第 38 卷 第 4 期
Vol.38 No.4

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)04—0126—03 文献标识码：A 中图分类号：TP18

# 基于双方交集计算的指纹认证方案

张淑苗[1a]，张书晔[2]，冯 全[1b]，杨 梅[1b]

(1. 甘肃农业大学 a. 信息科学技术学院；b. 工学院，兰州 730070；2. 兰州理工大学科技处，兰州 730050)

**摘 要：**针对开放网络中指纹认证的隐私保护问题，利用智能卡设计通用可组合安全的隐秘双方交集计算协议。该协议使用对称加密算法实现双方交集计算，具有较高的计算和通信效率。在此基础上，提出一种隐私保护型身份认证方案，使服务器能安全地比较现场指纹细节点集合与注册模板集合的匹配程度，确认用户身份。分析结果表明，该方案在认证过程中可保证双方私有数据的保密性。

**关键词：**双方交集计算；指纹；身份认证；智能卡；隐私保护

# Fingerprint Authentication Scheme Based on Two-party Intersection Computation

ZHANG Shu-miao[1a], ZHANG Shu-ye[2], FENG Quan[1b], YANG Mei[1b]

(1a. College of Information Sciences and Technology; 1b. College of Engineering, Gansu Agricultural University, Lanzhou 730070, China;
2. Scientific and Technical Department, Lanzhou University of Technology, Lanzhou 730050, China)

**【Abstract】**In order to protect privacy of biometric data in remote authentication, a protocol is presented for private two-party set intersection problem with Universally Composable(UC) security by using smart cart. The proposed protocol uses only a linear number of symmetric-key computations and thus achieves high efficiency on computation and communication. A remote authentication scheme is furtherly designed based on the proposed protocol, which allows a server securely matching the query fingerprint of a user against the stored template to verify his identity, without leaking these private data.

**【Key words】**two-party intersection computation; fingerprint; identity authentication; smart card; privacy protection

**DOI:** 10.3969/j.issn.1000-3428.2012.04.041

## 1 概述

开放网络中生物认证的隐私保护问题已经引起了研究者的广泛关注，这一课题的解决对电子护照、网上银行、电子政务及电子商务过程中使用生物认证具有重要意义。隐私保护通常包含 2 个要点：(1)用户生物特征数据在存储和匹配过程中不能为外界获悉(生物特征模板保护问题)；(2)认证过程中所涉及的服务器和客户端的数据不能泄露给对方(安全计算协议设计问题)。

文献[1]总结了一些典型的生物模板保护方法。一些结合安全计算协议的生物认证方案相继被提出。文献[2]提出基于隐秘双方交集计算的指纹认证方法；文献[3-4]设计了隐私保护的人脸识别协议，不同的是前者使用同态加密算法，后者则采用同态加密与加密电路混合的方法；文献[5-6]分别采用类似文献[3-4]的方法，结合指纹的 fingercode 特征表示方法设计了各自的指纹的隐私识别协议。目前，同态加密算法均为非对称加密算法，计算和通信负担很重，不利于隐私保护型生物认证协议的推广。细节点是指纹识别中最常用的特征，基于细节点的认证协议更具有实用性，文献[2]采用的就是细节点，但其认证协议采用的隐秘双方交集计算中使用了同态加密。本文提出一种基于智能卡和对称加密算法的隐秘双方交集计算协议，并以此为基础设计指纹细节点特征的隐秘匹配方法。

## 2 基于智能卡的隐秘双方交集计算协议

目前关于双方交集问题的计算方案有著名的 Freedman 方案[7]和 Kissner 等方案[8]，不过这些方案几乎都要借助于非对称加密算法来实现。

文献[9]提出基于智能卡的隐秘双方交集计算方案，采用了具有防篡改能力的高端智能卡(通过 FIPS 140-2 的 3 级或 4 级认证)，这种方案使用对称加密算法(如 AES 或 3DES)，因此，比以前的方案具有更高的效率；但他们的方案要求协议的双方都信任智能卡。文献[10]对文献[9]的协议做了改进，只要求智能卡发行方信任智能卡即可。2 种协议都是通用可组合(Universally Composable, UC)安全的，保证了它们和其他协议组合使用时的安全。不过两者均要求智能卡能保存协议执行的状态，这实际上要求智能卡上必须有非挥发性存储器，增加了使用成本。这 2 种协议更适合于私有信息检索(Private Information Retrieval)方面的应用，而不适用于构造隐私保护型指纹认证方案，原因是：(1)协议执行的结果是非智能卡发行方 $B$ 得到双方交集，而通常认证协议中的智能卡发行方 $A$(服务器)得到结果；(2)不能阻止恶意 $B$ 反复查询智能卡而获得 $A$ 的私有数据，为解决这个问题，在 2 种方案中智能卡记录 $B$ 查询总次数，当超过预先给定的值时，智能卡会删除其中的敏感信息。

