

集成员判定问题的安全多方计算解决方案

豆永丽*, 王海春, 康 剑

(成都信息工程学院 网络工程学院, 成都 610225)

(*通信作者电子邮箱 137850175@qq.com)

摘 要:对可交换密钥解决方案与同态加密解决方案进行了分析,并指出了二者在计算复杂度上的不足。在此基础上,提出了另外两种解决方案,一种是基于混沌加密解决方案,另一种是引入不可信第三方参与的非对称加密解决方案,并分析证明了这两种方案的正确性、安全性和复杂性。将提出的新方案与现有的方案进行实验对比,结果证实了新方案能降低算法的复杂度,极大地提高了算法的执行效率。

关键词:安全多方计算;集成员判定;混沌加密;可交换加密;不可信第三方

中图分类号: TP309 **文献标志码:** A

Secure multiparty computation solutions of collection member decision

DOU Yongli*, WANG Haichun, KANG Jian

(College of Network Engineering, Chengdu University of Information Technology, Chengdu Sichuan 610225, China)

Abstract: The exchangeable key solutions and homomorphic encryption solutions were analyzed. Meanwhile, the deficiencies of these two solutions on the computational complexity were pointed out. On the basis of that, two new solutions were put forward: one was based on chaotic encryption solution, and the other was asymmetric encryption solution which introduced the incredible third party. The correctness, security and complexity of them were analyzed and verified. The comparison between the proposed solutions and the existing ones was given. The experimental results show that the new solutions can reduce the complexity of the algorithm, and greatly improve the execution efficiency of algorithm.

Key words: secure multiparty computation; collection member decision; chaotic encryption; exchangeable encryption; incredible third party

0 引言

Yao^[1]于20世纪80年代初首先提出安全多方计算问题,目前许多学者在很多领域进行了相关研究,所研究的问题有:科学计算、计算几何、比较相等、多方排序与数据挖掘等领域,这些研究促进了安全多方计算理论的蓬勃发展。随后,Goldreich等^[2]提出了可以计算任何函数的安全多方计算协议,并证明了存在被动攻击时,拥有广播信道且用户间通过两两安全信道相连时, n -Secure的威胁是存在的;存在主动攻击者和广播信道时, $n/2$ -Secure的协议才是存在的。1998年,Goldreich^[3]比较完整地总结了被动式攻击与主动式攻击情况下串通攻击者数目的理论上限,并指出:用通俗的协议来解决安全多方计算问题中的特殊情况是不可行的,应该针对具体问题设计具体的安全多方计算协议。这一结论促使许多研究人员在安全多方计算的一些特殊领域进行研究。

近年来,很多学者对安全多方计算特殊实例进行了研究,产生了一些新的研究方向,包括保护隐私的数据挖掘(Privacy Preserving Data Mining, PPDm)、保护隐私的计算几何(Privacy Preserving Computation Geometry, PPCG)和私有信息检索(Private Preserving Statistical Analysis, PPSA)等。国内外对安全多方计算研究主要有以下几个问题:科学计算问题^[4]、计算几何问题^[5]和比较相等问题^[6]、多方排序问题与数据挖掘问题。对这些问题的研究虽然取得了较大的理论价值,但这些问题研究仅仅局限于少数几个领域,并且现有的协议远

远没有达到应用的目的,因为在这些研究中存在时间复杂度或空间复杂度或通信代价较高等复杂问题,还不能较好地解决实际应用问题。本文主要研究了集成员的判定问题。

安全多方计算(Secure Multiparty Computation)是指在一个互不信任的分布式网络中,两个或多个参与者在泄露各自私有输入信息时协同合作执行某项计算任务。安全多方计算在当今的军事和商业领域有广泛的用途,Goldwasser^[7]甚至预言:今天的安全多方计算就如同十几年前的公钥密码学一样,它是一个有着丰富理论基础的强大工具,目前它的实际应用才刚刚开始,但它必将成为计算机领域的一个完整的组成部分。因为受到计算复杂度和通信复杂度的制约,Goldreich^[8]指出:“因为效率的原因,应用通用解决方案来解决某个具体的多方保密计算问题是不现实的,应该针对不同的问题研究高效的解决方案”。

