doi:10.3969/j.issn.1000-436x.2014.02.008

通用可组合公平安全多方计算协议

田有亮[1,2]，彭长根[1]，马建峰[2]，林辉[2]，杨凯[3]

(1. 贵州大学 理学院，贵州 贵阳 550025；2. 西安电子科技大学 计算机学院，陕西 西安 710071；
3. 武警工程大学 电子技术系 中国人民武装警察部队信息安全保密重点实验室，陕西 西安 710086)

摘 要：在通用可组合框架下研究安全多方计算的公平性问题。在 UC 框架下，提出公平安全多方计算的安全模型。在模型中形式化定义了公平安全多方加法计算理想函数 F_{FSMPA} 和公平安全多方乘法计算理想函数 F_{FSMPM}。然后，基于双线性对技术和承诺方案理想函数 F_{COM}，在 F_{COM}-混合模型下分别设计公平加法协议 π_{FSMPA} 和公平乘法协议 π_{FSMPM} 安全实现理想函数 F_{FSMPA} 和 F_{FSMPM}。最后，性能分析表明所提协议的有效性，能更好地满足应用需求。

关键词：UC 框架；安全多方计算；公平性；双线性对；BDH 假设

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)02-0054-09

Universally composable secure multiparty computation protocol with fairness

TIAN You-liang[1,2], PENG Chang-gen[1], MA Jian-feng[2], LIN Hui[2], YANG Kai[3]

(1. College of Science, Guizhou University, Guiyang 550025, China; 2. School of Computer Science and Technology, Xidian University, Xi'an 710071, China; 3. Key Laboratory of Information Security and Secrecy of CAPF, Department of Electronic Technology, Engineering University of CAPF, Xi'an 710086, China)

Abstract: The fair problem of secure multiparty computation protocol was investigated in the universally composable framework. A fair secure multiparty computation model with ideal functionalities was firstly formulated such as a fair secure multiparty addition computation and a fair secure multiparty multiplicative computation. Next a fair addition computation protocol and a fair multiplicative computation protocol based on the bilinear paring and the ideal functionality of a commitment scheme was proposed. The proposed protocols can securely realize their ideal functionalities in the hybrid model respectively. Finally, analysis show that these schemes are effective, and it can be more applicable in special situation.

Key words: UC framework; secure multiparty computation; fairness; bilinear pairing; bilinear Diffie-Hellman assumption

1 引言

安全多方计算协议是诸多密码系统的核心基础协议，一直以来备受关注。目前对安全多方计算协议的研究更多的是考虑安全性和正确性，但在安全多方计算协议中，往往不再考虑可信第三方，参

收稿日期：2012-04-14；**修回日期**：2013-01-15

基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然基金委员会-广东联合基金重点基金资助项目(U1135002)；国家科技部重大专项基金资助项目(2011ZX03005-002)；国家自然科学基金资助项目(61170280, 61272398, 61262073, 61363068)；中国博士后基金资助项目(2013M530705)；贵州省自然科学基金资助项目(20132112)；贵州大学博士基金资助项目(2012024)

Foundation Items: Program for Changjiang Scholars and Innovative Research Team in University(IRT1078)；The Key Program of NSFC-Guangdong Union Foundation (U1135002)；The Major National Science and Technology program (2011ZX03005-002); The National Natural Science Foundation of China (61170280, 61272398, 61262073, 61363068); China Postdoctoral Science Foundation (2013M530705); The Nature Science Foundation of Guizhou Province (20132112); The Doctors Science Foundation of Guizhou University (2012024)

与者自成一个可信中心来联合完成协议功能，在这种情况下其公平性就显得很重要。安全多方计算的公平性是指要么所有的参与者都得到协议的输出结果，要么都没得到协议的输出结果。1982 年 Yao[1]提出安全多方计算时就引入了公平性的思想。然而，Cleve[2]在 1986 年指出只有存在大多数诚实参与者的情况下安全多方计算协议才能实现完全公平性，该结论极大地限制了安全多方计算的公平性的研究。2008 年，Dov Gordon[3]等对某些特殊函数的安全多方计算协议的公平性进行研究，论证即使不存在诚实参与者占大多数的情形下，安全多方计算也可以实现完全公平性，打破了 Cleve 的结论，为公平性的研究扩宽了领域。

密码协议的公平性问题一直是诸多学者研究的重要方面，公平交换是这方面最早研究问题之一。在一个公平交换协议中，要么交换两方都收到交换项目，要么双方都没收到。Cleve[2]证明完美的公平交换是不可能的。Boneh 和 Naor[4]给出了一个公平签约协议的类似下界，其也能达到公平性的宽松定义(relaxed definition of fairness)。更近些，公平交换被在乐观模型下进行研究，Asokan[5]于 1997 年引入这样的乐观模型，在该模型中用一个额外的可信第三方来实现和保证协议的公平性。

Dov Godon[6]等研究者在安全多方计算协议公平性方面的工作，扩展了公平的密码协议的研究领域。Katz[7]提出部分公平性的定义：一个协议实现 ε-partial 公平的函数，如果存在一个理想世界的模仿器的输出与现实世界敌手的输出被区分的概率不超过 ε。Katz 证明同步广播是 ε-partial 公平的完备性本原。Dov Gordon 和 Katz[6]研究两方安全计算的部分公平性，表明在 plain 模型(如无条件安全和通用可组合安全等)下通常其部分公平性是不可能达到的。在有大多数诚实参与者和广播信道的多方计算场景下，能完全公平计算任何函数，即使在无计算性假设的情况下也成立[8~10]。当没有大多数诚实参与者情况下，Cleve 的工作表明在 plain 模型下通用的公平计算是不能够完成的。这里仅概述了和本文相关的参考文献，该领域的更多详情请参阅文献[11]。

通用可组合(UC, universally composable)框架[12]分析密码协议安全性提供了非常强的安全性保障。特别是，一个协议在该框架被证明是安全的，则能保证即使该协议和其他协议并行运行或者该协议作为一个大协议的组件，该协议仍然是安全的。在 UC 框架下理想函数是一个非常重要的安全概念；它用作一个不可攻陷的可信方，并能实现执行协议的具体任务。目前为止，已有许多基本的理想函数被定义，如消息认证理想函数 F_{AUTH}、密钥交换理想函数 F_{KE}、公钥加密理想函数 F_{PKE}、签名理想函数 F_{SIG}、承诺理想函数 F_{COM}、零知识证明理想函数 F_{ZK}、忘传输理想函数 F_{OT}、匿名散列认证理想函数 F_{Cred}[13]、否认认证理想函数 F_{CDA}[14]、可信网络连接(TNC)理想函数 F_{TNC}[15]、一次签名理想函数 F_{OTS}[16]、广播认证理想函数 F_{BAUTH}[16]、基于身份的签名理想函数 F_{IDSC} 和群组通信模型的理想函数 F_{SAGCOM}[17]等，而文献[18]分析比较了现有 UC 安全计算的信任模型，并给出一种公钥基础设施风格的双陷门分离的信任模型。

