基于秘密共享模数的一般性多方求逆协议

胡华明 周展飞

(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 Catalano、Gennaro 和 Halevi 提出了一个实用的基于秘密共享模数的分布式求逆协议,然而他们仅仅考虑了门限敌手结构的情况.文中考虑了一般敌手结构的情况,针对半诚实敌手和恶意敌手,利用 Damgård 和 Thorbek 提出的线性整数秘密共享方案,分别构造了一个多方模求逆协议.该协议在敌手结构是 Q^2(对应 Q^3 以及强 RSA 假设)的条件下针对半诚实(对应恶意)敌手是安全的.该协议是 Catalano 等人方案的一个推广,可以用来分布式地计算 RSA 私钥以及构造标准模型下安全的分布式 Gennaro-Halevi-Rabin、Cramer-Shoup 和 Mames-Joye 签名方案.另外,文中的构造方法也是对环上的安全多方协议构造方法的一个有力补充.

关键词 模求逆;一般敌手结构;线性整数秘密共享;乘性张成方案;分布式 RSA 签名

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.01040

General Multi-Party Protocol for Computing Inverses Over a Shared Secret Modulus

HU Hua-Ming ZHOU Zhan-Fei

(*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract Catalano, Gennaro and Halevi proposed a practical distributed protocol for computing inverses over a shared secret modulus, however they only considered threshold adversary structures. In this paper the authors consider general adversary structures, construct two multi-party inversion protocols using linear integer secret sharing schemes proposed by Damgård and Thorbek, one for the semi-honest adversary model, and the other for the malicious adversary model. The protocol is secure against semi-honest (resp. malicious) adversaries if the adversary structure is Q^2 (resp. Q^3 as well as the strong RSA assumption). The protocol is a generalization of Catalano et al.'s, and can be used for distributed computation of the private RSA key, as well as for the construction of distributed variants for the secure signature schemes in the standard model proposed by Gennaro-Halevi-Rabin, Cramer-Shoup and Mames-Joye. In addition, the construction method is a useful supplement to the construction of multi-party protocols over rings.

Keywords modular inversion; general adversary structure; linear integer secret sharing; multiplicative span program; distributed RSA signature

1 引 言

本文考虑基于秘密共享模数进行求逆的问题,具体来讲就是:n 个参与方,在秘密共享 ϕ 的前提下,给定素数 e,如何有效地分布式共享 $e^{-1} \bmod \phi$?称解决该问题的协议为分布式模求逆协议.如果 ϕ 为 RSA 模数 N 的欧拉函数,即 $\phi=\phi(N)$,则相应的

收稿日期:2010-01-25;最终修改稿收到日期:2010-05-17.本课题得到国家自然科学基金(60573004)、国家"九七三"重点基础研究发展规划项目基金(2007CB311202)资助.**胡华明**,男,1984 年生,硕士,目前主要从事秘密共享与分布式数字签名方案的研究.E-mail: huaminghu@gmail.com. **周展飞**,男,1969 年生,博士,副研究员,研究方向为秘密共享、门限密码学等安全协议.

分布式模求逆协议可用于分布式生成 RSA 私钥以及构造标准模型下安全的分布式 Gennaro-Halevi-Rabin[1]、Cramer-Shoup[2] 和 Mames-Joye[3] 签名方案. 上述两个应用都需要高效的模求逆协议，尤其是后者，这是因为每次签名时都要使用不同的素指数 e 来运行模求逆协议. 因此设计高效的分布式模求逆协议具有现实意义.

1.1　相关工作

2000 年，Catalano、Gennaro 以及 Halevi[4] 针对上述分布式模求逆问题提出了一个高效的解决方案. 他们的基本思想是利用扩展的欧几里德算法（记为 GCD 运算）来计算 $e^{-1} \bmod \phi$. 他们采用了整数环上的秘密共享方案来避免 $\mathbb{Z}_{\phi(N)}$ 上的求逆运算. 然而，Catalano 等人的方案[4] 考虑的仅仅是门限敌手结构的情况，也即假设所有的参与方被攻破或者被收买的难度是相同的，唯一起决定作用的是被攻破或者被收买的参与方人数. 然而，在现实当中，可能某些参与方会比其他参与方更可靠一些，因此需要以一种更灵活的方式来明确地指出哪些参与方是非授权的，也即，需要一般性的敌手结构.

Cramer、Damgård 和 Maurer[5] 提出了利用有限域上的线性秘密共享方案来构造相同敌手结构的安全多方协议，他们给出了有限域上单调张成方案的乘性性质. 后来，Cramer、Fehr 等人[6] 又将文献[5]扩展到了任意的含 1 交换环上，证明了环上安全多方计算协议的存在性，并给出了整数张成方案的乘性性质. 利用乘性性质，Cramer、Fehr 等人[6] 使用一般敌手结构上的黑箱秘密共享（Black-Box Secret Sharing，BBSS）方案[7] 构造了一个非常有效的安全多方计算协议. 由于采用了黑箱秘密共享方案，在环上做运算时需要黑箱调用.

Damgård 和 Thorbek[8] 提出了线性整数秘密共享（Linear Integer Secret Sharing，LISS）方案来构造分布式 RSA 签名方案. 在一个 LISS 方案中，秘密为选自一个公开区间的整数，每个份额（share）为秘密和一些随机整数的线性组合，秘密的重构也是通过计算授权集中所有份额的一个整系数线性组合得到.

LISS 方案与 BBSS 方案[7] 有着紧密的联系，但两者并不相同. 在 BBSS 方案中，秘密为取自于任意的有限 Abel 群中的元素，所有的运算都是在该群中完成，对于环上的计算和元素的选取，需要通过黑箱调用来完成. 而在 LISS 方案中，所有的运算都是在整数环上进行.

1.2　我们的贡献

Catalano 等人[4] 的方案只考虑了门限敌手结构的情况，为此本文给出了一般敌手结构上的多方模求逆协议，首先构造了一个半诚实敌手模型下的简单高效的安全多方模求逆协议，该协议在给定保密信道的前提下以及敌手结构是 Q^2 的条件下是无条件安全的. 然后又在半诚实敌手模型下的协议基础上增加了鲁棒性，将其改造为恶意敌手模型下的多方模求逆协议. 该协议在强 RSA 假设下以及敌手结构是 Q^3 的条件下是安全的. 协议的鲁棒性是通过可验证线性整数秘密共享（Verifiable Linear Integer Secret Sharing，VLISS）方案以及一个零知识证明协议实现的. 该 VLISS 方案是 Pedersen-VSS[9] 的一般敌手结构上的变体. 相应的零知识证明协议是统计零知识的基于强 RSA 假设绑定的.

本文的想法主要来源于文献[5-6]，即利用敌手结构为 $\mathfrak{A}$ 的线性秘密共享方案来构造相同敌手结构的多方计算协议. 为了避免 $\mathbb{Z}_{\phi(N)}$ 上的求逆问题，与文献[6]中采取黑箱秘密共享方案不同，本文采用了敌手结构为 $\mathfrak{A}$ 的 LISS 方案来构造针对 $\mathfrak{A}$ 敌手安全的多方模求逆协议，这样可以在整数环上做所有运算，从而避免了黑箱调用. 因此本文构造多方协议的方法也是对文献[6]的一个有力补充.

1.3　本文的组织结构

第 2 节将介绍一些预备知识；第 3 节是本文的重点，3.1 节给出协议的系统模型，3.2 节给出多方模求逆协议及其安全性的定义，3.3 节和 3.4 节分别介绍半诚实敌手模型下和恶意敌手模型下的多方模求逆协议，并给出安全性证明，3.5 节简单分析协议的效率；第 4 节总结全文.

2　张成方案和线性整数秘密共享

2.1　整数张成方案

Karchmer 和 Wigderson[10] 引入了有限域上的单调张成方案（Monotone Span Programs，MSP），并证明了 MSP 和域上的线性秘密共享方案是一一对应的. 后来，Damgård 和 Thorbek[8] 提出了线性整数秘密共享方案，并证明了整数张成方案（Integer Span Programs，ISP），即 $\mathbb{Z}$ 上的单调张成方案，与线性整数秘密共享方案有着类似的对应关系.

