整数上鲁棒分布式乘法计算方案*

王 宏[1], 冯登国[1,2], 肖国镇[3]

[1](中国科学院 研究生院 信息安全国家重点实验室,北京 100039);
[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100080);
[3](西安电子科技大学 综合业务网国家重点实验室 信息安全与保密研究所,陕西 西安 710071)
E-mail: hong.wang@eyou.com

摘要: 分布式乘法计算是安全多方计算中的重要部分,也是设计门限密码体制的基本协议.应用可验证秘密共享的方法,设计了两种不同情况下的整数环上多项相乘的鲁棒分布式乘法计算方案.其中并行不交互的鲁棒多项相乘的分布式乘法计算方案效率较高,且保持了不交互特性,而另一种方案却能达到最优弹性.

关 键 词: 秘密共享;门限密码学;分布式乘法计算;安全多方计算
中图法分类号: TP309 文献标识码: A

实际密码应用有时需要有一个公认的信任实体,如一个可信任的权威机构或一个防窜扰的设备.但这种信任关系不易实现和达到.一个实用的解决方案就是将信任分布到多方,以使系统能具有既容错又不泄露秘密等鲁棒性.秘密共享使得能分布式地持有秘密.当关于秘密输入的某个应用函数(如签名或解密等)需要计算时,各方利用各自掌握的信息碎片,不揭示秘密,能共同合作计算出函数值(生成签名或解出明文),但这个过程却没有泄露关于秘密的任何其他信息.至今,这类多方计算的研究已取得很多成果.有时,也称这类实用的安全多方计算为"函数共享"或"门限密码学"[1].

分布式乘法计算是安全多方计算中的重要部分.在以往的分布式乘法计算方案中,都存在着大量的交互,使得通信效率很低.Gennaro 等人在文献[2]中提出了鲁棒分布式乘法计算方案,其中每个成员都调用了四步零知识证明协议,因而交互量仍然相当大.M.Abe 基于文献[2],给出了一种新的不交互的鲁棒分布式乘法计算方案[3],该方案设计在标准密码学环境下,应用可验证秘密共享[4]巧妙地避免了直接调用零知识证明,具有非交互性、标准密码学模型下可证明安全以及最优弹性等多种优良特性,同时大大减少了轮复杂度,提高了通信效率.但是,以上方案都是针对两项相乘的,且限于有限域上的计算方案.由于分布式乘法计算协议是安全多方计算和门限密码体制设计的一个基本协议,关于在更一般的应用环境,如整数上的多项相乘计算方案的研究,具有很重要的应用价值.

本文基于文献[3]的思想方法,提出了整数上两种不同情况下的多项相乘的分布式乘法计算方案.基于应用可验证秘密共享,重新设计得到整数上分布式多项相乘方案,保持了不交互的良好性质.重复调用设计基本的两项乘法协议,可得到具有最优弹性的计算方案.这类方案可用于构造一些密码协议,如鲁棒门限 Fiat-Shamir 签名协议.

* 收稿日期: 2001-03-13; 修改日期: 2001-07-05
基金项目: 国家自然科学青年基金资助项目(60025205);国家重点基础研究发展规划 973 资助项目(G1999035802)
作者简介: 王宏(1972－),男,江西玉山人,博士,助理研究员,主要研究领域为网络安全技术,秘密共享与门限密码协议;冯登国(1965－),男,陕西靖边人,博士,研究员,博士生导师,主要研究领域为信息安全理论与技术,密码学理论与技术;肖国镇(1934－),男,吉林四平人,教授,博士生导师,主要研究领域为信息安全理论与技术,编码密码学与信息论.

1 模型及基本模块

1.1 基本模型

信道模型:协议假设的通信网络是同步保密网络.网络是安全和完全的,即任意两个成员服务器的连接是可以相互认证的,且不可搭线窃听的信道.并且,我们还假设有一个广播信道.这种模型假设可使我们集中注意力于高层关键的技术.

成员和攻击者模型:设 P 为成员集, $P=\{1,2,...,n\}$.各成员 $i\in P$ 模型为概率多项式图灵机.攻击者为静态攻击者,最多能入侵并完全控制 t 个服务器.

1.2 整数环上(*t*,*n*)无条件安全可验证秘密共享协议

无条件安全可验证秘密共享是由 Pedersen 首先提出的,我们的版本与文献[5]的版本有所不同.设 N 为 RSA 模数, $L=n!$,g 和 h 均为模 N 的最大阶元,且相互之间模 N 的离散对数对各成员是未知的.秘密 $S\in[0,M]\cap Z$,对偶秘密 $R\in_R[0,N^2M]\cap Z$.如 M=N.

