无信息泄漏的比较协议*

秦 静[1,2+], 张振峰[2], 冯登国[2], 李 宝[2]

[1](山东大学 数学与系统科学学院,山东 济南 250100)

[2](信息安全国家重点实验室(中国科学院 研究生院),北京 100039)

A Protocol of Comparing Information without Leaking

QIN Jing[1,2+], ZHANG Zhen-Feng[2], FENG Deng-Guo[2], LI Bao[2]

[1](School of Mathematics and System Science, Shandong University, Ji'nan 250100, China)

[2](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100039, China)

+ Corresponding author: Phn: +86-531-6189566, Fax: +86-531-8364652, E-mail: houtui3@263.net, http://www.sdu.edu.cn

Received 2002-12-19; Accepted 2003-09-09

Qin J, Zhang ZF, Feng DG, Li B. A protocol of comparing information without leaking. *Journal of Software*, 2004,15(3):421~427.

http://www.jos.org.cn/1000-9825/15/421.htm

Abstract: At present, research on secure multi-party computation is of great interest in modern cryptography. It should be acknowledged that if any function can be computed securely, then it results in a very powerful tool. In fact, all natural protocols are, or can be rephrased to be, special cases of the multi-party computation problems. Design and analysis of the special multi-party computation protocols is meaningful and has attracted much interest in this field. Based on the combination of a public-key cryptosystem of the homomorphic encryption and on the theoretic construction relying on the Φ-hiding assumption, a protocol for comparing information of equality is proposed. The protocol needs only a single round of interaction and ensures fairness, efficiency and security. The protocol is fair, which means that one party knows the sound result of the comparison if and only if the other one knows the result. The protocol is efficient with the help of an oblivious third party for calculating. However, the third party cannot learn any information about the participant's private inputs and even about the comparison result, and cannot collude with any participant. The protocol is secure for the two participants, that is, any information about their secret input will not leak except the final computation result. A precise proof of security of the protocol is presented. Applications of this protocol may include private bidding and auctions, secret ballot elections,

* Supported by the National Natural Science Foundation of China under Grant No.60373039 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2001AA144040, 2003AA144151 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Outstanding Young Scientists Foundation of China under Grant No.60025205 (国家杰出青年科学基金); the Natural Science Foundation of Shandong Province of China under Grant No.Y2003A03 (山东省自然科学基金)

作者简介: 秦静(1960－),女,山东济南人,教授,主要研究领域为密码学,安全协议;张振峰(1972－),男,副研究员,主要研究领域为密码学/网络与信息安全;冯登国(1965－),男,研究员,博士生导师,主要研究领域为信息与网络安全;李宝(1962－),男,研究员,博士生导师,主要研究领域为信息安全,安全协议.

commercial business, identification in a number of scenarios and so on. It is believed that the protocol may be of practical significance for electronic transaction.

Key words: secure multi-party computation; computationally indistinguishable; public-key cryptosystem; homomorphic encryption; Φ-hiding assumption; Δ-universal hash function

摘 要: 关于安全多方计算的研究是目前国际密码学界的研究热点.如果能够安全地计算任何函数,就掌握了一个很强大的工具,实际上任何一个密码协议都可以化归一个特殊的安全多方计算协议.特殊的安全多方计算协议的设计与分析又是当前人们致力研究的课题.基于Φ-隐藏假设以及同态公钥加密体制的语义安全性假设,给出了一个特殊的安全双方计算协议——无信息泄漏的比较相等协议.该协议具有公平性:一方知道最后结果的等价条件为另一方也知道这个结果;安全性:除了最后结果以外,不泄露有关双方输入的任何信息;有效性:借助于茫然第三方协助完成计算任务,使协议简单有效,但这个第三方不知道最后结果及参与方的秘密,也不能与参与方串谋作弊;并对协议的正确性与安全性进行了理论证明.该协议在网上投标(拍卖)、网上商业谈判、电子选举等领域中有着广阔的应用前景.

