doi:10.3969/j.issn.1000-436x.2014.11.016

新的安全分布式 *n* 个秘密乘积共享方案

陈振华[1,2]，李顺东[1]，王保仓[3]，李吉亮[1]，刘新[1]

(1. 陕西师范大学 计算机科学学院，陕西 西安 710062；2. 西安科技大学 计算机科学与技术学院，陕西 西安 710054；
3. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

摘 要：由于 Shamir 的秘密共享方案并不具有乘法的同态性质，因此针对安全分布式乘法计算中利用传统的 Shamir 线性多项式进行 *n* 个秘密乘积共享时需要不断调用两方秘密乘积子协议的缺点，首先用哥德尔数对保密数据进行编码，接着利用这种具有乘法同态的编码方法和一种加法同态承诺方案，实现了一种新的安全分布式一次性共享 *n* 个秘密乘积的方案，并证明了即使有恶意的参与者存在时，此方案仍为安全的。分析表明，本方案不但简单可行，而且相比传统方案效率明显提高。

关键词：哥德尔编码；秘密共享；分布式；安全多方求积；同态承诺

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)11-0139-07

New secure distributed secret sharing scheme of *n* product

CHEN Zhen-hua[1,2], LI Shun-dong[1], WANG Bao-cang[3], LI Ji-liang[1], LIU Xin[1]

(1. School of Computer Science, Shanxi Normal University, Xi'an 710062, China;
2. School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710054 ,China;
3. State Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, China)

Abstract: Since Shamir's secret sharing scheme does not have the property of the multiplicative homomorphism, an encoding method is utilized for privacy-preserving data to overcome the drawbacks in secure distributed multiplication calculation when using traditional Shamir's polynomial to share the product of *n* secrets. Using this encoding method with multiplicative homomorphism and a commitment scheme supporting additive homomorphism, a new secure distributed secret sharing scheme of *n* product in one session is implemented and the proposed scheme is secure under the presence of malicious participants. The analysis shows that proposed scheme is not only more simple and feasible but also more efficient than previous schemes.

Key words: Gödel encoding; secret sharing; distribution; secure multi-party multiplication; homomorphic commitment

1 引言

安全分布式乘法问题是指在不存在可信第三方的情况下，既不泄露各方的输入数据(隐私性)，又能在即使有恶意参与者存在的情况下也能正确完成输入数据的乘积计算(正确性)。安全分布式乘法计算是安全多方计算中的重要部分，它在科学计算、电子商务、数据挖掘、保密存储、计算外包、云计算等方面有着广泛的应用。

由于安全分布式乘法计算在安全多方计算中的重要性，因此基于不同子协议的安全分布式乘法计算协议不断被构建。其中一个发展主流就是可验证的秘密共享(VSS)作为子协议被用于构建安全分布式乘法计算。秘密共享使参与者各方能分布式地持有秘密，当关于秘密输入的乘积需要计算时，各方利用各自掌握的信息碎片，不揭示秘密，能共同合作计算出秘密的乘积。这个过程没有泄露秘密的任何其他信息，而由于 VSS 的验证性，又可以检查出恶意参与者的欺骗行为，因此可以保证秘密乘积的正确性。以往基于 VSS 子协议的分布式乘法计算[1,2]大

收稿日期：2014-07-31；**修回日期**：2014-11-02

基金项目：国家自然科学基金资助项目(61272435, 61272404, 61173152)

Foundation Item: The National Natural Science Foundation of China (61272435, 61272404, 61173152)

多利用了传统的 Shamir 秘密共享方案[3]，采取线性多项式进行秘密分配和重构,而线性多项式只保持加法的同态运算，因而这种方法对多个秘密的加法计算高效可行，但对多个秘密的乘法计算却并不简单高效,主要存在的缺点如下。