(1) dealer 选取两个 t 次随机多项式 $f(x)$,$d(x)$:

$$f(x)=L^2S+a_1x+a_2x^2+...+a_tx^t,\ d(x)=L^2R+b_1x+b_2x^2+...+b_tx^t,$$

其中 $a_k\in_R\{0,L,2L,...,L^3NM\}$, $b_k\in_R\{0,L,2L,...,L^3N^2M\}$,广播 $E_0=g^Sh^R \bmod N$, $E_k=g^{a_k}h^{b_k} \bmod N$, $k=1,2,...,t$, 通过保密信道发送 $(S_i,R_i)=(f(i),d(i))$ 给成员 $i,i=1,2,\ldots,n$.

(2) 各成员服务器 i 验证:

$$S_i\overset{?}{\in}[0,tn^tL^3NM+L^2M]\cap LZ,\ R_i\overset{?}{\in}[0,tn^tL^3N^2M+L^2N^2M]\cap LZ,$$

$$g^{S_i}h^{R_i}\overset{?}{\equiv}E_0{}^{L^2}\prod_{k=1}^{t}E_k{}^{i^k} \bmod N,$$

若不满足,则广播对 dealer 的 Complaint.dealer 收到后,须广播 (S_i,R_i) ,成员们公开验证.

(3) 若 dealer 收到多于 t 个 Complaint 或拒绝广播或公开验证不通过,则 dealer 被取消资格.

我们记该协议 $INT-(t,n)-US-VSS$ 的执行过程 step1 为

$$IntVSS(S,R)[g,h]\to(S_i,R_i)(E_0,...,E_t),$$

记对 (S_i,R_i) 的验证承诺为

$$VS_i=E_0{}^{L^2}\prod_{k=1}^{t}E_k{}^{i^k} \bmod N.$$

秘密恢复:

(1) 各成员服务器 i 广播对应碎片 (S_i,R_i) ;

(2) 任何成员均可找到集合 $I\subset\{1,2,...,n\}$, $\|I\|=t+1$,且 $\forall i\in I$, (S_i,R_i) 满足上面(2)的验证,然后恢复秘密.

$$S\overset{\Delta}{=}\left(\sum_{i\in I}\prod_{j\in I,j\neq i}(-j)\frac{S_i}{\prod_{k\in I,k\neq j}(j-k)}\right)\Big/L^2.$$

2 分布式乘法计算方案

基于文献[3]的方法,我们给出两种不同情况下的多项相乘分布式乘法计算方案.我们的课题是在成员们已安全地共享了 K 个秘密后,构造协议使得他们能安全地共享这 K 个秘密的积.

假设 K 个秘密 $A_1,A_2,...,A_K$ 已被安全地共享,即

$$IntVSS(A_k,R^k)[g,h]\to(A_{ki},R_i^k)(EA_0^k,...,EA_t^k)\ ,\ k=1,2,...,K,$$

其中的符号与表示请参见文献[3].

2.1 *n*≥(*K*+1)*t*+1分布式乘法计算方案

假设 K 个秘密是被 $INT-(t,n)-US-VSS$ 方案共享的,以下方案均为如此情况.

IDM1-1:每个成员 i 选取 t 次随机多项式,执行相应 $INT-(t,n)-US-VSS$ 方案如下:

$$IntVSS(A_{1i},R_i^1)[g,h]\to(U_{ij}^1,R_{ij}^1)(\langle VA_{1i}\rangle,EU_{i1}^1,...,EU_{it}^1),$$

$$IntVSS(A_{2i},R_i^2)[g,h]\to(U_{ij}^2,R_{ij}^2)(\langle VA_{2i}\rangle,EU_{i1}^2,...,EU_{it}^2),$$

$$IntVSS(A_{2i},R_i^{22})[\langle VA_{1i}\rangle,h]\to(\langle U_{ij}^2\rangle,R_{ij}^{22})(EW_{i0}^2,...,EW_{it}^2),$$

$$IntVSS(A_{ki},R_i^k)[g,h]\to(U_{ij}^k,R_{ij}^k)(\langle VA_{ki}\rangle,EU_{i1}^k,...,EU_{it}^k),$$

$$IntVSS(A_{ki},R_i^{kk})[\langle EW_{i0}^{k-1}\rangle,h]\to(\langle U_{ij}^k\rangle,R_{ij}^{kk})(EW_{i0}^k,...,EW_{it}^k),$$

$$k=3,...,K,$$

$$IntVSS(\prod_{k=1}^K A_{ki},R_i^1\prod_{k=2}^K A_{ki}+\sum_{k=2}^{K-1}R_i^{kk}\prod_{l=k+1}^K A_{li}+R_i^{KK})[g,h]\to(C_{ij},R_{ij})(\langle EW_{i0}^K\rangle,EC_{i1},...,EC_{it}).$$

