文章编号:1001 - 9081(2006)11 - 2576 - 02

基于加同态公钥密码体制的两方安全议价协议

赵 洋,蓝 天,马新新,张凤荔
(电子科技大学 计算机科学与工程学院,四川 成都 610054)
(zhaoyang@uestc.edu.cn)

摘 要:安全多方计算及其应用是目前密码学领域的一个重要研究方向。在不需要第三方参与且保证安全的前提下,如何完成多方的协作运算是其研究的核心。基于加同态公钥加密算法的议价协议,是安全多方计算应用的一个具体实现,通过协议的执行,参与方可以进行商品价格的协商,并保障输入的私密性和结果的正确性。协议的执行过程中不需要第三方的参与,协议的安全性基于所采用的同态公钥加密算法。

关键词:安全多方计算;百万富翁问题;同态公钥密码体制;议价
中图分类号: TP309.7 **文献标识码**:A

A secure two-party bargaining protocol based on additive homomorphic public key cryptosystem

ZHAO Yang, LAN Tian, MA Xin-xin, ZHANG Feng-li
(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: Secure multi-party computation with its applications is an important direction in current cryptography research field. The research focuses on how to accomplish the secure cooperative computation among multi-party without the participation of the third party. The two-party bargaining protocol, based on homomorphic public key cryptosystem, was an example of secure multi-party computation's applications. One participant can make a bargain with the other by implementing the protocol. During the implementation of protocol, the privacy of input and the correctness of output could be preserved. The protocol can be implemented without the participation of the third party and its security was based on additive homomorphic public key cryptosystem.

Key words: secure multi-party computation; millionaires' problem; homomorphic public key cryptosystem; bargain

0 引言

Internet 的迅猛发展为通过网络进行协作创造了大量的机会,例如,用户和商家通过网络对某种服务或商品的交易价格进行协商;两个竞争公司对联合投资一个必须满足双方隐私和利益考虑的项目进行评估等。由于这些协作可能发生在信任或半信任的伙伴、甚至对手之间,所以在协议达成一致之前无人愿意透露自己的私密信息。这样的问题可以简要描述为: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,计算过程中不需要第三方的参与,这个问题就是安全多方计算研究的核心问题。

理论上,一般性的安全多方计算问题是可解决的,但是 Goldreich 指出这些解决方法是不切实际的和低效的。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[1]。本文提出的基于加同态公钥加密算法的两方议价安全协议,就是针对两方价格协商这一特定应用提出的。议价协议完成的工作可以简要描述如下:Alice 和 Bob 是价格协商的参与方,Alice 是商品的拥有者,她对出售商品的价格期望是 a,Bob 是商品的购买者,他对购买商品的价格期望是 b。如果 $a \leqslant b$,价格协商成功,输出最后的成交价格 $(a+b)/2$;否则价格协商失败。该协议在不需要第三方的参与的情况下,可以保证输入的私密性和结果的正确性。

1 相关工作

安全多方计算问题最初由 A. Yao 提出,他在文献[2]中首次提出安全两方函数计算的问题,并引入一个特例——百万富翁问题,即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。随后 Goldreich 在文献[1]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 $f(x, y)$ 的第二个元素。Goldreich 等在文献[3]中进一步将两方扩展到多方。

两方议价协议可以看作百万富翁问题的一个变形,文献[2]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 RSA 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]中给出了一个复杂性为 $O(l\lambda)$ 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。在本协议的实现中,提出了一种用加同态的公钥密码算法

收稿日期:2006 - 08 - 22 **基金项目**:国家自然科学基金资助项目(60473090,60573129);教育部高等学校博士学科点专项科研基金资助项目(20050614018);四川省科技攻关计划项目(05GG007-011-01)

作者简介:赵洋(1973 -),男,重庆人,博士研究生,主要研究方向:安全多方计算; 蓝天(1977 -),男,四川宜宾人,博士研究生,主要研究方向:安全多方计算、网络安全; 马新新(1973 -),男,陕西蓝田人,博士研究生,主要研究方向:对等计算、网络安全; 张凤荔(1963 -),女,河南南阳人,教授,主要研究方向:数据库应用和安全.