1) 输入的秘密被多方通过多项式插值点的方式共享，因此在多方乘积运算中，需要实施多项式随机化和降低多项式次数这 2 个步骤。

2) 需要预先假设已经把秘密碎片分配给多个参与者，即需要 3 次分布式传输阶段和提前假设一个分发者存在。

3) 在重构阶段需要通过重构多项式来共享多个秘密乘积。

4) 大多方案都是针对 2 个秘密乘积共享,多方秘密乘积共享需要不断调用 2 个秘密乘积共享的子协议。

针对以上存在的问题，Gennaro[4]提出了一种到目前为止最为有效可行的基于 VSS 的 2 个秘密乘积共享的方案，可以避免多项式随机化和降低多项式次数，并提出了不是针对多项式系数，而是针对多项式插值点承诺的方法，使方案的效率极大提高。Abe [5]利用 Pedersen[6] 的 VSS 方法对文献[4]方案做了改进，又回归到对多项式系数承诺的方法，避免了文献[4]中的交互式零知识证明。王宏等[7]在文献[4,5]的基础上，将有限域上的 2 个秘密乘积共享推广到整数环上的多个秘密乘积共享，但是该方案要求参与方必须大于一定的个数才可以共享多个秘密乘积，因此并没有完全解决一次性安全分布式多个秘密乘法问题。

由于上述方案都使用了传统的 Shamir 线性多项式[3]进行秘密乘积共享，而对于一个一般的线性秘密共享体制，它通常不满足乘法同态，所以无法高效实现两方甚至多方秘密乘积共享。而只有满足乘性同态的线性秘密共享体制才可以用于一次性安全分布式多个秘密乘积计算。文献[8~10]通过线性秘密共享体制的对偶构造等方法设计出新的线性秘密共享体制，使之具有乘法同态。但是，改造具有乘法同态的秘密共享体制需要消耗大量的计算成本和通信成本，使效率低下。另外，上述方案使用传统 Shamir 线性多项式[3]存在的一个共同问题是协议需要 3 次分布式传输阶段，并且提前假设有一个分发者存在。此外，都需要通过重构多项式来共享多方秘密乘积，使效率低下。这些没有解决的问题，不但在不需要可信第三方存在的安全多方乘法中是不可行的，而且通信效率和计算效率也比较低。

本文利用一种全新的秘密共享子协议的方法构造安全分布式多个秘密乘积共享方案。首先，利用哥德尔数对秘密进行编码，把编码后的码字作为每个参与者的碎片，由于这种编码方法具有乘法同态性质，因此很容易一次性共享多个秘密的乘积，从而避免了利用传统的多项式进行多方秘密乘积仍然存在的缺点。接着，利用这种编码方案和同态承诺方案，实现了一种新的安全分布式 n 个秘密乘积共享方案，并证明了即使有恶意的参与者存在时,此方案仍为安全的。本文方案的主要优点如下。

1) 不需要实施多项式随机化和降低多项式次数。

2) 本方案只有二次分布式分配阶段，不需要提前假设碎片已经被分发给参与者，即不需要提前假设一个分发者存在。

3) 在重构阶段不需要通过重构多项式来共享多个秘密乘积。

4) 可以一次性构造出安全分布式 n 个秘密乘积协议，不需要反复调用两方乘积子协议。

2 预备知识

2.1 基本模型

信道模型：协议假设参与者之间存在一条安全信道，除此，还假设有一个广播信道。

成员和攻击者模型：设 $P=\{P_1,P_2,\cdots,P_n\}$ 为 n 个成员集，每个成员具有概率多项式计算能力，成员可以是恶意参与者。敌手为概率多项式计算能力的静态攻击者，而被敌手攻破的参与者最多有 $n-2$ 个。

2.2 哥德尔编码

哥德尔数可以为一个有限正整数序列编码，将一个有限正整数序列和一个自然数建立一个对应关系，且此对应关系是唯一的。

定义 1 （哥德尔数）

设 $(x_1,x_2,\cdots,x_n)$ 为一个有限正整数序列，$(2,3,\cdots,n)$ 为连续的素数序列，s 为任意一个自然数，令 $s=2^{x_1}3^{x_1}\cdots n^{x_n}$，则 s 称为序列 $(x_1,x_2,\cdots,x_n)$ 的哥德尔数。