定义 1.　设 $P=\{P_1,\cdots,P_n\}$ 为 n 个参与方组

成的集合，称 $\Gamma\subset 2^P$ 为 P 上的存取结构，如果 $\varnothing\notin\Gamma$ 且 Γ 满足：$\forall A\in\Gamma, A'\supseteq A$，则 $A'\in\Gamma$. 称 $\mathfrak{A}\subset 2^P$ 为 P 上的敌手结构，如果 $\overline{\mathfrak{A}}=2^P\setminus\mathfrak{A}$ 是一个存取结构.

考虑 $\mathbb{Z}$ 上的一个 l 行 m 列矩阵 $\boldsymbol{M}$（记作 $\boldsymbol{M}\in\mathbb{Z}^{l\times m}$），一个标号函数 $\psi:\{1,\cdots,l\}\to P$，ψ 为满射以及目标向量 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}^m$. ψ 以 P 中的参与方标记 $\boldsymbol{M}$ 的行，不同的行可以有相同的标记，因此可以看作是每个参与方拥有 $\boldsymbol{M}$ 的一行或者多行. 如果 $A\subseteq P$，则 $\boldsymbol{M}_A$ 表示 $\boldsymbol{M}$ 中由行 i 组成的矩阵，其中 $\psi(i)\in A$，l_A 表示 $\boldsymbol{M}_A$ 的行数. 类似地，如果 $\boldsymbol{x}$ 表示任意的 l 维向量，则 $\boldsymbol{x}_A$ 表示 $\boldsymbol{x}$ 中由坐标 i 标识的部分向量，其中 $\psi(i)\in A$. 如果 $A=\{P_i\}$，则用 $\boldsymbol{M}_i,\boldsymbol{x}_i,l_i$ 代替 $\boldsymbol{M}_A,\boldsymbol{x}_A,l_A$. 最后，$\mathrm{im}(\cdot)$ 和 $\ker(\cdot)$ 分别表示矩阵对应的像(image)和核(kernel).

定义 2. 设 $\mathfrak{M}=(\mathbb{Z},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$ 为如上定义的四元组，Γ 为 P 上的一个存取结构. 称 $\mathfrak{M}$ 为存取结构 Γ 或者敌手结构 $\mathfrak{A}=\overline{\Gamma}$ 对应的整数张成方案(ISP)，如果任意的 $A\subseteq P$ 都满足：

(1) 如果 $A\in\Gamma$，则存在 $\boldsymbol{\lambda}_A=(\lambda_1,\cdots,\lambda_{l_A})^{\mathrm{T}}\in\mathbb{Z}^{l_A}$，使得 $\boldsymbol{M}_A^{\mathrm{T}}\boldsymbol{\lambda}_A=\boldsymbol{\varepsilon}$，其中 $\boldsymbol{\lambda}_A$ 被称为 A 所对应的张成向量；

(2) 如果 $A\notin\Gamma$，则存在 $\boldsymbol{\kappa}_A=(\kappa_1,\cdots,\kappa_m)^{\mathrm{T}}\in\mathbb{Z}^m$，使得 $\boldsymbol{M}_A\boldsymbol{\kappa}_A=\boldsymbol{0}$，其中 $\kappa_1=1$，$\boldsymbol{\kappa}_A$ 被称为 A 所对应的消去向量.

有时也称 $\mathfrak{M}$ 计算 Γ 或 $\mathfrak{A}$. 定义 $\lambda_{\max}=\max\{|a|\ |a$ 为某一张成向量中的元素$\}$，$\kappa_{\max}=\max\{|b|\ |b$ 为某一消去向量中的元素$\}$.

注 1. 由线性代数的基本知识可知，由 $\boldsymbol{\kappa}_A\in\ker(\boldsymbol{M}_A)$ 且 $\kappa_1=1$ 可推出 $\boldsymbol{\varepsilon}\notin\mathrm{im}(\boldsymbol{M}_A^{\mathrm{T}})$，然而另一个方向一般只在有限域内成立.

2.2 线性整数秘密共享

现在引入 Damgård 和 Thorbek[8] 提出的线性整数秘密共享(Linear Integer Secret Sharing, LISS)方案. 在 LISS 方案中，秘密为选自一个公开区间的整数，每个份额是秘密和分发者(dealer)随机选取的一些整数的线性组合. 秘密的重构也是通过计算一个授权集中份额的整系数线性组合来完成.

设 P,Γ 的定义如前，现在有一个分发者(dealer) $\mathfrak{D}$ 想在 P 对应的参与方中共享一个取自公开区间 $[0,N]$ 的秘密 s，对应的存取结构是 Γ. 为了实现上述目标，$\mathfrak{D}$ 构造如下的秘密共享方案，称之为 LISS 方案：$\mathfrak{D}$ 首先构造一个计算 Γ 的 ISP $\mathfrak{M}$（构造方法详见文献[8]的完整版），称 $\mathfrak{M}$ 中的矩阵 $\boldsymbol{M}$ 为分发矩阵. 然后 $\mathfrak{D}$ 选择一个分发向量 $\boldsymbol{\rho}=(s,\rho_2,\cdots,\rho_m)^{\mathrm{T}}$，其中 s 为秘密，ρ_i 为均匀随机选自 $[0,\kappa_{\max}(m-1)2^kN]$ 的整数，$2\le i\le m$，k 为一个安全参数. $\mathfrak{D}$ 通过下式来共享秘密 s：

$$\boldsymbol{M}\boldsymbol{\rho}=(s_1,\cdots,s_l)^{\mathrm{T}} \tag{1}$$

记每个 s_i 为一个份额，$1\le i\le l$. $\mathfrak{D}$ 将第 i 个份额秘密地发送给参与方 $\psi(i)$. 记参与方 P_i 的所有份额为 $\boldsymbol{s}_{P_i}$，参与方集合 A 的所有份额为 $\boldsymbol{s}_A$.

定义 3. 称一个 LISS 方案是正确的，如果份额 $\boldsymbol{s}_A$ 和 A 的张成向量的线性组合可以重构秘密 s，其中 A 为任意一个授权集.

定义 4. 称一个 LISS 方案是保密的，如果对于公开区间内的任意两个秘密 s,s'，独立随机的掷币 r,r' 以及任意的非授权集 A，$\boldsymbol{s}_A$ 和 $\boldsymbol{s}'_A$ 的分布是统计不可区分的，其中 $\boldsymbol{s}_A$ 为由 s,r,k 所生成的份额，$\boldsymbol{s}'_A$ 为由 s',r',k 所生成的份额.

显然，定义 2 中的第一个条件使得方案是正确的，因为对于任意的授权集 A 通过计算份额的线性组合都能够重构出秘密，也即存在一个张成向量 $\boldsymbol{\lambda}_A\in\mathbb{Z}^{l_A}$ 使得 $\boldsymbol{M}_A^{\mathrm{T}}\boldsymbol{\lambda}_A=\boldsymbol{\varepsilon}$，从而有 $\boldsymbol{s}_A^{\mathrm{T}}\boldsymbol{\lambda}_A=(\boldsymbol{M}_A\boldsymbol{\rho})^{\mathrm{T}}\boldsymbol{\lambda}_A=\boldsymbol{\rho}^{\mathrm{T}}(\boldsymbol{M}_A^{\mathrm{T}}\boldsymbol{\lambda}_A)=\boldsymbol{\rho}^{\mathrm{T}}\boldsymbol{\varepsilon}=s$.

下面的引理证明了定义 2 中第 2 个条件是保证方案是保密的充分条件.

引理 1. 如果 $s\in[0,N]$，而且对于所有的 $2\le i\le m$，ρ_i 都是均匀随机地选自 $[0,\kappa_{\max}(m-1)2^kN]$，则由 $\mathfrak{M}$ 得来的 LISS 方案是保密的(证明请参见文献[8]).

从上面的介绍可以看到，ISP 与线性整数秘密共享方案是一一对应的. 可以看到使用 ISP 来描述协议会更加方便，因此后续的协议将使用 ISP 来描述 LISS.

2.3 乘性张成方案

Cramer、Damgård 以及 Maurer[5] 引入了有限域上张成方案的乘性性质. 后来 Cramer、Fehr 等人[6] 将乘性性质引入到了任意含 1 交换环上的张成方案当中. 乘性性质的本质是要求两个共享秘密的乘积可以由本地份额乘积的线性组合重构得到. 然而在某些情况下，给定相应的张成方案，并不清楚秘密以及份额将选自于哪个环，因此 Cramer、Fehr 等人[6] 将乘性性质定义为张成方案自身的性质. 该性质在文献[6]中被用来构造门限黑箱安全多方计算协议，本文将该性质具体到整数环 $\mathbb{Z}$ 上，然后利用乘

性 ISP 来构造一般敌手结构下的多方模求逆协议.