近年来，具有防篡改功能的智能卡在电子护照、网上银行中得到了广泛的应用，故借助于智能卡和隐秘双方交集计

**基金项目：**国家自然科学基金资助项目(61062012)

**作者简介：**张淑苗(1979－)，女，助理研究员、硕士研究生，主研方向：信息安全；张书晔，工程师；冯 全(通讯作者)，教授、博士；杨 梅，讲师

**收稿日期：**2011-10-11 **E-mail：**fquan@gsau.edu.cn

算协议实现的指纹认证方案很容易集成到现有的认证技术中，而低成本的、不需保存状态的智能卡则具有更好的推广性。为此，本文设计了一种新的基于智能卡的隐秘双方交集计算协议，在该协议中，双方隐私受到了无条件的保护。

### 2.1 协议场景和安全模型

考虑一般场景如下：协议双方，$A$ 和 $B$ 各自拥有私有集合 $Y=\{y_1, y_2,\cdots,y_N|y_i\in F\}$和 $X=\{x_1, x_2,\cdots,x_M|x_j\in F\}$，他们要共同计算双方交集 $f_\cap(Y, X)=Y\cap X$，但只有 $A$ 得到输出结果，而 $B$ 什么也得不到。$F$ 是 $x$ 和 $y$ 的取值域，假设和对称加密密钥取值域相同，且 $N\leqslant Max$，$M\leqslant Max$，其中 $Max$ 是集合元素的上限。为适应指纹细节点认证的安全要求，要求当 $A$ 接收到的 $B$ 的集合元素数量大于 $Max$ 时，$A$ 取消执行协议。

在本文协议中，$A$ 可以发行智能卡 $T$，即对 $T$ 进行初始化后给 $B$(初始化主要是设置 $T$ 与 $A$ 的共享密钥)。假定 $B$ 一旦拥有 $T$，$A$ 就不能和 $T$ 进行通信。敌手只能通过发给或接受 $B$ 的消息与智能卡通信。在本文的安全模型中，各参与方(不诚实智能卡 $T$ 指恶意制作的智能卡)都可以是不诚实，且所有恶意方只被一个敌手控制。在笔者考虑的信任模型中，$B$ 不信任 $T$，这种模型是有道理的，因为 $B$ 被要求用 $A$ 提供的智能卡，而 $A$ 可能不被 $B$ 信任。

### 2.2 基本协议

图 1 给出了非交互双方交集计算协议 TBPSI，该协议以 $A$ 和 $B$ 各自的私有集合 $Y$ 和 $X$ 为输入，安全地计算双方交集 $f_\cap(Y, X)=Y\cap X$。其中，$H_K(.)$为带密钥的单向哈希函数；“||”表示 2 个二进制串连接；$E_K(.)$和 $D_K(.)$为对称加、解密函数。本协议要点在于，如果 $A$ 和 $B$ 具有相同的元素，则以这些元素为密钥，对相同的二进制串计算得到的哈希值一定相同，$A$ 可以通过比较这些哈希值找出双方的交集。

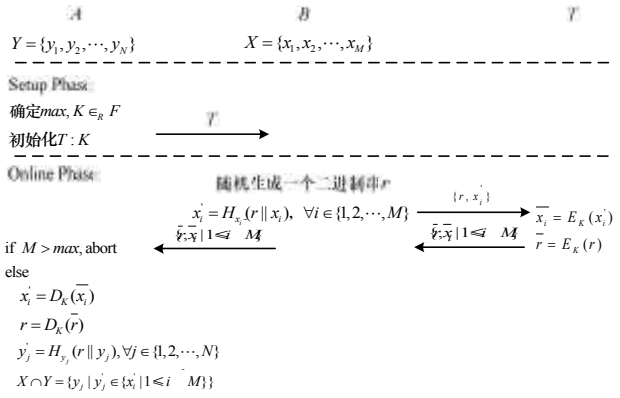


**图 1 双方交集协议 TBPSI**

**定理** 如果 $E$ 是一个强的伪随机排列(Strong Pseudo-random Permutation, SPRP)，$H$ 是单向的，则由 TBPSI 协议可以：(1)安全计算 $f_\cap(Y, X)$，当双方都信任 $T$；(2)安全计算 $f_\cap(Y, X)$，无论 $T$ 和 $B$ 是否是恶意的；(3)保持 $A(B)$的输入是无条件隐秘的，对于恶意 $B(A)$在不开区分意义上。