关键词: 安全多方计算;计算不可区分;同态加密;公钥密码体制;Φ-隐藏假设;Δ-通用 hash 函数

中图法分类号: TP309 **文献标识码**: A

安全多方计算是指在一个互不信任的多用户网络中,各用户能够通过网络来协同完成可靠的计算任务,同时又能保持各自数据的安全性[1].实际上,安全多方计算是一种分布式协议,在这个协议中,n 个成员 $P_1,P_2,\ldots,P_n$ 分别持有秘密的输入 $x_1,x_2,\ldots,x_n$,试图计算函数值 $(y_1,y_2,\ldots,y_n)=f(x_1,x_2,\ldots,x_n)$,其中 f 为给定的函数.安全的含义是指既要保证函数值的正确性,又不暴露任何有关各自秘密输入的信息,即使参与方有欺骗行为,并对协议的安全性给出证明.国外关于安全多方计算的研究已有一些成果,并已经成为理论密码学的研究热点.安全多方计算有很强的应用背景,特别是在电子信息的时代,如网上电子投标(拍卖),网上商业谈判,电子选举计票,比较薪水、年龄等趣味问题,很多情况下还可用来认证[2]等等.而且我们如果能够安全地计算任何函数,就掌握了一个很强大的工具,实际上任何一个密码协议都可以化归一个特殊的安全多方计算协议.

Andrew C. Yao 较早开始研究安全多方计算,他在文献[3]中提出了安全多方计算的概念.他给出了一个趣味性的例子,被称为“百万富翁”问题:两个富翁在街头相遇,如何在不暴露各自财富的前提下比较出谁更富有?这个问题可数学化为:A 有数值 a,B 有数值 b,能否安全地比较 $a<b$ 或 $a>b$? 有时也需要比较相等的情况,甲、乙双方各有一个消息,如何在不暴露各自消息的前提下比较出二者的消息是否一致?也可数学化为:甲有数值 a,乙有数值 b,能否安全地比较 $a=b$? 这里,安全的含义是指除最后结果($a\neq b$ 或 $a=b$)以外,不泄漏各自的任何信息.Yao 就比较大小问题给出了一个协议,但效率极低,对比较相等问题没有讨论.文献[4]对比较大小给出了一个有效且公平的协议,并对安全性进行了证明,但却没有涉及比较相等的问题;文献[5,6]虽然分别对比较相等给出了一些协议,但对协议的安全性却没有证明.如何设计高效、安全的保密比较双方或多方数值大小(或相等)的协议是一个极具挑战的问题,也是密码学中的一项重要研究任务.

直接将一般的安全多方计算协议的研究成果应用于特殊情形是不实际的,因为这会影响特殊情形下的计算效率或安全性.因此研究特殊情形下的安全多方计算问题,给出效率高、安全性强的特殊安全多方计算协议并从理论上给出协议安全性的证明是一项有意义的工作,也是人们目前致力于研究的热门课题.

本文基于Φ-隐藏假设和同态公钥加密体制的语义安全性假设,对双方比较相等问题给出一个有效的协议,并对协议的正确性与安全性给出严格的理论证明.假设 A 的输入为 a,B 的输入为 b,我们的协议能够保证:

(1) 公平性:A 知道 $a=b$ 的等价条件为 B 也知道这个结果;A 知道 $a\neq b$ 的等价条件为 B 也知道这个结果.

(2) 安全性:虽然我们的协议使用了茫然第三方 T(oblivious third party,参与协议的某些工作如计算工作,但不能主动作弊,也不能与其他参与方串谋作弊,即 T 为半诚实的,故也称为茫然可信方),让其协助完成计算任务,但因为对输入进行了单向置换,因此 T 不能获得其他参与方的秘密输入的任何信息,也不知道最终计算结果,也就是说,T 对 $a,b,a=b,a<b,a>b$ 均一无所知;并且在 A,B 获知 $a\neq b$ 时,双方均不能从 $a\neq b$ 中得到对方输入的

信息,甚至不能得到 a 与 b 之间的大小关系.

(3) 有效性:借助于茫然第三方 T,并由 T 提供一些计算服务,使协议具有较高的效率.

1 预备知识

我们首先简要介绍协议要用到的两个概念.

