一种改进的两方安全议价协议

赵 洋，刘 勇，王佳昊，秦志光

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出了一种基于Paillier同态公钥密码体制的两方安全议价协议。该协议在保障出价信息的私密性和结果正确的前提下，协议参与双方可以完成对商品交易价格的协商，仅在价格协商成功的情况下由第三方参与计算出最终的成交价格。通过对复杂度和安全性的分析可知，该协议具有较高的执行效率和安全特性，在电子商务应用中具有一定的实用价值。

关 键 词 价格协商; 同态公钥密码体制; 百万富翁问题; 安全两方计算
中图分类号 TP389.1 文献标识码 A

An Improved Secure Two-Party Bargaining Protocol

ZHAO Yang，LIU Yong，WANG Jia-hao，QIN Zhi-guang

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract In this paper a secure two-party bargaining protocol is proposed which is based on Pallier homomorphic public key cryptosystem. The participant can make a bargain with another one by implementing the protocol. During the protocol, the privacy of input and the correctness of output should be preserved. The third party will participate in working out the final price only under the condition of success agreement. Through the analysis of complexity and security, this protocol holds higher implementing efficiency and security characters, and therefore has application value in the e-commerce.

Key words bargaining; homomorphic public key cryptosystem; millionaires' problem; secure two-party computation

随着计算机网络和通信技术的迅速发展，基于网络的互联合作也越来越普遍。由于网络上的合作双方之间在身份认证、信任建立上存在着先天性的不足，网络合作双方之间往往需要在半信任甚至完全不信任的状态下进行，所以在合作意向未达成一致之前无人愿意透露自己的私密信息。网络合作可以简要描述为：在保证输入的私密性和输出的正确性的前提下，合作者基于各自的输入协同完成一个计算任务。本文提出了一个可用于电子商务中价格协商的两方安全议价协议。

1 两方安全议价协议工作简要

该协议的工作可以简要描述如下：(1) 价格协商阶段，卖家Seller和买家Buyer是价格协商的参与方，Seller是商品的拥有者，对出售商品的价格期望是 a，Buyer是商品的购买者，对购买商品的价格期望是 b，如果买家出价高于卖家要价，即 $a \le b$，价格协商成功；否则价格协商失败。这一阶段完全由Seller和Buyer完成，不需要第三方参与，且双方都不希望在价格协商阶段泄漏自己的出价信息；(2) 成交价计算阶段，仅在协商成功的情况下，在第三方协作下输出最后的成交价格 $(a+b)/2$。本协议使用Paillier加同态的公钥密码算法来实现安全的价格协商，其计算复杂度和通信复杂度均为常数阶，计算开销不会随着问题规模的增大而快速增长，因此适用于大数值的比较，具有较强的实用性。

2 相关工作

两方安全议价协议可以视为安全多方计算问题的一个实例。文献[1]中首次提出安全两方函数计算的问题，即著名的百万富翁问题：在不透露自己拥有的财富数额的情况下，两个百万富翁比较出谁更富有；文献[2]中对两方计算问题给出了较完整的定义：对于每一对输入 (x,y)，期望输出 $f(x,y)$ 是在多对字符串上的一对随机值。输入x的一方希望获得 $f(x,y)$ 的第一个元素，另一方希望得到 $f(x,y)$ 的第

收稿日期：2006－06－15
基金项目：教育部博士点基金资助项目(20050614018)；四川省科技攻关计划项目(05GG007-011-01)
作者简介：赵 洋(1973－)，男，博士生，主要从事网络安全协议及其应用方面的研究.

