基本初等函数的保密云计算服务协议

刘 新[1,2] 李顺东[1] 陈振华[1]
(陕西师范大学计算机科学学院 西安 710062)[1] (内蒙古科技大学信息工程学院 包头 014010)[2]

摘 要 目前云计算已经成为解决很多问题的一个有力平台,同时也带来了大量的安全隐患。其中,关于基本初等函数的保密计算是所有云计算的基础和核心。提出了所有基本初等函数的保密云计算服务协议,其基本思想是将原始数据做变换后,把计算复杂部分发给云平台,通过云计算将结果反馈给接受服务方,从而保密地计算相应函数。通过广泛接受的模拟范例证明了协议的安全性。协议中接受计算服务方可用很少的计算资源解决复杂的计算问题,保证了较低的计算复杂度和通信复杂度,因此提出的协议是有效可行的,可以成为云保密计算中的基础子协议。

关键词 云计算,保密计算服务协议,基本初等函数,安全性
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.10.032

Secure Cloud Computing Service Protocols of Elementary Functions

LIU Xin[1,2] LI Shun-dong[1] CHEN Zhen-hua[1]
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)[1]
(School of Information and Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China)[2]

Abstract Cloud computing has become a powerful platform to solve many problems, while it has brought a lot of secure troubles. Cloud computing of elementary functions is the foundation and core of all cloud computation. We presented secure cloud computing service protocols for elementary functions. After transforming primitive parameters into other forms, we sent the complex parts to the cloud platform to compute. Using the well-accepted simulation paradigm, we proved that the protocols are secure. In the protocols, the service receiver can solve complicated computation problems with less computation sources. The protocols have lower computation and communication overheads. Therefore, the protocols are effective and feasible, and can become the based subprotocols of cloud computing.

Keywords Cloud computing, Secure computation service protocols, Elementary functions, Security

1 引言

随着云计算向电子商务和电子政务迅速渗透,其受到IT、金融等行业的广泛关注,国内外研究机构提出了成功的云计算案例[1],如亚马逊的EC2/S3、Google的Mapreduce/AppEngine、IBM蓝天、国内360云盘等。此外,银行金融业对云计算起着助推作用,例如著名投资银行MorganStanley和法国投资银行等都有云平台。云计算服务模式拥有很多传统服务模式所不具备的特性,它融合多种技术以集约化的资源管理方式向用户提供自由、方便和灵活的服务,这种新的服务模式将引起又一次重大的产业变革,但同时也将带来不少严重的安全问题。

例如,Alice是某银行资金计划高级主管,新年伊始,行长要求Alice要在一周内对上一年度财务指标进行评估测算,包括拆借资金比率、流动负债依存率、核心资本充足率等40多项指标。对于Alice来说,工作量很大而且各项指标计算繁琐,她想如果能利用"云计算"技术,就可以大大减轻工作量并提高效率,但是她又有所担心:如果银行的内部保密数据泄漏出去,后果不堪设想。

针对上述实例,Alice如果可以将原始数据进行保密处理后再发送至云端进行计算,则通过解密反馈结果即可得到所需指标。这样,她既减轻了工作量,提高了效率,又对原始数据进行了保密。我们把这一过程称为"保密计算服务协议",这一概念由Feigenbaum[2]提出。Gramer[3]认为:"如果能够保密地计算所有函数,那么计算科学就有了一个新的强有力的工具"。将多方保密计算协议应用到云计算中,是保证云计算安全的一个重要方面。鉴于各类复合函数的运算均由基本初等函数经过有限次复合后构成,那么在云计算服务中,基本初等函数的保密计算服务方案就显得尤为重要。

目前,多方保密计算已经研究的主要领域包括:数据的保密比较(百万富翁问题),集合关系和几何关系的保密判定,数据的保密挖掘和查询,保密拍卖,保密投票等许多科学计算领域问题[4-6]。Du[7-10]提出了保密的计算向量点积问题、保密的计算线性方程回归问题、最小二乘问题等;此外,他还指出了