集成员的判定问题是安全多方计算的重要内容之一,它要求保密地判断参与一方所拥有的元素是否在另一方的集成员中。集成员的判定问题在生活中应用较为广泛,例如,Bob手上掌握一份机密文件,机密文件中包含若干关键问题,Alice知道一个关键问题,现在Alice想确定自己知道的关键问题是不是Bob的机密文件中所提到的,又不能泄露此关键问题给Bob;同时,Bob除了能够让Alice验证自己手中所掌握的机密文件到底有没有他所掌握的那个关键问题,但又不泄露其他关键问题的信息。以上问题的数学模型就是集成员的判定问题。

收稿日期:2013-07-01;修回日期:2013-08-29。 基金项目:四川省科技基金资助项目(2011ZK00012)。

作者简介:豆永丽(1987-),女,河南周口人,硕士研究生,主要研究方向:混沌加密、物联网安全;王海春(1957-),男,四川成都人,教授,主要研究方向:混沌加密、物联网安全、实时软件工程;康剑(1987-),男,湖北孝感人,硕士,主要研究方向:混沌加密、物联网安全。

在文献[9]提出使用可交换的加密算法来解决集合成员判定问题,文献[10]中使用同态加密算法来解决集合成员的判定问题,这两种算法计算复杂度较高。本文提出了两种新的解决集合成员判定问题的方案:一种方案是采用混沌密钥流对元素 α 与集合 S 中的成员分别进行加密,然后求 α 加密后的结果是否在 S 加密后的集合 S' 中;另一种方案是引入不可信的第三方,改进使用同态加密的方案来解决集合成员的判定问题,只需要使用一般的加密算法即可,这样可以降低算法复杂性,大大提高算法的执行效率。

1 预备知识

1.1 集合成员判定问题

在 Alice 和 Bob 都想知道元素 a 是不是属于集合 S 中的成员,而不能泄露 a 与 S 中成员信息。

1.2 混沌系统及实时密钥产生

混沌是确定的非线性系统中存在的一种貌似无规则、类随机现象,是连续或离散动力系统产生的无固定周期的循环行为^[11]。混沌具有很好的混合特性可以保证混沌加密器的扩算,混乱作用正好与传统密码学的加密特性类似,因此可以将混沌理论应用于密码学领域^[12]。本文使用 Logistic 混沌方程来产生密钥流,Logistic 方程如式(1)所示。

$$x_{n+1} = u \times x_n \times (1 - x_n) \quad (1)$$

其中: $u \in (0, 4)$ 为参数, $x_0 \in (0, 1)$ 为初始值。

1.2.1 混沌系统特性

Logistic 混沌映射分岔图如图1所示。当 $u \in (0, 4)$, 该映射 x_n 的值在 $[0, 1]$ 的范围内随着 u 值得变化而变化,该映射出现分叉后,最后呈现混沌现象。

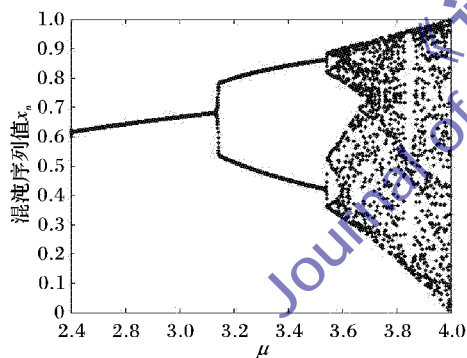


图1 Logistic 映射分叉图

若将初始值微小变化,迭代结果值将会出现巨大差异。如图2所示,其中, $u = 4$,初始值 x_0 分别取0.200 000(用菱形标识对应混沌序列值)与0.200 001(用圆形标识对应混沌序列值)时,迭代20次后所得的结果分别为0.8200和0.0314。

