本群的密钥不能被泄露给群体之外的人。

1.2.2 正确性

对安全两群体计算模型的正确性分析如下:若大家都遵循规则,最终每个群体的 A_1 内部多方参与者 $A_{1_1},A_{1_2},\cdots,A_{1_k_1}$和 A_2 多方参与者 $A_{2_1},A_{2_2},\cdots,A_{2_k_2}$在不泄露密钥的情况下,群体 A_1、A_2之间通过认证。

1.2.3 安全性

对安全两群体计算模型的安全性分析如下:安全两群体计算模型的安全性需要保证群体内部多方参与者的安全性,同时保证两方群体之间的安全性。

1)内部多方参与者 $A_{1_1},A_{1_2},\cdots,A_{1_k_1}$和 $A_{2_1},A_{2_2},\cdots,A_{2_k_2}$安全性定义。

定义功能性函数 $f:(\{0,1\}^*)\rightarrow(\{0,1\}^*)$,定义 $f(x_1,x_2,\cdots,x_m)$的随机函数 $f_I(x_1,x_2,\cdots,x_m)$。

内部多方参与者 $I=(i_1,i_2,\cdots,i_t)\in[m]=\{1,2,\cdots,m\}$,$f_I(x_1,x_2,\cdots,x_m)\in\{f_{i1}(x_1,x_2,\cdots,x_m),f_{i2}(x_1,x_2,\cdots,x_m),\cdots,f_{it}(x_1,x_2,\cdots,x_m)\}$的子集,$\pi$ 是用来计算 f^1 的多方协议,在协议 π 的执行过程中,$\bar{x}=(x_1,x_2,\cdots,x_m)$,$VIEW_i^\pi(\bar{x})$是内部多方参与者 $I=(i_1,i_2,\cdots,i_t)$得到的输出信息,可以表示为 $VIEW_i^\pi(\bar{x})=(I,VIEW_{i1}^\pi(\bar{x}),VIEW_{it}^\pi,\cdots,VIEW_{it}^\pi(\bar{x}))$且满足[9-10]:

$$\{S[I,(x_{i1},x_{i2},\cdots,x_{it}),f_I(\bar{x})]\}_{\bar{x}\in\{0,1\}^m}\overset{c}{\equiv}\{View_I^\Pi(\bar{x})\}_{\bar{x}\in\{0,1\}^m}$$

对于更一般的功能函数 f^1,本文定义协议 π 在半诚实模型下秘密计算当且仅当存在概率多项式算法满足:

$$\{S[I,(x_{i1},x_{i2},\cdots,x_{it}),f_I(\bar{x}),f(\bar{x})]\}_{\bar{x}\in\{0,1\}^m}\overset{c}{\equiv}\{View_I^\Pi(\bar{x}),OUTPUT^\pi(\bar{x})\}_{\bar{x}\in\{0,1\}^m}$$

2)外部两群体 A_1、A_2 安全性定义。

两群体安全性定义是基于半诚实模型下的秘密计算,在协议 π 的执行过程中,参与者 P_1 和 P_2 分别输入 x、y,参与者 P_1 和 P_2 两方合作执行 f 的协议是 π。在协议的执行过程中,需要保护 x、y 的隐私性,计算函数 $f(x,y)=(f_1(x,y),f_2(x,y))$,参与者 P_1 和 P_2 得到各自的输出信息,可以表示为:$VIEW_1^\pi(x,y)=(x,r^1,m_1^1,m_2^1,\cdots,m_t^1)$,$VIEW_2^\pi(x,y)=(x,r^2,m_1^2,m_2^2,\cdots,m_t^2)$,其中,$r^i$ 表示 P_i 产生的随机数,m_j^i 表示 P_i 接收到的第 j 个信息。协议执行完后,参与者 P_i 的输出结果是 $OUTPUT_i^\pi(x,y)$。可见,$OUTPUT_i^\pi(x,y)$ 实际上是 $VIEW_i^\pi(x,y)$中的一部分。对于确定性功能函数 f,协议在半诚实模型下计算 f 当且仅当存在概率多项式算法 S_1 和 S_2 满足[11-12]:

$$\{S_1(x,f_1(x,y))\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\{VIEW_1^{\pi}(x,y)\}_{x,y\in\{0,1\}^*}$$

$$\{S_2(y,f_2(x,y))\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\{VIEW_2^{\pi}(x,y)\}_{x,y\in\{0,1\}^*}$$

其中,$|x|=|y|$。

对于一般的功能函数 f,本文定义协议 π 在半诚实模型下秘密计算当仅当存在概率多项式算法 S_1 和 S_2 满足[13]:

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}_{x,y^*}\overset{c}{\equiv}\{VIEW_1^{\pi}(x,y),OUTPUT_2^{\pi}(x,y)\}_{x,y}$$

$$\{f_1(x,y),S_2(y,f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{OUTPUT_1^{\pi}(x,y),VIEW_2^{\pi}(x,y)\}_{x,y}$$

其中,$|x|=|y|$。

2　多方求和协议

关于多方求和协议目前有较多研究,例如:文献[14]提出了一种简单的安全多方求和协议,但该协议无法避免共谋;文献[15]提出了一种经典的安全多方求和协议,该协议能够有效避免共谋,但效率较低;文献[16]提出了一种基于节点的安全多方求和协议,但没有考虑恶意节点提供假数据造成求和结果不正确的情况。本文提出了一种多方求和协议,通过构造多项式和安全信道传递矩阵,以及求解方程组求出参与多方的和。在安全两群体的认证模型中,需要保证群体内部的身份认证的合法性,而多方求和协议能够保证群体内部认证的合法性。同时,多方求和协议基于方程组的求解理论,安全性高,能够有效避免共谋攻击。

2.1　协议描述

本文多方求和协议的具体描述如下:

协议 1　多方求和协议

输入　m 个用户 $C_1,C_2,\cdots,C_m(m>2)$,每个 C_i 拥有 t 维列向量 $\boldsymbol{x}_i=(a_{i1},a_{i2},\cdots,a_{it})^{\mathrm{T}}$