二个元素；文献[3]将两方扩展到多方。理论上，一般性的安全多方计算问题是可以解决的，但是文献[3]指出这些解决方法运用到具体的例子中是不切实际的、低效的。考虑到效率，在实际应用中必须针对具体问题寻找解决方法。

在本文提出的两方议价协议中价格协商阶段可以看作求解百万富翁问题的一个实例。文献[1]中给出了第一个百万富翁问题的求解，该解法基于RSA公钥密码体制，在计算上需要 2^l 次加解密运算，其中l为比较值的二进值长度。文献[3-4]给出了一般性的解法，但这些解法的计算复杂度都是指数阶的，所以很难在实际中应用。文献[5]中给出了复杂性为 $O(l\lambda)$ 的实用协议，其中l是被比较整数的二进制长度；λ 为差错参数。但是协议依赖于设计特殊的计算电路，因此在应用上存在着一定的局限。本文提出一种用加同态的公钥密码算法来求解百万富翁问题的方法，在进行大数值比较的情况下，与原有的方法相比效率上有显著的提高。本文并构建了一个实用的两方安全议价协议，对其正确性、安全性、计算复杂度和通信复杂度进行了分析。

3　记号和符号

设P为公钥加密算法、P_{encr}为P加密算法、P_{decr}为P解密算法；PK为P中的公钥、SK为P中与PK对应的私钥；$P_{\text{encr}}(PK, M)$为使用PK加密明文M的加密输出(密文C)、$P_{\text{decr}}(SK, C)$为使用SK解密密文C的解密输出(明文M)；E为对称密钥加密算法、D为与E对应的对称密钥解密算法；$E(K, M)$为使用密钥K加密明文M的加密输出(密文C)、$D(K,C)$为使用密钥K解密密文C的解密输出(明文M)；$|n|$为n的二进制长度；Seller为商品的销售者、Buyer为商品的购买者；TTP为一个可信第三方。

4　Paillier同态公钥密码体制

对于两个代数结构A和B，如果 $\forall x, y \in A$，有 $f(x \circ y) = f(x) * f(y)$，其中“$\circ$”是$A$中的运算；“$*$”是$B$中的运算，则映射 $f: A \mapsto B$ 为A到B的同态[11]。对于公钥加密算法 $E(\cdot)$，如果给定 $E(x)$ 和 $E(y)$，在没有私钥的情况下能够计算出 $E(x \circ y)$，则称该公钥加密算法具有同态性质。文献[6]中提出的Paillier加密算法具有加同态性质，算法简要描述如下：(1) 参数选择和预定义：选择$n = pq$，p和q为大素数；$\lambda(n)$为Carmichael函数，即 $\lambda(n) = \text{lcm}(p-1, q-1)$；$G$为模$n^2$的乘法群，$G = \{w \mid w \in Z_{n^2}^*\}$，$B_\alpha = \{g \mid g \in G, g^{\alpha n} = 1 \bmod n^2\}$，$B = \bigcup_{\alpha=1,2,\cdots,\lambda} B_\alpha$。文献[6]中证明，如果 $g \in B$，$f_g(x, y) = g^x y^n$ 是 $Z_n \times Z_n^* \to Z_{n^2}^*$ 的双射。定义函数 $L(u) = (u-1)/n$，$\forall u \in S_n = \{u < n^2 \mid u = 1 \bmod n\}$，显然$L$是良定义的(只具有唯一解)。(2) 密钥生成：随机选择 $g \in B$ 且 $\gcd(L(g^\lambda \bmod n^2),\ n) = 1$，$PK = (n, g)$ 为公钥，$SK = \lambda(n)$ 为私钥。(3)加密过程：对于明文 $M \in Z_n$，随机选择 $r \in Z_n^*$，密文 $C = P_{\text{encr}}(PK, M) = g^m r^n \bmod n^2$。(4) 解密过程：$C \in Z_{n^2}^*$，明文$M$= $P_{\text{decr}}(SK, C) = L(C^\lambda \bmod n^2) / L(g^\lambda \bmod n^2) \mod n$。

Paillier公钥加密算法具有语义安全性和加同态的性质，即在给定明文 M_0、M_1 不存在多项式时间算法区分 $P_{\text{encr}}(PK, M_0)$ 和 $P_{\text{encr}}(PK, M_1)$，且有：

$$P_{\text{encr}}(PK, M_0) P_{\text{encr}}(PK, M_0) = P_{\text{encr}}(PK, M_0 + M_1)$$

$$P_{\text{encr}}(PK, M)^k = P_{\text{encr}}(PK, kM), k \in N$$

5　两方安全议价协议

本文提出的两方安全议价协议有Seller、Buyer和TTP三个参与实体。协议的执行分为协商和计算两个阶段。在协商阶段，Seller和Buyer通过协议的执行可以判断议价是否成功，如果Buyer的出价大于或等于Seller的要价，则议价成功进入计算阶段，在TTP的协助下得出最终的成交价格；否则输出议价失败的结果。其求解的问题可描述如下：

If (Seller.price <= Buyer.price)
then return (Seller.price + Buyer.price)/2;
else return　“no transaction.”