可以在通用可复合框架下证明本文定理，因此，本文协议是 UC 安全的，可以安全地嵌入后面的指纹在线认证协议中。限于篇幅限制，本文略去严格证明，这里只给出启发性的讨论：(1)定理的第 1 种情形证明的关键在于对于 $A$，若其某个输入元素与 $B$ 的某个元素相同时，有相同的哈希值，否则是随机的。(2)$A$ 的私有数据不会传递给 $T$ 或 $B$，无论恶意的 $B$ 是否与 $T$ 合谋，都不会影响(1)的结果。(3)由于协议是单向的，$B$ 不会得到 $A$ 的任何信息，因此，$A$ 的隐私被无条件的保护。$H$ 是单向的，$T$ 只是加密了 $B$ 的输入元素的哈希值，而非原始值，故 $B$ 的隐私性也得到了保护。注意，对称加密算法 AES 被认为是一种 SPRP。

## 3 基于双方交集计算的指纹认证方案

### 3.1 隐秘模板的生成

本文方案中采用现场用户指纹细节点是否匹配模板中的细节点作为身份认证的依据。细节点是指纹中的端点和分岔点，端点是指一条纹线的末端点，分岔点指的是一条纹线分岔成 2 条分支所对应的点。一般细节点可以用一个三元组 $(x, y, \theta)$来表示，细节点特征是指纹中多个细节点的集合。

为了在开放网络环境中实现隐私型指纹认证，首先要解决存储过程中用户指纹特征模板信息泄露问题，本文方案采用了文献[11]的方法。这种方法包括 2 个要点：(1)生成一个隐秘模板，它由均匀分布的随机数组成，与细节点模板没有任何关系，因此，隐秘模板可以安全地存放在服务器中，不必担心用户的生物数据会被恶意服务器滥用。(2)生成一个具有随机性变换多项式，它由隐秘模板与原始细节点模板共同导出，由用户持有(存放在智能卡中)，由于具有随机性，即使智能卡被攻破也不会泄露用户指纹细节点的信息。模板生成算法如下：

**算法 1** PVTM

**公共参数** 安全参数 $k$，域 $F$

**输入** 用户指纹细节点模板 $U_T=\{u_1,u_2,\cdots,u_{N_T}\}$

**输出** 隐秘模板 $Y_T$，变换多项式 $f_T$

**Step1** 如果 $N_T<k$，则退出，否则继续，其中，$N_T=|Y_T|$。

**Step2** 从 $F$ 中独立地且随机地选择 $N_T$ 个值 $y_1,y_2,\cdots,y_{N_T}$。

**Step3** 用拉格朗日插值法从点对集合 $\{(u_i,y_i)\}_{i=1}^{N_T}$ 中构造一个 $N_T$–1 阶多项式 $f_T$: $f_T(x)=\sum_{i=1}^{N_T}y_il_i(x)=a_{N_T}x^{N_T-1}+\cdots+a_2x+a_1$，其中，$l_i(x)=\prod_{\substack{j=1\\ j\neq i}}^{N_T}\frac{x-u_i}{u_i-u_j}$。

**Step4** 输出 $\{f_T, Y_T=\{y_1,y_2,\cdots,y_{N_T}\}\}$。

在调用本文算法之前，原始细节点的属性$(x, y, \theta)$必须经过适当的量化，以便在变换空间中进行匹配时能够容忍一定的指纹形变和对齐误差。还要进行适当映射，将一个细节点的参数 $x, y$ 和 $\theta$ 映射为 $F$ 中的一个数。本文算法中输入的 $U_T$ 是用户注册时的细节点模板(集合)经过这些处理后的结果。认证时，用户现场样本细节点同样经过上述处理后代入变换多项式 $f_T$ 计算，若现场样本中某个细节点和 $U_T$ 中某个细节点匹配，则得到的计算值一定存在隐秘模板中。

### 3.2 基于指纹的远程身份认证方案

本文的目标集中在执行认证协议期间用户与服务器通信连接的安全性以及认证数据(包括用户及服务器)的隐私性上。用户的指纹数据需在合法的客户端进行采集和处理，本文假定客户端的指纹采集、处理模块、读卡器以及通信模块都是可以防假冒的，它们之间的数据传输是安全的。也不讨论使用假指纹欺骗系统的问题，这涉及活体探测，已经超出本文讨论的范围。