输出　用户 C_1 得到 t 维列向量 $\boldsymbol{Z}=\sum_{i=1}^{m}\boldsymbol{x}_i$,其余各方没有输出

协议准备　假定协议 1 开始前,已对 m 个用户进行编号,用户 $C_1,C_2,\cdots,C_m$ 的编号是确定的。

步骤 1　每个用户 C_i 构造多项式 $f_i(x)=a_{i1}+a_{i2}x+\cdots+a_{it}x^{t-1}$,$C_i$ 分别计算 $f_i(1),f_i(2),\cdots,f_i(t)$ 的值。

步骤 2　分以下 2 种情况进行讨论:

1)若 $m\geqslant t$,C_i 分别通过安全信道把 $f_i(j)$ 发送给用户 $C_j,j=1,2,\cdots,t$(当 $m>t$ 时,用户 $C_{t+1},C_{t+2},\cdots,C_m$ 不接收信息)。在以下矩阵中,第 i 行表示用户 C_i 发送的数据,第 j 列表示用户 $C_j(j=1,2,\cdots,t)$ 收到的数据:

$$\boldsymbol{M}=\begin{bmatrix}f_1(1) & f_1(2) & \cdots & f_1(t)\\ f_2(1) & f_2(2) & \cdots & f_2(t)\\ \vdots & \vdots & & \vdots\\ f_m(1) & f_m(2) & \cdots & f_m(t)\end{bmatrix}$$

用户 $C_j(j=1,2,\cdots,t)$ 计算矩阵 $\boldsymbol{M}$ 的第 j 列元素的和 $F(j)=\sum_{q=1}^{m}f_q(j)$,并将 $F(j)$ 通过安全信道发送给用户 C_1;C_1 计算矩阵 $\boldsymbol{M}$ 第 1 列元素的和 $F(1)=\sum_{q=1}^{m}f_q(1)$。

2)若 $m<t$,C_i 分别通过安全信道把 $f_i(j)(j=1,2,\cdots,m)$ 发送给用户 C_j,并通过安全信道把 $f_i(j)(j=m+1,m+2,\cdots,t)$ 传给 C_1。在以下矩阵中,第 $i(i=1,2,\cdots,m)$ 行表示用户 C_i 发送的数据,第 $j(j=1,2,\cdots,m)$ 行表示用户 C_i 收到的数据,第 $k(k=m+1,m+2,\cdots,t)$ 行表示用户 C_1 收到的数据。

$$\boldsymbol{M}=\begin{bmatrix}f_1(1) & f_1(2) & \cdots & f_1(m+1) & \cdots\\ f_2(1) & f_2(2) & \cdots & f_2(m+1) & \cdots\\ \vdots & \vdots & & \vdots & \vdots\\ f_m(1) & f_m(2) & \cdots & f_m(m+1) & \cdots\end{bmatrix}$$

用户 $C_j(j=2,3,\cdots,m)$ 计算矩阵 $\boldsymbol{M}$ 的第 j 列元素的和 $F(j)=\sum_{q=1}^{m}f_q(j)$,并将 $F(j)$ 通过安全信道发送给用户 C_1;C_1 分别计算矩阵 $\boldsymbol{M}$ 第 1 列元素之和 $F(1)=\sum_{q=1}^{m}f_q(1)$,以及第 $k(k=m+1,m+2,\cdots,t)$ 列元素之和 $F(k)=\sum_{q=1}^{m}f_q(k)$。

步骤 3　用户 C_1 根据 $F(1),F(2),\cdots,F(t)$ 构造关于变量 $a_1,a_2,\cdots,a_t$ 的方程组:

$$\begin{cases}F(1)=a_1+a_2+\cdots+a_t\\ F(2)=a_1+2a_2+\cdots+a_t2^{t-1}\\ \vdots\\ F(t)=a_1+a_2t+\cdots+a_tt^{t-1}\end{cases}$$

C_1 求解此方程组,得到 $a_1,a_2,\cdots,a_t$,输出 t 维列向量 $\boldsymbol{Z}=(a_1,a_2,\cdots,a_t)^{\mathrm{T}}$。

2.2　正确性分析

对本文多方求和协议正确性分析如下:

定理 1　在半诚实模型下,协议执行结束后,C_1 的输出向量 $\boldsymbol{Z}=(a_1,a_2,\cdots,a_t)^{\mathrm{T}}=\sum_{q=1}^{m}\boldsymbol{x}_q$,即表明协议是正确的。

证明　在半诚实模型下,协议的参与各方都严格执行协议步骤。已知 $f_i(x)=a_{i1}+a_{i2}x+\cdots+a_{it}x^{t-1}$,在协议执行的过程中,$C_1$ 拥有 $F(i),i=1,2,\cdots,t$,并且:

$$F(1)=\sum_{q=1}^{m}f_q(1)=(a_{11}+a_{12}+\cdots+a_{1t})+(a_{21}+a_{22}+\cdots+a_{2t})+\cdots+(a_{m1}+a_{m2}+\cdots+a_{mt})=$$
$$(a_{11}+a_{21}+\cdots+a_{m1})+(a_{12}+a_{22}+\cdots+a_{m2})+\cdots+(a_{1t}+a_{2t}+\cdots+a_{mt})$$

$$F(2)=\sum_{q=1}^{m}f_q(2)=(a_{11}+2a_{12}+\cdots+2^{t-1}a_{1t})+(a_{21}+2a_{22}+\cdots+2^{t-1}a_{2t})+\cdots+(a_{m1}+2a_{m2}+\cdots+2^{t-1}a_{mt})=$$
$$(a_{11}+a_{21}+\cdots+a_{m1})+2(a_{12}+a_{22}+\cdots+a_{m2})+\cdots+2^{t-1}(a_{1t}+a_{2t}+\cdots+a_{mt})$$
$$\vdots$$

$$F(t)=\sum_{q=1}^{m}f_q(t)=(a_{11}+a_{12}t+\cdots+a_{1t}t^{t-1})+(a_{21}+a_{22}t+\cdots+a_{2t}t^{t-1})+\cdots+(a_{m1}+a_{m2}t+\cdots+a_{mt})t^{t-1}=$$
$$(a_{11}+a_{21}+\cdots+a_{m1})+(a_{12}+a_{22}+\cdots+a_{m2})t+\cdots+(a_{1t}+a_{2t}+\cdots+a_{mt})t^{t-1}$$