IDM1-2:各成员 j 检查从成员 i 收到的数据是否在正确的范围内,并验证如下:

$$g^{U_{ij}^1}h^{R_{ij}^1}\equiv VA_{1i}{}^{L^2}\prod_{l=1}^t EU_{il}^1{}^{j^l}\bmod N,$$

$$g^{U_{ij}^2}h^{R_{ij}^2}\equiv VA_{2i}{}^{L^2}\prod_{l=1}^t EU_{il}^2{}^{j^l}\bmod N,$$

$$VA_{1i}{}^{U_{ij}^2}h^{R_{ij}^{22}}\equiv EW_{i0}^2{}^{L^2}\prod_{l=1}^t EW_{il}^2{}^{j^l}\bmod N,$$

$$g^{U_{ij}^k}h^{R_{ij}^k}\equiv VA_{ki}{}^{L^2}\prod_{l=1}^t EU_{il}^k{}^{j^l}\bmod N,$$

$$EW_{i0}^{k-1}{}^{U_{ij}^k}h^{R_{ij}^{kk}}\equiv EW_{i0}^k{}^{L^2}\prod_{l=1}^t EW_{il}^k{}^{j^l}\bmod N,$$

$$k=3,...,K,$$

$$g^{C_{ij}}h^{R_{ij}}\equiv EW_{i0}^K{}^{L^2}\prod_{l=1}^t EC_{il}{}^{j^l}\bmod N.$$

若验证失败,则要求成员 i 广播他秘密发送给成员 j 的全部数据.如果这些数据能通过 t+1 个以上成员如上验证,成员 j 必须接受成员 i 秘密发送给他的全部数据.如果成员 i 拒绝广播或广播的数据不能通过 t+1 个以上成员的验证,那么成员 i 被取消资格.

注:设 I 为资格成员集,则因为 $n\ge(K+1)t+1$ 且攻击者最多能控制 t 个成员,所以 $\|I\|\ge Kt+1$.

IDM1-3:各成员 j 计算

$$S_j=\sum_{i\in I}\lambda_{i,I}C_{ij},\ R_j=\sum_{i\in I}\lambda_{i,I}R_{ij},$$

$$ES_l=\prod_{i\in I}EC_{il}^{\lambda_{i,I}}\bmod N,l=0,...,t,\ EC_{i0}=EW_{i0}^K.$$

2.2 $n\ge 2t+1$分布式乘法计算方案

设文献[3]中的协议为 2DMP,我们用 $INT-(t,n)-US-VSS$ 替代 PedersenVSS 改造该协议.我们称改造后的子协议为 I2DMP.

I2DMP-1:每个成员 i 选取 t 次随机多项式,执行相应 $INT-(t,n)-US-VSS$ 方案如下:

$$IntVSS(A_i,R_i^a)[g,h]\to(A_{ij},R_{ij}^a)(\langle VA_i\rangle,EA_{i1},...,EA_{it}),$$

$$IntVSS(A_i,R_i^{ab})[\langle VB_i\rangle,h]\to(\langle A_{ij}\rangle,R_{ij}^{ab})(EAB_{i0},...,EAB_{it}),$$

$$IntVSS(A_i\cdot B_i,R_i^b\cdot A_i+R_i^{ab})[g,h]\to(C_{ij},R_{ij}^c)(\langle EAB_{i0}\rangle,EC_{i1},...,EC_{it}).$$

I2DMP-2:各成员 j 检查从成员 i 收到的数据是否在正确的范围内,并验证如下:

$$g^{A_{ij}}h^{R_{ij}^a}\equiv VA_i{}^{L^2}\prod_{l=1}^t EA_{il}{}^{j^l}\bmod N,$$

$$VB_i{}^{A_{ij}}h^{R_{ij}^{ab}}\equiv EAB_{i0}{}^{L^2}\prod_{l=1}^t EAB_{il}{}^{j^l}\bmod N,$$

$$g^{C_{ij}}h^{R_{ij}^c}=EAB_{i0}{}^{L^2}\prod_{l=1}^t EC_{il}{}^{j^l}\bmod N.$$

若验证失败,则成员 j 广播对 i 的 Complaint,并执行子协议 DQ(disqualified protocol),同文献[3].