1.1 Φ-隐藏假设

Φ-隐藏假设(Φ-hiding assumption,简记为ΦHA)[7]是与大数分解的困难性与高次剩余假设相关的.设 m 为一个不知其因数的合数,φ 为欧拉函数,ΦHA 表明确定一个小素数能否整除 $\varphi(m)$在计算上是困难的,对 m 计算 $\varphi(m)$与分解 m 一样困难.同时ΦHA 还表明,对给定的素数 p,存在有效的算法使我们能够找到一个随机的合数 m,使 $p|\varphi(m)$[7].

设 m 为一个正整数,$\varphi(m)$为欧拉函数.记 $P_{k'}$ 为 k'-比特的素数所成之集合;$R_{k''}$ 为合数 m 做成的集合,其中 $m=p'q'$, p'与 q'为 k''-比特的素数且其中一个为安全素数,即形如 $2q_1+1$ 且 q_1 为素数,另一个为准安全素数,即形如 $2pq_2+1$ 且 p,q_2 为奇素数, $p\in P_{k'}$.若有 $p\in P_{k'}$使$p|\varphi(m)$,则称 $m\in R_{k''}$ 隐藏了素数 p.

由ΦHA 可以断言[7]:若随机选取 $m\in R_{k''}$ 隐藏了素数 p_1,而 $p_2\in P_{k'}$ 是独立地随机选取的素数,则(m,p_1)与(m,p_2)是计算不可区分的[1].

1.2 同态公钥加密体制

设 S 为公钥密码体制,k 为其安全参数,X 为消息空间, $E_k:\{0,1\}^k\times X\to C$ 为公开加密函数, $E_k(u,x)\in C, u\in\{0,1\}^k$为随机串,$x\in X$为消息,$C$为密文空间;$D_k:C\to X$ 为保密的解密函数.并假定 X 为 Abel 加群, C 为 Abel 乘群.对两个任意的消息 $x_1,x_2\in X$及随机串$u_1,u_2\in\{0,1\}^k$,若$E_k(u_1,x_1)$与$E_k(u_2,x_2)$ 是计算不可区分的,则称公钥密码体制 S 是语义安全的;若还存在 $u\in\{0,1\}^k$,使

$$E_k(u,x_1+x_2)=E_k(u_1,x_1)\cdot E_k(u_2,x_2),$$

则称 S 是语义安全的同态公钥加密体制[8~10].

我们总假定 k为安全参数,k'与k''为附加的安全参数,且他们均为k的多项式形式.

2 半诚实模型下保密比较相等的协议

参与比较的双方 A 与 B 首先将自己的消息数字化,分别记为 a,b,并将a,b 表示为二进制的形式,即 $a=\sum_{i=0}^{l-1}a_i2^i, b=\sum_{i=0}^{l-1}b_i2^i$,其中$a_i,b_i\in\{0,1\}, i=0,1,...,l-1$. 双方保密比较 $a=b$ 的协议是一个有茫然第三方 T 及两个用户 A,B 参与的协议,A,B 的保密输入分别为 a,b; 在茫然第三方 T 的参与下确定 a与b是否相等 .

2.1 模 型

假设 A,B,T 均形式化为概率多项式时间的图灵机并通过安全信道交互,用来计算的函数为

$$f:D_A\times D_B\times D_T\to\{0,1\}^2\times\{0,1\}^2\times D_T,$$

其中D_A=D_B=$[0,2^l-1], D_T=\{\varepsilon\}$,且

$$f(a,b,\varepsilon)=\begin{cases}(O,O,\varepsilon), & 若a=b\\ (e_1,e_2,\varepsilon), & 若a>b\\ (e_2,e_1,\varepsilon), & 若a<b\end{cases},$$

这里, $O=(0,0), e_1=(1,0), e_2=(0,1)$.

A,B 的输入 a,b 均为 l-比特的正数,T 的输入和输出仅仅是一个空字母 ε,表示 T 作为茫然第三方,既没有输入也没有得到任何输出.用 $(A(a),B(b),T(\varepsilon))$表示输入为$(a,b)$ 时,A,B,T 的输出.