构造多项式 $Q(x)=a_1+a_2x+a_3x^2+\cdots+a_tx^{t-1}$，其中：

$a_1=a_{11}+a_{21}+\cdots+a_{m1}$

$a_2=a_{12}+a_{22}+\cdots+a_{m2}$

$\vdots$

$a_t=a_{1t}+a_{2t}+\cdots+a_{mt}$

则 $F(i)=Q(i),i=1,2,\cdots,t$。

因此，C_1 求解的方程组：

$$\begin{cases}F(1)=a_1+a_2+\cdots+a_t\\F(2)=a_1+2a_2+\cdots+a_t2^{t-1}\\\vdots\\F(t)=a_1+a_2t+\cdots+a_tt^{t-1}\end{cases}$$

即为如下方程组。

$$\begin{cases}Q(1)=a_1+a_2+\cdots+a_t\\Q(2)=a_1+2a_2+\cdots+a_t2^{t-1}\\\vdots\\Q(t)=a_1+a_2t+\cdots+a_tt^{t-1}\end{cases}$$

由于该方程组系数矩阵的行列式 $\begin{vmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t-1}\\\vdots&\vdots&&\vdots\\1&t&\cdots&t^{t-1}\end{vmatrix}\neq0$（关于数 $1,2,\cdots,t$ 范德蒙行列式），因此方程组有唯一解，且满足：

$$\begin{pmatrix}a_1\\a_2\\\vdots\\a_t\end{pmatrix}=\begin{pmatrix}a_{11}+a_{21}+\cdots+a_{m1}\\a_{12}+a_{22}+\cdots+a_{m2}\\\vdots\\a_{1t}+a_{2t}+\cdots+a_{mt}\end{pmatrix}=\sum_{q=1}^{m}\boldsymbol{x}_q$$

2.3 安全性分析

对本文多方求和协议安全性分析如下：

定理 2 在半诚实攻击者模型下，在 C_1 不参与共谋的情况下，即使有 $m-1$ 方共谋也不危机协议的安全；在 C_1 参与合谋的情况下，即使有 $m-2$ 方共谋也不危机协议的安全。

证明：讨论 $m<t$ 的情况。

1）C_1 不参与合谋，$C_2,C_3,\cdots,C_m$ 合谋，即 $I=\{2,3,\cdots,m\}$，则：

$$View_I^{\Pi}(\bar{x})=(I,View_2^{\Pi}(\bar{x}),View_3^{\Pi}(\bar{x}),\cdots,View_m^{\Pi}(\bar{x}))$$
$$View_2^{\Pi}(\bar{x})=(x_2,r_2,f_1(2),f_3(2),f_4(2),\cdots,f_m(2))$$
$$View_3^{\Pi}(\bar{x})=(x_3,r_3,f_1(3),f_2(3),f_4(3),\cdots,f_m(3))$$
$$\vdots$$
$$View_m^{\Pi}(\bar{x})=(x_m,r_m,f_1(m),f_2(m),f_3(m),\cdots,f_{m-1}(m))$$

并且 $C_2,C_3,\cdots,C_m$ 的联合输出 $g_I(\bar{x})=\#$（为空）。

模拟器 S 以 $[I,(x_2,x_3,\cdots,x_m),\#]$ 为输入，执行如下步骤：

随机选取 $x_1'=\begin{pmatrix}a_{11}'\\a_{12}'\\\vdots\\a_{1t}'\end{pmatrix}$，构造多项式：

$$f_1'(x)=a_{11}'+a_{12}'x+\cdots+a_{1t}'x^{t-1}$$
$$f_2(x)=a_{21}+a_{22}x+\cdots+a_{2t}x^{t-1}$$
$$\vdots$$
$$f_m(x)=a_{m1}+a_{m2}x+\cdots+a_{mt}x^{t-1}$$

计算：

$$f_1'(2),f_3(2),f_4(2),\cdots,f_m(2)$$
$$f_1'(3),f_2(3),f_4(3),\cdots,f_m(3)$$
$$\vdots$$
$$f_1'(m),f_2(m),f_3(m),\cdots,f_{m-1}(m)$$

令：

$$S[I,(x_2,x_3,\cdots,x_m),\#]=$$
$$(I,View_2^{\Pi}(\bar{x})^*,View_3^{\Pi}(\bar{x})^*,\cdots,View_m^{\Pi}(\bar{x})^*)$$
$$View_2^{\Pi}(\bar{x})^*=(x_2,r_2',f_1'(2),f_3(2),f_4(2),\cdots,f_m(2))$$
$$View_3^{\Pi}(\bar{x})^*=(x_3,r_3',f_1'(3),f_2(3),f_4(3),\cdots,f_m(3))$$
$$\vdots$$
$$View_m^{\Pi}(\bar{x})^*=(x_m,r_m',f_1'(m),f_2(m),\cdots,f_{m-1}(m))$$

由于：

$View_2^{\Pi}(\bar{x})$ 中 $f_1(2)\overset{c}{\equiv}View_2^{\Pi}(\bar{x})^*$ 中的 $f_1(2)'$；

$View_3^{\Pi}(\bar{x})$ 中 $f_1(3)\overset{c}{\equiv}View_3^{\Pi}(\bar{x})^*$ 中的 $f_1(3)'$；

$\vdots$

$View_m^{\Pi}(\bar{x})$ 中 $f_1(m)\overset{c}{\equiv}View_m^{\Pi}(\bar{x})^*$ 中 $f_1(m)'$。

