一个基于签密技术的安全多方乘积协议*)

张 华 陈智雄 肖国镇

(西安电子科技大学 ISN 综合业务网国家重点实验室 西安 710071)

(福建省蒲田学院数学系 蒲田 351100)

摘 要 本文利用签密技术和不经意传递提出一个两方安全乘积协议,同时用归纳的方法得出一个多方安全乘积协议。此协议不需要可信任第三方的参与,从而避免了其导致的瓶颈问题,并且可以防止攻击者篡改信息,提高安全性。

关键词 安全多方计算,签密,不经意传递

A Protocol of Secure Multi-Party Multiplication Based on Signcryption

ZHANG Hua CHEN Zhi-Xiong XIAO Guo-Zhen

(National Key Lab of Integrated Service Network, Xidian University, Xi'an, 710071)

Abstract In this paper, we propose a protocol of secure two-party multiplication using the techniques of signcryption and oblivious transfer and deduce a protocol of secure multi-party multiplication. In the protocol, the adversary can't tamper the message signcrypted by the parties. And the neck-problem, which results from the trusted party participating in the protocol, is avoided. Security is improved.

Keywords Secure multi-party computation, Signcryption, Oblivious transfer

在现实生活中我们经常会碰到这样的问题:两方或多方各自掌握一些秘密,为了实现一个共同的目的,他们需要共享一些信息。安全多方计算协议(SMC)就是解决这种问题的一种途径。而在多方安全计算的许多问题中,秘密乘积都有重要的应用,譬如求解线性规划问题的约束域,求矩阵积,解线性方程组,求矩阵特征值及组密钥协商等。这些问题的解决在信息安全与通信保密中有重要的意义。当前,解决这个问题的一般方法是假定存在一个可信赖部门或可信任第三方实现秘密共享,但是这种方法存在瓶颈问题即:a. 可信任第三方处理大量信息会造成排队等待现象;b. 可信任第三方系统的不安全性会导致秘密泄漏;c. 可信任第三方成为敌手的主要攻击对象。文[1]利用可验证秘密共享方案(VSS)给出的安全多方乘积协议,在多个参与者中实现了两个秘密的乘积运算,但是此协议需要可信任第三方的参与。

签密可以在一个合理的逻辑步骤内同时完成数字签名和共钥加密两项功能,从而大大降低信息的保密认证传输所需的通信和时间代价。采用公钥体制的不经意传递协议无需可信任第三方就可实现信息的安全传递。本文利用签密技术和不经意传递提出一个有效的安全两方乘积协议并用归纳方法得到了一个安全多方乘积协议,实现了多个量的乘积运算。此协议不需要可信任第三方参与,同时可以防止攻击者篡改信息。本文假设参与者是半诚信的;敌手可以搭线窃听和篡改信息但不能阻止协议的执行,且在 k 个参与者中敌手最多可以侵袭 $k-1$ 个参与者。本文第 1 节介绍签密技术和不经意传递技术,第 2 节提出一个使用签密技术的安全两方乘积协议,并在此基础上用归纳的方法得到一个安全多方乘积协议,第 3 节给出一个实例。

1 预备知识

本文提出的协议主要用到签密技术和不经意传递技术。

签密:可以在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能,从而大大降低信息的保密认证传输所需的通信和时间代价。为了便于说明,本文采用文[2]中的签密方案,根据安全性的要求不同也可以使用其它改进的签密方案。方案描述如下:

p 是一个大素数;q 是 $p-1$ 的一个大素因子;g 是在 $\{1,2,\cdots,p-1\}$ 中随机选取的在 Z_p 中乘法阶为 q 的整数;$hash$ 是输出至少为 128bit 的一个单向抗碰撞 hash 函数;(E,D) 是一个对称密码体制的加解密算法;KH_k 是由密钥 k 控制的单向 hash 函数;x_a 是发送的私钥,是从 $\{1,2,\cdots,p-1\}$ 中随机选取的整数;y_a 是发送方的公钥($y_a=g^{x_a} \bmod p$);x_b 是接收方的私钥,y_b 是接收方的公钥($y_b=g^{x_b} \bmod p$);m 是要被保密认证的传送给接收方的消息。签密方案如表 1 所示。