定义 2.1. 在半诚实模型下,称有茫然第三方参与的保密比较相等协议是安全的,如果对每一个实际模型中的被动敌手 D,都相应地有一个理想模型中的被动敌手 $\overline{\mathrm{D}}$,在多项式时间内,对一切 $a\in D_A$,

$b\in D_B$, 有$(A(a),B(b),T(\varepsilon),D)$与$(\overline{A}(a),\overline{B}(b),\overline{T}(\varepsilon),\overline{D})$是计算不可区分的;一个协议具有鲁棒性是指,在相同的情况下,D 和 $\overline{\mathrm{D}}$ 都是主动敌手.

这里,被动敌手的含义是:协议参与方均严格执行协议,只是企图获得更多的信息.半诚实模型中的敌手都是被动的.主动敌手的含义是:协议参与方可随时终止执行协议,并企图修改输入,窜改输出.

特别指出:除了 $a=b$ 是否成立以外,A,B 均不能从自己的输入与输出 $f(a,b,\varepsilon)$ 中得到关于对方输入的任何信息;同样,茫然第三方对于参与方的输入也是一无所知的,而且不知道最后是否有 $a=b$ 成立.

2.2 协 议

我们首先描述半诚实模型下的协议.

设 S 为语义安全的同态公钥加密体制,消息空间为 X,满足 $|X|>2^{k'}$,并设λ: $\{0,1\}^{k'}\to${素数} 为单向映射,$\widetilde{P}=\{P|P$为$\{0,1\}^l\to\{0,1\}^l$的单向置换$\}$.

第 1 步:T 产生公开加密密钥 E_T及保密解密密钥D_T,并将E_T 通过安全信道发送给 A,B 两方.

第 2 步:A 与 B 通过安全信道协商产生单向置换 $P\in\widetilde{P}$,并分别对a,b的二进制系数进行置换,得

$$(\widetilde{a}_0,\widetilde{a}_1,...,\widetilde{a}_{l-1})=P(a_0,a_1,...,a_{l-1}),\ \text{并记}\ \widetilde{a}=\sum_{i=0}^{l-1}\widetilde{a}_i2^i;$$

$$(\widetilde{b}_0,\widetilde{b}_1,...,\widetilde{b}_{l-1})=P(b_0,b_1,...,b_{l-1}),\ \text{并记}\ \widetilde{b}=\sum_{i=0}^{l-1}\widetilde{b}_i2^i.$$

第 3 步:(i) A 选取独立的随机数 $x_l,x_{l-1},...,x_0\in X$和$s_{l-1},...,s_0\in X$ 及 Δ-通用 hash 函数[11]H 与它的密钥 κ ,H: $\kappa\times\{0,1\}^*\to\{0,1\}^{k'}$;

(ii) A 选取随机串 t_1与$t_1'\in\{0,1\}^{k'}$, 确定 k'-比特的素数 p_1与 p_1',使 $p_1=\lambda(t_1),p_1'=\lambda(t_1')$ 并产生正整数 m_1与 m_1',使它们分别隐藏素数 p_1与 p_1';对每一个$j=0,1,...,l-1$,随机选取$u_j\in\{0,1\}^k$,计算

$$\delta_{1,j}=H(\kappa,x_j+s_j)\oplus t_1;\delta_{1,j}'=H(\kappa,x_j-s_j)\oplus t_1';\ y_{1,j}=E_T(u_j,x_j-x_{j+1}+\widetilde{a}_js_j),$$

并通过安全信道将 κ,x_l,x_j,s_j; $y_{1,j}$, $\delta_{1,j}$, $\delta_{1,j}'$ $(j=0,1,...,l-1)$及 m_1 , m_1' 发送给 B;

(iii) B 选取随机串 t_2与$t_2'\in\{0,1\}^{k'}$, 确定 k'-比特的素数 p_2与 p_2',使 $p_2=\lambda(t_2),p_2'=\lambda(t_2')$, 并产生正整数 m_2与 m_2',使它们分别隐藏素数 p_2与 p_2';对每一个$j=0,1,...,l-1$,随机选取$u_j'\in\{0,1\}^k$, 计算

$$\delta_{2,j}=H(\kappa,x_j-s_j)\oplus t_2;\delta_{2,j}'=H(\kappa,x_j+s_j)\oplus t_2';\ y_{2,j}=E_T(u_j',-\widetilde{b}_js_j)$$