来求解百万富翁问题的方法,其计算复杂度为常数阶,计算开销不会随着问题的规模增大而快速增长,所以适用于大数值的比较,具有较强的实用性。

2　加同态公钥密码体制

对于两个代数结构 A 和 B,其中 $\circ$ 是 A 中的运算, $*$ 是 B 中的运算, 如果 $\forall x, y \in A$,有 $f(x \circ y) = f(x) * f(y)$,则映射 $f: A \mapsto B$ 称为 A 到 B 的同态。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。例如,RSA[6] 公钥密码算法具有乘同态性质,而 Paillier[7],Bresson[8] 算法具有加同态性质。本文提出的两方议价协议采用了 Paillier 等人提出的公钥加密算法,算法描述如下。

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 $\lambda(n) = lcm(p-1, q-1)$,$G$ 为模 n^2 的乘法群,即 $G = \{w \mid w \in Z_{n2}^*\}$。

$B_\alpha = \{g \mid g \in G, g^{\alpha n} = 1 \bmod n^2\}$, $B = \bigcup_{\alpha=1,\cdots,\lambda} B_\alpha$,文献[7]中证明,如果 $g \in B$, $f_g(x, y) = g^x y^n$ 是 $Z_n \times Z_n^* \to Z_{n2}^*$ 的双射。定义函数 $L(u)$, $\forall u \in S_n = \{u < n^2 \mid u = 1 \bmod n\}$, $L(u) = (u-1)/n$,显然 L 是良定义的(只具有唯一解)。

密钥生成:随机选择 $g \in B$ 且 $\gcd(L(g^\lambda \bmod n^2), n) = 1$, (n, g) 为公钥, $\lambda(n)$ 为私钥。

加密过程:对于明文 $m \in Z_n$,随机选择 $r \in Z_n^*$,密文 $c = g^m r^n \bmod n^2$。

解密过程: $c \in Z_{n2}^*$, $m = L(c^\lambda \bmod n^2)/L(g^\lambda \bmod n^2) \bmod n$。

Paillier 公钥加密算法具有语义安全性和加同态的性质[7],即在给定明文 m_0, m_1 不存在多项式时间算法区分 $E(m_0)$ 和 $E(m_1)$,且 $E(m_0)E(m_1) = E(m_0 + m_1)$, $E(m)^k = E(km)$, $k \in N$。

3　两方议价的协议实现

两方议价协议有两个参与实体:销售者和购买者。协议的执行分为两个阶段:比较阶段和计算阶段。在比较阶段,销售者和购买者可以通过协议的执行判断议价是否成功,如果购买者的出价大于或等于销售者的要价,则议价成功进入计算阶段,得出最终的成交价格;否则输出议价失败的结果。其求解的问题可以形式化描述如下:

$$a, b \in Z_n, f(a, b) = \begin{cases} 0, & \text{if } a > b \\ (a+b)/2, & \text{if } a \leqslant b \end{cases}$$

假设协议的参与方是半可信的,即参与者在价格协商的过程中不会偏离协议,但是都希望获取关于对方输入更多的信息;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。

在协议的执行过程中要求保证参与双方输入的私密性和结果的正确性,即根据参与双方的输入,协议执行后必须输出正确的结果,除了可以从结果中推导出的信息外,不会泄漏关于双方输入的任何信息。对本协议而言,正确性可具体描述为当购买者的出价低于销售者的要价时输出议价失败的结果,当购买者的出价大于或等于销售者的要价时输出正确的成交价格 $(a+b)/2$;私密性可具体描述为在议价失败的情况下,参与双方仅知道议价失败的结果,而无法获取关于对方输入的更多信息。

3.1　两方议价协议的具体描述

假定协议的参与者为 Alice 和 Bob,Alice 为销售者,对商品的要价为 a,Alice 拥有公钥为 (n, g),私钥为 $\lambda(n)$ 的 Paillier 公钥加密算法密钥对。Bob 为购买者,对商品的出价为 b,已经获得了 Alice 使用的公钥。a, b 属于模 n 的绝对值最小完全剩余系,即 $-n/2 \leqslant a, b \leqslant n/2$。

协议详细描述如下:$E(\cdot)/D(\cdot)$ 分别表示 Paillier 加/解密运算。

1) Alice 选择 r_a,计算 $C_a = E(a) = g^a r_a^n \bmod n^2$,发送给 Bob;

2) Bob 选择随机选择 r_v, r_ω, v, $\omega \in Z_n$, $\mu \in Z_n^*$,其中 $0 < v - \omega < \mu$,计算 $A = C_a^\mu E(\omega) = C_a^\mu g^\omega r_\omega^n \bmod n^2$, $B = E(\mu b + v) = g^{\mu b + v} r_v^n \bmod n^2$,发送给 Alice;

3) Alice 计算 $D(A)$ 和 $D(B)$,并判断 $D(A) - D(B)$,如果 $D(A) - D(B) > 0$,则 $a > b$;如果 $D(A) - D(B) < 0$,则 $a \leqslant b$。

4) 如果 $a > b$,Alice 将议价失败的结果通知 Bob;如果 $a \leqslant b$,表示议价成功,Alice 将 $D(A) - D(B)$ 发送给 Bob;