表 1 签密方案

发送方对 m 的签密	密文	接收方对密文(c,r,s)的解签密
随机选取 $x\in\{1,\cdots,q-1\}$ 计算: $(k_1,k_2)=hash(y_b^x \bmod p)$ $c=E_{k_1}(m)$,$r=KH_{k_2}(m)$ $s=x/(r+x_a) \bmod q$	(c,r,s)	计算: $(k_1,k_2)=\text{hash}(y_a g^r)^{x_b} \bmod p)$ $m=D_{k_1}(c)$ 当且仅当 $KH_{k_2}(m)$ $=r$ 时接受 m

不经意传递:即一种协议,它使 A 以 1/2 的概率向 B 传递秘密,B 有一半的机会能收到 A 送来的秘密,也有一半的机会得不到任何有关秘密的信息;B 知道它收到的秘密,而 A 则不知道 B 收到了什么秘密。采用公钥体制的不经意传递协议无需可信任第三方就可实现[3]。

2 安全多方乘积协议

与其他协议不同,本文的协议没有采用可验证秘密共享

*)基金项目:"十五"国家科技预研项目(41001040102)。张 华 硕士研究生,研究方向:密码学,信息安全。陈智雄 博士研究生,研究方向:密码学,信息安全。肖国镇 教授,博士生导师,研究方向:密码学,信息安全。

方案(VSS),而是采用了签密技术和不经意传递技术实现消息的安全认证传输,因此不需要可信任第三方参与。与文[1]相同,协议将一般的求积问题转化为求和问题。协议中 $P=\{P_1,P_2,\cdots,P_k\}$ 表示 k 个参与者的集合,$S=\{S_1,S_2,\cdots,S_k\}$ 表示 P 中参与者所持有的秘密,其中 P_i 持有秘密 S_i。$P=\{P_1,P_2,\cdots,P_k\}$ 共同拥有一个单向抗碰撞 hash 函数和 (E,D),g 是在 $\{1,2,\cdots,p-1\}$ 中随机选取的在 Z_p 中的乘法阶为 q 的整数,$x_{p1},x_{p2},\cdots,x_{pk}$ 是 $P_1,P_2,\cdots,P_k$ 对应的私钥,$y_{p_1},y_{p_2},\cdots,y_{p_k}$ 是 $P_1,P_2,\cdots,P_k$ 的公钥($y_{p_i}=g^{x_{Pi}} \bmod p, i=1,2,\cdots,k$)。

2.1 安全两方乘积协议

设 P_1 有一秘密 S_1,P_2 有一秘密 S_2,当协议结束时 P_1 得到 Q_1,P_2 得到 Q_2,且有 $Q_1+Q_2=S_1S_2$。协议描述如表 2 所示。