根据算数基本定理，满足以上定义 1 的 $s=2^{x_1}3^{x_1}\cdots n^{x_n}$ 和有限正整数序列 $(x_1,x_2,\cdots,x_n)$ 建立了唯一的对应关系，把这种对应关系叫哥德尔编码。

定理 1　哥德尔编码为一个具有乘法同态的编码。

证明　设 s_1 为序列 $(x_1,x_2,\cdots,x_n)$ 对应的哥德尔数，s_2 为序列 $(y_1,y_2,...,y_n)$ 对应的哥德尔数，则 $s_1s_2=2^{x_1+y_1}3^{x_2+y_2}\cdots n^{x_n+y_n}$。因此 s_1s_2 为序列 $(x_1+y_1, x_2+y_2,\cdots,x_n+y_n)$ 对应的哥德尔数。

2.3　同态承诺

同态承诺最先是 Grammer 和 Damgard 在文献[11]中提出的，任何一种单向双射二元函数 $C=H(x,r)$ 可以作为承诺函数，其中，C 是对 x 的承诺，r 是随机数。同态承诺分为加法同态承诺和乘法同态承诺，大多数方案都是基于离散对数的同态承诺，本文给出一种基于合数阶高次剩余的加法同态承诺方案。

定义 2　（加法同态承诺）

设 H 是承诺函数，$C_1=H(x_1,r_1)$ 是对 x_1 的承诺，$C_2=H(x_2,r_2)$ 是对 x_2 的承诺，其中，r_1,r_2 是随机数，若对于某个随机数 r，有 $C_1C_2=H(x_1+x_2,r)$，则称 C_1C_2 是对 x_1+x_2 的一个加法同态承诺。

Paillier 在文献[12]中提出了一种同态加密方案，具体如图 1 所示。

1) 系统建立。系统选取 $N=pq$，其中 p,q 为 2 个素数，$\lambda=lcm(p-1,q-1)$，$g\in \mathrm{B}$，其中 $\mathrm{B}=\bigcup_{\alpha=1}^{\lambda}\mathrm{B}_\alpha$，$\mathrm{B}_\alpha\subset Z_{N^2}^*$ 且每个集合 B_α 中元素的阶分别为 $N\alpha$。公钥 (N,g)，私钥 λ。

2) 加密过程。明文：$m<N$，任取随机数 $r\in Z_N$，密文：$c=g^m r^N \bmod N^2$。

3) 解密过程。密文：$c<N^2$，明文 m 为 $m=\dfrac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)}\bmod N$，其中 $L(u)=\dfrac{u-1}{N}$。

图 1　Paillier 的同态加密方案

若此方案中加密函数记为 $E(m,r)$，则 $E(m_1,r_1)E(m_2,r_2)=E(m_1+m_2,r_1r_2)$。

因此该加密方案具有加法同态性质。

命题 1　若把 Paillier 方案中的 (N,g) 当作系统参数，则 Paillier 的加密函数 $E(m,r)$ 为一个基于合数阶高次剩余的加法同态承诺方案。

证明　在文献[12]中通过引理 1 和定理 4，证明了 $E(m,r)$ 为一个基于合数阶高次剩余的单向双射函数，而任何一个二元的单向双射函数都可以作为一个承诺函数。因此若把 (N,g) 当成系统参数，则 $E(m,r)$ 为一个承诺方案。又因为若 $c_1=E(m_1,r_1)$ 为对 m_1 的承诺，$c_2=E(m_2,r_2)$ 为对 m_2 的承诺，则 $c_1c_2=E(m_1+m_2,r_1r_2)=E(m_1+m_2,r)$ 为对 m_1+m_2 的承诺，其中 $r_1r_2=r$。因此 $E(m,r)$ 为一个具有加法同态承诺方案。

3　方案构建

设 $\{P_1,P_2,\cdots,P_j,\cdots,P_n\}$ 为 n 个成员集，每个成员分别对应一个素数，假设 j_P 为成员 P_j 对应的素数，则此 n 个成员集按顺序对应一个 n 元素数集 $\{2,3,\cdots,j_P,\cdots,n\}$，其中 $n>2$。系统按照图 1 中 Paillier 的同态加密方案选择参数，公开参数为 (N,g)。