到稿日期:2014-10-08 返修日期:2015-01-04 本文受国家自然科学基金资助项目(61272435),中央高校基本科研业务费专项资金项目(GK201504017),包头市科技局项目(2014S2004-2-1-15)资助。

刘 新(1983-),男,博士生,讲师,主要研究方向为多方保密计算、密码学、信息安全,E-mail:LX2001.LX@163.com;李顺东(1962-),男,教授,博士生导师,主要研究方向为密码学与信息安全;陈振华(1976-),女,博士,副教授,主要研究方向为密码学与信息安全。

其他值得研究的问题，包括解线性方程组、矩阵特征值、特征向量和矩阵分解等问题的保密计算。在此基础上，罗文俊[11,12]提出了指数函数和幂函数的两方保密计算方案，但他多次使用模运算和同态加密来计算函数，计算复杂度较高，效率低，而且并没有给出反三角函数的保密计算协议，因此该方案不能广泛地扩展到其他复合函数的运算。李顺东[15]提出了对数函数的保密计算服务协议，利用算术基本定理将自变量进行因子分解，但只能对整数进行分解，计算范围有限，而且分解效率不高。

鉴于以上不足，提出了高效的基本初等函数保密云计算服务协议，包括指数函数、幂函数、对数函数、三角函数和反三角函数。本文所提方案主要具有以下优点：

(1)对原始参数只做简单预处理，即可分为计算简单数据和计算复杂数据。简单数据自行计算，加以保密；复杂数据交由云端来计算。

(2)协议不局限于整数范围，在整个实数范围内均适用。

(3)接受服务方在保密数据的前提下应用较少的计算资源解决复杂的计算问题，大大提高了计算效率。

(4)通过半诚实模型下模拟范例证明协议是安全的，攻击者无法通过部分信息推断出原始数据，具有“信息论安全性”。

(5)基本初等函数的保密计算是云计算的基础，方案有效可行。在多方保密计算和密码学研究中也具有理论意义，将Gramer提出的“保密地计算所有函数”推进一步。

本文第2节的预备知识给出了保密性定义、模拟范例定义以及离散对数的通用解决方案；第3节给出了5个基本初等函数协议的构造方案，以及对每个协议的安全性和正确性分析；第4节为安全性证明；第5节是计算复杂性和通信复杂性的性能分析与比较；最后给出了总结。

2 预备知识

2.1 保密性定义

(1)半诚实参与者

本协议的保密性建立在半诚实参与者模型下。如果半诚实模型下的多方保密协议调用Goldreich[14]设计的模拟器，该模拟器就可输出一个恶意模型下的多方安全协议。因此，只研究半诚实模型下的多方安全计算协议。

(2)双方保密计算的模拟范例

一个双方计算是一个随机计算过程，记为 $f:(0,1)^*\times(0,1)^*\to(0,1)^*\times(0,1)^*$，其中 $f=(f_1,f_2)$，对于输入$(x,y)\xrightarrow{\pi}(f_1(x,y),f_2(x,y))$。

在执行协议 π 的过程中，如果参与者所获得的信息都可以通过他自己的输入和输出进行模拟，但他得不到任何额外的信息，则说明该协议是安全的。这就是研究多方保密计算问题时普遍接受的模拟范例。

定义1(半诚实模型的安全性) 对于一个函数 f，如果存在概率多项式时间算法 S_1 与 S_2，使得

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}\overset{c}{=}\{view_1^{\pi}(x,y),output_2^{\pi}(x,y)\} \quad (1)$$

$$\{(f_1(x,y),S_2(y,f_2(x,y)))\}\overset{c}{=}\{output_1^{\pi}(x,y),view_2^{\pi}(x,y)\} \quad (2)$$