从所引文献可见，安全多方计算公平协议已在理论上进行研究，其实现方法主要有 2 种：一种是引入第三方作为仲裁者以实现公平性；另一种是采用信息逐步释放的方法。由于后一种方法避免可信第三方的加入，从而具有很好的实际应用背景和价值，是目前的研究热点。本文从一个全新的角度研究公平的安全多方计算协议。首先，在 UC 框架下提出公平安全多方计算模型。然后，在模型的基础上设计通用可组合的公平安全多方计算协议。本文贡献如下。

1) 提出通用可组合的公平安全多方计算模型，并针对公平安全加法协议和乘法协议分别设计了理想函数 F_{FSMPA} 和 F_{FSMPM}。

2) 基于双线性对技术，设计知识承诺方案 π_{BCOM}；证明若 BDH 假设成立，则协议 π_{BCOM} 在混合模型下安全实现承诺方案理想函数 F_{COM}。

3) 在 F_{COM} -混合模型下构造了一个安全实现理想函数 F_{FSMPA} 和 F_{FSMPM} 的协议 π_{FSMPA} 和 π_{FSMPM}。

4) 根据秘密共享方案信息率的定义，定义了安全多方计算协议的信息率；根据该定义分别求出所提协议 π_{FSMPA} 和 π_{FSMPM} 的信息率，并给出进一步改善方法。

5) 本文的方法在 UC 框架下能实现公平的安全两方计算协议，解决 Dov Gordon 和 Katz[6]不能实现两方公平的安全计算结论。

2　准备知识

本节概述双线性对和相关假设[19]、通用可组合

框架及承诺方案的理想函数[12]等基础相识。

2.1 双线相对及相关假设

定义 1 双线性对。设 G_1, G_2 是 2 个相同素数阶为 q 的加法群和乘法群，q 是一大素数。设 P 为 G_1 的任一生成元。aP 记为 a 个 P 相加。假设在群 G_1 和 G_2 上的离散对数问题（DLP）都是困难的。映射 $e: G_1 \times G_1 \to G_2$ 满足如下性质 1)~3)被称为密码学上的双线性映射。

1) 双线性：对 $\forall P,Q \in G_1$ 和 $a,b \in Z_q^*$, $e(aP,bQ) = e(P,Q)^{ab}$；或者对 $\forall P,Q,R \in G_1$，$e(P+Q,R) = e(P,R)e(Q,R)$ 和 $e(P,Q+R) = e(P,Q)e(P,R)$。

2) 非退化性：如果 P 是 G_1 的生成元，则 $e(P,P)$ 是 G_2 的生成元，也即 $e(P,P) \neq 1$。

3) 可计算性：对 $\forall P,Q \in G_1$，都存在有效的算法来计算 $e(P,Q)$。

Diffie-Hellman 问题定义如下：考虑加法群 $G = <g>$，G 的 2 个元素 $g_1 := a \cdot g$ 和 $g_2 := b \cdot g$，并且知道生成元 g，但不知道 a 和 b。问题是：计算 $g_3 = (ab) \cdot g$。有如下相关定义。

定义 2 DLP、CDHP、DDHP 问题。设 G 是有限循环群，g 是 G 的生成元。

1) 离散对数问题(DLP)：给定 $(g, a \cdot g)$，对任意的 $a \in Z_{|G|}^*$，求 a。

2) 计算性 Diffie-Hellman 问题(CDHP)：给定 $(g, a \cdot g, b \cdot g)$，对任意的 $a,b \in Z_{|G|}^*$，计算 $(ab) \cdot g$。

3) 判定性 Diffie-Hellman 问题(DDHP)：给定 $(g, a \cdot g, b \cdot g)$，对任意的 $a,b \in Z_{|G|}^*$，判断 $(ab) \cdot g = c \cdot g$ 是否成立。

在群 G 上，DDHP 是易解的，即 DDHP 在多项式时间内能够被解决；而 CDHP 是难解的，即没有任何可能的算法可以解决 CDHP。此时称群 G 为 GDH 群。

考虑 G_1 是素数阶的加法群，其阶为 q，并且 P 是它的生成元。设 q 阶乘法群 G_2 且它们之间存在双线性映射 $e: G_1 \times G_1 \to G_2$，能被有效计算。

定义 3 BDHP。双线性 Diffie-Hellman 问题(BDHP) 描述如下：在 (G_1, G_2, e) 中，给定 (P, aP, bP, cP)，对任意的 $a,b,c \in_R Z_q^*$，计算 $e(P,P)^{abc} \in G_2$。

BDH 假设可描述为：在求解 BDH 问题上，没有概率多项式时间算法有不可忽略的优势。

2.2 通用可组合框架

UC 框架首先定义了现实环境。现实环境描述协议的真实运行情况，其中所有参与者在与现实敌手 A 存在的环境下运行真实协议。其次定义理想环境来描述密码协议的理想运行。在理想环境下，存在虚拟参与者、理想敌手 S 和理想函数 F。参与者间以及敌手 S 与参与者不直接通信；所有参与者和敌手均与理想函数 F 交互。理想函数本质上是一个不可攻陷的可信角色，用来完成协议所需的理想运行和功能。在 UC 框架中，环境 Z 模拟协议的整个外部环境(包括其他并行的协议、攻击者等)，Z 可以与所有参与者及敌手 A 和 S 直接通信，Z 不允许直接访问理想函数 F。

定义 4 UC 仿真。协议 π 能够 UC 仿真理想函数 F 当且仅当对任意的现实敌手 A，存在一个理想敌手 S，使得任意的环境 Z，至多以可忽略的概率区分：与真实环境下的敌手 A 和协议 π 交互还是与理想环境下的敌手 S 和理想函数 F 交互。如果协议 π 能够 UC 仿真理想函数 F，就称协议 π 在 UC 框架下安全实现了理想函数 F，也称协议 π 是 UC 安全的。