及 $z_j=y_{1,j}\cdot y_{2,j}$, 并将

$$\kappa,\ x_l,\ z_j;\ \delta_{1,j},\ \delta_{1,j}',\delta_{2,j},\ \delta_{2,j}',j=0,1,...,l-1;\ m_i,m_i',i=1,2 \tag{*}$$

通过安全信道发送给 T;

第 4 步: T 取 $c_l=x_l$, 随机选取 $Z_{m_i}^*$ 中的一个元素将其平方后记为 $g_{i,l}$,并同样地选取 $g_{i,l}'$, $i=1,2$. 对 $j=0,1,...,l-1$,T 计算

(i) $c_j=c_{j+1}+D_T(z_j)$;

(ii) $q_{i,j}=\lambda[H(\kappa,c_j)\oplus\delta_{i,j}];g_{i,j}=(g_{i,j+1})^{q_{i,j}}\bmod m_i$, $i=1,2$;

$q_{i,j}'=\lambda[H(\kappa,c_j)\oplus\delta_{i,j}'];g_{i,j}'=(g_{i,j+1}')^{q_{i,j}'}\bmod m_i'$, $i=1,2$.

最后,T 随机选取 $r_i\in Z_{m_i}^*,r_i'\in Z_{m_i'}^*,i=1,2$, 计算 $h_i=(g_{i,0})^{r_i}$, $h_i'=(g_{i,0}')^{r_i'}$, $i=1,2$. 并通过安全信道分别将 h_1 与 h_1'发送给 A, h_2 与 h_2' 发送给 B.

第 5 步:A 验证

$$h_1^{\varphi(m_1)/p_1}\equiv1(\bmod m_1) \tag{1}$$

$$h_1'^{\varphi(m_1')/p_1'}\equiv1(\bmod m_1') \tag{2}$$

是否成立.若式(1)成立,则式(2)必不成立,输出为 $e_1=(1,0)$;反之输出为$e_2=(0,1)$;此时 A 获知 $a\neq b$. 若式(1)与式

(2)都不成立,输出为 O=(0,0),此时 A 获知 $a=b$.

同样地,B 验证

$$h_2^{\varphi(m_2)/p_2}\equiv 1(\mathrm{mod}\, m_2) \tag{1′}$$

$$h_2'^{\varphi(m_2')/p_2'}\equiv 1(\mathrm{mod}\, m_2') \tag{2′}$$

是否成立.若式 (1′) 成立,则式 (2′)必不成立,输出为$e_1=(1,0)$; 反之输出为 $e_2=(0,1)$; 此时 B 获知 $a\neq b$. 若式(1′)与式(2′)都不成立,则输出为 O=(0,0),此时 B 获知$a=b$.

该协议实际进行了 3 步通信:

(1) A 将 κ, x_l, x_j, s_j; $y_{1,j}$; $\delta_{1,j}$; $\delta'_{1,j}$; $(j=0,1,...,l-1)$及 m_1, m_1' 发送给B;

(2) B 将 κ, x_l, z_j; $\delta_{1,j}$, $\delta'_{1,j}$; $\delta_{2,j}$, $\delta'_{2,j}$, $(j=0,1,...,l-1)$;$m_i, m_i', (i=1,2)$ 发送给 T;

(3) T 将 h_1与h_1'发送给 A, h_2与h_2' 发送给 B.

3 协议的安全性

关于上述协议的安全性,我们有

定理. 在半诚实模型中,在ΦHA 和同态公钥加密体制的语义安全性假设下,上述有茫然第三方参与的保密比较相等的协议是安全的.