因此有以上可推出结论：

$\{S[I,(x_2,x_3,\cdots,x_m),\#]\}_{\bar{x}\in\{0,1\}^N}\overset{c}{\equiv}\{View_I^{\Pi}(\bar{x})\}_{\bar{x}\in\{0,1\}^N}$

2)C_1参与合谋。此时最多只能有 $m-2$ 方参与合谋,不妨设 $C_1,C_2,\cdots,C_{m-2}$合谋,即 $I=\{1,2,\cdots,m-2\}$,则:

$$View_I^{\Pi}(\bar{x})=(I,View_1^{\Pi}(\bar{x}),View_2^{\Pi}(\bar{x}),\cdots,View_{m-2}^{\Pi}(\bar{x}))$$

$$View_1^{\Pi}(\bar{x})=(x_1,R_1,F(2),F(3),\cdots,F(m);f_k(1)(k=2,3,\cdots,m-2);f_{m-1}(1);f_m(1);f_i(j)(i=2,3,\cdots m-1;j=m+1,m+2,\cdots,t);f_{m-1}(j);f_m(j)(j=m+1,m+2,\cdots,t))$$

$$View_2^{\Pi}(\bar{x})=(x_2,R_2,f_1(2),f_3(2),f_4(2),\cdots,f_m(2))$$

$$View_3^{\Pi}(\bar{x})=(x_3,R_3,f_1(3),f_2(3),f_4(3),\cdots,f_m(3))$$

$$\vdots$$

$$View_{m-2}^{\Pi}(\bar{x})=(x_{m-2},R_{m-2},f_1(m-2),f_2(m-2),f_3(m-2),\cdots f_{m-3}(m-2),f_{m-1}(m-2),f_m(m-2))$$

并且 $C_1,C_2,\cdots,C_{m-2}$的联合输出 $g_I(\bar{x})=\sum_{i=1}^{m}x_i$。模拟器 S 以$[I,(x_1,x_3,\cdots,x_{m-2}),\sum_{i=1}^{m}x_i]$为输入,执行如下步骤:

随机选取 $x'_m=\begin{pmatrix}a'_{m1}\\a'_{m2}\\\vdots\\a'_{mt}\end{pmatrix}$,计算 $x'_{m-1}=\sum_{i=1}^{m}x_i-\sum_{i=1}^{m-2}x_i-x'_m$,令 $x'_{m-1}=\begin{pmatrix}a'_{m-1,1}\\a'_{m-1,2}\\\vdots\\a'_{m-1,t}\end{pmatrix}$。构造多项式:

$$f_1(x)=a_{11}+a_{12}x+\cdots+a_{1t}x^{t-1}$$

$$\vdots$$

$$f_{m-2}(x)=a_{m-2,1}+a_{m-2,2}x+\cdots+a_{m-2,t}x^{t-1}$$

$$f'_{m-1}(x)=a'_{m-1,1}+a'_{m-1,2}x+\cdots+a'_{m-1,t}x^{t-1}$$

$$f'_m(x)=a'_{m1}+a'_{m2}x+\cdots+a'_{mt}x^{t-1}$$

客户端 C_i 分别计算 $f_i(1),f_i(2),\cdots,f_i(t)(i=1,2,\cdots,m-2)$和的值,$f'_{m-1}(1),f'_{m-1}(2),\cdots,f'_{m-1}(t)$,$f'_m(1),f'_m(2),\cdots,f'_m(t)$。对于 $k=1,2,\cdots,m$,计算 $F'(k)=\sum_{q=1}^{m-2}f_q(k)+f'_{m-1}(k)+f'_m(k)$。

令:

$$S[I,(x_1,x_3,\cdots,x_{m-2}),\textstyle\sum_{i=1}^{m}x_i]=(I,View_1^{\Pi}(\bar{x})^*,View_2^{\Pi}(\bar{x})^*,\cdots,View_{m-2}^{\Pi}(\bar{x})^*)$$

$$View_1^{\Pi}(\bar{x})^*=(x_1,R'_1,F'(2),F'(3),\cdots,F'(m);f_k(1)(k=2,3,\cdots,m-2);f'_{m-1}(1);f'_m(1);f_i(j)(i=2,3,\cdots m-2;j=m+1,m+2,\cdots t);f'_{m-1}(j),f'_m(j)(j=m+1,m+2,\cdots t))$$

$$View_2^{\Pi}(\bar{x})^*=(x_2,R'_2,f_1(2),f_3(2),f_4(2),\cdots,f_{m-2}(2),f'_{m-1}(2),f'_m(2))$$

$$\vdots$$

$$View_{m-2}^{\Pi}(\bar{x})^*=(x_{m-2},R'_{m-2},f_1(m-2);f_2(m-2),f_3(m-2),\cdots f_{m-3}(m-2);f'_{m-1}(m-2)f'_m(m-2))$$

由于:

$View_1^{\Pi}(\bar{x})$中 $F(2),F(3),\cdots,F(m)\overset{c}{\equiv}View_1^{\Pi}(\bar{x})^*$中的 $F'(2),F'(3)\cdots F'(m)$;

$View_2^{\Pi}(\bar{x})$中 $f_{m-1}(2),f_m(2)\overset{c}{\equiv}View_2^{\Pi}(\bar{x})^*$中的 $f'_{m-1}(2),f'_m(2)$;

$$\vdots$$

$View_{m-2}^{\Pi}(\bar{x})$中 $f_{m-1}(m-2),f_m(m-2)\overset{c}{\equiv}View_{m-2}^{\Pi}(\bar{x})^*$中的$f'_{m-1}(m-2),f'_m(m-2)$。

因此可推出以下结论:

$$\{S[I,(x_1,x_2,\cdots,x_{m-2}),\sum_{i=1}^{m}x_i]\}_{\bar{x}\in\{0,1\}^N}\overset{c}{\equiv}\{View_I^{\Pi}(\bar{x})\}_{\bar{x}\in\{0,1\}^N}$$