定理 1 组合定理[12]。如果协议 ρ 安全实现理想函数 F，π 是 F-混合模型下的协议[12]，那么协议 $\pi^{\rho/F}$ (用协议 ρ 替换协议 π 中的理想函数 F 所得的组合协议)UC 仿真 F-混合模型下的协议 π。特别地，如果协议 π 在 F-混合模型下安全实现理想函数 ς，那么协议 $\pi^{\rho/F}$ 也安全实现理想函数 ς。

2.3 承诺方案的理想函数

下面介绍承诺方案的理想函数 F_{COM}，详情见文献[12]。

承诺方案包括 2 个阶段：承诺阶段和公开阶段。在承诺阶段，协议的一方将自己的承诺为一特定的值并保持这个值的保密性；在公开阶段，承诺值“被打开”，并产生一个在承诺阶段就被确定的值。其理想函数如图 1 所示。

理想函数 F_{COM}

1) 当从参与者 C 收到输入(Commit，*sid*，x)，验证 *sid*=(C, R, *sid*')对某些 R，否则忽略该输入。接下来，记录 x 并产生一个公开延迟输出(Receipt, *sid*)给 R。一旦 x 被记录，则忽略任何随后的承诺输入。

2) 当从参与者 C 收到输入(Open, *sid*)，处理如下：如果存在一个这样的记录值 x，则产生一个公开延迟输出(Open, *sid*, x)给 R。否则，什么都不做。

3) 当从敌手收到消息(Corrupt-committer, *sid*)，转发 x 给敌手。进一步，如果当前敌手提供另一个值 x' 并承诺阶段 Receipt 输出还没有输出，则改变该记录值为 x'

图 1 承诺方案理想函数

3 理想函数

首先，简单介绍公平安全多方计算协议及安全需求。

设有 n 位互不可信的参与者 $P_1,\cdots,P_n$ 想共同计算在多项式时间可计算的函数 $f(x_1,\cdots,x_n)=(y_1,\cdots,y_n)$，其中，$(x_1,\cdots,x_n)$ 是输入变量，$(y_1,\cdots,y_n)$ 是输出值。若 π 是计算该函数的一个公平安全多方计算协议，则满足如下内容。

1) 正确性：π 能使这 n 位参与者正确计算函数 f。

2) 保密性：每位参与者的输入信息是保密的，即每位参与者知道他人的信息不会比他从自己的结果中推导出来的信息多。

3) 公平性：协议 π 结束后，要么每一位参与者都得到正确的输出值，要么都没有得到合法的输出值。

本文设计的公平安全计算协议是能够通用的。根据上述安全需求和公平需求的概述，分别设计公平安全加法协议和乘法协议的理想函数 F_{FSMPA} 和 F_{FSMPM}。

在图 2 中，提出公平安全多方加法协议的理想函数 F_{FSMPA}。在理想函数中，其 SID 描述为一个参与者 $P=P_1,\cdots,P_n$ 的有序集，并由该有序集中第一个向理想函数提供输入的参与者决定。该理想函数能保证协议的公平性：当有一方收到协议的输出，则所有的参与者都能收到协议的输出结果。

理想函数 F_{FSMPA}

给定函数 $f: x_1+\cdots+x_n=y_1+\cdots+y_n$，$x_i,y_i\in Z_q^*\cup\{\perp\}$；有序集 $P=P_1,\cdots,P_n$，其身份也记为 $P_1,\cdots,P_n$；初始变量 $x_1\cdots,x_n;y_1,\cdots,y_n$ 的默认值均为 $\perp$。F_{FSMPA} 处理如下：

1) 当从参与者 $P_i\in P$ 收到输入(Input, *sid*, *v*)，如果 *sid*=(*P*, *sid*')，则：

① 置 $x_i=v$；

② 发送(Input, *sid*, P_i, |*v*|)给敌手 *S*；

③ 发送(Input.Receipt, *sid*)给 P_i。

2) 当从参与者 $P_i\in P$ 收到(Compute, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 当收到所有参与者的输入值且给每位参与者都发送(Input. Receipt, *sid*) 后，随机选取 $r_1,\cdots,r_n\in_R Z_q^*$，使得 $x_1+\cdots+x_n=r_1+\cdots+r_n$ 且 $x_i\neq r_i$ ($i=1,2,\cdots,n$)；

② 置 $y_i=r_i$，对于 $i=1,2,\cdots,n$。

3) 当从参与者 $P_i\in P$ 收到(Fair-output, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 如果当前存在标识为 Corrupted 的参与者，则给 Corrupted 的参与者发送 $\perp$，而其余参与者发送相应的 y_i；

② 否则，给每位参与者 P_i 发送 y_i。

4) 当从敌手 *S* 收到(Corrupt-Input, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 记录 P_i 是 Corrupted；

② 转发 x_i 给敌手 *S*；

③ 如果当前敌手 *S* 提供另一个值 *v*'，且输出阶段的 y_i 没有写在 P_i 的带子上，则置 $x_i=v'$。

5) 当从敌手 *S* 收到(Corrupt-Output, sid, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 记录 P_i 是 Corrupted；

② 转发 y_i 给敌手 *S*；

③ 如果当前敌手 *S* 提供另一个值 *v*'，且输出阶段的 y_i 没有写在 P_i 的带子上，则置 $x_i=v'$

图 2　公平安全加法计算理想函数

在图 2 中，提出公平安全多方乘法协议的理想函数 F_{FSMPM}。该理想函数类似于加法协议的理想函数，详情如图 3 所示。

理想函数 F_{FSMPM}

给定函数 $f: x_1\times\cdots\times x_n=y_1\times\cdots\times y_n$，$x_i,y_i\in Z_q^*\cup\{\perp\}$；有序集 $P=P_1,\cdots,P_n$，其身份也记为 $P_1,\cdots,P_n$；初始变量 $x_1\cdots,x_n;y_1,\cdots,y_n$ 的默认值均为 $\perp$。F_{FSMPM} 处理如下：

1) 当从参与者 $P_i\in P$ 收到输入(Input, *sid*, *v*)，如果 *sid*=(*P*, *sid*')，则：

①置 $x_i=v$；

②发送(Input, *sid*, P_i, |*v*|)给敌手 *S*；

③发送(Input.Receipt, *sid*)给 P_i。

2) 当从参与者 $P_i\in P$ 收到(Compute, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