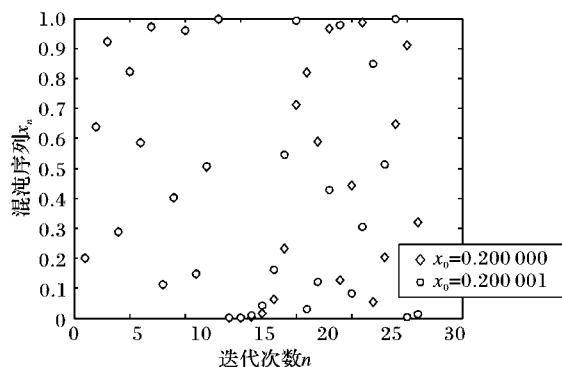


图2 不同初值敏感性对比图

从图2中的结果可知,该混沌序列所得的结果值分布在 $[0, 1]$ 区间,具有遍历性,且初始条件相差十万分之一,迭代20次以后,其结果正负相差26倍之多,这体现了混沌一个非常重要的特征,即初始值的微小变化将会导致系列结果值 x_n 的巨大差异。

1.2.2 混沌密钥加密模型

混沌加密算法流程如图3所示,由于 Logistic 映射具有初始值的极度敏感性,可以对初始值 x 采取简单的正弦映射绝对值 x_0 作为 Logistic 映射初始值,这样既可以保证初始值位于 $[0, 1]$,又可以保证混沌 Logistic 迭代后密钥流的随机性,提高对明文加密的抗攻击能力,正弦映射绝对值如式(2)所示。

$$x_0 = |\sin x| \quad (2)$$

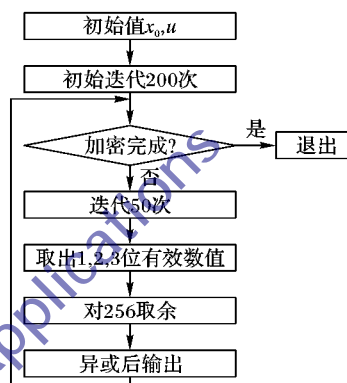


图3 混沌加密算法的实现

1.3 安全性定义

在半诚实模型下,不考虑可信的第三方,而是依靠安全多方计算的保密性协议进行保密通信,对模型的安全性作如下描绘:假设参与计算的双方分别为 Alice 和 Bob,设 $f = (f_1, f_2)$ 是一个概率多项式时间函数, π 则是参与合作计算的协议。在运行协议 π 的过程中,Alice 与 Bob 得到消息系列分别记为视图 $view_1^\pi(x, y) = (x, r^1, m_1^1, \dots, m_i^1)$ 和 $view_2^\pi(x, y) = (x, r^2, m_1^2, \dots, m_i^2)$ 。其中: x, y 分别为 Alice 与 Bob 的输入信息, r^1, r^2 分别表示 Alice 与 Bob 独立的硬币抛掷的结果,双方收到的第 i 个信息分别记为 m_i^1 和 m_i^2 。执行协议后,双方的输出分别为 $output_1^\pi(x, y)$ 和 $output_2^\pi(x, y)$ 。

定义1 在半诚实模型下,对于一个函数 f ,如果存在概率多项式时间算法 s_1, s_2 使得式(3)和式(4)成立:

$$\{s_1(x, f_1(x, y)), f_2(x, y)\}_{x, y} \stackrel{c}{=} \{view_1^\pi(x, y), output_2^\pi(x, y)\}_{x, y} \quad (3)$$

$$\{f_1(x, y), s_2(y, f_2(x, y))\}_{x, y} \stackrel{c}{=} \{output_1^\pi(x, y), view_2^\pi(x, y)\}_{x, y} \quad (4)$$

则认为 π 能保密地计算 f ,其中 $\stackrel{c}{=}$ 表示计算上的不可区分性。如果要证明一个协议是保密的,即可以通过构造满足式(3)和式(4)的模拟器来进行证明^[13]。

2 解决方案

2.1 可交换加密解决方案

集合成员判定问题的可交换加密协议的基本思想为: Alice 与 Bob 都有一个可交换的加密算法,分别选择一个相应的密钥 k_1 与 k_2 ,假设 U 是一个全集, $|U| = n$, Bob 拥有集合 $S, S = \{a_1, a_2, \dots, a_n\}, S \in U, S$ 的补集是 $\bar{S}, S \cup \bar{S} = U, |S| +$