设 $\mathfrak{M}=(\mathbb{Z},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$ 为敌手结构 $\mathfrak{A}$ 对应的 ISP. 下面的定义是文献[6]中定义 3 的一种特殊情况.

定义 5.　称张成方案 $\mathfrak{M}$ 是乘性的，如果存在一个块对角矩阵 $\boldsymbol{D}\in\mathbb{Z}^{t\times t}$，使得 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{D}\boldsymbol{M}=\boldsymbol{\varepsilon}\boldsymbol{\varepsilon}^{\mathrm{T}}$，$\boldsymbol{D}$ 被称为重构矩阵. 块对角矩阵可按如下理解：设 $\boldsymbol{D}$ 的行和列都被 ψ 所标记，那么 $\boldsymbol{D}$ 中的非零元素都被集中在块 $\boldsymbol{D}_1,\cdots,\boldsymbol{D}_n$ 中，使得对于任意的 $P_i\in P$，$\boldsymbol{D}_i$ 中的行和列都被 P_i 所标记.

称 $\mathfrak{M}$ 是强乘性的，如果对于任意的参与方集合 $A\in\mathfrak{A}$，$\mathfrak{M}_{\bar{A}}$ 是乘性的.

设 K 为一个含 1 的交换环，Q^2，Q^3 分别表示敌手结构中的任意两个和三个集合的并集都不等于参与者集合 P. Cramer、Fehr 等人[6]证明了对于任意的敌手结构 $\mathfrak{A}$，在 K 上存在一个(强)乘性张成方案 $\mathfrak{M}$ 当且仅当 $\mathfrak{A}$ 是 $(Q^3)Q^2$ 的. 本文将考虑一种特殊情况，即 $K=\mathbb{Z}$. 因此有如下相似的结论.

定理 1.　对于任意的敌手结构 $\mathfrak{A}$，存在一个(强)乘性 ISP $\mathfrak{M}$ 当且仅当 $\mathfrak{A}$ 是 $(Q^3)Q^2$ 的. 证明请参见文献[5,6,11].

与域上的情况类似，环上的乘性性质也可以保证分布式地计算两个共享秘密的乘积. 设 $s,s'\in[0,N]$ 为任意的两个秘密，令 $\boldsymbol{s}=\boldsymbol{M}\boldsymbol{\rho}$ 以及 $\boldsymbol{s}'=\boldsymbol{M}\boldsymbol{\rho}'$ 为 s，s' 所对应的份额，则乘积 ss' 可表示为 $ss'=\boldsymbol{\rho}^{\mathrm{T}}\boldsymbol{\varepsilon}\boldsymbol{\varepsilon}^{\mathrm{T}}\boldsymbol{\rho}'=\boldsymbol{\rho}^{\mathrm{T}}\boldsymbol{M}^{\mathrm{T}}\boldsymbol{D}\boldsymbol{M}\boldsymbol{\rho}'=(\boldsymbol{M}\boldsymbol{\rho})^{\mathrm{T}}\boldsymbol{D}(\boldsymbol{M}\boldsymbol{\rho}')=\boldsymbol{s}^{\mathrm{T}}\boldsymbol{D}\boldsymbol{s}'=\sum_i\boldsymbol{s}_i^{\mathrm{T}}\boldsymbol{D}_i\boldsymbol{s}_i'$，也即根据 $\boldsymbol{D}$ 的特殊形式，ss' 可写为本地可计算值的和.

3　多方模求逆协议

3.1　系统模型

网络模型. 考虑由集合 $P=\{P_1,\cdots,P_n\}$ 中的 n 个参与方组成的网络. 任意两个参与方之间都有一个保密的点对点信道，除此之外，所有的参与方还共享一个广播信道①. 假设通信是同步的.

敌手模型. 通常用一个外部敌手来模仿不诚实的参与方，外部敌手可以收买(corrupt)某些参与方集合. 本文考虑下面两种类型的敌手：

(1) 半诚实的. 敌手获得了被收买的参与方所掌握的所有信息，但并不干涉他们的行为，被收买的参与方仍然忠实地执行协议.

(2) 恶意的. 敌手完全控制了被收买的参与方. 被收买的参与方可能会破坏或者终止协议，或者任意地背离协议的运行.

诚实的参与方(至少初始时)并不知道哪些参与方被收买了. 敌手的收买能力由敌手所能收买的参与方集合组成的子集簇-敌手结构 $\mathfrak{A}$ 来表征. 本文假设敌手是静态的，也即在协议运行之前，敌手已经确定了要收买的参与方，而且在协议运行过程当中不再改变.

3.2　多方模求逆协议的定义

一个多方模求逆协议是一个 $(\mathfrak{A},P)$ 协议，P 中所有的参与方共享一个秘密模数 ϕ (P_i 的份额为 $\boldsymbol{\phi}_{P_i}$) 作为协议的一个私有输入，所有的参与方都知道公开输入 e(一个素数)和 N(ϕ 的近似界). 协议的最后，每个参与方 P_i 都获得一个秘密输出 $\boldsymbol{d}_{P_i}$，该输出是 $d=e^{-1}\bmod\phi$ 的秘密共享份额.

(1) 正确性. 称一个多方模求逆协议是正确的，如果 P 利用得到的份额能够重构 $d=e^{-1}\bmod\phi$，即使在敌手 $A\in\mathfrak{A}$ 存在的情况下.

(2) 保密性. 利用模拟的方法来定义保密性，也即，考虑协议运行当中敌手 A 的视图(view). 敌手的视图包括被收买的参与方所拥有的私有输入、协议运行期间收到的来自诚实方的消息. 称一个多方模求逆协议是保密的，如果对于任意的敌手 A，都存在一个多项式时间模拟器 S，使得 S 和 A 一起运行协议时，S 提供给 A 的视图与真实的视图是不可区分的.

(3) 安全性. 称一个多方模求逆协议是安全的，如果它既是正确的又是保密的.

3.3　半诚实敌手模型下的模求逆协议

设 k 为安全参数，RSA 模数为 N，$\phi=\phi(N)\in[0,N]$，公开素数 e. 协议的详细描述请参见图 1. 协议的大体流程如下.

1. 每个参与方 $P_i\in P$ 开始运行协议，输入其私有输入 $\boldsymbol{\phi}_{P_i}$，$i=1,2,\cdots,n$.

2. 协议第 1 轮，所有参与方共同生成三个随机的 m 维分发向量，相应的秘密分别为 Λ，R 以及 0.

3. 协议第 2 轮，参与方之间交换一些有用的信息来重构 $F=\Lambda\phi+Re$.

4. 最后，利用 GCD 算法计算出 a 和 b，使得 $aF+be=1$，并设 $d=aR+b\equiv e^{-1}\bmod\phi$. 每个参与方 P_i 利用 R 的份额计算出自己对应 d 的份额.

① 使用该网络模型，可以把精力集中到协议的高层描述上. 可以用加密、认证、承诺以及密钥协商等密码技术来代替该网络模型.

半诚实情况

私有输入：$\mathfrak{D}$已用$\mathfrak{A}$对应的乘性ISP $\mathfrak{M}$共享了ϕ，分发向量为$\boldsymbol{\rho}_\phi=(\phi,\rho_{\phi,2},\cdots,\rho_{\phi,m})^{\mathrm{T}}$，其中$\rho_{\phi,j}\in_R[0,\kappa_{\max}(m-1)N]$，$j=2,3,\cdots,m$，$P_i$将$\boldsymbol{\phi}_{P_i}$作为私有输入；

公开输入：RSA模数N，素数e，$e>n$，$(e,\phi)=1$；

第1轮. 每个参与方P_i按如下步骤运行协议第1轮：

1. 选择$\boldsymbol{\rho}_{\lambda_i}=(\lambda_i,\rho_{\lambda_i,2},\cdots,\rho_{\lambda_i,m})^{\mathrm{T}}$，其中$\lambda_i\in_R[0,2^kN]$，$\rho_{\lambda_i,j}\in_R[0,\kappa_{\max}(m-1)2^{2k}N]$，$j=2,3,\cdots,m$；

   选择$\boldsymbol{\rho}_{r_i}=(r_i,\rho_{r_i,2},\cdots,\rho_{r_i,m})^{\mathrm{T}}$，其中$r_i\in_R[0,2^kN^2]$，$\rho_{r_i,j}\in_R[0,\kappa_{\max}(m-1)2^{2k}N^2]$，$j=2,3,\cdots,m$；

   选择$\boldsymbol{\rho}_{0_i}=(0,\rho_{0_i,2},\cdots,\rho_{0_i,m})^{\mathrm{T}}$，其中$\rho_{0_i,j}\in_R[0,\kappa_{\max}(m-1)2^{3k}N^2]$，$j=2,3,\cdots,m$.