①当收到所有参与者的输入值且给每位参与者都发送(Input.Receipt, sid)后，随机选取 $r_1,\cdots,r_n\in_R Z_q^*$，使得 $x_1\times\cdots\times x_n=r_1\times\cdots\times r_n$ 且 $x_i\neq r_i$ ($i=1,2,\cdots,n$)；

② 置 $y_i=r_i$，对于 $i=1,2,\cdots,n$。

3) 当从参与者 $P_i\in P$ 收到(Fair-output, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 如果当前存在标识为 Corrupted 的参与者，则给 Corrupted 的参与者发送 $\perp$，而其余参与者发送相应的 y_i；

② 否则，给每位参与者 P_i 发送 y_i；

4) 当从敌手 *S* 收到(Corrupt-Input, *sid*, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 记录 P_i 是 Corrupted；

② 转发 x_i 给敌手 *S*；

③ 如果当前敌手 *S* 提供另一个值 *v*'，且输出阶段的 y_i 没有写在 P_i 的带子上，则置 $x_i=v'$

5) 当从敌手 *S* 收到(Corrupt-Output, sid, P_i)，如果 *sid*=(*P*, *sid*')，则：

① 记录 P_i 是 Corrupted；

② 转发 y_i 给敌手 *S*；

③ 如果当前敌手 *S* 提供另一个值 *v*'，且输出阶段的 y_i 没有写在 P_i 的带子上，则置 $x_i=v'$

图 3　公平安全乘法计算理想函数

4　公平安全计算协议

本节基于双线性对技术，根据安全多方计算协议的理想函数 F_{FSMPA} 和 F_{FSMPM} 设计其公平的加法协议和乘法协议。

4.1　协议 π_{FSMPA}

假定参与者集合 $P=\{P_1,\cdots,P_n\}$ 想公平安全地计算函数 $f(x_1,\cdots,x_n)=x_1+\cdots+x_n$。设 G_1 是素数阶的加法群（这里为椭圆曲线群），其阶为 q；P 和 Q 是它的 2 个生成元，且任何人都不知道 $n\in Z_q^*$，满足 $Q=nP$；设 q 阶乘法群 G_2 且它们之间存在双线性映射 $e:G_1\times G_1\to G_2$，能被有效计算；G_1 和 G_2 上的离

散对数（G_1 上是椭圆曲线离散对数）都是难解的。本文的公平安全加法计算协议分为 4 个阶段：准备阶段、输入阶段、计算阶段和公平输出阶段，如图 4 所示。

协议 π_{FSMPA}

输入：参与者 $P_i \in P$ 拥有输入值 $x_i \in Z_q$。k 是安全参数，$m = poly(k)$。

协议分为以下几个阶段。

1) 准备阶段：对任意的 $P_i \in P$，则：

①P_i 随机选取 $r_i \in_R Z_q^*$，计算 $C_i = e(x_i P + r_i Q, P)$

②P_i 随机选取 $x_{i1}, \cdots, x_{in}; r_{i1}, \cdots, r_{in} \in_R Z_q^*$，使得 $x_i = x_{i1} + \cdots + x_{in}$，$r_i = r_{i1} + \cdots + r_{in}$；计算 $C_{ij0} = e(x_{ij} P + r_{ij} Q, P)$

③P_i 随机选取 $t_{i1}, \cdots, t_{in} \in_R \{1, 2, \cdots, m\}$，设 $t_i = \max\{t_{i1}, \cdots, t_{in}\}$

④P_i 随机选取 $\alpha_{i1}, \cdots, \alpha_{it_i - 1}; \beta_{i1}, \cdots, \beta_{it_i - 1} \in Z_q^*$，计算 $C_{it} = e(\alpha_{it} P + \beta_{it} Q, P)$，$t = 1, \cdots, t_i - 1$。

⑤设 $f_{ij}(x) = x_{ij} + \alpha_{i1} x + \cdots + \alpha_{it_{ij}-1} x^{t_{ij}-1}$ 和 $g_{ij}(x) = r_{ij} + \beta_{i1} x + \cdots + \beta_{it_{ij}-1} x^{t_{ij}-1}$，计算 $x_{ijl} = f_{ij}(l)$ 和 $r_{ijl} = g_{ij}(l)$，对于 $i = 1, \cdots, n$，$j = 1, \cdots, n$，$l = 1, \cdots, m$。

2) 输入阶段。当收到(Input, *sid*, *v*)，其中 *sid*=(P, *sid'*)：

①参与者 $P_i \in P$ 公布 C_i，C_{ij0} 和 C_{it} 对于 $j = 1, \cdots, n$，$t = 1, \cdots, t_i - 1$。

②对于 $l = 1, 2, \cdots, m$ 处理如下：

P_i 发送(x_{ijl}, r_{ijl})给 P_j($P_j \in P_{-i} = P \backslash \{P_i\}$)，对于 $j = 1, \cdots, n$。

P_j 收到 P_i($P_i \in P_{-j}$)发送来的(x_{ijl}, r_{ijl})，验证：如果存在 $t_i^* \in \{1, \cdots, t_i\}$，使得 $e(x_{ijl} P + r_{ijl} Q, P) = C_{ij0} (\prod_{l=1}^{t_i^*} C_{it}^{l^t})$，则协议继续，否则停机。

在某 l 轮，对所有的 $i \in \{1, \cdots, j-1, j+1, \cdots, n\}$，$P_j$ 收到(x_{ij1}, r_{ij1}),…,(x_{ijl}, r_{ijl})后，利用 Lagrange 插值函数来计算出 x_{ij} 和 r_{ij}。如果 x_{ij} 和 r_{ij} 满足 $C_{ij0} = e(x_{ij} P + r_{ij} Q, P)$，则转入计算阶段。

③如果协议运行了 m 轮，则转入计算阶段。

3) 计算阶段。当收到(Compute, *sid*, P_j)，其中，*sid*=(P, *sid'*)：

①设输入阶段协议在 $l^* \in \{1, \cdots, m\}$ 轮结束，P_j 收到(x_{ij1}, r_{ij1}),…,(x_{ijl^*}, r_{ijl^*})对所有的 $i \in \{1, \cdots, j-1, j+1, \cdots, n\}$，利用 Lagrange 插值函数来计算出($x_{1j}$, r_{1j}),…,(x_{i-1j}, r_{i+1j}),(x_{nj}, r_{nj}),…,(x_{nj}, r_{nj})。