则认为 π 保密地计算 f。其中，Alice和Bob得到的信息序列分别记为 $view_1^{\pi}(x,y)=(x,r^1,m_1^1,m_2^1,\cdots,m_t^1)$ 和 $view_2^{\pi}(x,y)=(x,r^2,m_1^2,m_2^2,\cdots,m_t^2)$，输出结果分别记为 $output_1^{\pi}(x,y)$ 和 $output_2^{\pi}(x,y)$，$\overset{c}{=}$ 表示计算上不可区分。要证明一个多方计算协议是安全的，就必须构造满足式(1)和式(2)的模拟器 S_1、S_2。

2.2 离散对数的保密计算通用协议

Feigenbaum[2]提出了离散对数问题的多方保密计算通用协议，但是Goldreich[14]指出：“考虑到效率的问题，利用通用方案解决所有保密计算问题是不现实的，应该针对不同的问题研究出高效的解决方案”。本文针对基本初等函数，研究其各自的保密云计算服务解决方案。

3 保密云计算服务协议

对于Alice来说，她只会简单的加减乘除运算，面对复杂的函数运算，她却无能为力。但是，她通过对参数做一些变换，希望云计算平台能为其服务，并且要保证数据的保密性。本节给出包括指数函数、幂函数、对数函数、三角函数、反三角函数在内的初等函数的保密云计算服务协议。

3.1 指数函数的保密云计算服务协议

指数函数 a^y 的计算对于Alice来说是无法完成的，尤其当指数 y 为非整数(例如 $3^{2.3}$)时，计算更加困难。根据指数函数运算性质，可将 y 分解成 kx 和 b，即 $a^y=a^{kx+b}=a^{kx}\times a^b=(a^x)^k\times a^b$，其中，计算 a^x 对于Alice来说是困难的，而计算 k、b 整数次幂对于她来说是容易的，因此Alice只要求云端计算 a^x，保密参数 k 和 b，进而保密了指数 y。具体协议如下：

协议1 指数函数的保密云计算服务协议

输入：a^y，y_0

输出：a^{y_0}

(1)Alice先把 $y_0\to kx+b$，将底数 a 和指数 x 发送至云端来计算；

(2)云端计算 $a^x\to c$，将结果 c 发给Alice；

(3)Alice收到 c 后，计算 $c^k\times a^b$ 即为 a^{y_0}。协议结束。

安全性与正确性分析：

(1)Alice将实数 y_0 分解为 $kx+b$，发给云平台只要求计算 a^x，所以 k 和 b 是保密的，攻击者无法通过 a 和 x 推出 y_0；

(2)在本协议中，Alice保留地计算 c^k 和 a^b 是计算简单的，她可以完成；

(3)底数 a 的取值范围不局限在整数范围内，在实数范围内本协议均成立。

举例说明：

计算 $(\frac{2}{3})^{2.3}$，可将指数2.3分解为 $0.1\times3+2$，Alice要求云平台计算 $(\frac{2}{3})^{0.1}\to c$，并返回计算结果，她自己只需计算 $c^3\times(\frac{2}{3})^2$。

3.2 幂函数的保密云计算服务协议

Alice要计算幂函数 x^b，当底数 x 是计算较复杂的数字(如 17.5689^5)时，Alice无法完成。但她想到将 x 分解为 $\alpha\times\beta$，其中 α 为复杂的非整数部分，而 β 为简单的整数，因此将分解后的 α 发给云端，云端将计算结果 a^b 返给Alice，帮助她完