2.4　效率分析

在本文多方求和协议中的主要操作是:对于 m 个用户来说,输入:m 个用户 $C_1,C_2,\cdots,C_m(m>2)$,每个 C_i 拥有 t 维列向量 $\boldsymbol{x}_i=(a_{i1},a_{i2},\cdots,a_{it})^{\mathrm{T}}$,主要有 t 次多项式赋值计算 $O(t^2)$次,在求解方程组使用 1 次拉格朗日公式,t 个用户相互传递数据,通信开销 $O(t^2d)$,其中 d 为矩阵中每个元素的比特为长。

本文多方求和协议与文献[14-16]协议的效率对比如表 1 所示(k 为网络中共谋节点的数目)。其中,文献[14]不能有效避免共谋攻击和某个用户提供假数据进行恶意破坏,文献[15]和文献[16]效率没有本文协议的效率高。

表 1　多方求和协议通信开销对比

多方求和协议	通信开销
本文协议	$O(t^2d)$
文献[14]协议	$O(md)$
文献[15]协议	$O(m^2d)$
文献[16]协议	$O(m^2kd)$

3　安全两群体认证协议

3.1　模型与方案

在模型中有 3 类设备:可信任注册服务器,$n(n\geq2)$个应用服务器,$m(m\geq2)$个终端,在本文方案中,服务器端资源分布式存储 n 个应用服务器,m 个用户同时向 n 个应用服务器提出认证请求,n 个应用服务器同时通过认证,m 个用户推荐一方 C_1 为用户代理(计算能力较强的),n 个服务器推荐一方 S_1 为服务器代理。

本文方案的主要设计思想如下:假定存在 m 个用户 $C_1,C_2,\cdots,C_m$,拥有 n 维隐私向量 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m$,假定存在 n 个服务器 $S_1,S_2\cdots,S_n$,拥有 m 维隐私向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$,模型是在半诚实模型下,$m$ 个用户、n 个服务器之间没有共谋现象。C 和 S 两群体的认证模型如图 2 所示。

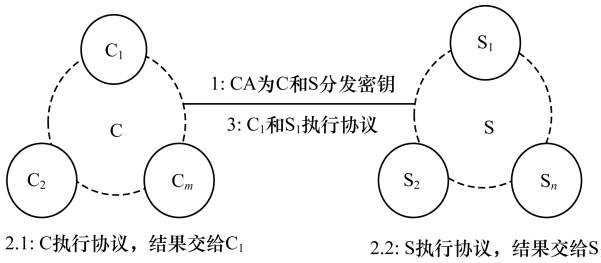

图 2 安全两群体认证模型

3.2 协议描述

安全两群体认证协议以安全多方求和协议为基础,利用线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 有多解的理论,采用安全高效的茫然传输协议 OT_n^1,避开了传统的复杂性高的公钥算法。该协议能够保证两群体之间以及群体内部参与者的隐私性,避免传统的 1-to-1 和 m-to-1 认证模式潜在的安全隐患,加强异构网络和大规模网络环境下系统认证的安全性,适用用于安全两群体的计算模型的 n-to-m 认证模式环境,如在异构网络计算受限的移动车载网环境中和大规模云计算网络环境中,安全两群体认证协议具有理论研究意义和实际应用价值。

协议 2 安全两群体认证协议

初始化阶段:

输入 密钥分发中心(TC)拥有一个 $s\times t$ 维的随机矩阵 $\boldsymbol{A}$ 和一个 s 维的随机列向量 $\boldsymbol{b}$,满足线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 有多个解,即 $r(\boldsymbol{A})=r(\boldsymbol{A},\boldsymbol{b})<t$

输出 客户端 $C_1,C_2,\cdots,C_m$ 分别得到 t 维的列向量 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m$ 满足 $\boldsymbol{A}(\boldsymbol{x}_1+\boldsymbol{x}_2+\cdots+\boldsymbol{x}_m)=\boldsymbol{b}$;服务器端 $S_1,S_2,\cdots,S_n$ 分别得到 s 维列向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 满足 $\boldsymbol{b}_1+\boldsymbol{b}_2+\cdots+\boldsymbol{b}_n=\boldsymbol{b}$;服务器 S_1 得到矩阵 $\boldsymbol{A}$

步骤 1 TC 生成线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 的一个解 $\boldsymbol{x}$。

步骤 2 TC 随机产生 $m-1$ 个 t 维的列向量 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_{m-1}$,计算 t 维的列向量 $\boldsymbol{x}_m=\boldsymbol{x}-(\boldsymbol{x}_1+\boldsymbol{x}_2+\cdots+\boldsymbol{x}_{m-1})$,记 $\boldsymbol{x}_i=\{a_{i1},a_{i2},\cdots,a_{it}\}^{\mathrm{T}}$;TC 随机产生 $n-1$ 个 m 维的列向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_{n-1}$,计算 s 维的列向量 $\boldsymbol{b}_n=\boldsymbol{b}-(\boldsymbol{b}_1+\boldsymbol{b}_2+\cdots+\boldsymbol{b}_{n-1})$。

步骤 3 TC 将 A 通过安全信道发送给服务器 S_1,通过安全信道将 $\boldsymbol{x}_i$ 分发给用户 C_i,将 $\boldsymbol{b}_j$ 分发给服务器 S_j。分发成功后,初始化阶段结束,TC 自动将数据删除。

上述过程示意图如图 3 所示。

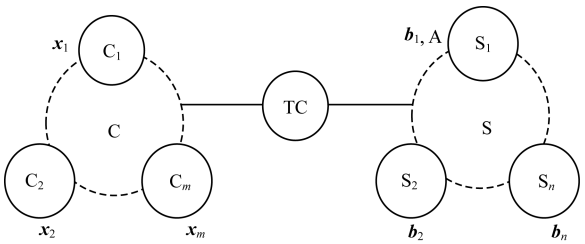

图 3 初始化阶段

认证阶段:

输入 客户端 $C_1,C_2,\cdots,C_m$ 分别拥有 t 维的列向量 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m$;服务器端 $S_1,S_2,\cdots,S_n$ 分别拥有 s 维列向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$;服务器 S_1 拥有矩阵 $\boldsymbol{A}$