表 2 安全两方乘积协议

1. P_1 和 P_2 共有一个数字 $m(2^m$ 很大)。
2. P_1 生成 m 个随机值 $X_1,\cdots,X_m$,且有 $S_1=\sum_{j=1}^{m}X_j$。
3. 从 $j=1,\cdots,m$,P_1 和 P_2 执行如下步骤:
   a. P_1 生成一个秘密的随机数 $k(k=1$ 或 $2)$。
   b. P_1 生成序列 (H_1,H_2),其中 $H_k=X_j$,序列的另一部分是 P_1 随机选取的。P_1 随机选取 $x\in(1,\cdots,q-1)$,用表 1 的方法对 (H_1,H_2) 签密后将密文发送给 P_2。
   c. P_2 接收 P_1 到传来的密文后用表 1 方法解签密,验证所接收到信息的正确性。若没有篡改现象则执行下一步,否则公开发出拒绝接收信息并停止执行。
   d. P_2 计算 $H_iS_2-R_j$,其中 $i=1,2$,R_j 是 P_2 随机选取的,$H_iS_2-R_j$ 中的每一个元素都在 Z_p 中。P_2 对其计算结果签密,具体做法这里不再详述。P_2 将签密后的结果发送给 P_1。
   e. P_1 首先对接收到的信息解签密,确认不存在欺诈后,P_1 使用不经意传递协议取回 $H_kS_2-R_j=X_jS_2-R_j$,否则公开发出拒绝接收信息并停止执行。
4. P_1 得到 $Q_1=\sum_{j=1}^{m}(X_jS_2-R_j)=S_1S_2-\sum_{j=1}^{m}R_j$,$P_2$ 得到 $Q_2=\sum_{j=1}^{m}R_j$。

协议的正确性及安全性

1. 协议使用了不经意传输协议,使得双方发送的信息被猜中的概率为 $1/2^m$。

2. 协议采用了签密技术,防止了因敌手在信息传输过程中对信息的篡改所导致的中间人攻击。文[2]中的签密方案存在的问题已经在一些文献中给出了证明。鉴于对安全性的要求不同,此协议中的签密部分可以采用此签密方案的改进方案,如文[4]中的方案,这里不再作详细的叙述。

3. 协议不需要可信任第三方参与,避免了因此而导致的瓶颈问题以及因为其系统不安全所导致的信息泄露。

4. 在得不到步骤 3 任何信息的情况下,根据 $X_1,\cdots,X_m$ 和 $R_1,R_2,\cdots,R_m$ 的生成方式可知 $X_1,\cdots,X_m$ 和 $R_1,R_2,\cdots,R_m$ 在 Z_p 中均匀分布,敌手要得到 X_i 或 $R_i,i=1,2,\cdots,m$ 无异于在 Z_p 中随机地猜测,那么完全猜对的概率为 $1/p^m$。因为我们所选的 p 很大,所以这个概率是可忽略的。

5. 攻击者要得到参与者的私钥 x_{p_i} 相当于解离散对数问题,这是困难的。此协议没有要求使用秘密信道,所以仅在计算上是安全的。

协议复杂度 协议在整个执行过程中每个参与者执行了 m 次不经意传输协议,$2m$ 次的签密。P_1 在执行步骤 2 时相当于执行了 m 个数的加法运算,其计算复杂度为 $O(\log m)$。P_2 在步骤 3 的 d 步共执行了 $2m$ 次的乘法运算和 $2m$ 次加法运算。P_1,P_2 在步骤 4 的计算复杂度均为 $O(\log m)$。

2.2 安全方乘积协议

P_1 有一个秘密 $S_1,\cdots,P_k$ 有一个秘密 S_k,当协议结束时 P_1 得到 $Q_1,\cdots,P_k$ 得到 Q_k,且有 $\sum_{i=1}^{k}Q_i=\prod_{i=1}^{k}S_i$。

已知 $k=2$ 时协议成立,假设安全的 $k-1$ 方协议是成立的 $(k\geqslant 3)$,则安全 k 方乘积协议描述如表 3 所示。

表 3 安全多方乘积协议

1. $P_1,P_2,\cdots,P_{k-1}$ 使用安全的 $k-1$ 方协议,P_1 得到 $Q'_1,\cdots,P_{k-1}$ 得到 Q'_{k-1},$\sum_{i=1}^{k-1}Q'_i=\prod_{i=1}^{k-1}S_i$。
2. $P_1(Q'_1)$ 和 $P_k(S_k)$ 使用安全的两方协议,P_1 得到 Q_1,P_k 得到 $Q_{k,1}$,$Q_1+Q_{k,1}=Q'_1S_k$。
3. $P_2(Q'_2)$ 和 $P_k(S_k)$ 使用安全的两方协议,P_2 得到 Q_2,P_k 得到 $Q_{k,2}$,$Q_2+Q_{k,2}=Q'_2S_k$。