成幂函数的计算。具体协议如下：

协议 2　幂函数的保密云计算服务协议

输入：x^b，x_0

输出：x_0^b

(1) Alice 将 x_0 分解为：$x_0=\alpha\times\beta$；

(2) Alice 将 α 和 b 发给云端，要求计算 α^b；

(3) 云计算 $\alpha^b\rightarrow c$，将 c 反馈给 Alice；

(4) Alice 收到 c 后计算 $c\times\beta^b$，所得结果即为 x_0^b。协议结束。

安全性与正确性分析：

(1) Alice 只将 α^b 发给云平台进行计算，并没有泄漏 β 的信息，云端攻击者无法推断出 x_0，因此 x_0 是保密的；

(2) 在协议中，Alice 计算 β^b 是简单可行的；

(3) Alice 对 x_0 的计算不局限于整数范围内，可扩展到实数范围内。

举例说明：

Alice 要计算 17.5689^5，对于她来说，计算是复杂的，但她将 17.5689 分解为 5.8563×3，只将因子 5.8563 和 5 次幂发给云端，要求云端计算 $5.8563^5\rightarrow\lambda$，云端将计算结果 $\lambda=5.8563^5$ 反馈给 Alice，Alice 只需计算 $\lambda\times3^5=243\lambda$。在这一过程中，Alice 并没有泄漏因子 3，而且 3^5 对于她来说是计算简单的，所以数据 17.5689 是保密的。

3.3　对数函数的保密云计算服务协议

计算对数函数 $\ln x$ 对于 Alice 来说是复杂的，尤其当 x 不是整数(如 ln12.586)时，计算就更加困难。那么她希望借助云计算资源来完成 $\ln x$ 的计算。$\ln x$ 的保密计算服务协议已经由李顺东提出[15]，其将 x 按照算术基本定理分解后再计算；而算术基本定理的分解只适用于整数情况，本文提出另一种解决方案，其相对算术基本定理的分解更加简单，而且适用于非整数情况，进一步推广到了实数范围。

Alice 将 x 分解为 $\alpha\times\beta$，根据对数性质：$\ln x=\ln(\alpha\times\beta)=\ln\alpha+\ln\beta$，Alice 将复杂的因子 β 发给云端，要求云平台计算 $\ln\beta$；而她自己可以计算简单的 $\ln\alpha$。具体协议如下：

协议 3　对数函数的保密云计算服务协议

输入：$\ln x$，x_0

输出：$\ln x_0$

(1) Alice 将 x_0 分解为 $\alpha\times\beta$，α 保密且 Alice 会计算 $\ln\alpha$，发送 β 给云端，要求云平台计算 $\ln\beta$；

(2) 云端按照要求计算 $\ln\beta\rightarrow b$，将 b 发给 Alice；

(3) Alice 收到 b 后计算 $\ln\alpha+b$，所得结果即为 $\ln x_0$。协议结束。

安全性和正确性分析：

Alice 将 x_0 分解为 α 和 β，计算 $\ln\alpha$ 对于 Alice 来说是简单的，将复杂的 $\ln\beta$ 交给云端来做，保证了 α 是保密的，因此 x_0 是保密的。此外，应用此方法保密计算 $\ln x$ 不受整数限制，所有实数范围内都可计算，拓展了文献[15]的计算范围。

3.4　三角函数和反三角函数的保密云计算服务协议

Alice 只会做特殊角度的三角函数(如 $\sin30^\circ=0.5$)，对于非特殊角度(如 $\sin72^\circ$)无能为力。那么，Alice 可以将 θ 分解为 $\theta_1+\theta_2$，θ_1 的三角函数运算对于 Alice 来说是简单可以完成的，而 θ_2 的运算是复杂的，可以借助云计算资源来计算，具体解决方案如下：

协议 4　三角函数的保密云计算服务协议

输入：$\sin x$，$\cos x$，θ

输出：$\sin\theta$，$\cos\theta$

(1) Alice 将 θ 分解为 $\theta_1+\theta_2$，并且自己计算 $\sin\theta_1$ 和 $\cos\theta_1$，要求云端计算 $\sin\theta_2$ 和 $\cos\theta_2$；

(2) 云端计算 $\sin\theta_2\rightarrow\alpha$ 和 $\cos\theta_2\rightarrow\beta$，将 α 和 β 发给 Alice；

(3) Alice 收到 α 和 β 后，计算 $\sin\theta_1\times\beta+\cos\theta_1\times\alpha$ 所得即为 $\sin\theta$；计算 $\cos\theta_1\times\beta-\sin\theta_1\times\alpha$ 所得即为 $\cos\theta$。协议结束。