证明:由定义 2.1,只需证明欺骗方在实际协议中不能比在理想模型中得到的信息多.记 D 为实际模型中的敌手, $\overline{\mathrm{D}}$ 为相应理想模型中的敌手,那么 $(A(\tilde{a}),B(\tilde{b}),T(\varepsilon))$与$f(\tilde{a},\tilde{b},\varepsilon)$ 计算不可区分和 $(A(\tilde{a}),B(\tilde{b}),\ T(\varepsilon),D)$与$(\overline{A}(\tilde{a}),\ \overline{B}(\tilde{b}),\ \overline{T}(\varepsilon),\overline{D})$ 计算不可区分将分别保证协议的正确性与安全性.

正确性:容易看出,

$$c_j=x_j+\sum_{i=j}^{l-1}(\tilde{a}_i-\tilde{b}_i)s_i\ ;g_{i,0}=(g_{i,l})^{\prod_{j=0}^{l-1}q_{i,j}}\ ;g'_{i,0}=(g'_{i,l})^{\prod_{j=0}^{l-1}q'_{i,j}}\ ;i=1,2.$$

固定输入 $\tilde{a},\tilde{b}$.

(1) 若$\tilde{a}=\tilde{b}$,则对一切$i=0,1,...,l-1$,有$\tilde{a}_i=\tilde{b}_i$,从而对一切 $j=0,1,...,l-1$,有$c_j=x_j$; 故对一切 j,$q_{1,j}\neq p_1$; $q'_{1,j}\neq p'_1$;$q_{2,j}\neq p_2$;$q'_{2,j}\neq p'_2$;因此式(1),式 (2),式(1′),式(2′)均不成立, 从而,除了一个可忽略的概率以外,输出$(A(\tilde{a}),B(\tilde{b}),\ T(\varepsilon))$与$(O,O,\varepsilon)$是相同的.

(2) 若 $\tilde{a}>\tilde{b}$,在$\tilde{a},\tilde{b}$的二进制表示中,从最高位比特起,设j^*是第1个使$\tilde{a}_j\neq\tilde{b}_j$的指标,而且 $\tilde{a}_{j^*}=1$, $\tilde{b}_{j^*}=0$. 对 j^* ,我们有 $c_{j^*}=x_{j^*}+s_{j^*}$,从而$q_{1,j^*}=p_1$且$q'_{2,j^*}=p'_2$,但$q_{2,j^*}\neq p_2$且$q'_{1,j^*}\neq p'_1$. 对一切 $j=0,1,...,\ j^*-1$, T得到$c_j=x_j+\sum_{i=j}^{j^*-1}(\tilde{a}_i-\tilde{b}_i)s_i+s_{j^*}$. 对一切 $j=j^*+1,...,l-1$, T 得到 $c_j=x_j$; 故 $h_1(\mathrm{mod}\, m_1)$ 有 p_1 次根, $h'_2(\mathrm{mod}\, m'_2)$有 p'_2 次根, 从而式 (1)与式(2′)成立,即

$$h_1^{\varphi(m_1)/p_1}\equiv 1(\mathrm{mod}\, m_1);$$

$$h_2'^{\varphi(m_2')/p_2'}\equiv 1(\mathrm{mod}\, m_2').$$

但式 (1′)与式(2) 不成立.所以除了一个可忽略的概率以外,输出 $(A(\tilde{a}),B(\tilde{b}),T(\varepsilon))$与 (e_1,e_2,ε)是相同的.

同理可证 $\tilde{a}<\tilde{b}$ 的情形.

显然有 $\tilde{a}=\tilde{b}\Leftrightarrow a=b, \tilde{a}\neq\tilde{b}\Leftrightarrow a\neq b$.

综上可知, $(A(\tilde{a}),B(\tilde{b}),T(\varepsilon))$与$f(\tilde{a},\tilde{b},\varepsilon)$ 是计算不可区分的,正确性得证. □

安全性:(反证法)假设协议是不安全的,即在实际模型中存在一个概率多项式时间的敌手 D,使得在理想模型中没有概率多项式时间的敌手 $\overline{\mathrm{D}}$,使 $(A(\tilde{a}),B(\tilde{b}),T(\varepsilon),D)$与 $(\overline{A}(\tilde{a}),\overline{B}(\tilde{b}),\overline{T}(\varepsilon),\overline{D})$ 计算不可区分.