$|\bar{S}| = |U|$; Bob 从 $\{S, \bar{S}\}$ 中选择一个集合, 记作 A , Bob 再构造一个集合, 记作 $B, B = \{b_1, b_2, \dots, b_k, b_{k+1}, \dots, b_t\} (t = \lfloor |U| \rfloor)$ 。当 $1 \leq i \leq k$ 时, 则 $b_i = a_i$; 如果 $k+1 \leq i \leq t$, $b_i \notin U$, 由构造形式可知 $A \subset B$ 。本文使用 $x \subseteq B$ 来判别 $x \subseteq A$, 从而隐藏 A , 进而隐藏 S 。可交换加密方案如方案 1 所示。

方案 1 可交换加密解决方案。

输入 Alice 拥有元素 a , Bob 拥有集合 $S = \{a_1, a_2, \dots, a_m\}$;

输出 $P(a, S)$ 。

1) Bob 用可交换的加密方案加密集合 $S = \{a_1, a_2, \dots, a_m\}$, 将加密结果 $E_{k_2}(S)$ 发送给 Alice。

2) Alice 加密 $E_{k_2}(S)$ 和 a , 得到加密结果为 $E_{k_1}(E_{k_2}(S))$ 与 $E_{k_1}(a)$, 并将得到的加密结果 $E_{k_1}(E_{k_2}(S))$ 与 $E_{k_1}(a)$ 发送给 Bob。

3) Bob 加密 $E_{k_1}(a)$ 得到 $E_{k_2}(E_{k_1}(a))$, 如果 $E_{k_2}(E_{k_1}(a)) \in E_{k_1}(E_{k_2}(S)) \wedge (A = S)$, 那么 $a \in S$, 否则, $a \notin S$; 如果 $E_{k_2}(E_{k_1}(a)) \in E_{k_1}(E_{k_2}(S)) \wedge (A \neq \bar{S})$, 那么 $a \in S$, 否则, $a \notin S$ 。

2.2 同态加密解决方案

同态加密方案的基本思路如方案 2 所示。

方案 2 同态加密解决方案。

输入 Alice 拥有元素 a , Bob 拥有集合 $S = \{a_1, a_2, \dots, a_n\}$, Alice 与 Bob 商定一个相同的同态加密体制 E , Bob 拥有自己公私钥, 并把自己的公钥传给 Alice;

输出 $P(a, S)$ 。

1) Bob 生成一个 n 维向量 $V_x = \{\partial_1, \partial_2, \dots, \partial_n\}$, 其中 a 满足: $a \in S \Leftrightarrow |\partial_i| = 1 (1 \leq i \leq n)$; 然后计算 $(\beta_1, \beta_2, \dots, \beta_n) = EK_{V_x} = (EK_{\partial_1}, EK_{\partial_2}, \dots, EK_{\partial_n})$, 并将加密向量 $(\beta_1, \beta_2, \dots, \beta_n)$ 发送给 Alice。

2) Alice 选择 a 对应位置 p 的向量 ∂_p , 首先计算 EK_0 , 随后计算 $C = EK_{(\partial_p \oplus 0)}$, 并将 C 送给 Bob。

3) Bob 计算明文 $\partial_p = EK_C$, 若计算的结果 $|\partial_p| = 1$, 则 $a \in S$; 否则, $a \notin S$ 。

4) Bob 将结果告诉 Alice。

2.3 混沌加密解决方案

集合成员判定问题的混沌加密解决方案的基本思想为: Alice 用混沌加密方式对元素 a 进行加密, Bob 用混沌加密方式加密集合 S 中的所有成员, 然后用 a 加密的结果与集合 S 中成员的加密结果逐一进行比较, 如果存在相等的结果, 说明 $a \in S$; 否则, $a \notin S$ 。混沌加密解决方案如方案 3 所示。

方案 3 混沌加密解决方案

输入 Alice 拥有元素 a , Bob 拥有集合 $S = \{a_1, a_2, \dots, a_m\}$;

输出 $P(a, S)$ 。

1) Alice 将 a 作为加密明文, 按照式(2)将 a 转化为 $[0, 1]$ 内的小数 a_0 , 将 a_0 作为混沌 Logistic 方程的初始值, 按照图 3 中所示的混沌加密算法, Alice 得到加密结果为 a' , 将加密结果 a' 传送给 Bob。