安全性与正确性分析：

因为云端只获得了 θ_2 的信息，所以在云计算过程中 θ_1 是保密的，因此 θ 是保密的。Alice 所做的工作就是简单的乘法和加法运算，计算简单可行。

协议 5　反三角函数的保密云计算服务协议

输入：$\arctan x$，x_0

输出：$\arctan x_0$

(1) Alice 将 x_0 分解为 α 和 β，满足 $\beta=\frac{x_0-\alpha}{1+\alpha x_0}$，Alice 会计算 $\arctan\alpha$，要求云端计算 $\arctan\beta$；

(2) 云端计算 $\arctan\beta\rightarrow\varepsilon$，将 ε 发给 Alice；

(3) Alice 收到 ε 后，计算 $\arctan\alpha+\varepsilon$ 所得即为 $\arctan x_0$。协议结束。

安全性与正确性分析：

以上通过云端的计算，Alice 既保证了 x_0 的保密性，又完成了反三角函数的运算，计算量很小。

综上所述，借助云计算服务，Alice 可以完成所有初等函数的运算，保证原始数据的保密性，而且计算复杂度不高，适用于所有实数，进一步可计算复合函数。此外，以上所有协议均建立在半诚实模型下，协议的传输过程中没有考虑中间人攻击和云平台的身份认证等问题，如需考虑，那么只需引入 Diffie-Hellmen[16] 公钥密码方案即可解决，这里不再赘述。

4　安全性证明

以上对协议进行了正确性和安全性分析，对于云计算平台，攻击者未能获取足够信息来推出原始数据，协议具有“信息论安全性”。下面通过在半诚实模型下构造满足式(1)、式(2)的模拟器 λ、$\perp$ 给出严格安全性证明。以协议 2“幂函数的保密云计算服务协议”为例，其他协议的证明方法类似。

定理 1　幂函数的保密云计算服务协议是安全的。

证明：按照式(1)、式(2)构造模拟器 S_1、S_2 来证明本定理。在协议 π 中，$x=x_0$，$y=P_0$，$f_1(x_0,P_0)=output_1^\pi(x_0,P_0)$，其中 P_0 是计算幂函数的算法。当云平台将结果 c 反馈给 Alice 后，Alice 不再给云平台任何信息，所以云端得到的最后结果可以看成是空串 $\perp$，即 $output_2^\pi(x_0,P_0)=f_2(x_0,P_0)=\perp$。这里需要保证 x_0 和 $f(x_0)$ 的保密性，所以只要能构造以下模拟器 S_2 即可。

$$\{f_1(x_0,P_0),S_2(P_0,\perp)\}\overset{c}{=}\{output_1(x_0,P_0),view_2^\pi(x_0,P_0)\}\tag{3}$$

在协议中云平台所获得的信息是 α 和 b。

假设云端用于决定算法选择的随机数为 r_0，那么 $view_2^\pi(x_0,P_0)=\{r_0,\alpha,b\}$。

S_2 的模拟过程如下：随机选择另一个数 x_0'，满足 x_0' 和 x_0 具有相同的因子 $\alpha'=\alpha$，但 $x_0'\neq x_0$，计算 $(\alpha')^b$，那么在计算

上不可区分 a^b 和 $(a')^b$，即 $S_2(P_0,\perp)=\{r_0,a',b\}=\{r_0,a,b\}$，则式(3)成立。

所以定理1成立。

用同样方法可以证明以上其他基本初等函数的保密云计算服务协议是安全的。

5 性能分析

本文提出了基本初等函数的多方保密云计算服务协议，接受计算服务方用很少的计算资源即可解决复杂的计算问题。密码学中，常利用计算复杂度和通信复杂度来评价协议的性能。与罗文俊提出的方案[12]、李顺东出的方案[15]和传统计算方法[17]相比，本方案性能有所提升。