输出 服务器 S_1 判断等式 $\boldsymbol{A}(\sum_{i=1}^{m}\boldsymbol{x}_i)=\sum_{i=1}^{n}\boldsymbol{b}_i$ 是否成立

步骤 1 客户端 $C_1,C_2,\cdots,C_m$ 分别以 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m$ 为输入调用协议 1,协议结束后,C_1 得到 $\boldsymbol{x}=\sum_{i=1}^{m}\boldsymbol{x}_i$,其余客户端没有输出;并行地,服务器 $S_1,S_2,\cdots,S_n$ 分别以 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 为输入调用协议 1,协议结束后,S_1 得到 $\boldsymbol{b}=\sum_{i=1}^{n}\boldsymbol{b}_i$,其余服务器没有输出。

步骤 2 客户端 C_1 以 $\boldsymbol{x}$ 为输入,服务器 S_1 以 $\boldsymbol{b}$ 和 $\boldsymbol{A}$ 为输入,执行如下步骤:

1)客户端 C_1 和服务器 S_1 约定 2 个随机数 p 和 q,满足 p^q 足够大,服务器 S_1 将自己的私有矩阵 $\boldsymbol{A}$ 分成 q 个随机矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_q$,满足 $\boldsymbol{A}=\boldsymbol{A}_1+\boldsymbol{A}_2+\cdots+\boldsymbol{A}_q$。

2)对于每个 $j=1,2,\cdots,q$,客户端 C_1 和服务器 S_1 执行如下步骤:

(1)服务器 S_1 随机产生一个数 $i,1\leqslant i\leqslant p$,随机产生 $p-1$ 个 $s\times t$ 维的矩阵。

(2)服务器 S_1 把消息($\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_p$)发给 C_1,其中 $\boldsymbol{H}_i=\boldsymbol{A}_j$,其余的 $\boldsymbol{H}_k(k\neq i)$ 是 S_1 随机产生的 $s\times t$ 维的矩阵。

(3)客户端 C_1 计算 $\boldsymbol{Q}_k=\boldsymbol{H}_k\boldsymbol{x}+\boldsymbol{r}_j$,其中 $\boldsymbol{r}_j$ 是 C_1 选取的随机向量。

(4)使用 OT_1^p 协议,服务器 S_1 取回结果:$\boldsymbol{Q}_i=\boldsymbol{H}_i\boldsymbol{x}+\boldsymbol{r}_j=\boldsymbol{A}_j\boldsymbol{x}+\boldsymbol{r}_j$。

3)客户端 C_1 计算 $\boldsymbol{r}=\sum_{j=1}^{q}\boldsymbol{r}_j$,并将 $\boldsymbol{r}$ 传递给 S_1。

4)服务器 S_1 先计算 $\boldsymbol{M}=\sum_{j=1}^{q}\boldsymbol{Q}_i=\sum_{j=1}^{q}\boldsymbol{A}_j\boldsymbol{x}+\sum_{j=1}^{q}\boldsymbol{r}_j$,然后计算 $\boldsymbol{b}'=\boldsymbol{M}-\boldsymbol{r}$。若 $\boldsymbol{b}'-\boldsymbol{b}=0$,则认证通过;反之,认证不通过。

3.3 正确性分析

对本文安全两群体认证协议正确性分析如下:

定理 3　在半诚实模型下,协议 2 执行结束后,S_1 的输出 $\boldsymbol{b}'=\boldsymbol{M}-\boldsymbol{r}$,判断 $\boldsymbol{P}=\boldsymbol{b}'-\boldsymbol{b}=0$,即协议 2 是正确的。

证明:在半诚实模型下,协议 2 的参与各方都严格执行协议步骤:

$$\boldsymbol{P}=\boldsymbol{b}'-\boldsymbol{b}=\boldsymbol{M}-\boldsymbol{r}-\boldsymbol{b}=\sum_{j=1}^{q}\boldsymbol{Q}_i-\boldsymbol{r}-\boldsymbol{b}=$$

$$\sum_{j=1}^{q}(\boldsymbol{H}_i\boldsymbol{x}+\boldsymbol{r}_j)-\boldsymbol{r}-\boldsymbol{b}$$

使用 OT_1^p 协议:$\boldsymbol{H}_i$ 是服务器 S_1 从客户端 C_1 的消息$(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_p)$随机选择一个消息且:

$$\boldsymbol{H}_i=\boldsymbol{A}_j,j=1,2,\cdots,q$$

$$P=\sum_{j=1}^{q}(\boldsymbol{A}_j\boldsymbol{x}+\boldsymbol{r}_j)-\boldsymbol{r}-\boldsymbol{b}=$$

$$(\boldsymbol{A}_1+\boldsymbol{A}_2+\cdots+\boldsymbol{A}_q)x+\sum_{j=1}^{q}\boldsymbol{r}_j-\boldsymbol{r}-\boldsymbol{b}$$

服务器 S_1 将自己的私有矩阵 $\boldsymbol{A}$ 分成 q 个随机矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_q$,满足 $\boldsymbol{A}=\boldsymbol{A}_1+\boldsymbol{A}_2+\cdots+\boldsymbol{A}_q$。

$$\boldsymbol{P}=\boldsymbol{A}\boldsymbol{x}+\sum_{j=1}^{q}\boldsymbol{r}_j-\boldsymbol{r}-\boldsymbol{b}$$

客户端 C_1 计算 $\boldsymbol{r}=\sum_{j=1}^{q}\boldsymbol{r}_j$。

$$\boldsymbol{P}=\boldsymbol{A}\boldsymbol{x}+\sum_{j=1}^{q}\boldsymbol{r}_j-\boldsymbol{r}-\boldsymbol{b}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{r}-\boldsymbol{r}-\boldsymbol{b}=$$

$$\boldsymbol{A}\boldsymbol{x}-\boldsymbol{b}=\boldsymbol{A}\boldsymbol{x}-\boldsymbol{A}\boldsymbol{x}=0$$