②P_j 计算 $x_j' = \sum_{i=1}^{n} x_{ij}$ 和 $r_j' = \sum_{i=1}^{n} r_{ij}$，置 $y_j = (x_j', r_j')$ 对于 $j = 1, \cdots, n$。

4) 输出阶段。当收到(Fair-output, *sid*, P_i)，其中，*sid*=(P, *sid'*)：参与者 $P_i \in P$ 输出 y_j

图 4 公平安全加法计算协议

4.2 协议 π_{FSMPM}

假定参与者集合 $P = \{P_1, \cdots, P_n\}$ 想公平安全地计算函数 $f(x_1, \cdots, x_n) = x_1 \times \cdots \times x_n$。其余假设同加法协议假设。本文的公平安全乘法计算协议分为 4 个阶段：准备阶段、输入阶段、计算阶段和公平输出阶段，如图 5 所示。

协议 π_{FSMPM}

输入：参与者 $P_i \in P$ 拥有输入值 $x_i \in Z_q$。k 是安全参数，$m = poly(k)$。

协议分为以下几个阶段。

1) 准备阶段。对任意的 $P_i \in P$，则：

①P_i 随机选取 $r_i \in_R Z_q^*$，计算 $C_i = e(x_i P + r_i Q, P)$。

②P_i 随机选取 $x_{i1}, \cdots, x_{in}; r_{i1}, \cdots, r_{in} \in_R Z_q^*$，使得 $x_i = x_{i1} \times \cdots \times x_{in}$，$r_i = r_{i1} \times \cdots \times r_{in}$；计算 $C_{ij0} = e(x_{ij} P + r_{ij} Q, P)$。

③P_i 随机选取 $t_{i1}, \cdots, t_{in} \in_R \{1, 2, \cdots, m\}$，设 $t_i = \max\{t_{i1}, \cdots, t_{in}\}$。

④P_i 随机选取 $\alpha_{i1}, \cdots, \alpha_{it_i - 1}; \beta_{i1}, \cdots, \beta_{it_i - 1} \in Z_q^*$，计算 $C_{it} = e(\alpha_{it} P + \beta_{it} Q, P)$，$t = 1, \cdots, t_i - 1$。

⑤设 $f_{ij}(x) = x_{ij} + \alpha_{i1} x + \cdots + \alpha_{it_{ij}-1} x^{t_{ij}-1}$ 和 $g_{ij}(x) = r_{ij} + \beta_{i1} x + \cdots + \beta_{it_{ij}-1} x^{t_{ij}-1}$，计算 $x_{ijl} = f_{ij}(l)$ 和 $r_{ijl} = g_{ij}(l)$，对于 $i = 1, \cdots, n$，$j = 1, \cdots, n$，$l = 1, \cdots, m$。

2) 输入阶段。当收到(Input, *sid*, *v*)，其中，*sid*=(P, *sid'*)。

①参与者 $P_i \in P$ 公布 C_i，C_{ij0} 和 C_{it} 对于 $j = 1, \cdots, n$，$t = 1, \cdots, t_i - 1$。

②对于 $l = 1, 2, \cdots, m$ 处理如下：

P_i 发送(x_{ijl}, r_{ijl})给 P_j($P_j \in P_{-i} = P \backslash \{P_i\}$)，对于 $j = 1, \cdots, n$。

P_j 收到 P_i($P_i \in P_{-j}$)发送来的(x_{ijl}, r_{ijl})，验证：如果存在 $t_i^* \in \{1, \cdots, t_i\}$，使得 $e(x_{ijl} P + r_{ijl} Q, P) = C_{ij0} (\prod_{l=1}^{t_i^*} C_{it}^{l^t})$，则协议继续，否则停机。

在某 l 轮，对所有的 $i \in \{1, \cdots, j-1, j+1, \cdots, n\}$，$P_j$ 收到(x_{ij1}, r_{ij1}),…,(x_{ijl}, r_{ijl})后，利用 Lagrange 插值函数来计算出 x_{ij} 和 r_{ij}。如果 x_{ij} 和 r_{ij} 满足 $C_{ij0} = e(x_{ij} P + r_{ij} Q, P)$，则转入计算阶段。

③如果协议运行了 m 轮，则转入计算阶段。

3) 计算阶段。当收到(Compute, *sid*, P_j)，其中，*sid*=(P, *sid'*)：

①设输入阶段协议在 $l^* \in \{1, \cdots, m\}$ 轮结束，P_j 收到(x_{ij1}, r_{ij1}),…,(x_{ijl^*}, r_{ijl^*})对所有的 $i \in \{1, \cdots, j-1, j+1, \cdots, n\}$，利用 Lagrange 插值函数来计算出($x_{1j}$, r_{1j}),…,(x_{i-1j}, r_{i+1j}),(x_{nj}, r_{nj}),…,(x_{nj}, r_{nj})。

②P_j 计算 $x_j' = \prod_{i=1}^{n} x_{ij}$ 和 $r_j' = \prod_{i=1}^{n} r_{ij}$，置 $y_j = (x_j', r_j')$，$j = 1, \cdots, n$。

4) 输出阶段。当收到(Fair-output, *sid*, P_i)，其中 *sid*=(*P*, *sid'*)：参与者 $P_i \in P$ 输出 y_j

图 5 公平安全乘法计算协议

5 安全性和公平性分析

首先，证明本文所提公平安全多方加法和乘法计算在协议中使用的承诺协议是安全的，记该承诺协议为 π_{BCOM}。简述 π_{BCOM} 如下：当收到(Commit, *sid*, *x*)，则参与者 C 随机选取 $r \in Z_q^*$，计算承诺 $C' = e(xP + rQ, P)$；当收到(Open, *sid*)，则 C 输出(*x*, *r*)给参与者 R。

引理 1 若 BDH 假设成立，则协议 π_{BCOM} 在混合模型下安全实现理想函数 F_{COM}。

证明 设 A 是现实环境下的敌手。构造一个理想环境下的敌手 S，使得对于任意的环境 Z 只能以可忽略的概率区分现实环境(协议 π_{BCOM} 及敌手 A 交互的环境，记为 *REAL*)与理想环境(理想函数 F_{COM}

及敌手 S 交互的环境，记为 *IDEAL*)。

下面构造理想环境下的敌手 S：任何来自环境 Z 的输入都转发给 A，A 的任何输出都被看作是 S 的输出。敌手 S 的具体操作如下。

1) 仿真承诺阶段

当从 F_{COM} 收到(Commit, *sid*, *x*)，为 A 仿真从参与者 C 收到的消息(Commit, *sid*, *x*)；当从 F_{COM} 收到(Receipt, *sid*)，为 A 仿真从参与者 C 收到的承诺消息 C'。