(1) 欺骗方为 A,B 中的一个,不妨假设为 B.

假设对于敌手 D 来说没有理想模型中的敌手 $\overline{D}$ 与之对应,他通过 B 的全部资料及输出 $f(\tilde{a},\tilde{b},\varepsilon)$ 企图获取更多的关于 A 的输入 a 的信息.

① 我们假设 $\tilde{a}\neq\tilde{b}$ 且不妨设 $\tilde{a}>\tilde{b}$,若敌手D能够获得 $\tilde{a}$ 的信息,则一定有 $\tilde{a}',\tilde{a}'',\tilde{b}\in[0,2^{l-1}]$ 且 $\tilde{a}'\neq\tilde{a}''$, $\tilde{a}'>\tilde{b}$, $\tilde{a}''>\tilde{b}$, D能够区分 $\tilde{a}'$ 与 $\tilde{a}''$. 可以证明,这将与同态公钥加密体制的语义安全性相矛盾,见文献[4].

② 假设敌手 D 已获知 $\tilde{a}\neq\tilde{b}$,此时不能获知 a 与 b 之间的大小关系.

不妨设 $\tilde{a}>\tilde{b}$, 根据协议的构造我们知道,在 $\tilde{a},\tilde{b}$ 的二进制表示中,存在一个 j^*,从最高位比特起, j^* 是第1个使 $\tilde{a}_j\neq\tilde{b}_j$ 的指标且 $\tilde{a}_{j^*}=1,\tilde{b}_{j^*}=0$. 但敌手 D 由 B 的全部资料及输出 $f(\tilde{a},\tilde{b},\varepsilon)$ 无法确定出该 j^*,所以更无法得知 a 与 b 之间的大小关系.

欺骗方为 A 时可同样证明.

(2) 欺骗方为 T.

假设对于敌手 D 而言没有理想模型中的敌手 $\overline{D}$ 与之对应,他利用 T 的全部资料能够获得 $\tilde{a},\tilde{b}$ 的信息,则必有 $\tilde{a}',\tilde{a}'',\tilde{b}',\tilde{b}''\in[0,2^{l-1}]$ 且 $\tilde{a}'\neq\tilde{a}''$ 或 $\tilde{b}'\neq\tilde{b}''$,不妨设 $\tilde{a}'\neq\tilde{a}'',\tilde{b}'=\tilde{b}''=\tilde{b}$,且 $\tilde{a}'>\tilde{b}$, $\tilde{a}''>\tilde{b}$, D能区分 $\tilde{a}'$ 与 $\tilde{a}''$. T 的资料为 (*) 式及它们的解密值与 T 计算的数值;设 D′是从输入 $(\tilde{a}',\tilde{b})$ 得到的输出, D″是从输入 $(\tilde{a}'',\tilde{b})$ 得到的输出,则有概率多项式时间算法区分 D′与D″.

① 若 D 利用 x_j 与 s_j 的关系及 $2l$ 个方程:

$$t_1=H(\kappa,x_j+s_j)\oplus\delta_{1,j};$$

$$t_2=H(\kappa,x_j-s_j)\oplus\delta_{2,j}\quad(\text{其中}t_1,t_2\text{未知})$$

能够确定某一个未知的 $t_i,i=1$或2,进而得到 a 的信息,则 T 计算的 $c_j=x_j+\sum_{i=j}^{l-1}(\tilde{a}_i-\tilde{b}_i)s_i$ 中必有一个 j^* 使得 $c_{j^*}=x_{j^*}+s_{j^*}$ 或 $c_{j^*}=x_{j^*}-s_{j^*}$ 且 c_{j^*} 满足两个等式中的一个.若 T 能够判断该 j^* 且不妨设 $c_{j^*}=x_{j^*}+s_{j^*}$),则必可得到 $H(\kappa,x_j+s_j)\oplus\delta_{1,j}=H(\kappa,c_{j^*})\oplus\delta_{1,j^*}$,从而

$$H(\kappa,x_j+s_j)=H(\kappa,c_{j^*})\oplus\delta_{1,j^*}\oplus\delta_{1,j}=H(\kappa,c_{j^*})\oplus\delta',$$

其中 δ' 是某些 $\delta_{1,j}$ 的和, 这与 Δ-通用 hash 函数的定义相矛盾.