5) Bob 根据 $D(A) - D(B)$,计算出最后的成交价格 $(a+b)/2$,然后选择随机数 r,加密 $(a+b)/2$,发送 $C_{(a+b)/2} = E[(a+b)/2] = g^{(a+b)/2} r^n \bmod n^2$ 给 Alice;

6) Alice 解密 $D(C_{(a+b)/2}) = (a+b)/2$,完成议价。

其中 1)~4)为比较阶段,如果议价失败,Alice 和 Bob 结束协议的执行,输出议价失败的结果;5)~6)为计算阶段,如果议价成功将输出最终的成交价格。

3.2　协议分析

3.2.1　正确性证明

比较阶段证明:

$\because D(A) = D(C_a^\mu E(\omega)) = \mu_a + \omega$,

$D(B) = D(E\mu b + v)) = \mu b + v$

$\therefore D(A) - D(B) = \mu(a-b) - (v - \omega)$

当 $a > b$ 时, $\because \mu(a-b) \geqslant \mu$, $0 < v - \omega < \mu$

$\therefore D(A) - D(B) = \mu(a-b) - (v-\omega) > 0$;

当 $a \leqslant b$ 时, $\because \mu(a-b) \leqslant 0$, $0 < v - \omega < \mu$

$\therefore D(A) - D(B) = \mu(a-b) - (v-\omega) < 0$。

计算阶段证明:

Bob 已知 v, ω, b 和 $\mu \in Z_n^*$,可以计算 $[D(A) - D(B) + (v-\omega)]\mu^{-1} = a - b$,从而可以计算 $(a+b)/2$。由上述证明可知,协议的正确性是显然的。

3.2.2　安全性分析

在比较阶段,由于 Paillier 加密算法的语义安全性,Bob 从 C_a 中无法提取到关于 a 的任何信息;对 Alice 而言,由于 v, ω, μ 是随机选择的,Alice 也无法从 $\mu(a-b) - (v-\omega)$ 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,因为协议参与者将输出包含对方输入信息的成交价格,所以不考虑协议参与双方之间对输入私密性的保障,其安全性体现在输出结果只为议价双方获得。攻击者通过信道的监听可以获得 $D(A) - D(B)$ 和 $C_{(a+b)/2}$,但在不知道 v, ω, μ 的情况下,无法计算 $a - b$;在不能有效破解 Paillier 算法的情况下,也无法通过 $C_{(a+b)/2}$ 获得议价的结果。从以上的分析可以看出,本协议的安全性基于 Paillier 加密算法的安全性,根据 Catalano 和 Cramer 等对 Paillier加密体制的安全性的分析[9,10],在假设计算和判断

(下转第 2582 页)

所构成的局部区域缓存中保存了尽可能多的广告信息。AdGossip 算法保证了共享资源广告信息的快速传播和新鲜性。根据共享资源管理算法所形成的共享资源布局设计了动态浅层泛洪查询的资源定位算法,节点首先进行本地 2-hop 泛洪查询请求,如果对查询结果不满意,可以再次执行查询操作,节点随机选择一个系统成员,该成员代理前者执行本地 2-hop 查询请求泛洪。分析和模拟结果均表明:RAP2P 对非结构化 P2P 系统的资源定位性能有较大提高,能够在低消息开销和低查询时延的条件下,获得与泛洪查询接近的查询结果。

参考文献:

[1] COHEN E, SHENKER S. Replication strategies in unstructured peer-to-peer networks[A]. ACM SIGCOMM[C]. New York: ACM Press, 2002. 177 - 190

[2] LV Q, CAO P, COHEN E, *et al.* Search and replication in unstructured peer-to-peer networks [A]. Proceedings of the 16th international conference on Supercomputing (ICS'02) [C]. New York: ACM Press, 2002. 84 - 95.

[3] GKANTSIDIS C, MIHAIL M, SABERI A. Hybrid search schemes for unstructured peer-to-peer Networks[A]. Proceedings of the INFOCOM[C]. New York: IEEE Computer and Communications Societies, 2005. 1526 - 1537.

[4] LIANG J, KUMAR R, XI Y, *et al.* Pollution in P2P file sharing systems[A]. Proceedings of the INFOCOM[C]. New York, USA: IEEE Computer and Communications Societies, 2005. 1174 - 1185.

[5] BLOOM BH. Space/time trade-offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422 - 426.

[6] BYERS JW, CONSIDINE J, MITZENMACHER M, *et al.* Informed content delivery across adaptive overlay networks[J]. IEEE/ACM Transactions on Network Parallel Distributed Systems, 2004, 12(5): 767 - 780.

[7] BRODER A, MITZENMACHER M. Network applications of bloom filters: A survey[J]. Internet Mathematics, 2005, 1(4): 485 - 509.