2) 仿真攻陷

当现实环境下的敌手 A 攻陷参与者 C，则理想环境下的敌手 S 也攻陷参与者 C 并将所有内部状态转发给 A(但这里不存在任何秘密的内部状态)。

3) *IDEAL* 和 *REAL* 的不可区分

定义事件 Event：对于消息(Corrupt-committer, *sid*)，当接收者 R 已经从 F_{COM} 收到(Receipt, *sid*)，但 F_{COM} 将承诺值 x 替换为 x'。根据协议 π_{BCOM}，若 BDH 假设成立，则事件 Event 是不可能发生的。原因如下。

假设 BDH 假设成立，但事件 Event 发生。那么存在算法 B：将任何 G_1 中的随机元素 Q_1、Q_2、$Q_3 \in_R G_1$ 作为算法 B 的输入时，算法 B 能以成功率 ε 计算出 x，满足：$C= e(xP+rQ, P) = e(Q_1 + Q_2, Q_3)$。记 $xP = \alpha P$，$r_iP = \beta P$，$\alpha, \beta \in Z_q^*$ 和 $Q_1 = \alpha_1 P$，$Q_2 = \alpha_2 P$，$Q_3 = \alpha_3 P$，$\alpha_1, \alpha_2, \alpha_3, \in_R Z_q^*$，则算法 B 能以成功率 ε 计算出 F_i 满足：$e((\alpha_1 + \alpha_2)P, \alpha_3 P) = e((\alpha + \beta)P, P)$。

由此可得 $e(P,P)^{(\alpha_1+\alpha_2)\alpha_3} = e(P,P)^{(\alpha+\beta)} \Rightarrow e(P, P)^{(\alpha_1+\alpha_2)\alpha_3(\alpha+\beta)^{-1}} = e(P,P)$。

令 $a = (\alpha_1 + \alpha_2)$，$b = \alpha_3$，$c = (\alpha + \beta)^{-1}$，这就表明算法 B 对于 G_1 中给定的 (P, aP, bP, cP)，算法 B 能以成功率 ε 计算出 $e(P,P)^{abc}$。这与假设矛盾！因此，若假设 BDH 假设成立，则事件 Event 不可能发生。

4) 仿真公开阶段

当从 F_{COM} 收到(Open, *sid*)，为 A 仿真从参与者 C 收到的消息(Open, *sid*)；当从 F_{COM} 收到(Open, *sid*, *x*)，为 A 仿真从参与者 C 收到的承诺值(*x*, *r*)。

因事件 Event 不可能发生，所以事件 Event 在 *IDEAL* 和 *REAL* 下是不可区分的。从而协议 π_{BCOM} 在混合模型下安全实现了理想函数 F_{COM}。

定理 2　若 BDH 假设成立，则协议 π_{FSMPA} 在 F_{COM}-混合模型下安全实现理想函数 F_{FSMPA}。

证明　设 A 是现实环境下的敌手。构造一个理想环境下的敌手 S，使得对于任意的环境 Z 只能以可忽略的概率区分：协议 π_{FSMPA} 及敌手 A 交互的现实环境(记为 *REAL*)与理想函数 F_{FSMPA} 及敌手 S 交互的理想环境(记为 *IDEAL*)。

下面构造理想环境下的敌手 S：任何来自环境 Z 的输入都转发给 A，A 的任何输出都被看作是 S 的输出。敌手 S 的具体操作如下。

1) 仿真输入阶段

当从 F_{FSMPA} 收到(Input, *sid*, *v*)，为 A 仿真从参与者 P_i 收到的消息(Input, *sid*, *v*)；当从 F_{FSMPA} 收到(Input, *sid*, P_i, $|v|$)，为 A 仿真从参与者 P_i 收到的公开消息 C_i，C_{ij0} 和 C_{it} 对于 $j = 1, \cdots, n$，$t = 1, \cdots, t_i - 1$；当从 F_{FSMPA} 收到(Input.Receipt, *sid*)，为 A 仿真从参与者 P_i 收到的消息(x_{ij}，r_{ij})。

2) 仿真计算阶段

当从 F_{FSMPA} 收到(Compute, *sid*, P_i)，为 A 仿真从参与者 P_i 收到的消息(Compute, *sid*, P_i)。

3) 仿真公平输出阶段

当从 F_{FSMPA} 收到(Fair-output, *sid*, P_i)，为 A 仿真从参与者 P_i 收到的消息(Fair-output, *sid*, P_i)。

4) 仿真攻陷

在现实环境下，敌手 A 攻陷某一参与方 P_i，则在理想环境下 S 也通过发生(Corrupt-Input, *sid*, P_i) 或 (Corrupt-Output, *sid*, P_i)给 F_{FSMPA} 攻陷该参与方，并将其相关内部状态转发给 A(但这里不存在任何秘密的内部状态)。

5) *IDEAL* 和 *REAL* 的不可区分

根据敌手 S，定义 3 个事件，并证明任何一个事件发生 *IDEAL* 和 *REAL* 都是不可区分。

Event 1：对于消息(Corrupt-Input, *sid*, P_i)，当接收方收到协议的公平输出后，被攻陷的参与者 P_i 变更他的输入值 x_i。根据协议 π_{FSMPA}，若 BDH 假设成立，由引理 1 知道该事件只能以不可忽略的概率发生，从而 *IDEAL* 和 *REAL* 在这种情况下不可区分。

Event 2：对于消息(Corrupt-Output, *sid*, P_i)，当接收方收到协议的公平输出后，被攻陷的参与者 P_i 变更他的输入值 x_i。根据协议 π_{FSMPA}，若 BDH 假设成立，同样由引理 1 知，*IDEAL* 和 *REAL* 在这种情况下不可区分。

Event 3：对于消息(Input, *sid*, *v*)，在某一轮 l' 参

与者 P_i 给某位参与者 P_j 提供不合法的$(x'_{ijl'}, r'_{ijl'})$而协议继续。根据协议 π_{FSMPA}，在每轮 P_j 收到的$(x'_{ijl'}, r'_{ijl'})$都要通过下式验证其合法性

$$e(x_{ijl}P + r_{ijl}Q, P) = C_{ij0}\left(\prod_{t=1}^{t_i^*} C_{it}^{l^t}\right)$$