2. 利用式(1)共享$\lambda_i,r_i,0$给所有的参与方，其中$\boldsymbol{\rho}$分别被$\boldsymbol{\rho}_{\lambda_i}$，$\boldsymbol{\rho}_{r_i}$以及$\boldsymbol{\rho}_{0_i}$代替.

3. 发送$\boldsymbol{\lambda}_{iP_j}$，$\boldsymbol{r}_{iP_j}$，$\boldsymbol{0}_{iP_j}$给每个参与方$P_j$.

第2轮. 每个参与方P_j按如下步骤运行协议第2轮：

1. 令$\boldsymbol{\Lambda}_j=\sum_{i=1}^{n}\boldsymbol{\lambda}_{iP_j}$，$\boldsymbol{R}_j=\sum_{i=1}^{n}\boldsymbol{r}_{iP_j}$以及$\boldsymbol{Z}_j=\sum_{i=1}^{n}\boldsymbol{0}_{iP_j}$(这些分别是$\Lambda=\sum_{i=1}^{n}\lambda_i$，$R=\sum_{i=1}^{n}r_i$以及$Z=\sum_{i=1}^{n}0$由$\boldsymbol{M}\boldsymbol{\rho}_\Lambda=\boldsymbol{M}(\sum_{i=1}^{n}\boldsymbol{\rho}_{\lambda_i})$，$\boldsymbol{M}\boldsymbol{\rho}_R=\boldsymbol{M}(\sum_{i=1}^{n}\boldsymbol{\rho}_{r_i})$以及$\boldsymbol{M}\boldsymbol{\rho}_Z=\boldsymbol{M}(\sum_{i=1}^{n}\boldsymbol{\rho}_{0_i})$共享得来的份额).

2. 将值$F_j=\boldsymbol{\Lambda}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{\phi}_{P_j}+e\langle\boldsymbol{t}_j,\boldsymbol{R}_j\rangle+\langle\boldsymbol{t}_j,\boldsymbol{Z}_j\rangle$广播出去.

($\Lambda\phi=\sum_j\boldsymbol{\Lambda}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{\phi}_{P_j}$，$eR=e\boldsymbol{\rho}_R^{\mathrm{T}}\boldsymbol{\varepsilon}=e\boldsymbol{\rho}_R^{\mathrm{T}}\boldsymbol{M}^{\mathrm{T}}\boldsymbol{t}=e\boldsymbol{R}^{\mathrm{T}}\boldsymbol{t}=e\sum_j\langle\boldsymbol{t}_j,\boldsymbol{R}_j\rangle$，0的情况与$eR$类似.)

输出：每个参与方P_i做如下操作：

1. 将所有的广播值加起来，计算$F=\sum_{i=1}^{n}F_i$；

2. 利用GCD算法求出a和b，使得$aF+be=1$. 如果找不到这样的a和b，则返回到第1轮；

3. e的逆为$d=aR+b$. 秘密地输出d的份额$\boldsymbol{d}_{P_i}=a\boldsymbol{R}_i+b\boldsymbol{M}_{P_i,1}$，其中$\boldsymbol{M}_{P_i,1}$表示$\boldsymbol{M}_{P_i}$的第1列.

注2. 为了便于表示和计算，参与方P_i的份额可以设置为$a\boldsymbol{R}_i$，在重构d时，可以首先重构得到aR，然后再加上常数b即可得到d.

图1 半诚实模型下的多方模求逆协议

定理2. 如果所有的参与方都正确地执行图1所描述的协议，并且敌手结构$\mathfrak{A}$是Q^2的，那么上述协议就是一个安全的多方模求逆协议.

证明. 不难看出，协议泄露的唯一信息就是值$F=\Lambda\phi+Re$. 但是可以证明F的分布是与ϕ(几乎)独立无关的. 具体来讲，可以证明当Λ和R遵从协议中所描述的概率分布时，$\{F=\Lambda\phi+Re\}$的分布和$\{\hat{F}=\Lambda N+Re\}$的分布是统计不可区分的(达$O(2^{-k})$). 下面就根据3.2节的安全性定义给出具体的证明.

正确性. 很容易验证协议可以得到正确的输出. 由于$\mathfrak{A}$是Q^2的，则存在一个与$\mathfrak{A}$对应的乘性ISP $\mathfrak{M}$，也即，存在一个重构矩阵$\boldsymbol{D}$，使得参与方利用该矩阵以及相应的份额可以重构$\Lambda\phi$. 另外也存在一个重构向量$\boldsymbol{t}$来重构R. 因此参与方可以计算得到$F=\Lambda\phi+Re$. 然后可以将它与e做GCD运算. 注意到$(e,\phi)=1$，$\mathrm{GCD}(F,e)\neq1$的概率约为$1/e$(也即e整除Λ的概率)，因此并不需要重复运行协议很多次. 一旦找到了a和b，使得$aF+be=1$，可将它写为$a(\Lambda\phi+Re)+be=1$，等式两边取$\bmod\phi$，则等式变为$(aR+b)e=1\bmod\phi$，这样就得到了$d=aR+b=e^{-1}\bmod\phi$. 注意到R已由$\mathfrak{M}$共享，而且a和b都是常数，所以由输出值$\boldsymbol{d}_{P_i}$确实可以重构d.

保密性.

(1) 初始输入. 敌手A知道所有被收买的参与方所拥有的私有输入. 模拟器可以利用相同的ISP $\mathfrak{M}$来共享N，并将相应的份额分发给A. 由于$N-\phi=O(\sqrt{N})$，仿照引理1，可以证明$\mathfrak{M}$是保密的，份额$\boldsymbol{N}_A$和$\boldsymbol{\phi}_A$是统计不可区分的.

(2) 接收到的消息. 协议第1轮，模拟器只需简单地遵从协议即可，这样第1轮过后，模拟器共享了$\hat{\Lambda},\hat{R}$和$\hat{Z}$. 显然，$\hat{\Lambda},\hat{R},\hat{Z}$与$\Lambda,R,Z$遵从相同的分布. 同时注意到，与初始输入类似，敌手不能获得$\hat{\Lambda}$，$\hat{R}$和$\hat{Z}$的任何信息. 协议第2轮，模拟器广播值$\hat{F}_j=\hat{\boldsymbol{\Lambda}}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{N}_{P_j}+e\langle\boldsymbol{t}_j,\hat{\boldsymbol{R}}_j\rangle+\langle\boldsymbol{t}_j,\hat{\boldsymbol{Z}}_j\rangle$(对于所有的$P_j\in\overline{A}$). 因为$\boldsymbol{\rho}_Z$和$\boldsymbol{\rho}_{\hat{Z}}$中的元素分别要比$\boldsymbol{\rho}_R,\boldsymbol{\rho}_\Lambda,\boldsymbol{\rho}_\phi$和$\boldsymbol{\rho}_{\hat{R}},\boldsymbol{\rho}_{\hat{\Lambda}},\boldsymbol{\rho}_{\hat{\phi}}$中的元素分别高出一到三阶(相对于安全参数$k$和$N$)，因此$\langle\boldsymbol{t}_j,\boldsymbol{Z}_j\rangle$和$\langle\boldsymbol{t}_j,\hat{\boldsymbol{Z}}_j\rangle$分别要比$\boldsymbol{\Lambda}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{\phi}_{P_j}$，$e\langle\boldsymbol{t}_j,\boldsymbol{R}_j\rangle$和$\hat{\boldsymbol{\Lambda}}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{N}_{P_j}$，$e\langle\boldsymbol{t}_j,\hat{\boldsymbol{R}}_j\rangle$高出一阶(相对于安全参数$k$)，从而$F_j$和$\hat{F}_j$的分布都在统计上与$\langle\boldsymbol{t}_j,\boldsymbol{Z}_j\rangle$的分布接近. 最后敌手将所有的广播值加起来，得到$\hat{F}=\hat{\Lambda}N+\hat{R}e$，而在实际的协议中敌手将得到$F=\Lambda\phi+Re$，这是模拟器与实际协议的唯一区别. 然而可以证明这两个值的分布是统计不可区分的. 此处省略了该证明过程，读者可参见文献[4]的完整版. 证毕.