服务器 S_1 计算 $\boldsymbol{P}=\boldsymbol{A}\boldsymbol{x}-\boldsymbol{b}=0$,若 $\boldsymbol{P}=0$,则认证通过。

3.4　安全性分析

对本文安全两群体认证协议安全性分析如下:

定理 4　在半诚实攻击者模型下,C_1 冒名攻击协议 2,或者 S_1 冒名攻击协议 2,也不威胁协议的安全。

证明:

1)初始化阶段安全性分析

线性方程组 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{b}$ 有多个解,随机选择一个解 $\boldsymbol{x}$,TC 随机产生 $m-1$ 个 t 维的列向量 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_{m-1}$,计算 t 维的列向量 $\boldsymbol{x}_m=\boldsymbol{x}-(\boldsymbol{x}_1+\boldsymbol{x}_2+\cdots+\boldsymbol{x}_{m-1})$,其中 $\boldsymbol{x}$ 是随机的,$\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_{m-1}$也是随机的,$\boldsymbol{x}_m$ 是随机的。同理,$\boldsymbol{b}_n$ 是随机的,初始化阶段结束,TC 自动将数据删除,$\boldsymbol{x}_m$、$\boldsymbol{b}_n$、$\boldsymbol{x}$ 都是安全的。

2)认证阶段的安全性分析

(1)代理客户端 C_1 冒名攻击协议 2:$View_1^{\Pi}(\bar{\boldsymbol{x}})=(\boldsymbol{x},R_1,(\boldsymbol{H}_1^{(j)},\boldsymbol{H}_2^{(j)},\cdots,\boldsymbol{H}_p^{(j)}),j=1,2,\cdots,q)$,$C_1$ 的输出为 1 个比特 B,即 $B=0$ 或 1,其中 $B=1$ 表示认证通过,$B=1$ 表示认证失败. 不妨假设认证是通过的,即 $B=1$。模拟器 S 以 $(x,'1')$ 为输入,执行如下步骤:

①S 选择一个 $s\times t$ 维的随机矩阵 $\boldsymbol{A}^*$,计算$\boldsymbol{b}^*=\boldsymbol{A}^*\boldsymbol{x}$。

②S 将 $\boldsymbol{A}^*$ 分成 q 个随机矩阵 $\boldsymbol{A}_1^*,\boldsymbol{A}_2^*,\cdots,\boldsymbol{A}_q^*$ 满足 $\boldsymbol{A}^*=\boldsymbol{A}_1^*+\boldsymbol{A}_2^*\cdots+\boldsymbol{A}_q^*$。

③对 $j=1,2,\cdots,q$,S 分别执行如下步骤:随机选择 $i_{(j)}^*(1\leqslant i_{(j)}^*\leqslant p)$,S 生成$(\boldsymbol{H}_1^{(j)*},\boldsymbol{H}_2^{(j)*},\cdots,\boldsymbol{H}_p^{(j)*})$,其中 $\boldsymbol{H}_{i_{(j)}^*}^*=\boldsymbol{A}_j^*$,$\boldsymbol{H}_k^*(k\neq i_{(j)}^*)$是 S 随机产生的 $s\times t$ 维的矩阵。

④S 将输出:

$$S(\boldsymbol{x},'1')=(\boldsymbol{x},R_1^*,(\boldsymbol{H}_1^{(j)*},\boldsymbol{H}_2^{(j)*},\cdots,\boldsymbol{H}_p^{(j)*}),$$

$$j=1,2,\cdots,q)$$

$$\{S(\boldsymbol{x},'1')\}_{\bar{x}\in\{0,1\}^N}\overset{c}{\equiv}\{View_1^{\Pi}(\bar{x})\}_{\bar{x}\in\{0,1\}^N}$$

(2)代理服务器 S_1 冒名攻击协议 2:$View_2^{\Pi}(\bar{\boldsymbol{x}})=((\boldsymbol{A},b),R_2,\boldsymbol{r},\boldsymbol{A}_j\boldsymbol{x}+\boldsymbol{r}_j(j=1,2,\cdots,q))$,$S_1$ 的输出为 1 个比特 B(即 $B=0$ 或 1,其中 $B=1$ 表示认证通过,表示 $B=0$ 认证失败),不妨假设认证是通过的,即 $B=1$。模拟器 S 以$((\boldsymbol{A},\boldsymbol{b}),'1')$为输入,执行如下步骤:

①S 选择一个 $s\times t$ 维的随机矩阵,计算 $\boldsymbol{b}^*=\boldsymbol{A}^*\boldsymbol{x}$。

②S 将 $\boldsymbol{A}^*$ 分成 q 个随机矩阵 $\boldsymbol{A}_1^*,\boldsymbol{A}_2^*,\cdots,\boldsymbol{A}_q^*$ 满足 $\boldsymbol{A}^*=\boldsymbol{A}_1^*+\boldsymbol{A}_2^*+\cdots+\boldsymbol{A}_q^*$。

③对 $j=1,2,\cdots,q$,S 分别执行如下步骤:随机选择 $i_{(j)}^*(1\leqslant i_{(j)}^*\leqslant p)$,S 生成$(\boldsymbol{H}_1^{(j)*},\boldsymbol{H}_2^{(j)*},\cdots,\boldsymbol{H}_p^{(j)*})$,其中 $\boldsymbol{H}_{i_{(j)}^*}^*=\boldsymbol{A}_j^*$,$\boldsymbol{H}_k^*(k\neq i_{(j)}^*)$是 S 随机产生的 $s\times t$ 维的矩阵。

④S 将输出:

$$S(\boldsymbol{x},'1')=(\boldsymbol{x},R_1^*,(\boldsymbol{H}_1^{(j)*},\boldsymbol{H}_2^{(j)*},\cdots,\boldsymbol{H}_p^{(j)*}),$$

$$j=1,2,\cdots,q)\{S(\boldsymbol{x},'1')\}_{\bar{x}\in\{0,1\}^N}\overset{c}{\equiv}$$

$$\{View_1^{\Pi}(\bar{x})\}_{\bar{x}\in\{0,1\}^N}$$

3.5　效率分析

在本文中提出的半诚实模型下,安全两群体认证协议执行 q 次茫然传输协议OT_1^p 和 p 次加法及乘法操作,服务器 S_1 和客户端 C_1 执行协议,通信开销 $O(p\times q\times m\times t\times d)$,其中 d 为矩阵中每个元素的比特位长(若在 $GF(2^n)$上,则 $d=1$),每个矩阵的比特位长$(m\times t\times d)$,在整个认证过程中,所涉及的计算是轻量级,对于目前的计算设备,计算是可行的。