5.1 计算复杂度

罗文俊方案[12]中指数函数和幂函数的计算复杂度为 $\exp(\sqrt{\ln(n)\ln\ln(n)})$。李顺东方案[15]中对数函数的计算复杂度为 $O(n)$，而且只适用整数范围内。如果不借助云平台的计算能力，利用朴素的方法[17]，Alice 自行计算指数函数、幂函数、对数函数、三角函数和反三角函数，目前算法的复杂度分别为 $O(2^n)$、$O(n^k)$、$O(\log n)$ 和 $O(n^{1/2}(\log n)^2)$。而通过以上协议，借助云计算服务，Alice 可以大大节约计算资源，接受服务方计算指数函数只需要1次乘法运算；计算幂函数需要1次乘法运算；计算对数函数只需要1次加法运算；计算三角函数需要2次乘法和1次加法运算；计算反三角函数需要1次加法运算。此外，本文方案在实数范围内均适用。

5.2 通信复杂度

在密码学中，主要用通信轮数来衡量通信复杂度。罗文俊方案[12]的通信复杂度为 n 轮；李顺东方案[15]的通信复杂度为1轮。在本文提出协议中，Alice 和云平台只需1轮信息交互即可完成运算，所以通信复杂度均为1轮。计算复杂度和通信复杂度比较见表1。

表1 计算复杂度和通信复杂度(通信轮数)比较

	指数函数			幂函数			对数函数			(反)三角函数	
	朴素方法	文献[12]	协议1	朴素方法	文献[12]	协议2	朴素方法	文献[12]	协议3	朴素方法	协议4、5
计算复杂度	$O(2^n)$	$\exp(\sqrt{\ln(n)\ln\ln(n)})$	1	$O(n^k)$	$\exp(\sqrt{\ln(n)\ln\ln(n)})$	1	$O(\log n)$	$O(n)$	1	$O(n^{1/2}(\log n)^2)$	2
通信复杂度	—	n	1	—	n	1	—	1	1	—	1

此外，本文协议应用于无线传感器网络中具有较高的能量效率[18]，从而提高了能量敏感节点的安全性能。

通过以上分析可知，Alice 借助云计算服务资源，大大降低了计算复杂度，而且通信复杂度仅为1轮，能量效率高，因此协议具有较好的性能。

结束语 本文研究了基本初等函数的保密云计算服务协议，接受服务方对函数的参数做简单变换后，将复杂运算发给云平台，自己仅保留简单计算部分，在保密信息的前提下完成函数的计算。通过模拟范例方法证明了协议在半诚实模型下是安全的，协议中接受服务方具有较低的计算复杂度和通信复杂度。对基本初等函数的保密云计算研究可扩展到所有复合函数的保密云计算，方案简单可行。

参 考 文 献

[1] Sun Cloud Architecture Introduction White Paper[EB/OL]. http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[2] Feigenbaum J, Can Y. Take advantage of someone without having to trust him [C]// Advances in Cryptology Crypto 1985. Berlin: Springer Verlag, 1986: 477-488

[3] Cramer R, Damgard I. Multiparty Computations, an Introduction [M]// Advanced Courses in Mathematics, 2005: 41-87

[4] Yao A C. Protocols for secure computations [C]// Proceedings of the 23th IEEE Symposium on Foundations of Computer Science. Washington, DC: IEEE Press, 1982: 160-164

[5] Goldreich O, Micali S, Wigderson A. How to play any mental game [C]// Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing. Piscataway: IEEE Press, 1987: 218-229

[6] Goldwasser S. Multiparty computations: Past and present [C]// Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. NY: ACM Press, 1997: 1-6

[7] Du W L, Atallah M J. Privacy-preserving cooperative scientific computations[C]// Proc. of the 14th IEEE Computer Security Foundations Workshop. Nova Scotia, Canada, 2001: 273-282

[8] Du W L, Atallah M J. Privacy-preserving cooperative statistical analysis[C]// 17th Annual Computer Security Applications Conference. New Orleans, Louisiana, USA, 2001: 102-110