假定：协议在通信过程使用认证信道，即攻击者可以截获协议执行过程中的所有消息，但不能篡改消息的内容；同时假定协议的参与者和攻击者的计算能力是有限的，即不能在多项式时间内解决某些计算难题。

5.1　两方安全议价协议描述

协议详细描述如下：Seller对商品的要价为 a，Seller 拥有公钥为 $PK_{\text{Seller}} = (n, g)$，私钥为 $SK_{\text{Seller}} = \lambda(n)$ 的Paillier公钥加密算法密钥对。Buyer为购买者，对商品的出价为 b，且已经获得Seller的公钥。TTP与Seller和Buyer之间分别拥有秘密的通信密钥 $K_{\text{TTP,Seller}}$ 和 $K_{\text{TTP,Buyer}}$。a、b属于模 n 的绝对值最小完全剩余系，即 $-n/2 \le a, b < n/2$。

价格协商步骤如下：(1) Seller选择 r_a，计算 $C_a = P_{\text{encr}}(PK_{\text{Seller}}, a) = g^a r_a^n \bmod n^2$，发送给Buyer；(2) Buyer选择随机选择 $r_v, r_\omega, v, \omega \in Z_n, \mu \in Z_n^*$，其中，$0 < v - \omega < \mu$ $A = C_a^\mu P_{\text{encr}}(PK_{\text{Seller}}, \omega) = C_a^\mu g^\omega r_\omega^n \bmod n^2$，

$B = P_{\text{encr}}(PK, \mu b + v) = g^{\mu b+v} r_v^n \bmod n^2$，发送给Seller；(3) Seller 计算 $M_A = P_{\text{decr}}(SK_{\text{Seller}}, A)$ 和 $M_B = P_{\text{decr}}(SK_{\text{Seller}}, B)$，并判断 $M_A - M_B$，如果 $M_A - M_B > 0$，则 $a > b$，Seller向Buyer发送议价失败的消息；如果 $M_A - M_B < 0$ 则 $a \le b$；如果 $a > b$，Seller向Buyer发送议价成功的消息。

计算阶段步骤如下(该阶段仅在价格协商成功时执行)：(1) Seller将自己的要价加密，发送 $E(K_{\text{Seller,TTP}}, a)$ 给TTP。(2) Buyer将自己的出价加密，发送 $E(K_{\text{Buyer,TTP}}, b)$ 给TTP。(3) TTP解密Seller的要价和Buyer的出价，计算出成交价 $(a+b)/2$，发送 $E(K_{\text{Seller,TTP}}, (a+b)/2)$ 给 Seller。(4) TTP 发送 $E(K_{\text{Buyer,TTP}}, (a+b)/2)$。

其中协商阶段步骤(1)~(3)完成价格比较，如果价格协商失败，Seller和Buyer结束协议的执行，输出议价失败的结果。计算阶段的步骤(1)~(4)完成交易价格计算，如果价格协商成功Seller和Buyer解密从TTP收到的消息将获得最终的成交价格$(a+b)/2$。