3.4 恶意敌手模型下的模求逆协议

本节来考虑恶意敌手模型下的多方模求逆协议. 我们构造了一个一般性模求逆协议，并证明了如果敌手结构$\mathfrak{A}$是Q^3的，那么该协议在强RSA假设之下是安全的. 协议的具体描述详见图2.

一般性模求逆协议

私有输入：$\mathfrak{D}$已用$\mathfrak{A}$对应的强乘性 ISP $\mathfrak{M}$共享了 ϕ，分发向量为 $\boldsymbol{\rho}_\phi=(\phi,\rho_{\phi,2},\cdots,\rho_{\phi,m})^{\mathrm{T}}$，并选择 $\boldsymbol{\rho}_{\hat{\phi}}=(\hat{\phi},\rho_{\hat{\phi},2},\cdots,\rho_{\hat{\phi},m})^{\mathrm{T}}$对 $\boldsymbol{\rho}_\phi$做承诺，其中

$\rho_{\phi,j},\rho_{\hat{\phi},j}\in_R[0,\kappa_{\max}(m-1)N]$，$j=2,3,\cdots,m$；$P_i$的私有输入为$\boldsymbol{\phi}_{P_i}$和$\hat{\boldsymbol{\phi}}_{P_i}$.

公开输入：RSA 模数 N，素数 $e,e>n,(e,\phi)=1$ 以及利用 $\boldsymbol{\rho}_{\hat{\phi}}$得到的关于$\boldsymbol{\rho}_\phi$的公开承诺.

第 1 轮：每个参与方 P_i选择$\lambda_i\in_R[0,N2^k]$和 $r_i\in_R[0,N^22^{2k}]$，然后进行如下操作：

1. 使用 VLISS 来共享 λ_i，界为 $N2^k$，得到的分发向量分别为 $\boldsymbol{\rho}_{\lambda_i}$和$\boldsymbol{\rho}_{\hat{\lambda}_i}$；

2. 使用 VLISS 来共享 r_i，界为 N^22^{2k}，得到的分发向量分别为 $\boldsymbol{\rho}_{r_i}$和 $\boldsymbol{\rho}_{\hat{r}_i}$；

3. 使用 VLISS 来共享 0，界为 N^32^{3k}，得到的分发向量分别为 $\boldsymbol{\rho}_{0_i}$和$\boldsymbol{\rho}_{\hat{0}_i}$.

注 3. 在此仅用到了 VLISS 的分发阶段，其中得到的 $\boldsymbol{\rho}_{\hat{\lambda}_i}$，$\boldsymbol{\rho}_{\hat{r}_i}$和$\boldsymbol{\rho}_{\hat{0}_i}$都是用来做承诺的，相应的承诺值在 VLISS 中给出.

设 A 为第 1 轮中所有通过 VLISS 验证的参与方组成的集合，令 $\Lambda=\sum_{P_i\in A}\lambda_i$，$R=\sum_{P_i\in A}r_i$，$Z=0$. 另外指定

$$\boldsymbol{\rho}_\Lambda=\sum_{P_i\in A}\boldsymbol{\rho}_{\lambda_i},\ \boldsymbol{\rho}_R=\sum_{P_i\in A}\boldsymbol{\rho}_{r_i},\ \boldsymbol{\rho}_Z=\sum_{P_i\in A}\boldsymbol{\rho}_{0_i},$$

$$\boldsymbol{\rho}_{\hat{\Lambda}}=\sum_{P_i\in A}\boldsymbol{\rho}_{\hat{\lambda}_i},\ \boldsymbol{\rho}_{\hat{R}}=\sum_{P_i\in A}\boldsymbol{\rho}_{\hat{r}_i},\ \boldsymbol{\rho}_{\hat{Z}}=\sum_{P_i\in A}\boldsymbol{\rho}_{\hat{0}_i}.$$

第 2 轮：每个参与方 P_j进行如下操作：

1. 将从第 1 轮中收到的所有来自 A 中参与方的份额加起来，也即，令

$$\boldsymbol{\Lambda}_j=\sum_{P_i\in A}\boldsymbol{\lambda}_{iP_j},\ \boldsymbol{R}_j=\sum_{P_i\in A}\boldsymbol{r}_{iP_j},\ \boldsymbol{Z}_j=\sum_{P_i\in A}\boldsymbol{0}_{iP_j},$$

$$\hat{\boldsymbol{\Lambda}}_j=\sum_{P_i\in A}\hat{\boldsymbol{\lambda}}_{iP_j},\ \hat{\boldsymbol{R}}_j=\sum_{P_i\in A}\hat{\boldsymbol{r}}_{iP_j},\ \hat{\boldsymbol{Z}}_j=\sum_{P_i\in A}\hat{\boldsymbol{0}}_{iP_j}.$$

注 4. 这些份额是由分发矩阵 $\boldsymbol{M}_A$和分发向量$\boldsymbol{\rho}_\Lambda,\boldsymbol{\rho}_R,\boldsymbol{\rho}_Z,\boldsymbol{\rho}_{\hat{\Lambda}},\boldsymbol{\rho}_{\hat{R}},\boldsymbol{\rho}_{\hat{Z}}$生成的.$\boldsymbol{\Lambda}_j,\boldsymbol{R}_j,\boldsymbol{Z}_j$的承诺值可以由 VLISS 得到.

2. 将值 $F_j=\boldsymbol{\Lambda}_j^{\mathrm{T}}\boldsymbol{D}_j\boldsymbol{\phi}_{P_j}+e\langle\boldsymbol{t}_j,\boldsymbol{R}_j\rangle+\langle\boldsymbol{t}_j,\boldsymbol{Z}_j\rangle$广播出去.

输出：每个参与方 P_i进行如下操作：

1. P_i利用图 4 描述的子协议 Prove-Correct 来证明 F_i是正确的. 令 A'为所有能够正确执行 Prove-Correct 的参与方组成的集合. 如果 $A'=A$，则继续执行后续步骤；否则返回到第 2 轮，并将 A'赋值给 A，重新运行，直至运行到这一步满足 $A'=A$ 为止.

2. A'中的每个参与方 P_i计算 $F=\sum_{P_i\in A'}F_i$.

3. 利用 GCD 算法，求出 a 和 b，满足 $aF+be=1$. 如果不存在满足上述条件的 a 和 b，则返回到第 1 轮.

4. 每个参与方 P_i秘密地计算相应的份额 $\boldsymbol{d}_{P_i}=a\boldsymbol{R}_i+b\boldsymbol{M}_{P_i,1}$，其中 $\boldsymbol{M}_{P_i,1}$为 $\boldsymbol{M}_{P_i}$的第 1 列.

图 2　恶意敌手模型下的多方模求逆协议

在恶意敌手模型中，恶意的参与方可能任意地背离协议来干扰诚实方得到正确的输出，或者想方设法地获取诚实方的私有信息. 多方模求逆协议要求即使在恶意敌手存在的情况下，诚实方仍然能够保密地计算得到正确的输出. 为了做到这一点，本文采用了如下两种常用技术：

(1) 将第 1 轮中简单的线性整数秘密共享方案替换为可验证线性整数秘密共享(VLISS，Pedersen-VSS[9]的一个变体)方案，来保证参与方在分布式生成随机数时执行正确的秘密共享，保证每个参与方共享得到的份额是一致的. 图 3 给出了 VLISS 的详细描述.

VLISS

分发阶段

公开输入：RSA 模数 N，两个生成元 $G,H\in Q_N$以及界 β.

分发者(dealer)的输入：秘密 $s\in[0,\beta]$.