2) Bob 按照与 Alice 相同的加密方式, 将集合 S 中的成员逐一进行混沌加密, 得到加密结果为 $S' = \{a_1', a_2', \dots, a_m'\}$ 。

3) Bob 将 Alice 传送的结果 a' 与 $S' = \{a_1', a_2', \dots, a_m'\}$ 进行逐一比较, 如果存在 $a' = a'_i (1 \leq i \leq m)$, 则 $a \in S$; 否则,

$a \notin S$ 。

4) Bob 将结果告诉 Alice。

定理 1 集合成员判定问题的混沌加密解决方案是安全的。

证明

1) 正确性。Alice 拥有的元素 a 经过混沌加密得到的结果为 a' , Bob 的集合 S 经过混沌加密得到的结果为 S' , 由混沌流加密的特性可知 a' 与 S' 中混沌加密成员的结果 a_1', a_2', \dots, a_m' 都是唯一的, 因此当 a' 与集合加密成员 a_1', a_2', \dots, a_m' 中存在某个元素相同时, 则说明在集合 S 中也存在与 a' 相同的成员, 即 $a \in S$; 反之, 当 Alice 元素 a 加密后得到的结果 a' 与集合中加密的元素 a_1', a_2', \dots, a_m' 都不相同时, 则说明集合 S 中不存在与 a 相同的成员, 故 $a \notin S$ 。

2) 安全性。构造两个模拟器 S_1 和 S_2 使式(3)与式(4)成立来证明定理的安全性, 利用 S_1 来模拟 Alice, S_2 来模拟 Bob。 S_1 接收输入 $(a, P(a, S))$, 由 $P(a, S)$ 来构造一个 a_i , 使得 $P(a, S) = P(a_i, S)$ 。如果 $P(a, S) = 1$, 则令 $a_i \in S$; 如果 $P(a, S) = 0$, 可以任意设置一个 $a_i \notin S$ 。现在模拟器 S_1 利用 a_i 与集合 S 来模拟该协议的执行过程, 最后输出 $P(a_i, S)$ 的值。在该协议中, $output_1^\pi(a, S) = P(a, S)$ 。在协议执行的过程中, Alice 所得到的信息为 $view_1^\pi(a, S) = \{a, a', P(a, S)\}$; 模拟器模拟过程中, Alice 所得到的信息为 $S_1 = \{a_i, f_1(a_i, S)\} = \{a_i, r, a_i\}$, r 为随机数。因为 a 与 a_i 在计算上不可区分, 所以 a 与 a_i 在计算上也不可区分, 因此存在等式: $P(a, S) = P(a_i, S)$ 。所以模拟器 S_1 满足等式: $\{S_1(a, f_1(a, S)), f_2(a, S)\} \stackrel{c}{=} \{view_1^\pi(a, S), output_2^\pi(a, S)\}$; 类似, 构造一个模拟器 S_2 , 可使等式 $\{f_1(a, S), S_2(a, f_2(a, S))\} \stackrel{c}{=} \{output_1^\pi(a, S), view_2^\pi(a, S)\}$ 成立。因此该协议是安全的。

3) 复杂性。

①计算复杂度: 在此方案中, 采用混沌流加密的方法, 需要进行 $m+1$ 次加密运算过程, 加密过程是通过与产生流密钥的异或运算, 安全性较高, 算法复杂度为 $O(m)$ 。

②通信复杂性: 通信复杂性是指协议执行过程中需要进行通信的总次数或通信轮数。此方案中混沌加密的方案需要进行 $2m+2$ 次交互通信过程。

2.4 不可信第三方解决方案

集合成员判定问题不可信第三方解决方案的基本思想为: 引进不可信的第三方 Cent, 使用一般的加密算法来代替同态加密算法, 其解决方案如方案 4 所示。

方案 4 基于不可信第三方解决方案。

输入 Alice 拥有元素 a , Bob 拥有集合 $S = \{a_1, a_2, \dots, a_n\}$, 全集 $U_{(|S|=n)}, S \subset U, a \in U$;