5.2 正确性证明

协议的正确性证明如下：因为 $M_A = P_{\text{decr}}(SK_{\text{Seller}}, A) = P_{\text{decr}}(SK_{\text{Seller}}, C_a^{\mu} E(\omega)) = \mu a + \omega$，$M_B = P_{\text{decr}}(SK_{\text{Seller}}, B) = P_{\text{decr}}(SK_{\text{Seller}}, E(\mu b + v)) = \mu b + v$，所以 $M_A - M_B = \mu(a-b) - (v-w)$。当 $a > b$ 时，因为 $\mu(a-b) \ge \mu$，$0 < v - w < \mu$，所以 $M_A - M_B = \mu(a-b) - (v-w) > 0$；当 $a \le b$ 时，因为 $\mu(a-b) \le 0$，$0 < v - w < \mu$，所以 $M_A - M_B = \mu(a-b) - (v-w) < 0$。由上述的分析可知，在价格协商阶段协议可以输出正确的结果。

5.3 安全性分析

在比较阶段，由于Paillier加密算法的语义安全性，Buyer从 C_a 中无法提取到关于 a 的任何信息。对Seller而言，由于 v, ω, μ 是随机选择的，Seller也无法从 $\mu(a-b)-(v-w)$ 中提取到关于 b 的任何信息。同理攻击者也不能提取到任何关于a、b的信息，除非他能够有效破解Paillier加密算法，因此输入的私密性在比较阶段可以得到保障。在计算阶段，Seller与Buyer均通过加密信道与TTP通信，攻击者除非可以有效破解通信过程中使用的对称加密算法，否则无法获得最终的成交价格。同时由于TTP参与最后成交价格的计算，因此可以为协议的执行提供公平性保障，即Seller和Buyer要么都获得最终的成交价格，要么都得不到最终的成交价格。从以上的分析可以看出，该协议的核心部分，即价格协商阶段的安全性是基于Paillier加密算法的安全性，根据文献[7-8]中对Paillier加密体制的安全性分析，在假定计算和判断 $Z_{n^2}^*$ 上的 n 次剩余问题是困难的条件下，Paillier加密体制具有很好的安全性能。

5.4 复杂度分析

通信复杂度：从本文5.1中可知，协议在执行过程中，比较阶段需要进行2轮通信，计算阶段需要1轮通信，如表1所示。

表**1** 协议通信复杂度比较

	本协议	文献[1]	文献[5]
比较阶段通信轮数	2	2	1
计算阶段通信轮数	1	—	—

计算复杂度：协议在执行过程中，比较阶段需要进行3次Paillier加密运算和2次Paillier解密运算，计算阶段需要6次对称加密算法的加/解密运算，如表2所示。

表**2** 协议计算复杂度比较

	本协议	文献[1]	文献[5]
比较阶段	5Paillier加解密	$O(2^l)$ RSA加解密	$O(l\lambda)$ GM加解密
计算阶段	6对称加解密	—	—

备注：l为比较数的二进制长度，λ为差错参数。

由表2所示可知协议执行过程中只需要常数次的Paillier加解密运算和对称加解密运算，由于对称加密算法运算的速度远高于公钥加密算法，所以主要的计算开销由Paillier加密算法的运算效率决定。虽然Paillier加密算法运算速度低于RSA加密算法，但是由于协议只需要进行常数次的Paillier加解密运算，所以计算开销不会随着问题的规模增大而快速增长，较适用于大数值的比较。表3所示为Paillier加密算法与RSA和ElGamal加密算法的计算复杂度比较。

表**3** **Pailler**加密算法计算复杂度比较[6]

	Pailler	RSA(n,e)	ElGamal
	$\lvert n\rvert, \lvert p\rvert = 512$	$\lvert n\rvert, \lvert p\rvert = 512, e = 2^{16}+1$	$\lvert n\rvert, \lvert p\rvert = 512$
加密	5 120	17	1 536
解密	768	192	768

备注：表中数值为进行加解密运算所需要进行模$(\lvert n\rvert = 512)$乘运算的次数。

(下转第558页)

进行了对比，结果如表1所示，延迟合并伙伴系统的性能比无结构链表分配策略大约高4%，也比经典算法优越。

表1 伙伴系统与无结构链表在平均情况下的性能比

测试方法	无结构链表	延迟合并伙伴系统	经典的伙伴系统
jess	1.00	1.04	1.02
raytrace	1.00	1.03	0.92
db	1.00	1.02	1.01
javac	1.00	1.02	1.00
jack	1.00	1.05	1.03