[8] AGRAWAL D, ABBADI AE, STEINKE RS. Epidemic algorithms in replicated databases (extended abstract)[A]. Proceedings of the Sixteenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems[C]. New York, USA: ACM Press, 1997. 161 - 172.

[9] MOSK-AOYAMA D, SHAH D. Information dissemination via gossip: applications to averaging and coding[EB/OL]. http://arxiv.org/abs/cs.NI/0504029, 2005.

[10] KERMARREC A-M, MASSOULIÉL, GANESH AJ. Probabilistic reliable dissemination in large-scale systems[J]. IEEE Transactions on Parallel Distributed Systems, 2003, 14(3): 248 - 258.

[11] JUN S, AHAMAD M, JUN XU. Robust information dissemination in uncooperative environments[A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)[C]. Washington, DC, USA: IEEE Computer Society, 2005. 293 - 302.

[12] GANESH AJ, KERMARREC A-M, MASSOULIÉ L. Peer-to-peer membership management for gossip-based protocols[J]. IEEE Transactions on Computers, 2003, 52(2): 139 - 149.

[13] JELASITY M, GUERRAOUI R, KERMARREC A-M, *et al.* The peer sampling service: experimental evaluation of unstructured gossip-based implementations[A]. Proceedings of the 5th ACM/IFIP/USENIX international conference on Middleware[C]. New York, USA: Springer-Verlag, 2004. 79 - 98.

[14] AWAN A, FERREIRA RA, JAGANNATHAN S, *et al.* Distributed uniform sampling in unstructured peer-to-peer networks[A]. Proceedings of the 39th Annual Hawaii International Conference on System Sciences [C]. Washington, DC, USA: IEEE Computer Society, 2006. 223.

[15] GANESH AJ, KERMARREC A-M, MASSOULIÉ L. SCAMP: peer-to-peer lightweight membership service for large-scale group communication [A]. Proceedings of the Third International COST264 Workshop on Networked Group Communication (NGC'01) [C]. London, UK: Springer-Verlag, 2001. 44 - 55.

(上接第 2577 页)

$Z_{n^2}^*$ 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。

3.2.3 执行效率分析

从 3.1 协议描述可知,协议在执行过程中,如果议价失败共需要进行 4 轮通信和 5 次 Paillier 加密算法的加/解密运算;如果议价成功共需要 6 轮通信和 7 次 Paillier 加密算法的加/解密运算,协议的通信复杂度和计算复杂度均为常数阶。因此适合于较大数值的秘密比较,具有很好的实用性。

4 结语

本文提出的基于加同态公钥加密体制的两方议价协议,是高效的实用安全多方计算协议研究工作的组成部分之一。该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,因此该协议在电子商务中具有较好的实用价值。除了 Paillier 加密算法,其构造方法也适用于其他的加同态公钥加密体制。

参考文献:

[1] GOLDREICH O. Secure Multi-Party Computation(Draft, Version 1.4)[EB/OL]. http://www.wisdom.weizmann.ac.il/ oded/pp.html, 2002.

[2] YAO AC. Protocols for Secure Computations[A]. 23rd IEEE Symposium on Foundations of Computer Science (FOCS)[C], 1982.160 - 164.

[3] GOLDREICH O, MICALI S, WIGDERSON A. How to Play Any Mental Game[A]. 19th Annual ACM Symposium on Theory of Computing[C]. 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. A Cost-Effective Pay-Per-Multiplication Comparison Method for Millionaires[A]. RSA Security 2001 Cryptographer's Track at RSA Conference, LNCS2020[C], 2001. 457 - 471.

[6] SCHNEINIER B. Applied Cryptography: Protocols, Algorithms, and Source Code in C[M]. 2nd ed. New York: John Wiley & Sons, 1996. 334 - 340.

[7] PAILLIER P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[A]. STERN J, ed. Eurocrypt'99, LNCS 1592[C]. Berlin: Springer-Verlag, 1999. 223 - 238.

[8] BRESSON E, CATALANO D, POINTCHEVAL D. A Simple Public Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications [A]. LAIH CS, ed. Asiacrypt 2003, LNCS2894[C]. Berlin: Springer-Verlag, 2003.37 - 54.

[9] CATALANO D, GENNARO R, GRAPHAMN H. The Bit Security of Paillier Encryption Scheme and Its Applications[A]. Advances in Cryptology - Eurocrypt'01, LNCS2045[C]. Berlin: Springer-Verlag, 2001.229 - 243.

[10] CRAMER R, SHOUP V. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption[A]. Advances in Cryptology - Eurocrypt'02, LNCS 2332[C]. Berlin: Springer-Verlag, 2002.45 - 94.