[9] Du W L. A study of several specific secure two-party computation problems[D]. West Lafayette: Purdue University, 2000

[10] Du W L, Atallah M J. Secure multiparty computation problems and their applications: A review and open problems[C]// Proceedings of New Security Paradigms Workshop 2001. NY: ACM Press, 2001: 11-20

[11] 罗文俊，李祥. 双向零知识证明与初等函数两方保密计算[J]. 贵州大学学报(自然科学版)，2004，21(1)：36-42
Luo Wen-jun, Li Xiang. Two-directional Zero-Knowledge Proof and Secure Two-Party Computation[J]. Journal of Guizhou University(Natural Science), 2004, 21(1): 36-42

[12] 罗文俊，李祥. 多方安全矩阵乘积协议及应用[J]. 计算机学报，2005，28(7)：1230-1235
Luo Wen-Jun, Li Xiang. The secure multi-party protocol of matrix product and its application[J]. Chinese Journal of Computers, 2005, 28(7): 1230-1235

[13] 肖倩，罗守山，陈萍，等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报，2008，34(4)：709-714
Xiao Qian, Luo Shou-shan, Chen Ping, et al. Research on the Problem of Secure Multi-party Ranking Under Semi-honest Model[J]. Acta Electronica Sinica, 2008, 34(4): 709-714

[14] Goldreich O. The Fundamental of Cryptography: Basic Applications [M]. London: Cambridge University Press, 2004

[15] 李顺东. 3个保密计算服务协议[J]. 陕西师范大学学报，2010，38(4)：1-6
Li Shun-dong. Three specific secure computation service protocols[J]. Journal of Shaanxi Normal University, 2010, 38(4): 1-6

[16] Diffie W, Hellman M E. New direction in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 29-40

[17] 李顺东，王道顺. 现代密码学：理论、方法与研究前沿[M]. 北京：

科学出版社，2009
Li Shun-dong, Wang Dao-shun. Modern Cryptography: Theory, Method, Research Fronts[M]. Beijing: Science Press, 2009
[18] Rabaey J, Ammer J, Da Silva Jr J L. Pieo Radio: Ad-hoc wireless networking of ubiquitous low-energy sensor and monitor nodes [C]// Proceedings of IEEE Computer Society Workshop on VLSI. April 2000: 9-12
[19] William P, Brian F, Saul T, et al. LU Decomposition and its applications[M]// 2nd Numerical Recipes in Fortran: The Art of Scientific Computing. Cambridge: University Press, 1992
[20] Lin H Y, Tzeng W G. An efficient solution to the millionaires problem based on homomorphic encryption [C]// Proceedings of Applied Cryptography and Network Security 2005 (LNCS3531). NY: Springer, 2005: 456-466
[21] 李顺东，戴一奇，尤启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报，2005，33(5)：770-773
Li Shun-dong, Dai Yi-qi, You Qi-you. An Efficient Solution to Yao's Millionaires Problem[J]. Acta Electronica Sinica, 2005, 33(5): 770-773
[22] Li S D, Wang D S, Dai Y Q, et al. Symmetric cryptographic solution to yao's millionaires problem and an evaluation of secure multiparty computations [J]. Information Sciences, 2008, 178 (2): 244-255
[23] 李顺东，王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报，2013，41(4)：798-803
Li Shun-dong, Wang Dao-shun. Efficient Secure Multiparty Computation Based on Homomorphic Encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798-803
[24] Malek B, Miri A. Combining attribute-based and access systems [C]// Proc. of 12th IEEE International Conference on Computational Science and Engineering (CSE 2009). IEEE Computer Society, 2009: 305-312

（上接第 158 页）

全需求，设计了 TCPAA 可信应用架构。架构通过把可信计算技术应用到网络信息系统中，分别在访问认证子系统和信息交互子系统中构建了面向场景需求的应用模式和相应的应用流程，并经过实验进行分析，验证了该架构的合理性和通用性。此架构的研究在弥补可信计算相关规范不足的同时，发挥了可信技术的实用性，为如何运用可信计算来增强环境体系安全性和完整性提供了一种思路，使可信计算平台在面对网络信息系统的信息安全应用需求时有依据可循，从而能够实现信息系统真正的信息安全共享的功能。