I2DMP-3:设 I 为资格成员集,且满足 $\|I\|\ge 2t+1$.各成员 j 计算

$$C_j=\sum_{i\in I}\lambda_{i,I}C_{ij},\ R_j^c=\sum_{i\in I}\lambda_{i,I}R_j^c,$$

$$EC_l=\prod_{i\in I}EC_{il}^{\lambda_{i,I}} \bmod N, l=0,...,t,\ EC_{i0}=EAB_{i0}.$$

注:若 $n\ge 3t+1$,则不需要执行 DQ 步骤.若 $3t+1>n\ge 2t+1$,$\|I\|<2t+1$,可利用碎片恢复技术得到 $\|I\|\ge 2t+1$的资格成员集,具体如文献[6]所述.

我们循环调用协议 I2DMP,可得到 $n\ge 2t+1$分布式 K 项乘法计算协议 IDM2.

IDM2-1:设 $A=A_1$, $B=A_2$,执行 I2DMP.

IDM2-2:设 $A=L^4AB$,B=A_3,执行 I2DMP.

IDM2-3:如此类推,执行 K–2 次 IDM2-2.

3 安全性分析

引理 **1**. 令 $\gamma\in[1,N]$, $f(x)=L^2S+a_1x+a_2x^2+...+a_tx^t$, $d(x)=L^2R+b_1x+b_2x^2+...+b_tx^t$,其中 $S\in[0,N]$, $R\in[0,N^3]$, $a_k\in_R\{0,L,2L,...,L^3N^2\}$, $b_k\in_R\{0,L,2L,...,L^3N^3\}$, $k=1,2,...,t$.令 Λ为 t 个成员服务器的集合,则对 $\forall\widetilde{S}\in[0,N]$,至少以概率 $1-(4t+2)/N$ 存在多项式 $\widetilde{f}(x)=L^2\widetilde{S}+\widetilde{a}_1x+\widetilde{a}_2x^2+...+\widetilde{a}_tx^t$ 和 $\widetilde{d}(x)=\widetilde{b}+\widetilde{b}_1x+\widetilde{b}_2x^2+...+\widetilde{b}_tx^t$,其中 $\widetilde{a}_k\in_R\{0,L,2L,...,L^3N^2\}$, $\widetilde{b}_k\in_R\{0,L,2L,...,L^3N^3\}$, $k=1,2,...,t$, $\widetilde{b}=L^2(\gamma S+R-\gamma\widetilde{S})$,使得对 $\forall i\in\Lambda$ 都有 $f(i)=\widetilde{f}(i)$, $d(i)=\widetilde{d}(i)$ 成立,且 $\gamma f(x)+d(x)=\gamma\widetilde{f}(x)+\widetilde{d}(x)$.

证明:参见文献[6]的引理 2 的证明.

引理 **2(**正确性**)**. 若所有成员诚实地执行协议 IDM1,则每个成员 $i\in P$ 得到碎片 (S_i,R_i) 和承诺值 $(ES_0,ES_1,...,ES_t)$ 且满足 $g^{S_i}h^{R_i}\equiv ES_0^{L^2}\prod_{l=1}^{t}ES_l^{i^l} \bmod N$,并对任意成员集合 $Q\subseteq P$, $\|Q\|\ge t+1$,能计算出 $\prod_{k=1}^{K}A_k$,即 K 个秘密的乘积.

简要证明:由协议 $INT-(t,n)-US-VSS$ 的秘密恢复算法,可以有 $L^2\prod_{k=1}^{K}A_{ki}=\sum_{j\in Q}\lambda_{j,Q}C_{ij}$. 然而 $L^{2K}\prod_{k=1}^{K}A_k=\sum_{i\in I}\lambda_{i,I}\prod_{k=1}^{K}A_{ki}$, $S_j=\sum_{i\in I}\lambda_{i,I}C_{ij}$,故有 $\prod_{k=1}^{K}A_k=(\sum_{j\in Q}\lambda_{j,Q}S_j)/L^{2K+1}$.

引理 **3(**安全性**)**. 设成员集 $\Lambda\subset P$,且 $\|\Lambda\|\le t$.令 $View_\Lambda$ 为 Λ中成员执行协议 IDM1 的所有识见,而 $View_\Lambda{}^{\sim}$ 为 Λ 中成员以 $(\widetilde{A}_k,\widetilde{R}_k),k=1,...,K$ 为输入执行 IDM1 的所有识见,且满足 $g^{A_k}h^{R_k}\equiv g^{\widetilde{A}_k}h^{\widetilde{R}_k} \bmod N$,则 $View_\Lambda$ 与 $View_\Lambda{}^{\sim}$ 是统计上不可区分的.