② D 利用 T 的资料及 $p_1|\varphi(m_1)$ 得到 $\tilde{a}$ 的信息,可以证明这与 ΦHA 相矛盾,见文献[4].

③ 假若 T 已获知 $\tilde{a}$ 的信息,则 T 从 $\tilde{a}$ 中获得 a 的信息的概率为一个可忽略函数.

设 $I=\{I_i\}$ 为概率多项式算法的逆变器,则 P 为单向置换的充要条件为

$$P_r[P(I(P(x)))=P(x)]=\mu(|x|)^{[12]},$$

其中 $\mu(|x|)$ 为可忽略函数[1],故

$$P_r[P(I(\tilde{a}))=\tilde{a}]=P_r[P(I(P(a)))=P(a)]=\mu(|x|),$$

即 T 以可忽略的概率而从 $\tilde{a}$ 中获得 a 的信息(其中 $P_r(\cdot)$ 表示(·)的概率).

4 结 语

上述协议不具备鲁棒性.主动的欺骗方 A 或 B 可以通过改变输入得到其他方输入的信息或终止协议.但因我们总假定 T 是半诚实的,因此这一问题可通过在已有的协议前加一个输入承诺协议来解决.限于篇幅,此处省略,也可参见文献[4].

本文所给出的双方保密比较协议也可推广到 n 方去,限于篇幅,本文不再讨论.

在线交易、拍卖、竞标等是网络时代出现的新概念,保密比较问题的有效解决使得这种新型的电子交易成为现实.

References:

[1] Goldreich O. Secure multi-party computation, manuscript version 1.3. 2002. htttp://theory.lcs.mit.edu/~oded

[2] Cramer R. Introduction to secure computation. In: Damgaard I, ed. Lectures on Data Security-Modern Cryptology in Theory and Practice. Lecture Notes in Computer Science, Vol 1561. Springer-Verlag, 1999. 16~62.

[3] Yao AC. Protocols for secure computation. In: Proc. of the 23rd IEEE Symp. on Foundation of Computer Science. Chicago: IEEE Computer Society, 1982. 160~164.

[4] Cachin C. Efficient private bidding and auctions with an oblivious third party. In: ACM Conf. on Computer and Communications Security, ed. Proc. of the 6th ACM Conf. on Computer and Communications Security. Assn for Computing Machinery, 1999. 120~127.

[5] Fagin R, Naor M, Winkler P. Comparing information without leaking it. Communications of the ACM, 1996,39(5):77~85.

[6] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed., John Wiley & Sons, Inc., 1996.

[7] Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication. In: Slern J, ed. Proc. of the Advances in Cryptology-EUROCRYPT'99. Lecture Notes in Computer Science, Vol.1592, Springer-Verlag, 1999. 402~414.

[8] Naccache D, Stern J. A new public-key cryptosystem based on higher residues. In: Association for Computing Machinery, ed. Proc. of the 5th ACM Conf. on Computer and Communications Security. San Francisco: ACM, 1998. 59~66.

[9] Okamoto T, Uchiyama S. A new public key cryptosystem as secure as factoring. In: Nyberg K, ed. Proc. of the Advances in Cryptology-EUROCRYPT'98. Lecture Notes in Computer Science, Vol 1403, Springer-Verlag, 1998. 308~318.

[10] Paillier P. Public-Key cryptosystem based on composite degree residuosity classes. In: Proc. of the Advances in Cryptology-EUROCRYPT'99. Lecture Notes in Computer Science, Vol 1592, Springer-Verlag, 1999. 223~238.

[11] Naor M, Yung M. Universal one-way hash functions and their cryptographic applications. In: Association for Computing Machinery, ed. Proc. of the 21st Annual ACM Symp. on Theory of Computing (STOC). Seattle: ACM, 1989. 33~43.

[12] Bellare M. A note on negligible functions. Journal of Cryptology, 2002,15(4):271~284.