……

k. $P_{k-1}(Q'_{k-1})$ 和 $P_k(S_k)$ 使用安全的两方协议 P_{k-1} 得到 Q_{k-1},P_k 得到 $Q_{k,(k-1)}$,$Q_{k-1}+Q_{k,(k-1)}=Q'_{k-1}S_k$。

k+1. P_k 估计 $Q_k=Q_{k,1}+\cdots+Q_{k,(k-1)}$ 的值。

k+2. 在第 2 步,P_1 得到 $Q_1,\cdots$,在第 $k+1$ 步,P_k 得到 Q_k,$\sum_{i=1}^{k}Q_i=\prod_{i=1}^{k}S_i$。

协议的正确性及安全性:

命题 1 这个安全多方乘积协议是正确的。

证明:这个安全多方乘积协议只用到了安全两方乘积协议和一个合理的假设(安全方乘积协议成立)。因为安全两方乘积协议的正确性已经在 2.1 节中得到了证明,所以这个安全多方乘积协议也是正确的。

命题 2 任何 $k-1$ 方合谋不能获得另一方的秘密输入。

证明:基于上面的假设,只有 $k-1$ 方时秘密是安全的。下面首先讨论 $P_1,P_2,\cdots,P_{k-1}$ 合谋获得 P_k 的秘密输入的情况。$P_1,P_2,\cdots,P_{k-1}$ 可知道关于秘密 S_k 的 k 个方程:$R_1+R_{k1}=R'S_k,\cdots,R_{k-1}+R_{k(k-1)}=R'_{k-1}S_k$ 和 $\sum_{i=1}^{k}R_i=\prod_{i=1}^{k}S_i$,但有 $k+1$ 个未知值 $R_1,R_2,\cdots,R_{k-1},R_k$ 和 M_k。显然线性程组有无穷解。也就是说 $P_1,P_2,\cdots,P_{k-1}$ 不能获知 P_k 的任何信息。其次,因为 P_k 不知道其它方的任何信息,所以 P_k 与其它 $k-2$ 方合作,不能获知另一方的秘密输入。命题得证。

协议复杂度 当只有两方时需要执行 $\binom{2}{2}=1$ 次安全的两方协议;当有三方时需要执行 $\binom{3}{2}=3$ 次安全的两方协议;当有 k 方时需要执行 $\binom{k}{2}=k(k-1)/2$ 次安全的两方协议。

3 示例

假设 $p=31$,P_1 的秘密 $S_1=5$,P_2 的秘密 $S_2=7$,P_3 的秘密 $S_3=11$,P_1,P_2,P_3,在 Z_{31} 内求 $Q_1+Q_2+Q_3=S_1S_2S_3$。

1. P_1 和 P_2 共有数字 $m=3$。
2. P_1 生成 3 个随机值 $X_1=3,X_2=8,X_3=25$。
3. $j=1$ 时,P_1 和 P_2 执行如下步骤:

a. P_1 生成一个秘密的随机数 k,假设 $k=1$。

b. P_1 生成序列(3,5),5 是 P_1 在 Z_p 中随机选取的。用表 1 的方法对(3,5)签密后将密文发送给 P_2。

c. P_2 接收到 P_1 传来的密文后用表 1 的方法解签密,验证所接收到信息的正确性。若没有篡改现象则执行下一步,否则公开发出拒绝接收的信息并停止执行下一步。

d. P_2 取 $R_1=4$，计算 $H_1S_2-R_1=3\times7-4\equiv17(\text{mod }31)$，$H_2S_2-R_1=5\times7-4\equiv0(\text{mod }31)$，$P_2$ 对其计算结果(17,0)签密，具体做法这里不再详述。P_2 将签密后的结果发送给 P_1。