为了保证用户生物数据的隐私，本文方案引入一个可信的第三方——生物认证权威(*BA*)。*BA* 事先要决定认证协议中的公共参数，如安全参数 $k$、集合尺寸限制参数 $max$(其目的是防止认证协议中恶意客户端方使用很大集合来提高身份假冒的成功概率)、运算域 $F$、量化参数 $Q$、哈希函数 $H(\cdot)$等。

本方案分为用户注册、在线认证 2 个阶段。

(1)用户注册

当用户向 $ID$ 为 $S_n$ 的服务器进行注册时，$BA$ 分配给该用户一个 $ID$：$U_m$，并采集用户的指纹图像、提取细节点模板 $M^{\mathrm{T}}$ 和对齐辅助数据 $W$，然后 $BA$ 根据量化参数 $Q$ 把 $M_T$ 量化，并映射为 $U_T$，调用算法 PVTM($U_T$)，生成并输出$\{f_T, Y_T\}$，并为该用户随机分配一个密钥 $K_{init}$。通过安全方式，$\{U_m, Y_T, K\}$ 被送到 $S_n$；$S_n$ 将该数据存储在一个安全数据库中。公共参数 $\{F, g, H(\cdot), Q\}$、变换多项式 $f_T$(实际上是多项式的系数 $\{a_1,a_2,\cdots,a_{N_T}\}$)、$U_m$、$S_n$、$W$ 以及 $K_{init}$ 都被存在一张智能卡中，并由 $BA$ 安全地颁发给用户。最后 $BA$ 删除所有与本用户指纹相关的信息，如 $Y_T$、$f_T$ 以及 $W$。注意智能卡由可信的 $BA$，而非服务器颁发，因此，如果在 2.2 节的双方交集计算协议中使用，会提高安全性。当然并不排除服务器向用户发行自己的智能卡。

(2)在线认证

当用户 $U_m$ 要求服务器 $S_n$ 的提供某种服务时，首先要通过服务器的认证。他将智能卡 $SC$ 插入客户端 $C$ 的读卡器中(若是无线读卡器则无须插卡)，$SC$ 和 $C$ 首先进行某种互认证，确保双方都是合法的，为简单起见，本文忽略这一过程。$C$ 读出存储在 $SC$ 上的对齐辅助数据 $W$ 以及变换多项式 $f_T$。用户在传感器上按下指纹，客户端的指纹处理模块提取出现场指纹细节点集合 $M_Q$ 及其对齐辅助数据 $W'$，利用 $W$ 和 $W'$ 实现现场细节点和模板细节点的对齐，同时根据量化参数 $Q$ 把 $M_Q$ 量化，并映射成 $U_Q$。$U_Q$ 被带入 $f_T$，计算出现场变换细节点集合 $X_Q=\{x_1,x_2,\cdots,x_{N_Q}\}$，其中 $N_Q$ 是现场细节点的数量。然后在 $C$ 和 $S_n$ 之间执行身份认证协议。在本文的认证协议中，当 $S_n$ 确定 $X_Q$ 和 $Y_T$ 的交集之势大于等于安全参数 $k$，说明现场指纹细节点集合与模板集合之间有很高的相似性，则 $S_n$ 接受用户 $U_m$ 的身份，从而实现远程认证。通常认为如果 2 枚指纹的细节点能匹配上 8 个~12 个，即可确定它们来自同一个手指。但文献[12]指出，12 个以上匹配点才是可靠的，因此，$k$ 可以取 13。基于指纹的远程身份认证方案算法如下：