4.3 延迟合并伙伴系统的定性分析

本文仿真运行了经典伙伴系统和延迟回收伙伴系统，通过跟踪每次内存分配的过程，定性地分析了请求的满足状况。数据显示延迟合并伙伴系统有约90%的机会从伙伴忙或者伙伴闲空闲链表中直接得到满足。其成功之处在于每次分配的都是相对较小的内存块；而经典伙伴系统只有50%的机会立即找到合适的空闲块。

5 结 论

本文在分析经典伙伴系统的基础上，针对面向对象语言特点提出了延迟合并的伙伴系统。通过延迟合并机制使得约90%的内存分配请求能够立即得到满足，并降低了合并造成的系统开销；通过外部碎片整理能够以较少的负担实现内存整理的功能，从而降低内存分配失败的机率；通过位图机制加速了伙伴块的查询过程，从而加速了伙伴系统的分配和回收流程。仿真试验表明延迟合并伙伴系统与经典伙伴系统相比具有更高的执行效率，有更多的机会能够马上找到合适大小的空闲块以满足请求。

参 考 文 献

[1] KNUTH D E. 计算机程序设计艺术, 第1卷: 基本算法[M]. 第3版. 苏运霖, 译. 北京: 国防工业出版社, 2002.
[2] ARIE K. Tailored-list and recombination-delaying buddy systems[J]. ACM Transactions on Programming Languages and Systems, 1984, 6(1): 118-125.
[3] 曹全欣. 动态存储管理机制的改进及实现[D]. 南京: 南京航空航天大学, 2003.
[4] LO C-T D, SRISA-AN W, CHANG J M. Performance analyses on the generalized buddy system[J]. Computers and Digital Techniques, IEEE Proceedings, 2001, 148(45): 167-175.
[5] 郭福顺, 王世铀, 臧天仪. 一种动态存储管理机制[J]. 计算机研究与发展, 1999, 36(1): 62-66.

编 辑 漆 蓉

(上接第540页)

6 结 论

本文提出的两方安全议价协议具有较高的执行效率，其通信复杂度和计算复杂度均为常数阶，并能够提供私密性和公平性的保障，因此在电子拍卖、公平交换等电子商务中具有较好的实用价值。目前该协议适用于两方的价格协商，在下一步的工作中将进一步研究将其拓展到多方的方法和途径。

参 考 文 献

[1] YAO A C. Protocols for secure computations[C]// Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Chicago: IEEE Computer Society, 1982: 160-164.
[2] GOLDREICH O. Secure multi-Party computation[EB/OL]. http://www.wisdom.weizmann.ac.il/~oded/pp.html, 2006-08-06.
[3] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[C]//Proceedings of the 19th Annual ACM Symposium on the Theory of Computing. New York: ACM Press, 1987: 218-229.
[4] GOLDREICH O, MICALI S, WIGDERSON A. Proofs that yield nothing about their validity -or- all languages in NP have zero-knowledge proof systems[J]. Journal of the ACM, 1991, 8(1): 691-729.
[5] FISCHLIN M, EFFECTIVE C A. Pay-per-multiplication comparison method for millionaires[C]//RSA Security 2001 Cryptographer’s Track at RSA Conference. LNCS2020, London: Springer-Verlag, 2001: 457-471.
[6] PAILLIER P. Public-key cryptosystems based on Composite degree residuosity classes[C]//Proceedings of Eurocrypt'99, Prague, Czech Republic, LNCS1592. Berlin: Springer-Verlag, 1999: 223-238.
[7] CATALANO D, GENNARO R, GRAHAMN H. The bit security of paillier encryption scheme and its applications[C]//In Advances in Cryptology-Eurocrypt '01, Aarhus, Denmark, LNCS2045. Berlin: Springer-Verlag, 2001: 229-243.
[8] CRAMER R, SHOUP V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]//In Advances in Cryptology-Eurocrypt '02, Amsterdam Netherlands, LNCS 2332. Berlin: Springer-Verlag, 2002: 45-94.

编 辑 孙晓丹