协议 1　（安全分布式 n 个秘密乘积共享）

输入：n 个成员分别持有秘密 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots n^{x_{in}}$，$i=1,2,\cdots,n$，$s_i$ 为正整数。

输出：n 个成员共享秘密乘积 $s_1s_2\cdots s_n$。

1) 对于每个协议参与者 P_i 所持有的秘密 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots n^{x_{in}}$，$P_i$ 选取随机 $r_{ij}, r_{ij}',r_i\in Z_N$，分别计算

$C_{ij}=g^{x_{ij}\bmod N}r_{ij}^{\ N}\bmod N^2$,

$C_{ij}'=g^{j_P{}^{x_{ij}}\bmod N}r_{ij}'^{N}\bmod N^2$,

$C_i=g^{s_i\bmod N}r_i^N\bmod N^2$。

P_i 传送给参与者 P_j 的碎片为 (x_{ij},r_{ij})，并且广播承诺 C_{ij},C_{ij}',C_i $(j=1,2,\cdots,n)$。

2) 每个参与者 P_j 通过以下等式在本地验证自己收到的碎片 (x_{ij},r_{ij}) $(i=1,2,\cdots,n)$是否正确，若出现一个不成立，则广播对 P_i 的不信任。若出现不信任，则要求 P_i 公开分发给 P_j 的碎片 (x_{ij},r_{ij})。

$$g^{x_{ij}\bmod N}r_{ij}^{\ N}\bmod N^{\ 2}=C_{ij}$$

3) P_i 使用协议 2 中乘积的零知识证明方法，确定自己所持有的秘密 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots n^{x_{in}}$ 被各方正确的分享。若出现不信任，则要求 P_i 公开分发给其他参与者 P_j 的碎片 (x_{ij},r_{ij})。

4) 若通过以上验证，协议各个参与者 P_j 在本地计算自己的碎片 $x_j'=\sum_{i=1}^{n}x_{ij}$，$r_j'=\prod_{i=1}^{n}r_{ij}\bmod N$，并广播对应的承诺 $C_j'=\prod_{i=1}^{n}C_{ij}\bmod N^2$。

5) 各个参与者 P_j 出示自己的碎片 $x_j'=\sum_{i=1}^{n}x_{ij}$，$r_j'=\prod_{i=1}^{n}r_{ij} \bmod N$，其他参与者通过以下等式验证碎片 (x_j',r_j') 是否正确，若出现不信任，则要求 P_j 重新出示碎片。

$$g^{x_j' \bmod N} r_j'^{N} \bmod N^2 = C_j'$$

6) 若所有的碎片 (x_j',r_j') $(j=1,2,\cdots,n)$ 通过验证，各个参与者 P_i 在本地计算 $2^{x_1'}3^{x_2'}\cdots j_P^{x_j'}\cdots n^{x_n'}$，最后每个参与者得到秘密乘积 $s_1s_2\cdots s_n$，其中 $\{2,3,\cdots,j_P,\cdots,n\}$ 为 n 个成员集 $\{P_1,P_2,\cdots,P_j,\cdots,P_n\}$ 对应的 n 元素数集。

协议 2 (乘积 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots j_P^{x_{ij}}\cdots n^{x_{in}}$ 的零知识证明)对于 $j=1,2,\cdots,n$，证明者 P_i 分别公开承诺

$C_{ij}'=g^{j_P^{x_{ij}} \bmod N} r_{ij}'^{N} \bmod N^2$，

$C_i=g^{s_i \bmod N} r_i^{N} \bmod N^2$。

P_i 用零知识证明方法向任何一个验证者 V 证明

1) C_{ij}' 是对 $j_p^{x_{ij}}$ 的一个承诺；

2) C_i 是对乘积 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots j_P^{x_{ij}}\cdots n^{x_{in}}$ 的一个承诺，即 s_i 被各方正确分享。