4　结束语

在 1-to-1 和 m-to-1 认证模式基础上,本文提出 m-to-n 认证模式。将 m-to-n 认证模式抽象为两群体计算模型,在线性方程组的理论求解基础上,利用半诚实模型构造一个基于多方求和协议的安全两群体认证协议方案。该方案安全性和效率较高,能够解决两群体的群内及群体间的隐私安全问题,并且避免使用传统计算复杂的公钥算法。下一步工作将把安全两群体计算扩展到安全多群体计算,将其应用于银行国防、金融等安全性要求高的信息系统认证中。

参考文献

[1] YAO A C. Protocols for secure computations[C]// Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science. Washington D. C., USA:IEEE Press,1982:160-164.

[2] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game: a completeness theorem for protocols with honest majority[C]//Proceedings of STOC'87. New York, USA: ACM Press, 1987:218-229.

[3] BEN-OR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for non-cryptographic fault-tolerant distributed computation[C]//Proceedings of STOC'98. New York, USA: ACM Press, 1988:1-10.

[4] CHAUM D, CRÉPEAU C, DAMGARD I. Multi-party unconditionally secure protocols(extended abstract)[C]// Proceedings of STOC'88. New York, USA: ACM Press, 1988:11-19.

[5] RABIN T, BEN-OR M. Verifiable secret-sharing and multiparty protocols with honest majority[C]// Proceedings of STOC'89. New York, USA: ACM Press, 1989:73-85.

[6] BEAVER D. Secure multi-party protocols and zero-knowledge proof systems tolerating a faulty minority[J]. Journal of Cryptology, 1991, 4(2):75-122.

[7] PINKAS B. Fair secure two-party computation[C]// Proceedings of EUROCRYPT'03. Warsaw, Poland: [s. n.], 2003:87-105.

[8] LINDELL Y, PINKAS B. An efficient protocol for secure two party computation in the presence of malicious adversaries[C]//Proceedings of EUROCRYPT'07. Barcelona, Spain: [s. n.], 2007:52-78.

[9] 魏晓超,蒋 瀚,赵 川. 一个高效可完全模拟的 n 取 1 茫然传输协议[J]. 计算机研究与发展,2016,53(11):2475-2481.

[10] 窦家维,马 丽,李顺东. 最小值问题的安全多方计算及其应用[J]. 电子学报,2017,45(7):1715-1721.

[11] 罗永龙,黄刘生,荆巍巍,等. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展,2006,43(3):410-416.

[12] 李顺东,杨晓莉,左祥建,等. 保护私有信息的图形相似判定[J]. 电子学报,2017,45(9):2184-2189.

[13] 陈振华,李顺东,王道顺,等. 集合成员关系的安全多方计算及其应用[J]. 电子学报,2017,45(5):1109-1116.

[14] 魏晓超. 高效安全两方计算基础理论及关键技术研究[D]. 济南:山东大学,2017.

[15] 宋 成,张明月,彭维平,等. 基于安全多方计算的车载网隐私保护机制[J]. 北京邮电大学学报,2017,40(3):67-71.

[16] 蒋 瀚,徐秋亮. 实用安全多方计算协议关键技术研究进展[J]. 计算机研究与发展,2015,52(10):2247-2257.

编辑 金胡考

(上接第 140 页)

[3] THOMAS S A. Lies, damn lies, and rumors: an analysis of collective efficacy, rumors, and fear in the wake of Katrina[J]. Sociological Spectrum, 2007, 27(6):679-703.

[4] SERRANO E, IGLESIAS C A, GARIJO M. A survey of Twitter rumor spreading simulations[C]//Proceedings of ICCCI'15. Berlin, Germany: Springer 2015:113-122.

[5] KNAPP R H. A psychology of rumor[J]. Public Opinion Quarterly, 1944, 8(1):22-37.

[6] DALEY D J, KENDALL D G. Stochastic rumours[J]. IMA Journal of Applied Mathematics, 1965, 1(1):42-55.

[7] ANDERSON R M, MAY R M, ANDERSON B. Infectious diseases of humans: dynamics and control[M]. Oxford, UK: Oxford University Press, 1992.

[8] 宋之杰,乔 芬,石 蕊. 基于 BASS 模型的突发事件谣言信息扩散研究[J]. 情报杂志,2016,35(1):100-104.

[9] CLEMENTI A, CRESCENZI P, DOERR C, et al. Rumor spreading in random evolving graphs[J]. Random Structures and Algorithms, 2016, 48(2):290-312.

[10] ARRUDA G F, RODRIGUES F A, RODRIIGUEZ P M, et al. Unifying Markov chain approach for disease and rumor spreading in complex networks[EB/OL]. [2017-06-02]. https://arxiv.org/pdf/1609.00682.pdf.

[11] HE Z, CAI Z, YU J, et al. Cost-efficient strategies for restraining rumor spreading in mobile social networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3):2789-2800.

[12] WANG Y Q, WANG J. SIR rumor spreading model considering the effect of difference in nodes' identification capabilities[J]. International Journal of Modern Physics C, 2017, 28(5).

[13] BROWN R. Social identity theory: past achievements, current problems and future challenges[J]. European Journal of Social Psychology, 2000, 30(6):745-778.

[14] ROGERS E M, SHOEMAKER F F. Communication of innovations: a cross cultural approach[M]. New York, USA: Free Press, 1971.

[15] BASS F M. A new product growth for model consumer durables[J]. Management Science, 1969, 15(5):215-227.

编辑 金胡考