输出 $P(a, S)$ 。

1) 第三方 Cent 生成一对公钥和私钥, 然后将公钥传送给 Alice 和 Bob, EK 和 DK 分别表示其加密算法和解密算法。

2) Bob 根据规则生成一个 n 维向量 $V_x = \{\partial_1, \partial_2, \dots, \partial_n\}$, $\partial_i = 1 \Leftrightarrow a \in S$ 。Bob 用 Cent 传过来的密钥进行加密计算: $EK_{V_x} = (EK_{\partial_1}, EK_{\partial_2}, \dots, EK_{\partial_n})$, 并传送 EK_{V_x} 给 Cent。

3) Alice 选择 a 对应位置 p 的向量 ∂_p , 并计算 EK_{∂_p} , 将 EK_{∂_p} 发送给第三方 Cent。

4) Cent 收到 EK_{∂_p} 后, 利用自己的私钥进行解密, 得到 $\partial_p = DK(EK_{\partial_p})$, $V_x = DK(EK_{V_x})$, 找出 ∂_p 在 V_x 中的位置, 若 $\partial_p = 1$, 则 $a \in S$; 否则, $a \notin S$ 。

定理 2 基于不可信第三方解决方案是安全的。

证明

1) 正确性。由于 Cent 解密得到 $V_x = \{\partial_1, \partial_2, \dots, \partial_n\}$, 可以从中得到 Alice 元素对应向量的模是否等于 1; 又由 $a_i = 1 \Leftrightarrow a_i \in S$ 可知, 如果 $|\partial_p| = 1$, 则 $a \in S$; 否则, $a \notin S$ 。因此, 协议是正确的。

2) 安全性。在方案 4 中引入不可信第三方 Cent。Alice 只是选择 a 在数值中所对应的 ∂_p 经过加密发送给 Cent, Bob 没有发送自己的集合给 Cent, 而是通过加密向量 V_x 发送给第三方 Cent, 因为只有 Cent 才有私钥可以进行解密, 因此, 其他人即使获得了结果也没有用。当 Cent 得到 Alice 和 Bob 传输过来的数据后, 解密仅仅能得到 V_x 和 ∂_p , 根据 $|\partial_i| = 1 \Leftrightarrow \partial_i \in S$, 不可信第三方 Cent 只能确定 $a \in S$ 是否成立, 而不能知道具体的 a 和 S 的数值。

3) 复杂性。在该方案中引入了不可信的第三方, 使用的解决方案是对同态加密解决方案的改进, 该方案需要进行 $m+1$ 次的加密运算和 $m+1$ 次的解密运算, 而不需要复杂的同态运算, 算法运算性能大大提高, 其算法复杂度为 $O(m)$; 该方案需要进行 $n+3$ 次通信过程。

各个方案计算复杂度与通信复杂度见表 1, 其中: $n > m$, g, r 为随机数, λ 为同态加密算法中选取两个素数的最大公约数。

表 1 各方案计算复杂度与通信复杂度对比

方案	计算复杂度	通信复杂度
1	$O(m \times n)$	$2m + 2$
2	$O(m \times g^m \times r^\lambda)$	$n + 2$
3	$O(m)$	$2m + 2$
4	$O(m)$	$n + 3$

3 结语

本文针对集合成员的判定问题, 在介绍现有的一般解决方案的基础上提出了两种高效解决方案, 即混沌加密解决方案和引入不可信第三方解决方案; 并分别从协议的实现、正确性、安全性以及性能对各种协议进行了分析。结果表明, 混沌加密是通过 Logistic 系统产生密钥流来对明文字节流进行加密, 其安全性能较好, 复杂性不高; 引入不可信的第三方解决方案是对同态加密方案的一种改进, 它使得协议的复杂度大大降低, 提高了协议的执行效率。目前研究的集合判定解决方案大都是基于半诚实模型下进行的, 然而, 当有恶意参与者

的情况下, 计算协议的安全性将会大大降低, 因此, 全面研究恶意模型下安全多方计算问题仍然是后期需要继续研究的课题。

参考文献:

- [1] YAO A. Protocols for secure computation [C]// Proceeding of the 1982 23th IEEE Annual Symposium on Foundations of Computer Science. Washington, DC: IEEE Computer Society, 1982: 160 - 164.
- [2] GOLDREICH O, MICALI S, WIGEDERSON A. How to play any mental game [C]// Proceedings of the 1987 19th Annual ACM Symposium on Theory of Computing. New York: ACM, 1987: 218 - 229.
- [3] GOLDREICH O. Secure multi-party computation [EB/OL]. (2001 - 06 - 24) [2013 - 04 - 05]. <http://www.wisdom.weizmann.ac.il/~oded/pp.html>.
- [4] DU W L, ATALLAH M J. Privacy-preserving cooperative scientific computations [C]// Proceedings of the 2001 14th IEEE Computer Security Foundations Workshop. Washington, DC: IEEE Computer Society, 2001: 273 - 282.
- [5] ATALLAH MIKHAIL J, DU W L. Secure multi-party computational geometry [C]// Proceedings of the 2001 7th International Workshop on Algorithms and Data Structures, LNCS 2125. Berlin: Springer-Verlag, 2001: 165 - 179.
- [6] 刘文, 罗守山, 陈萍. 利用 El Gamal 密码体制解决安全多方多数数据排序问题[J]. 通信学报, 2007, (11): 1 - 5.
- [7] GOLDWASSER S. Mutiparty Computations: past and present [C]// PODC '97: Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM, 1997: 1 - 6.
- [8] GOLDREICH O. Foundations of cryptography: basic applications [M]. London: Cambridge University Press, 2004: 599 - 729.
- [9] 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: 193 - 232.
- [10] 马敏耀. 安全多方计算及其扩展问题的研究[D]. 北京: 北京邮电大学, 2010.
- [11] 廖晓峰, 肖迪, 程勇, 等. 混沌密码学原理及其应用[M]. 北京: 科学出版社, 2009: 2 - 4.
- [12] 邓绍江, 肖迪, 涂风华. 基于 Logistic 映射混沌加密算法的设计与实现[J]. 重庆大学学报, 2004, 27(4): 61 - 63.
- [13] 刘文, 王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报, 2012, 5(5): 871 - 876.
- [14] LIU X Y, ZHOU Y M, ZHENG R S. Sentence similarity based on dynamic time warping [C]// ICSC 2007: Proceedings of the 2007 International Conference on Semantic Computing. Washington, DC: IEEE Computer Society, 2007: 250 - 256.
- [15] HO C F, MURAD M A A, DORAISAMY S C, et al. Measuring sentence similarity from both the perspectives of commonalities and differences [C]// ICTAI '10: Proceeding of the 22nd IEEE International Conference on Tools with Artificial Intelligence. Washington, DC: IEEE Computer Society, 2010: 318 - 322.
- [16] ATALLAH M J, RASKIN V, HEMPELMANN C, et al. Natural language watermarking and tamperproofing [C]// IH '02: Proceedings of the 5th International Workshop on Information Hiding, LNCS 2578. Berlin: Springer-Verlag, 2003: 196 - 212.
- [17] 黄友荣. 自然语言文本水印技术研究[D]. 长沙: 湖南大学, 计算机与通信学院, 2007.
- [18] Online Ebooks [EB/OL]. [2013 - 03 - 15]. <http://ebooks.adelaide.edu.au/>.
- [19] 马光平, 张雅轩, 何路, 等. 针对语法变换信息隐藏的主动攻击算法[C]//第9届全国信息隐藏暨多媒体信息安全学术大会论文集. 成都: [出版者不详], 2010: 152 - 158.

(上接第 3526 页)

- [11] PECINA P. An extensive emipirical study of collocation extraction methods [C] // ACLstudent '05: Proceedings of the ACL Student Research Workshop. Stroudsburg: Association for Computational Linguistics, 2005: 13 - 18.
- [12] LI Y, BANDAR Z, McLEAN D. An approach for measuring semantic similarity between words using multiple information sources [J]. IEEE Transactions on Knowledge and Data Engineering, 2003, 15(1): 871 - 882.
- [13] ACHANANUPARP P, HU X, YANG C C. Addressing the variability of natural language expression in sentence similarity with semantic structure of the sentences [C]// Proceedings of the 13th Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining, LNCS 5476. Berlin: Springer-Verlag, 2009: 548 - 555.
- [14] LIU X Y, ZHOU Y M, ZHENG R S. Sentence similarity based on dynamic time warping [C]// ICSC 2007: Proceedings of the 2007 International Conference on Semantic Computing. Washington,