1. 分发者选择 $\hat{s}\in_R[0,\beta]$以及 $\rho_2,\hat{\rho}_2,\cdots,\rho_m,\hat{\rho}_m\in_R[0,\kappa_{\max}(m-1)2^k\beta]$. 令 $\boldsymbol{\rho}_s=(s,\rho_2,\cdots,\rho_m)^{\mathrm{T}}$，$\boldsymbol{\rho}_{\hat{s}}=(\hat{s},\hat{\rho}_2,\cdots,\hat{\rho}_m)^{\mathrm{T}}$. 利用式(1) 在 P 中共享 $s,\hat{s}$，将值 $\boldsymbol{s}_{P_i},\hat{\boldsymbol{s}}_{P_i}$秘密地发送给 P_i，并广播 $C_1=G^sH^{\hat{s}}\bmod N$，　$C_j=G^{\rho_j}H^{\hat{\rho}_j}\bmod N$，$j=2,3,\cdots,m$.

2. 参与方 P_i验证

$$G^{s_{P_i,j}}H^{\hat{s}_{P_i,j}}=\prod_{w=1}^{m}(C_w)^{M_{P_i,j,w}}\bmod N \tag{2}$$

其中 $s_{P_i,j}$和 $\hat{s}_{P_i,j}$分别为 $\boldsymbol{s}_{P_i}$和 $\hat{\boldsymbol{s}}_{P_i}$中的第 j 个元素，$M_{P_i,j,w}$为 $\boldsymbol{M}_{P_i}$中第 j 行的第 w 个元素. 如果验证失败，P_i则公开投诉. 如果所有投诉的参与方能够形成一个授权集，那么分发者将被弹劾.

3. 如果分发者没有被弹劾，他会公开满足式(2)的值 $\boldsymbol{s}_{P_i}$和 $\hat{\boldsymbol{s}}_{P_i}$. 如果分发者不能正确执行这一步，他将被弹劾.

4. P_i验证他接收到的值以及分发者之前广播的值在绝对值上是否都被限制在界 $\kappa_{\max}^2(m-1)^22^k\beta+\kappa_{\max}\beta$之内. 如果验证失败，$P_i$则会公开他的份额. 如果公开的份额确实比 $\kappa_{\max}^2(m-1)^22^k\beta+\kappa_{\max}\beta$大，而且满足式(2)，那么分发者将被弹劾.

重构阶段

每个参与方 P_i出示 $\boldsymbol{s}_{P_i}$和 $\hat{\boldsymbol{s}}_{P_i}$，只有满足式(2)的值才会被接受. 利用常用的 LISS 来重构秘密 s，然后将它输出.

图 3　可验证线性整数秘密共享方案(VLISS)

Prove-Correct

P 的私有输入：$\boldsymbol{a},\hat{\boldsymbol{a}},\boldsymbol{b},\hat{\boldsymbol{b}},\boldsymbol{c},\hat{\boldsymbol{c}}$(定义如上所述).
公开输入：RSA 模数 N,两个生成元 $G,H\in Q_N$,素数 $e,e>n,(e,\phi)=1$. F 和承诺值 $A_i,B_i,C_i,i=1,2,\cdots,u$, $C_{\rho_\phi,j}$, $j=1,2,\cdots,m$.
目标：证明 $F=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{D}_{\mathrm{P}}\boldsymbol{b}+e\langle\boldsymbol{t},\boldsymbol{c}\rangle$
1. V 验证公开承诺值 A_i,B_i,C_i 和 $C_{\rho_\phi,j}$ 是否满足式(2).
2. P 随机选择一个矩阵 $\boldsymbol{\Lambda}\in[0,N^2]^{u\times u}$ 并且公开 $E_{ij}=G^{a_i b_j}H^{\Delta_{ij}}$, $i,j=1,2,\cdots,u$.
3. P 以零知识的形式(向验证者 V)证明 E_{ij} 相对 $A_i,B_j(i,j=1,2,\cdots,u)$ 是正确的：
(a) P 随机选择 $\boldsymbol{\alpha},\hat{\boldsymbol{\alpha}},\boldsymbol{\beta},\hat{\boldsymbol{\beta}}\in[0,N^3 2^{3k}]^u$ 以及 $\hat{\boldsymbol{\Lambda}}\in_R[0,N^3 2^{3k}]^{u\times u}$,并将 $M_i=G^{\alpha_i}H^{\alpha_i}$, $X_i=G^{\beta_i}H^{\hat{\beta}_i}$, $Y_{ij}=B_j^{\alpha_i}H^{\hat{\Delta}_{ij}}$ 发送给 V.
(b) V 随机选择 $\theta\in[0,N]$,并将其发送给 P.
(c) P 返回 $x_i=\alpha_i+\theta a_i,\hat{x}_i=\hat{\alpha}_i+\theta\hat{a}_i,y_i=\beta_i+\theta b_i,\hat{y}_i=\hat{\beta}_i+\theta\hat{b}_i,z_{ij}=\hat{\Delta}_{ij}+\theta(\Delta_{ij}-\hat{b}_j a_i)$.
(d) V 接受 E_{ij} 是正确的,如果 $G^{x_i}H^{\hat{x}_i}=M_i A_i^{\theta},B_j^{x_i}H^{z_{ij}}=Y_{ij}E_{ij}^{\theta},G^{y_i}H^{\hat{y}_i}=X_i B_i^{\theta}$.
4. P 公开 $F=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{D}_{\mathrm{P}}\boldsymbol{b}+e\langle\boldsymbol{t},\boldsymbol{c}\rangle$ 和 $\hat{F}=\sum_{ij}\Delta_{ij}D_{\mathrm{P}_{ij}}+e\langle\boldsymbol{t},\hat{\boldsymbol{c}}\rangle$($D_{\mathrm{P}_{ij}}$ 表示 $\boldsymbol{D}_{\mathrm{P}}$ 中的第 i 行第 j 列元素). 上述值被接受当且仅当

$$G^F H^{\hat{F}}=\prod_{ij}(E_{ij})^{D_{\mathrm{P}_{ij}}}\prod_i(C_i)^{e t_i}\bmod N$$

图 4 如何证明 $F=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{D}_{\mathrm{P}}\boldsymbol{b}+e\langle\boldsymbol{t},\boldsymbol{c}\rangle$

(2)第 2 轮重构 F 时,利用 Prove-Correct 零知识证明协议来防止恶意的参与方提供错误的份额。图 4 给出了 Prove-Correct 协议的具体实现.

为了便于理解和描述,本文先给出一般性模求逆协议的具体描述,之后再分别给出 VLISS 和 Prove-Correct 的具体描述.

设 k 为安全参数,RSA 模数为 $N,\phi=\phi(N)\in[0,N]$,公开素数 e. 一般性模求逆协议的完整描述见图 2.

在一般性模求逆协议中,“使用 VLISS 共享 s,界为 β”表示共享 s 时,选取区间 $[0,\beta]$ 的元素来为 s 做承诺,分发向量中其它元素也由 β 的常数倍界定.

假设所有的参与方都会通过下面的承诺方案对分发向量 $\boldsymbol{\rho}_\phi$ 中的元素做承诺,并作为公开输入的一部分,在执行 Prove-Correct 协议时会用到这些承诺. VLISS 协议也会用到下面的承诺方案 C：

公开参数为一个 RSA 模数 $N=pq$($p=2p'+1,q=2q'+1,p,p',q,q'$ 都是素数)以及两个随机元素 $G,H\in Q_N$. Q_N 为 $\mathbb{Z}_N^*$ 中的所有平方元组成的 $p'q'$ 阶循环群. 可设 G,H 为 Q_N 的两个生成元,因为它们不是生成元的概率是可忽略的. 消息空间为一个整数集. 为了对整数 α 做承诺,发送方在某个给定的区间内(比如 $[0,N^2]$)随机选择一个整数 $\hat{\alpha}$,将 $C(\alpha,\hat{\alpha})=G^{\alpha}H^{\hat{\alpha}}\bmod N$ 发送给接收方.

解承诺时,发送方给出 $\alpha,\hat{\alpha}$,接收方验证他们是否与 $C(\alpha,\hat{\alpha})$ 匹配.

引理 2. 在分解 N 是困难的假设之下,上述承诺方案是一个信息论意义下保密、计算意义下绑定的承诺方案. 相关证明请参见文献[4]的完整版.