参 考 文 献

[1] 冯登国，秦宇，汪丹，等. 可信计算技术研究[J]. 计算机研究与发展，2011，48(8)：1332-1349
Feng D G, Qin Y, Wang D, et al. Research on Trusted Computing Technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1332-1349
[2] McDysan D, Lee T H, Yao Lei. Network Access System Including a Programmable Access Device Having Distributed Service Control 7499458B2[P]. 2009-03-03
[3] Frias-Martines V, Sherrick J, Stolfo S J. A Network Access Control Mechanism Based on Behavior Profiles[C]// Annual Computer Security Application Conference (ACSAC'09). Honolulu, 2009: 03-12
[4] 梅芳，刘衍珩，王健，等. 基于可信网络的修复建模与实现[J]. 计算机研究与发展，2009，46(zl)：328-331
Mei F, Liu Y Y, Wang J, et al. Modeling and Realizing of Remediation Based on Trusted Network[J]. Journal of Computer Research and Development, 2009, 46(zl): 328-331
[5] 张焕国，陈璐，张立强. 可信网络连接研究[J]. 计算机学报，2010，33(4)：706-717
Zhang H Q, Chen L, Zhang L Q. Research on Trusted Network Connection[J]. Chinese Journal of Computers, 2010, 33(4): 706-717
[6] 沈昌祥，张焕国，王怀民，等. 可信计算的研究与发展[J]. 中国科学：信息科学，2010，40(2)：139-166
Shen C X, Zhang H G, Wang H M, et al. Research and Development of Trusted Computing[J]. Science China Information Sciences, 2010, 40(2): 139-166
[7] 孙守胜. 基于国产可信计算平台的可信终端的应用研究[D]. 北京：北京交通大学，2011
Sun S S. Research on Application of Secrecy-involved Terminal Based on Trusted Computing Platform[D]. Beijing: Beijing Jiaotong University, 2011
[8] 王浩，陈泽茂，李铮，等. 基于可信网络连接的多级涉密网安全接入方案[J]. 计算机科学，2012，39(12)：65-69
Wang H, Chen Z M, Li Z, et al. Secure Access Scheme Based on TNC for Multi-level Classified Network[J]. Computer Science, 2012, 39(12): 65-69
[9] 王宇，王飞. 涉密信息系统网络安全需求分析与解决方案[J]. 装备学院学报，2013，24(4)：105-109
Wang Y, Wang F. Trusted Security Demand Analysis and Solution of the Secret Information System Network[J]. Journal of Academy of Equipment, 2013, 24(4): 105-109
[10] 谷德丽. 可信网络接入远程证明方案的研究[D]. 哈尔滨：哈尔滨工程大学，2013
Gu D L. Research on Trusted Network Access and Remote Attestation and Scheme[D]. Harbin: Harbin Engineering University, 2013
[11] 刘迎春，郑小林，陈德人. 信任网络中基于角色信誉的信任预测[J]. 北京邮电大学学报，2013，36(1)：72-76
Liu Y C, Zheng X L, Chen D R. Trust Predication Based on The Credibility of The Role in Trust Network[J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(1): 72-76
[12] 刘一博，殷肖川，高培勇，等. 基于可信计算的网络互联模型[J]. 计算机应用，2014，34(7)：1936-1940
Liu Y B, Yin X C, Gao P Y, et al. Network Interconnection model Based on Trusted Computing[J]. Journal of Computer Applications, 2014, 34(7): 1936-1940
[13] 戴桦. 基于可信计算技术的信任评估机制研究[D]. 南京：南京邮电大学，2011
Dai H. Research on Trust Evaluation Mechanism Based on Trusted Computing Technology[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2011