**算法 2** REMOTEAUTHEN

**公共参数** $k, F, max$

**输入** $X_Q, Y_T, K_{init}$

**输出** 接受或拒绝用户身份

**Step1** $C$ 以用户 ID $U_m$ 向 $S_n$ 请求身份认证。

**Step2** $S_n$ 在数据库中查询 $U_m$，并取出与 $U_m$ 对应的 $K_{init}$。

**Step3** 智能卡 $SC$ 与 $S_n$ 用相同的共享秘密 $K_{init}$，通过 $C$ 执行双方密钥分发协议 2DKDP，如果执行成功，则 $SC$ 与 $S_n$ 获得临时会话密钥 $K$，否则中止退出。

**Step4** $S_n$、$C$ 和 $SC$ 分别作为 $A$、$B$ 和 $T$ 执行 TBPSI($Y_T, X_Q$)协议，如果成功，则 $S_n$ 获得 $G=X_Q\cap Y_T$，否则中止退出。

**Step5** $S_n$ 判断$|G|$是否大于等于 $k$，如果是，则接受用户身份，否则拒绝。

以上认证方案中，步骤(3)智能卡通过客户端与服务器执行双方密钥分发协议 2DKDP，这样可以实现服务器与智能卡之间互认证，同时双方获得会话密钥 $K$。双方密钥分发协议采用文献[13]的方案，它具有紧凑安全的特点，只需要 3 条消息的交换，是基于 $nonce$ 值的协议中最少的。与 2.2 节的基本协议有所不同，步骤(4)客户端与服务器执行 TBPSI 协议时，智能卡与服务器并不使用 $K_{init}$，而是 $K$ 来加密双方消息以及后续可能需要加密的其他信息，显然 $K$ 不影响 TBPSI 协议的安全性。此外，公共参数 $Max$ 是在执行 TBPSI 协议时设定的阈值，由于通常固体指纹传感器采集的指纹细节点不会超过 100 个，$max$ 可以设置为略高于 100 即可，它可以用来防止恶意客户端一次给服务器传送很多伪造的细节点来通过认证。

在本文方案中，主要的通信量来自于双方交集计算协议 TBPSI，通信量近似为 $O(N_Q\times l_S)$位，其中，$N_Q$ 为用户现场指纹细节点的数目；$l_S$ 为密文长度，对于 AES 可取 128 位。客户端的计算量主要是智能卡计算 $O(N_Q)$次对称加密，服务器端的主要计算量是执行 $O(N_Q)$次对称解密。而在文献[11]中，由于使用基于同态加密的双方交集计算协议，即便是单向认证(服务器认证用户的合法性)，客户端和服务器也需要一次交互，通信量近似为 $O((N_Q+N_T)\times l_A)$位，其中，$N_T$ 是模板 $Y^T$ 之势；$l_A$ 是同态加密算法密文长度，若采用 Paillier 加密算法，则长度至少为 1 024 位，与本文方案相比，通信负担要重的多。文献[11]中客户端主要计算量是 $O(N_T+N_Q\mathrm{lnln}N_T)$次长指数运算(2 048 位)，服务器计算量主要是执行 $O(N_Q)$次非对称解密。而无论长指数运算还是非常对称解密，比起对称解密都更加耗时。因此，本文方案的通信和计算效率较高。

### 3.3 安全性分析

对本文方案进行安全性分析：

(1)用户假冒

本方案的用户认证要经过 2 步认证：1)用户和服务器执行基于共享秘密的双方密钥分发协议，这要求用户持有合法的智能卡；2)服务器验证用户是否满足一定匹配条件的指纹细节点；因此，本文方案是双因子认证，具有较高的安全性。Janson 等双方密钥分发协议能抵抗重放攻击，该方案也能防止敌手利用以前的旧数据进行用户假冒。即便某个用户智能卡被敌手获得，敌手要成功假冒用户，也必须能够提交与该用户指纹足够相似的指纹，此时用户假冒攻击成功的概率等于系统的错误接受率(False Accept Rate, FAR)。

(2)服务器假冒

虽然本文方案从生物认证角度是单向认证，但 Janson 等双方密钥分发协议可以使得用户和服务器在交换会话密钥的同时，完成相互的认证。由于不同服务器与某个用户共享秘密 $K_{init}$ 是不同的，因此本文方案可以抵御服务器假冒攻击。

(3)用户指纹数据隐私

由模板生成算法 PVTM 可知，服务器中存储的用户模板是完全的随机数，因此不可能将用户指纹数据泄漏。在认证过程中，根据 2.2 节中的定理可知，双方执行的 TBPSI 协议可以保证除了双方集合的交集外的其他数据都不会泄漏给对方，而交集中的数据对于服务器来说是自己已经拥有的随机数，因此，在存储和匹配过程中都不会暴露用户指纹信息。

## 4 结束语

在生物认证过程中，如何保护用户生物数据的隐私是一个迫切需要解决的难题。现有的多种采用同态加密方案的缺点之一在于隐私保护计算和通信的成本很高，影响其推广。

本文提出的使用智能卡实现的隐秘双方交集计算协议能大幅减少计算和通信成本，可与基于指纹细节点匹配方法相结合，为开放网络中进行隐私保护型身份认证提供一种可行的方法。本文方案假定现场指纹和模板已经对齐，虽然有研究者已经开发出一些算法实现在隐秘状态下的“盲”对齐或“预”对齐，但效果不理想，因此，今后将在这方面进行研究。

(下转第 133 页)