当在多方模求逆协议中执行子协议 Prove-Correct 时,每一个参与方都会充当证明者运行 Prove-Correct 一次. 验证者的挑战将由其他所有的参与方共同生成. Canetti 等人[12]证明了该协议是一个诚实验证者零知识协议,因为每个运行该协议的证明者面对的是由其他所有参与方组成的一个“虚拟”的验证者. 该验证者被强制是诚实的,因为其它所有的参与方中的大多数都是诚实的.

3.4.1 可验证线性整数秘密共享方案

在一般性模求逆协议中,考虑到是在整数环上进行秘密共享,因此本文给出了 Pedersen-VSS[9]的一个变体-可验证线性整数秘密共享(VLISS)方案. 在 Pedersen 的方案中,秘密和份额被视为某个循环群 $\langle g\rangle$ 的“指数”. 因此在份额和群元素之间存在一个有效的映射 $x\mapsto g^x$,参与方可以利用群运算来验证份额的各种性质. 在 VLISS 中,秘密和份额则被视为循环群 Q_N 的“指数”,因此参与方同样可以利用群运算来验证份额的正确性. 后面将证明,在分解 N 是困难的假设下,VLISS 是一个安全的 VSS. 协议 VLISS 的具体描述请参见图 3.

注 5. 为了保证 VLISS 是一个安全的 VSS,协议中的第 4 步并不是必须的. 多方模求逆协议需要这一步是因为 Pedersen-VSS 并没有提供工具来保证所共享的秘密是“足够小的”,而协议的保密性就依赖于我们知道秘密大小的某个界值. 例如,如果 $F=\Lambda\phi+eR$ 中 Λ 的大小比其它项大很多,那么 F 就会泄露 ϕ 的部分信息. 因此,每个参与方都要验证一下相应的份额是否界定在某个区间 $[0,\kappa_{\max}^2(m-1)^2 2^k\beta+\kappa_{\max}\beta]$ 之内,以此确定相应的秘密是否落在区间 $[0,\lambda_{\max}\kappa_{\max}^2 n(m-1)^2 2^k\beta+\lambda_{\max}\kappa_{\max}n\beta]$ 内.

引理 3. 如果 $\mathfrak{A}$ 是 Q^2 的,那么在分解 N 是困难的假设之下,针对敌手结构 $\mathfrak{A}$,图 3 描述的协议

VLISS 是一个安全的 VSS.

证明.　正确性. 由于 $\mathfrak{A}$ 是 Q^2 的，对于任意 $A\in\mathfrak{A}$，$\overline{A}$ 是一个授权集，正确性可由 $\overline{A}$ 实现. 而且，协议中的承诺是计算意义下绑定的，敌手在解承诺时，无法给出两个不同的解. 因此任何恶意的参与方都能够被检测出来.

保密性. 很容易验证敌手所拥有的份额其分布是和其它秘密所生成份额的分布是统计不可区分的，也即敌手从拥有的份额中无法获得秘密的相关信息. 这一点是由 LISS 的保密性来保证的(参见引理 1). 另外，敌手看到的对分发向量的承诺是信息论意义下保密的，因此从中敌手也无法获得秘密的相关信息.　　证毕.

3.4.2　份额正确性的证明

在一般性模求逆协议第 2 轮重构 F 时，必须要防止恶意的参与方提供错误的份额，这是通过图 4 介绍的 Prove-Correct 零知识证明协议实现的. 该协议使用了 Fujisaki 和 Okamoto[13] 提出的一项基于强 RSA 假设的技术，其中 N 同样是两个安全素数的乘积.

定义 6(强 RSA 假设).　给定 RSA 模数 N 和一个随机元素 $y\in\mathbb{Z}_N^*$，在多项式时间内找到一个整数对 (e,x)，其中 $x\in\mathbb{Z}_N^*$，e 为大于 1 的素数，使得 $x^e=y(\mathrm{mod}N)$ 的成功概率是可忽略的.

强 RSA 假设是由文献[14]提出来的，后来被很多协议[1-3,13]使用.

假设使用前面介绍的基于分解困难性假设的承诺方案来对共享 ϕ 时的分发向量做承诺. 这样一般性模求逆协议的公开输入就包括 $C_{\rho_{\phi,j}}=G^{\rho_{\phi,j}}H^{\rho_{\hat{\phi},j}}\mathrm{mod}N$，$j=1,2,\cdots,m$，其中 $\rho_{\phi,1}=\phi,\rho_{\hat{\phi},1}=\hat{\phi}$.

在一般性模求逆协议中，参与方面临的问题可以概括如下：有如下公开值：

$$A_1=G^{a_1}H^{\hat{\alpha}_1},\cdots,A_u=G^{a_u}H^{\hat{\alpha}_u},$$

$$B_1=G^{b_1}H^{\hat{b}_1},\cdots,B_u=G^{b_u}H^{\hat{b}_u},$$

$$C_1=G^{c_1}H^{\hat{c}_1},\cdots,C_u=G^{c_u}H^{\hat{c}_u}$$

以及其它公开输入，例如 $e,\boldsymbol{D},\boldsymbol{t}$ 以及上面介绍的 $C_{\rho_{\phi,j}}$. 参与方 P 已知 $\boldsymbol{a}=(a_1,\cdots,a_u)^{\mathrm{T}},\hat{\boldsymbol{\alpha}}=(\hat{\alpha}_1,\cdots,\hat{\alpha}_u)^{\mathrm{T}},\boldsymbol{b}=(b_1,\cdots,b_u)^{\mathrm{T}},\hat{\boldsymbol{b}}=(\hat{b}_1,\cdots,\hat{b}_u)^{\mathrm{T}},\boldsymbol{c}=(c_1,\cdots,c_u)^{\mathrm{T}},\hat{\boldsymbol{c}}=(\hat{c}_1,\cdots,\hat{c}_u)^{\mathrm{T}}$，并公开了一个值 F，现在需要证明 $F=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{D}_{\mathrm{P}}\boldsymbol{b}+e\langle\boldsymbol{t},\boldsymbol{c}\rangle$.

在一般性模求逆协议中，每个参与方 P_i 都要执行上述证明过程，并将 $\boldsymbol{a}=\boldsymbol{\phi}_{P_i},\hat{\boldsymbol{\alpha}}=\hat{\boldsymbol{\phi}}_{P_i},\boldsymbol{b}=\boldsymbol{\Lambda}_i,\hat{\boldsymbol{b}}=\hat{\boldsymbol{\Lambda}}_i,\boldsymbol{c}=\boldsymbol{R}_i,\hat{\boldsymbol{c}}=\hat{\boldsymbol{R}}_i$ 以及 $\boldsymbol{D}_{\mathrm{P}}=\boldsymbol{D}_i$ 作为输入. 为了便于描述，此处没有考虑随机化子(randomizers)$\boldsymbol{Z}_i$ 和 $\hat{\boldsymbol{Z}}_i$.

该零知识证明是一个统计零知识协议，这是因为 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{D}_{\mathrm{P}}\boldsymbol{b}$ 是 $O(N^2 2^{2k})$ 的，通过在区间 $[0,N^3 2^{3k}]$ 中随机选择元素，可以保证在协议中第 3(c)步时，证明者的回答与区间内的随机数是统计不可区分的.

上面介绍了 VLISS 和 Prove-Correct 协议，并做了简单分析和证明. 本节最后，给出一般性模求逆协议的安全性证明.

定理 3.　如果敌手结构 $\mathfrak{A}$ 是 Q^3 的，那么在强 RSA 假设下，图 2 描述的一般性模求逆协议，在恶意敌手存在的情况下是一个安全的多方模求逆协议.

证明.　正确性. 利用 VLISS 和 Prove-Correct 两个子协议，可以筛选出一般性模求逆协议中的恶意参与方. 而且很容易验证一般性模求逆协议能够计算出正确的输出. 因为 $\mathfrak{A}$ 是 Q^3 的，所以在输出的第一步时，可以找到一个 $A'=A$，并且 $\mathfrak{M}_{A'}$ 是乘性的，因此可以由所有诚实方的份额 $\boldsymbol{d}_{P_i}(P_i\in A')$ 重构得到 d.