为了简单说明问题，取 $n=3$，即只有 3 个参与者，分别记

$C_A=g^{A \bmod N} r_A^{N} \bmod N^2$，

$C_B=g^{B \bmod N} r_B^{N} \bmod N^2$，

$C_C=g^{C \bmod N} r_C^{N} \bmod N^2$，

$C_0=g^{(ABC) \bmod N} r_0^{N} \bmod N^2$。

为了向验证者 V 说明 C_0 是证明者 P_i 对乘积 ABC 的一个承诺。Gennaro 在文献[4]附录 C 中采用 Cramer 等人[11]的方法进行了一个简便的 4 步交互式零知识证明，即 P_i 只需向 V 证明 $C_0=C_A^{(BC) \bmod N}\left(\frac{r_0}{r_A^{BC}}\right)^N \bmod N^2$。具体方案参见文献[4]。

4 安全性分析

命题 2 （正确性）如果参与方遵守协议 1, 在即使敌手最多攻破 $n-2$ 个参与者的情况，每个成员最后也能得到正确碎片 $x_j'=\sum_{i=1}^{n}x_{ij}, r_j'=\prod_{i=1}^{n}r_{ij} \bmod N$，及其承诺值 $C_j'=\prod_{i=1}^{n}C_{ij} \bmod N^2$，$j=1,2,\cdots,n$。满足 $g^{x_j' \bmod N} r_j'^{N} \bmod N^2 = C_j'$。并能正确计算出 $2^{x_1'}3^{x_2'}\cdots j_P^{x_j'}\cdots n^{x_n'}$。即协议 1 正确的共享了 n 个秘密的乘积。

证明 协议 1 中步骤 2)是基于合数阶高次剩余的承诺，若能通过验证等式 $g^{x_{ij} \bmod N} r_{ij}^{N} \bmod N^2 = C_{ij}$，则只有唯一正确的碎片 (x_{ij}, r_{ij})。步骤 3)利用乘积的零知识证明方法确定各方所持的碎片 (x_{ij},r_{ij}) 确实是发送者所持秘密 $s_i=2^{x_{i1}}3^{x_{i2}}\cdots j_P^{x_{ij}}\cdots n^{x_{in}}$ 的一个正确乘积。步骤 5)中

$$\begin{aligned} C_J' &= \prod_{i=1}^{n} C_{ij} \bmod N^2 \\ &= g^{\sum_{i=1}^{n} x_{ij} \bmod N} \left(\prod_{i=1}^{n} r_{ij} \bmod N\right)^N \bmod N^2 \\ &= g^{x_j' \bmod N} r_j'^{N} \bmod N^2 \end{aligned}$$

上式是基于合数阶高次剩余的承诺，只有唯一正确的碎片满足此等式。因此每个参与者都能得到唯一正确碎片。

$$x_j'=\sum_{i=1}^{n}x_{ij}, r_j'=\prod_{i=1}^{n}r_{ij} \bmod N$$

每个参与者计算

$$\begin{aligned} \prod_{j=1}^{n} j_P^{x_j'} &= \prod_{j=1}^{n} j_P^{\sum_{i=1}^{n} x_{ij}} = 2^{\sum_{i=1}^{n} x_{i1}} 3^{\sum_{i=1}^{n} x_{i2}} \cdots j_P^{\sum_{i=1}^{n} x_{ij}} \cdots n^{\sum_{i=1}^{n} x_{in}} \\ &= \sum_{i=1}^{n} 2^{x_{i1}}3^{x_{i2}}\cdots j_P^{x_{ij}}\cdots n^{x_{in}} = \sum_{i=1}^{n} s_i \end{aligned}$$