简要说明:由引理 1 之结论,又如文献[3]引理 3 方法构造模拟机协议 SIM,即可证明协议 IDM1 的安全性.

引理 **4(**鲁棒性**)**. 设成员集 $\Lambda\subset P$ 为被入侵控制成员集.若 $\|\Lambda\|\le t$ 且 $n\ge(K+1)t+1$,则各成员 $i\in P\setminus\Lambda$ 执行协议 IDM1 后得到正确的碎片 (S_i,R_i) 和承诺值 $(ES_0,ES_1,...,ES_t)$.

简要证明:证明是显然的,设 I 为资格成员集,则因为 $n\ge(K+1)t+1$ 且攻击者最多能控制 t 个成员,所以 $\|I\|\ge Kt+1$.故各成员 $i\in P\setminus\Lambda$ 执行协议 IDM1 后得到正确的碎片和承诺值.需要说明的是必须有 $A_{ki}\ne 0$,从而使得计算 $\log_h EW_{i0}^k$ 是不可行的.而我们对各 A_k 是安全共享的,故 $A_{ki}=0$ 的概率小于 $1/N$,而 RSA 模数 N 一般为 1024bits,所以可以忽略这种情况.

协议 IDM2 的安全性分析同文献[3],秘密积的恢复为 $\prod_{k=1}^{K}A_k=(\sum_{j\in Q}\lambda_{j,Q}S_j)/L^{4(k-2)+2}$.

4 结束语

我们基于文献[3]提出的方法,给出了整数环上多项相乘的鲁棒分布式乘法计算方案.该方案在 $n\ge(K+1)t+1$ 时是不交互的,可并行的,且鲁棒性较好.多次调用文献[3]提出的子协议,可实现 $n\ge 2t+1$ 串行的鲁棒多项相乘的分布式乘法计算方案.并行不交互鲁棒多项相乘的分布式乘法计算方案效率更高,而串行的多项相乘的分布式乘法计算协议却能达到最优伸展性 $n\ge 2t+1$.另外,这类方案可改造成对抗移动攻击和自适应

攻击,是进一步研究的课题.

References:

[1] Desmedt, Y.G., Frankel, Y. Threshold cryptosystems. In: Brassard, G., ed. Advances in Cryptology-CRYPTO'89. Volume 435 of LNCS, Berlin: Springer-Verlag, 1990. 307~315.

[2] Gennaro, R., Rabin, M., Rabin, T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proceedings of the 17th ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1998. 101~111.

[3] Masayuki, Abe. Robust distributed multiplication without interaction. In: Wiener, M., ed. Advances in Cryptology-CRYPTO'99. Volume 1666 of LNCS, Berlin: Springer-Verlag, 2000. 130~147.

[4] Pedersen, T.P. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J., ed. Advances in Cryptology-CRYPTO'91. Volume 576 of LNCS, Berlin: Springer-Verlag, 1992. 129~140.

[5] Frankel, Y., Yung, M. Adaptively-Secure distributed public key systems. In: Proceedings of the ESA'99. Volume 1643 of LNCS, Berlin: Springer-Verlag, 1999. 4~27.

[6] Herzberg, A., Jarecki, S., H., *et al*. Proactive secret sharing or: how to cope with perpetual leakage. In: Coppersmith, D., ed. Advances in Cryptology-CRYPTO'95. Volume 963 of LNCS, Berlin: Springer-Verlag, 1995. 339~352.

Robust Distributed Multiplication Schemes over Integer*

WANG Hong[1], FENG Deng-guo[1,2], XIAO Guo-zhen[3]

[1](*State Key Laboratory of Information Security*, *Postgraduate Research Institute*, *The Chinese Academy of Sciences*, *Beijing* 100039, *China*);

[2](*State Key Laboratory of Information Security*, *Institute of Software*, *The Chinese Academy of Sciences*, *Beijing* 100080, *China*);

[3](*Institute of Information Security and Privacy*, *State Key Laboratory of Integrate Service Network*, *Xidian University*, *Xi'an* 710071, *China*)

E-mail: hong.wang@eyou.com

Abstract: Distributed multiplication computation is an important part of secure multi-party computation and a basic protocol of threshold cryptography. Based on the verifiable secret sharing techniques, two robust distributed multiple multiplication schemes over integer are presented. One of them, the parallelizable non-interactive scheme is more efficient, and remains the property of non-interaction. The other can achieve the optimal resilience.

Key words: secret sharing; threshold cryptography; distributed multiplication computation; secure multi-party computation

* Received March 13, 2001; accepted July 5, 2001

Supported by the Youth Foundation of the National Natural Science of China under Grant No.60025205; the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802