保密性. 在强 RSA 假设下，分解 N 是困难的，因此子协议 VLISS 是一个安全的 VSS. 同时，子协议 Prove-Correct 是一个统计零知识协议. 因此一般性模求逆协议的保密性大部分可以由 VLISS 的保密性和 Prove-Correct 的零知识性来保证，其它部分与半诚实敌手模型下的证明类似. 与半诚实模型不同的是敌手在选择 λ_i 时可能会超出指定的区间 $[0,N2^k]$. 但是，正如在注 5 中所说的，敌手能够通过 VLISS 验证仅当 λ_i 是 $O(N2^{2k})$ 的，最终 Λ 将是 $O(N2^{3k})$ 的. 为了补偿 Λ 扩大的范围，有必要增加 R 的取值范围以及共享 0 时的界，这就是为什么要求 r_i 取自区间 $[0,N^2 2^{2k}]$ 以及共享 0 时界为 $N^3 2^{3k}$. 证毕.

3.5　协议的效率分析

为了研究一般敌手结构上多方模求逆协议的存在性，本文并没有花费过多的精力去提高协议的效率和减小运算中整数的大小. 但相关的协议确实能够更优化一些，运算中的一些整数大小是可以减小的，这一点对于份额 $\boldsymbol{d}_{P_i}$ 来讲尤为重要，因为在多方 RSA 签名中会使用该份额来做指数运算，显然份额越小，计算起来越方便. 在半诚实模型下的多方模求逆协议中，每个份额的大小都限定在 $O(N^2 2^{3k})$，而在恶意敌手模型下的多方模求逆协议中，每个份额的大小都限定在 $O(N^3 2^{3k})$. 根据不同的应用场景，可以选择合适的安全参数 k 和 RSA 模数 N 来减小份额的大小.

多方模求逆协议是 Catalano、Gennero 和 Halevi[4] 门限协议的一个推广. 实际应用时，如果面临的

是门限敌手结构，可以使用 Vandermonde 矩阵作为分发矩阵，因此相应的 ISP 是乘性的（如果 $n>2t$，t 为门限值）或者强乘性的（如果 $n>3t$）. 因此两个协议拥有相同的效率.

但多方模协议同样适合其它非门限类型的敌手结构. 对于其它非门限类型的敌手结构，可以根据计算 $\mathfrak{A}$ 的一般 ISP 来构造乘性或者强乘性的 ISP. Cramer、Damgård 和 Maurer[5] 证明了对于 Q^2 类型的敌手结构 $\mathfrak{A}$，存在有效的算法将计算 $\mathfrak{A}$ 的一般的 ISP $\mathfrak{M}$ 转化成计算相同敌手结构的乘性 ISP $\mathfrak{M}'$，而乘性 ISP $\mathfrak{M}'$ 的大小仅是原 ISP $\mathfrak{M}$ 大小的两倍. 然而，如何有效地将计算 Q^3 类型的敌手结构的一般性 ISP $\mathfrak{M}$ 转化成计算相同敌手结构的强乘性 ISP $\mathfrak{M}'$ 仍然是一个公开难题，但 Cramer、Damgård 和 Maurer[5] 给出了 $\mathfrak{M}'$ 的上界. 因此最终协议运行完之后，每个参与方可能持有多个份额，所有份额的大小将会比门限情况下的份额大小要大一些.

在两种敌手模型下的多方模求逆协议中，本文都将文献[4]中的拉格朗日插值替换为简单的加法运算，只需将所有广播的份额简单加起来即可，因此计算起来会比文献[4]略快一些. 有兴趣的朋友可以尽一步优化和改进上述协议，也欢迎更多的朋友去设计新的高效协议来解决分布式模求逆问题.

4 总 结

本文构造了两个一般敌手结构下的多方模求逆协议：一个是半诚实模型下的，在敌手结构是 Q^2 的条件下是安全的；另一个是恶意敌手模型下的，在敌手结构是 Q^3 的条件下以及强 RSA 假设下是安全的. 在协议的构造中，使用了线性整数秘密共享方案，在做环上的运算时，避免了黑箱调用. 因此，本文构造多方协议的方法对文献[6]是一个有力的补充.

参 考 文 献

[1] Gennaro R, Halevi S, Rabin T. Secure hash-and-sign signatures without the random oracle//Proceedings of the EUROCRYPT'99. Berlin: Springer-Verlag, 1999: 123-139

[2] Cramer R, Shoup V. Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security, 2000, 3(3): 161-185

[3] Chevallier-Mames B, Joye M. A practical and tightly secure signature scheme without hash function//Proceedings of the CT-RSA 2007. Berlin: Springer-Verlag, 2006: 339-356

[4] Catalano D, Gennaro R, Halevi S. Computing inverses over a shared secret modulus//Proceedings of the EUROCRYPT 2000. Berlin: Springer-Verlag, 2000: 190-206

[5] Cramer R, Damgård I, Maurer U. General secure multi-party computation from any linear secret-sharing scheme//Proceedings of the EUROCRYPT 2000. Berlin: Springer-Verlag, 2000: 316-334

[6] Cramer R, Fehr S, Ishai Y, Kushilevitz E. Efficient multi-party computation over rings//Proceedings of the EUROCRYPT 2003. Berlin: Springer-Verlag, 2003: 596-613

[7] Cramer R, Fehr S. Optimal black-box secret sharing over arbitrary abelian groups//Proceedings of the CRYPTO 2002. Berlin: Springer-Verlag, 2002: 272-287

[8] Damgård I, Thorbek R. Linear integer secret sharing and distributed exponentiation//Proceedings of the PKC 2006. Berlin: Springer-Verlag, 2006: 75-90

[9] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing//Proceedings of the CRYPTO'91. Berlin: Springer-Verlag, 1992: 129-140

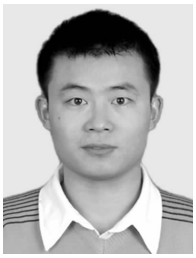
[10] Karchmer M, Wigderson A. On span programs//Proceedings of the Structure in Complexity Theory Conference, 1993. USA: IEEE Computer Society, 1993: 102-111

[11] Cramer R, Damgård I, Maurer U. Span programs and general secure multi-party computation. Department of Computer Science, University of Aarhus, DK: Technical Report, BRICS Report Series RS-97-28, 1997

[12] Canetti R, Gennaro R, Jarecki S, Krawczyk H, Rabin T. Adaptive security for threshold cryptosystems//Proceedings of the CRYPTO'99. Berlin: Springer-Verlag, 1999: 98-116

[13] Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations//Proceedings of the CRYPTO'97. Berlin: Springer-Verlag, 1997: 16-30

[14] Barić N, Pfitzmann B. Collision-free accumulators and fail-stop signature schemes without trees//Proceedings of the EUROCRYPT'97. Berlin: Springer-Verlag, 1997: 480-494



HU Hua-Ming, born in 1984, M. S.. His current research interests include secret sharing scheme and distributed signature schemes.

ZHOU Zhan-Fei, born in 1969, Ph. D., associate professor. His research interests include secret sharing scheme, threshold cryptography etc.

Background

This work was supported by National Natural Science Foundation of China (grant No. 60573004) and National Basic Research Program of China (973 Program, grant No. 2007CB311202).

In CRYPTO'87, Desmedt introduced the notion of distributed signatures. Subsequently, many distributed RSA signature schemes were proposed. The most well-known distributed RSA signature scheme was the one proposed by Shoup, which was proven secure in the random oracle model.

The random oracle model assumes that the output of a hash function behaves like a random function, which is an idealized situation that does not exist in the real world. What's more, a scheme that is proven secure in the random oracle model should not be viewed as secure in the standard model (the real world). It is entirely possible that a scheme is proven secure in the random oracle model, and yet be broken without violating any particular intractability assumption, and without exhibiting any particular weakness in the cryptographic hash functions. Therefore, constructing secure distributed signature schemes in the standard model has more practical sense.

Efficient RSA signature schemes without random oracles are due to the Gennaro-Halevi- Rabin (GHR) signature scheme, the Cramer-Shoup (CS) signature scheme and to the Mames-Joye (MJ) signature scheme (which is a variant of the CS scheme). They are all secure under the strong RSA assumption.

Catalano, Gennaro and Halevi proposed an efficient inversion protocol to construct distributed CS and GHR schemes. However they only considered threshold adversary structure, which is a special case in reality. In this paper the authors extend the Catalano-Gennaro-Halevi's inversion protocol to general adversary structures. Using the general multi-party inversion protocol, we can construct distributed CS, GHR and MJ signature schemes that are secure against general adversaries in the standard model.