即协议 1 正确共享了 n 个秘密的乘积 $s_1s_2...s_n$。

命题 3 （隐私性）在即使敌手最多攻破 $n-2$ 个参与者的情况下, 协议 1 仍然保密地共享了 n 个秘密乘积。

证明 1) 在协议 1 执行过程中, 任何一方得不到其他方的私有信息。

通过构造一个协议模拟器 S_i 来论证此命题。给定参与者 P_i 的输入 s_i，$f_i(s_i,s_1,\cdots,s_j,\cdots,s_n)$ 为 P_i 在整个协议中获得的输出，S_i 随机取 $<s_1>,\cdots,<s_j>,\cdots,<s_n>$，使

$$\begin{aligned} &f_i(s_i,<s_1>,\cdots,<s_j>,\cdots,<s_n>) \\ &= f_i(s_i,s_1,\cdots,s_j,\cdots,s_n) \end{aligned}$$

用 $s_i,<s_1>,\cdots,<s_j>,\cdots,<s_n>$ 进行模拟，$view_i$ 为 P_i 在整个协议中的视图。

每个协议参与者 P_i 传送给其他参与者 P_j 的碎

片为 (x_{ij}, r_{ij})，广播承诺 C_{ij}, C_{ij}', C_i。

P_i 验证从参与者 P_j 收到的碎片 $(< x_{ji} >, < r_{ji} >)$ 和承诺 $< C_{ji} >$ 是否正确。

P_i 传送给其他参与者 P_j 的碎片为 (x_i', r_i')，广播承诺 C_i'。

P_i 验证从参与者 P_j 收到的碎片 $(< x_j' >, < r_j' >)$ 和承诺 $< C_j' >$ 是否正确。

记

$$\{x_{ij}, r_{ij}, C_{ij}, C_{ij}', C_i, x_i', r_i', C_i'\} = I_i$$

$$\{x_{ji}, r_{ji}, C_{ji}, x_j', r_j', C_j'\} = R_j$$

$$\{< x_{ji} >, < r_{ji} >, < C_{ji} >, < x_j' >, < r_j' >, < C_j' >\} = < R_j >$$

令

$$S_i(s_i, f_i(s_i, s_1, \cdots, s_j, \cdots, s_n)) = (I_i, < R_j >),$$

$$view_i = (I_i, R_j)$$

由于

$$f_i(s_i, < s_1 >, \cdots, < s_j >, \cdots, < s_n >) = f_i(s_i, s_1, \cdots, s_j, \cdots, s_n)$$

因此，$< R_j >$ 和 R_j 在计算上不可区分。于是，$S_i(s_i, f_i(s_i, s_1, \cdots, s_j, \cdots, s_n))$ 和 $view_i$ 在计算上不可区分。由此说明了参与者视图中的信息只能从自己输入和所获得的输出中得到，即说明视图中不包含额外的信息，即在协议执行过程中，任何一方得不到其他方的私有信息。

2) 在即使最多 $n-2$ 个参与者合谋时，也得不到任何其他未被攻破参与者的私有信息。

$n-2$ 个参与者合谋时，想得到其他未被攻破参与者的私有信息但此时仍有至少 2 个原始秘密未知，而这 2 个秘密可以是乘积固定的任意 2 个数值，因此敌手得不到任何其他未被攻破参与者的私有信息。同理可以用 1)中构造协议模拟器的方法进行证明。令 A 为 $n-2$ 个腐败参与者集合，$view_A$ 为 A 中成员执行协议 1 的视图，而 $\overline{view_A}$ 为 A 中成员以 $(\overline{x}_{ij}, \overline{r}_{ij}, \overline{x}_i', \overline{r}_i')\ (i = 1, 2, \cdots, n-2)$ 为输入执行协议 1 的识图，且满足

$$g^{x_{ij} \bmod N} r_{ij}^{\ N} \bmod N^2 = g^{\overline{x}_{ij} \bmod N} \overline{r}_{ij}^{\ N} \bmod N^2$$

$$g^{x_j' \bmod N} r_j'^{N} \bmod N^2 = g^{\overline{x}_j' \bmod N} \overline{r}_j'^{N} \bmod N^2$$