由引理 1 知，不合法的$(x'_{ijl'}, r'_{ijl'})$就不能通过验证，因此在这种情况下 *DEAL* 和 *REAL* 不可区分。

Event 4：对于消息(Input, *sid*, *v*)，存在参与者 P_i 在 t_i 轮前收到所有其他参与者发送的信息后退出分发阶段。根据协议 π_{FSMPA}，要求

$$t_i \geqslant \max\{t_j \mid (j \neq i) \wedge (j \in \{1, \cdots, m\})\}$$

而 $t_i = \max\{t_{i1}, \cdots, t_{in}\}$；再由 $t_{i1}, \cdots, t_{in} \in_R \{1, 2, \cdots, m\}$，则使得 $t_i \geqslant \max\{t_j \mid (j \neq i) \wedge (j \in \{1, \cdots, m\})\}$ 的概率服从几何分布，其数学期望 $1/m = 1/poly(k)$ 为忽略的函数。因此，*IDEAL* 和 *REAL* 在这种情况下不可区分。

Event 5：对于消息(Fair-output, *sid*, P_i)，存在某位参与者 P_i 收到 $\perp$ 而其他参与者 $P_j \in P_{-i}$ 收到相应合法的 y_j。根据协议 π_{FSMPA}，通过分发阶段和计算阶段后，要么每位参与者 P_i 都得到合法的输出 y_i 或不合法的输出 $y_i(=\perp)$；若事件 Event 5 发生，则事件 Event 3 或 Event 4 之一发生。然而，上述分析表明 Event 3 和 Event 4 都只能以可忽略的概率发生。因此，*IDEAL* 和 *REAL* 在这种情况下不可区分。

综上所述，若 BDH 假设成立，则协议 π_{FSMPA} 在 F_{COM}-混合模型下安全实现理想函数 F_{FSMPA}。

定理 3 若 BDH 假设成立，则协议 π_{FSMPM} 在 F_{COM}-混合模型下安全实现理想函数 F_{FSMPM}。

证明 该定理的证明类似于定理 2 的证明，由于篇幅所限，故省略。

6 性能分析

由于公平安全计算协议的具体实现方案较为少见，而所引文献主要从理论方面研究公平安全计算协议，所以这类协议性能无法从定量方面和本文的协议进行对比。本节仅从本文所提协议的计算开销、存储开销、通信开销及信息率方面进行协议的性能分析，并以加法协议 π_{FSMPA} 为例，对乘法协议可以进行类似分析。

6.1 计算量

在协议 π_{FSMPA} 的各个阶段，有限域 Z_q 上的运算可以忽略不计。在准备阶段，参与者 P_i 需进行 $(n + t_i + 1)$ 次对运算(n 是参与者数目、t_i 是参与者 P_i 选取的门限值中最大者)和 $2(n + t_i + 1)$ 次群 G_1 上的点乘运算。在输入阶段，为实现参与者 P_i 收到信息的验证，需进行 2 次群 G_1 上的点乘运算和 $t_i^* \leqslant t_i$ 次群 G_2 上的乘法运算。在计算阶段和输出阶段都无需群 G_1 和 G_2 上的运算。可见，协议 π_{FSMPA} 计算开销主要集中在准备阶段和输入阶段，但这些计算量都与参与者数目成线性关系。更为重要的是，大部分计算开销集中在准备阶段，而这阶段的计算量可以作预处理，这样可以较大地提高协议效率。

6.2 存储量

协议 π_{FSMPA} 中 P_i 的存储开销主要体现在自己秘密信息的存储开销、公开信息的存储开销及在分发阶段每轮所收到信息的存储开销。P_i 秘密信息的存储开销为

$$n(|x_{ij}| + |r_{ij}|) + t_i(|\alpha_{ij}| + |\beta_{ij}|) = 2(n + t_i)q$$

公开信息存储量为

$$n|C_i| + n^2|C_{ij0}| + n(t_i - 1)|C_{it}| + |P| + |Q|$$

$$= (n^2 + t_i n + 4)q$$

分发阶段(最多交互 m 轮)每轮的存储开销为 $(n-1)(|x_{ijl}| + |r_{ijl}|) = (n-1)q$，所以参与者 P_i 的总存储量为

$$2(n + t_i)q + (n^2 + t_i n + 4)q + m(n-1)q$$

$$= [n^2 + (m + t_i + 2)n + (2t_i - m + 4)]q$$

6.3 通信量

协议 π_{FSMPA} 的通信量主要体现在输入阶段，包括 2 部分：公布公开信息的通信开销和协议输入阶段每轮的通信开销。其他阶段都不需要参与者间的交互，所以这些阶段无通信开销。公布公开信息参与者 P_i 可采用一轮广播通信，所以其通信量为 $(n^2 + t_i n)q$；每一轮参与者 P_i 需要 $(n-1)$ 次点对点通信，所以其通信量为 $(n-1)q$。由于在分发阶段最多通信 m 轮，最少通信 1 轮，故平均通信轮数为 $\lceil (m+1)/2 \rceil$。从而得到参与者 P_i 的总通信量为 $[n^2 + (\lceil (m+1)/2 + t_i \rceil)n + \lceil (m+1)/2 + t_i \rceil]q$。

6.4 信息率

信息率是协议效率的重要体现。许多研究者研究秘密共享方案的信息率，对安全多方计算协议的信息率涉及较少，甚至在安全多方协议中未见其信息率的定义。秘密共享方案的信息率定义如下：

$$IR_{SS}=\frac{\text{共享秘密的长度}}{\text{秘密份额的长度}}$$

下面根据秘密共享方案的信息率的定义来定义安全多方计算协议的信息率。

设 $f(x_1,\cdots,x_n)$ 为安全计算的函数，$x_1,\cdots,x_n$ 分别是参与者 $P_1,\cdots,P_n$ 的秘密输入；$f_1(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n)$ 是安全计算协议计算函数 $f(x_1,\cdots,x_n)$ 的输出。则其信息率定义如下：

$$IR_{SMPC}=\frac{|f(x_1,\cdots,x_n)|}{|f_i(x_1,\cdots,x_n)|}$$

根据该定义，协议 π_{FSMPA} 的信息率为：

$$IR_{\pi_{\mathrm{SMPA}}}=\frac{|f(x_1,\cdots,x_n)|}{|f_i(x_1,\cdots,x_n)|}=\frac{|x_1+\cdots+x_n|}{|(x_j^{'},r_j^{'})|}=\frac{q}{2q}=\frac{1}{2}$$