e. P_1 首先对接收到的信息解签密，确认不存在欺诈后，使用 $1/n$ 不经意传输协议取回 $H_1S_2-R_1=X_1S_2-R_1=17$。

同理 $j=2,3$ 时 P_2 取 $R_2=11,R_3=10$，P_1 得到 $X_2S_2-R_2=14,X_3S_2-R_3=10$。

4. P_1 得到 $Q'_1=\sum_{j=1}^{3}(X_jS_2-R_j)=17+14+10\equiv10(\text{mod }31)$，$P_2$ 得到 $Q'_2=\sum_{j=1}^{3}R_j=4+11+10\equiv25(\text{mod }31)$。

5. 为简单起见，P_1 和 P_3 仍取 $m=3$，P_1 取 $X_1=4,X_2=9,X_3=28$，P_3 取 $R_1=5,R_2=6,R_3=7$，P_1 和 P_3 执行完协议后 P_1 得到 $Q\equiv30(\text{mod }31),Q_{3,1}\equiv18(\text{mod }31)$。$P_2$ 和 P_3 仍取 $m=3$，P_2 取 $X_1=5,X_2=13,X_3=7$，P_3 取 $R_1=8,R_2=10,R_3=16$，P_2 和 P_3 执行完协议后 P_2 得到 $Q_2\equiv24(\text{mod }31),Q_{3,2}\equiv3\text{ mod }(31)$。

6. $Q_3=Q_{3,1}+Q_{3,2}=18+3\equiv21(\text{mod }31)$，$Q_1+Q_2+Q_3=30+24+21\equiv13(\text{mod }31)$，$S_1S_2S_3=5\times7\times11\equiv13\text{ mod }(31)$，所以有 $Q_1+Q_2+Q_3=S_1S_2S_3$。

结束语 多方安全计算在信息和通信安全中占有重要的地位。签密是实现保密认证通信的新理论和技术。本文将两者结合起来，在文[1]和[5]的启发下提出了一个安全两方乘积协议，并由此得到安全多方乘积协议。此协议实现了多个数的乘积运算且不需要仲裁方或可信任第三方参与，避免了因此所导致的瓶颈问题，同时可以防止攻击者篡改信息。但本文假设参与者是半诚信的，恶意参与者的情况仍然是一个值得我们继续研究的问题。

参 考 文 献

1 Maurer U. Secure multi-party computation made simple. In: Proc. of SCN '02, LNCS 2576, 2002
2 Zheng Yuliang. Signcryption and its application in efficient public key solution [A]. In: Proc. of Information Security Workshop (ISW? 7)[C]. springer Verlag. ,1997. 201～218
3 王育民，刘建伟. 通信网的安全——理论与技术. 西安电子科技大学出版社，1999. 357～373
4 Malone-Lee J, Mao W. Two Birds One Stone: Signcryption using RSA. Lecture Notes in Computer Science, Springer-Verlag Heidelberg, 2003, 2612
5 Yao A C. Protocols for secure computation. In: Proc. 23rd IEEE Symposium on Foundation of Computer Science. 1982
6 Brassard G, Crépeau C, Lempel A. All-or-nothing disclosure of secrets. In Advances in Cryptology-Crypo86, Lecture Notes in Computer Science, Volume. 234～238, 1987
7 Du Wenliang, Atallah M J. Secure Multi-party Computation Problems and Their Applications: A Review and Open Problems. Available at: http://citeseer. ist. psu. edu/ 552294. html
8 Goldreich O. Secure multi-party Computation. Working Draft, Version 1. 3 June 24, 2001. Available at: http://www. wisdom. weizmann. ac. il/～oded/ pp. html/

(上接第 49 页)

②存储服务供应商；③需要远程数据备份或有灾难性恢复数据要求的组织；④按照地理分布的，在实时基础上，要求使用同一份数据的组织。例如，需要使用最新工程数据的同一工作队的成员们可以不必按照传统的复制/备份/兼容步骤等候 24 个小时。⑤仅有有限的 IT 资源、基础设施以及经费的公司和研究机构就应该寻找 iSCSI 装置。此装置是通过标准的十亿比特的以太网 CAT-5 铜制电缆起作用的，而电缆在当今的大部分建筑物中都有。