则 $view_A$ 与 $\overline{view_A}$ 是计算上不可区分的。

综合 1)，2)，协议 1 保密地计算了 n 个秘密的乘积 $s_1 s_2 \cdots s_n$。

定理 2　在即使最多攻破 $n-2$ 个参与者的情况下，协议 1 正确的共享了 n 个秘密的乘积，同时保护了各方的私有信息。

证明　由于命题 2、命题 3 已被论证为真命题，因此根据命题 2、命题 3，立即得到定理 2 的结论。

5　效率分析

5.1　计算复杂性和通信复杂性

忽略方案中的随机数选择开销和准备阶段参数选择的计算开销，计算复杂性考虑开销成本较大的模指数运算和模乘运算。本文方案的模为 N^2，其他方案的模为 q，为便于比较，模指数运算的单位统一记为 M_q，而模乘运算单位统一记为 M_p。

衡量通信复杂的指标用协议交换信息的比特数，或者用通信轮数，在安全多方计算研究中通常以通信轮数来衡量。

协议 1 共分 6 个阶段，各阶段计算开销和通信开销如表 1 所示。

表 1　**协议 1 的计算开销和通信开销**

阶段	计算开销（每个参与者）	通信开销/轮
第一阶段	$(2n+1)\ M_q$	1
第二阶段	$n\ M_q$	0
第三阶段	$6n\ M_q$	4
第四阶段	$2n\ M_p$	0
第五阶段	$n\ M_q$	1
第六阶段	$n(n-1)$	0

从表 1 可以看出，在协议 1 的第六阶段（重构阶段），本文方案并不需要进行模乘运算。协议 1 总的计算开销为 $(10n^2 + n)M_q + 2n^2 M_p$，总的通信开销需要每个参与者并行进行 6 轮。

5.2　方案比较

由于文献[7]方案是在文献[5]方案的基础上，通过改造文献[5]方案的两方协议实现的多方协议，所以效率低下。因此将本文的方案和现有的方案[4,5]在计算成本和性能方面做一个比较。

文献[4,5]都是通过线性多项式的方法共享秘密的乘积，整体上都需要 3 轮分布式分配过程，需要提前假设有一个分发者存在，并且最后都需要通过

表 2 本文方案与现有方案的比较

方案	计算成本	性能 1	性能 2	性能 3	性能 4
文献[4]	$(10n^2+n)M_q+(t^3+3n(2t+1)+3t+1)M_p$	是	否	否	否
文献[5]	$(7n^2+3(t+1))M_q+(t^3+3n(3t+2))M_p$	是	否	否	否
本文方案	$(10n^2+n)M_q+2n^2\ M_p$	是	是	是	是

重构多项式来共享秘密的乘积。除此，文献[4,5]都需要不断调用两方秘密乘积共享子协议来构造多方秘密乘积共享协议。

文献[4]方案和本文方案相似，但需要验证 VSPS[4]性质，并且通过重构多项式来共享秘密的乘积。协议所需要的计算开销为 $(10n^2+n)M_q+(t^3+3n(2t+1)+3t+1)M_p$。文献[5]用非交互式知识验证过程代替了文献[4]中的交互式零知识证明过程，其他过程都是一样的，协议所需要的计算开销 $(7n^2+3(t+1))\ M_q+(t^3+3n(3t+2))M_p$。

以上方案具体比较如表 2 所示。表 2 中，性能 1 是乘积共享是否不需要实施多项式随机化和降低多项式次数；性能 2 是乘积共享是否不需要 3 次分布式传输阶段和提前假设一个分发者存在；性能 3 是共享多方秘密乘积是否不需要通过重构多项式完成；性能 4 是共享多方秘密乘积是否不需要不断调用两方乘积子协议。

从表 2 可以看出，本文设计的协议 1 直接是一个一次性多个秘密乘积共享的协议，而其他的协议都只是 2 个秘密乘积共享协议，计算成本小于其他协议的计算成本，因此本文方案效率较高。此外，文献[4,5]除了满足性能 1 以外，其余的都不满足。而本文方案 4 个性能同时满足。