同理可得协议 π_{FSMPM} 的信息率为：$IR_{\pi_{\mathrm{SMPM}}}=\frac{1}{2}$。

可见，本文方案的信息率相对较低，是因协议中使用较高安全级别的承诺方案所致。若要提高协议的信息率，可以通过减弱承诺方案的安全性质来实现。比如用 $C=e(xP,P)$ 对 x 进行承诺，则此时公平安全多方计算协议的信息率改善为 1。

7 结束语

本文首先提出通用可组合安全的公平安全多方计算模型，其中包括理想函数 F_{FSMPA} 和 F_{FSMPM}。其次，根据这些模型设计公平安全加法协议 π_{FSMPA} 和乘法协议 π_{FSMPM}。随后，证明协议 π_{FSMPA} 和 π_{FSMPM} 在混合模型下分别安全实现理想函数 F_{FSMPA} 和 F_{FSMPM}；同时也证明协议 π_{FSMPA} 和 π_{FSMPM} 中所使用的承诺方案 π_{BCOM} 在混合模型下安全实现其理想函数。最后，通过对协议的计算开销、存储开销、通信开销及信息率的分析说明协议的有效性。本文提出的公平安全多方计算协议是通用的，包括公平安全地实现加法和乘法运算。因此，本文的工作也表明所提的方法能公平安全地实现任何函数的计算。

参考文献：

[1] YAO A. Protocols for secure computations[A]. Proc 23rd IEEE Symp On the Foundation of Computer Science, IEEE[C]. 1982. 160-164.

[2] CLEVE R. Limits on the security of coin flips when half the processors are faulty[A]. 18th STOC[C]. 1986. 364-369.

[3] DOV GORDON S, HAZAY C, KATZ J. Complete fairness in secure two-party computation[A]. STOC'08[C]. 2008.17-26.

[4] BONEH D, NAOR M. Timed commitments[A]. Crypto 2000[C]. 2000. 236-254.

[5] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchange[A]. CCS[C]. ACM, 1997.7-17.

[6] KATZ J. On achieving the "best of both worlds" in secure multiparty computation[A]. STOC[C]. ACM, 2007.11-20.

[7] DOV GORDON S, KATZ J. Partial fairness in secure two-party computation[A]. EUROCRYPT 2010[C]. Springer-Verlag, 2010.157-176.

[8] BENOR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for noncryptographic fault-tolerant distributed computation (extended abstract)[A]. STOC1988[C]. ACM. 1988.1-10.

[9] CHAUM D, CCREPEAU C, DAMGARD I. Multiparty unconditionally secure protocols (extended abstract)[A]. STOC1988[C]. ACM, 1988. 11-19.

[10] RABIN T, BENNOR M. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract)[A]. STOC1989[C]. ACM, 1989.73-85.

[11] DOV GORDON S, ISHAI Y, MORAN T, OSTROVSKY R, *et al*. On complete primitives for fairness[A]. TCC2010 IEEE[C]. 2010. 91-108.

[12] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols. a revised version (2005) is available at IACR eprint archive[EB/OL]. http://eprint.iacr.org/2000/067.

[13] ZHANG F, MA J F, MOON S J. Universally composable anonymous Hash certification model[J]. Sci China Inf Sci, 2007, 50: 440-455.

[14] FENG T, LI F H, MA J F, *et al*. A new approach for UC security concurrent deniable authentication[J]. Sci China Inf Sci, 2008, 51:352-367.

[15] ZHANG J W, MA J F, MOON S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T[J]. Sci China Inf Sci, 2010, 53: 465-482.

[16] ZHANG J W, MA J F, MOON S J. Universally composable one-time signature and broadcast authentication[J]. Sci China Inf Sci, 2010, 53: 567-580.

[17] 田有亮, 马建峰, 彭长根等. 群组通信的通用可组合机制[J] 计算

机学报, 2012, 35(4): 645-653.
TIAN Y L, MA J F, PENG C G, *et al*. Universally composable mechanism for group communication[J]. Chinese Journal of Computers, 2012, 35(4): 645-653.

[18] 张妤, 胡杰. UC 安全计算的一种信任模型[J]. 四川大学学报(工程科学版), 2012, 44(3): 106-111.
ZHANG Y, HU J. A trust model of UC secure computation[J]. Journal of Sichuan University(Engineering Science Edition), 2012, 44(3): 106-111.

[19] BONEH D, FRANKLIN M. Identity based encryption from the weil pairing[J]. SIAM J of computing, Extended Abstract in Crypto, 2003, 32(3): 586-615.

作者简介：

田有亮（1982-），男，贵州盘县人，博士，贵州大学副教授、硕士生导师，主要研究方向为算法博弈论、密码学、信息安全。

彭长根[通信作者]（1963-），男，侗族，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为密码学、信息安全。E-mail: sci.cgpeng@gzu. edu.cn.

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授，博士生导师，主要研究方向为网络与信息安全、密码学等。

林辉（1977-），男，福建福州人，西安电子科技大学博士生，主要研究方向为下一代网络、网络 QoS 技术。

杨凯（1983-），男，山东莱芜人，博士，武警工程大学讲师，主要研究方向为无线 mesh 网络、OPNET 仿真。

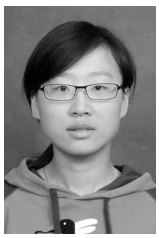
（上接第 53 页）

[14] ZHENG V W C, ZHENG Y, XIE X. Collaborative location and activity recommendations With GPS history data[A]. Proceeding of International Conference on World Wide Web[C]. 2010. 1029-1038.

[15] http://en.wikipedia.org/wiki/Markov_model[EB/OL]. 2011.

[16] http://www.chorochronos.org/Default.aspx?tabid=75 [EB/OL]. 2012.

作者简介：



李雯（1988-），女，河北邢台人，中国矿业大学博士生，主要研究方向为轨迹数据挖掘。

夏士雄（1961-），男，辽宁抚顺人，中国矿业大学教授、博士生导师，主要研究方向为数字化矿山、智能信息处理等。

刘峰（1967-），男，甘肃平凉人，中国矿业大学兼职教授、主要研究方向为轨迹数据挖掘。

张磊（1977-），男，江苏沛县人，博士后，中国矿业大学副教授、硕士生导师，主要研究方向为轨迹数据挖掘。

袁冠（1982-），男，江苏睢宁人，博士，中国矿业大学讲师，主要研究方向为轨迹数据挖掘。