4.4 实际应用

4.4.1 *通过 iSCSI 进行网络储存服务* 在与标准以太网 NIC 连接时可以用到两个 iSCSI 主机总线适配器，而此连接则需通过一个与具有 iSCSI 功能的磁盘阵列(如图 3)连接在一起的功能为十亿比特的转换器。这种构造既适用于第一级的 iSCSI SAN 结构，也适用于第二级的 iSCSI SAN 结构。

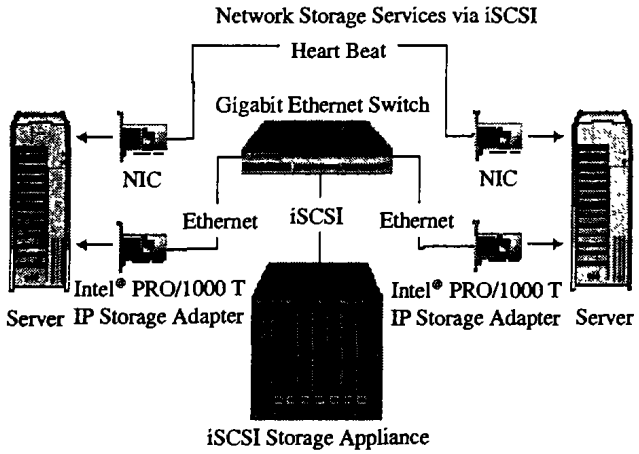

图 3

4.4.2 *ISCSI 主机总线适配器光纤管道磁带备份* ISCSI 主机总线适配器与具有十亿比特以太网转换器相连接，转换器同时连接到 iSCSI 的光纤通道的路由器上，再通过光纤与光纤通道转换器相连，而此光纤通道转换器又与磁带驱动器相连接(如图 4)。这一构造可以利用现有以太网基础设施实现备份和复制功能。

结论 iSCSI 适用于那些数据变化量较大，特别是那些更重视数据存储的安全性或灾难恢复的组织。虽然 iSCSI 技术在存储市场上的应用仍处于幼年期，不过其未来远景是不可限量的。随着功能的不断加强，iSCSI 必将成为存储领域内的核心技术，ISCSI SAN 将无所不在，他将逐步成为 TCP/IP 网络的一部分。

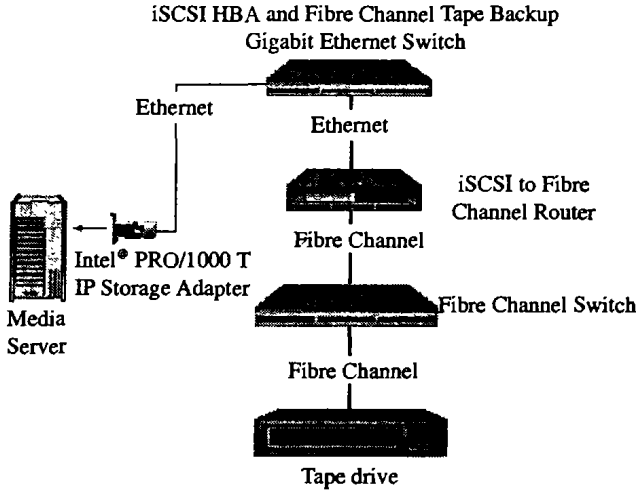

图 4

参 考 文 献

1 http://www. sina. org
2 http://www. ietf. org
3 http://www-cn. netapp. com/solutions/iscsi-technology. html
4 http://publish. it168. com/2004/0819/20040819005201. shtml
5 http://www. cnw. com. cn/issues/article. asp? filename=n12022. txt
6 http://www. cww. net. cn/technique