综上，本文所构造的方案在保持效率较高的情况下，取得了较好的性能。

6 结束语

本文针对安全分布式多个秘密乘积共享中利用传统的 Shamir 线性多项式存在的缺点，即线性多项式只具有加法同态性质，对多个秘密的加法计算高效可行，但对多个秘密的乘法计算却并不简单高效，提出了一种新的一次性安全分布式多个秘密乘积方案。首先利用哥德尔数对秘密进行编码，把编码后的码字作为每个参与者的碎片。由于此编码方法具有乘法同态性质，因此克服了传统方案中利用线性多项式进行 n 个秘密乘积共享的缺点。接着，利用这种编码方法和一种加法同态承诺方案，实现了一种即使有恶意参与者存在时的一次性安全分布式 n 个秘密乘积共享方案。最后通过分析显示，在保持效率较高的情况下，取得了较好的性能。

本文方案稍加改造可以成为群组密钥协商的子协议。而如何设计此子协议，以及设计抵抗 $n-1$ 个参与者合谋时的 n 个秘密乘积共享方案将是以后研究的重点。

参考文献：

[1] BEN-OR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for non-cryptographic fault-tolerant distributed computations[A]. Proceedings of the 20th Annual ACM Symposium on the Theory of Computing[C]. New York, USA, 1988.l-10.

[2] RABIN T, BEN-OR M. Verifiable secret sharing and multiparty protocols with honest majority[A]. Proceedings of the 21th Annual ACM Symposium on Theory of Computing[C]. New York, USA, 1989. 73-85.

[3] SHAMIR A. How to share a secret[J]. Communications of the Association for Computing Machinery, 1979, 22(3):612-613.

[4] GENNARO R, RABIN M, RABIN T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography[A]. Proceedings of the 27th Annual ACM Symposium on Principles of Distributed Computing[C]. New York, USA, 1998.101-111.

[5] ABE M. Robust distributed multiplication without interaction[A]. Cryptology-CRYPTO' 99[C]. Santa Barbara, California, USA, 2000. 130-147.

[6] PEDERSEN T. Non-interactive and information-theoretic secure verifiable secret sharing[A]. Cryptology-CRYPTO' 91[C]. Santa Barbara, California, USA, 1992.129-140.

[7] 王宏, 冯登国, 肖国镇. 整数上鲁棒分布式乘法计算方案[J]. 软件学报,2002, 13(8): 1412-1416.
WANG H, FENG D G, XIAO G Z. Robust distributed multiplication schemes over integer[J]. Journal of Software, 2002, 13(8): 1412-1416.

[8] DAMGARD I, KÖLKER J, MILTERSEN P. Secret sharing and secure computing from monotone formulae[J]. IACR Cryptology ePrint Archive, 2012, 2012: 536.

[9] CRAMER R, DAMGARD I, MAURER U. General secure multi-party computation from any linear secret-sharing scheme[A]. Cryptology-EUROCRYPTO 2000[C]. Bruges, Belgium, 2000.316-334.

[10] NIKOV V, NIKOVA S, PRENEEL B. Secure multi-party computation from any linear secret sharing scheme[A]. Cryptology-EUROCRYPT 2000[C]. 2000.316-334.

[11] CRAMER R, DAMGARD I. Zero-knowledge proofs for finite field arithmetic, or: can zero-knowledge be for free?[A]. Cryptology-CRYPTO' 98[C]. Santa Barbara, California, USA, 1998. 424-441.

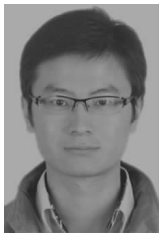
[12] PAILLIER P. Public-key cryptosystems based on composite degree residue classes[A]. Cryptology-EUROCRYPTO'99[C]. Prague, Czech Republic, 1999.223-238.

作者简介：

陈振华（1976-），女，陕西宝鸡人，陕西师范大学博士生、副教授，主要研究方向为密码学与信息安全、秘密共享、多方保密计算。

李顺东（1963-），男，河南平顶山人，陕西师范大学教授、博士生导师，主要研究方向为密码学与信息安全。

王保仓（1979-）,男，河南郸城人，博士，西安电子科技大学教授、硕士生导师，主要研究方向为公钥密码学及其网络安全应用。



李吉亮（1989-），男，山东聊城人，陕西师范大学硕士生，主要研究方向为密码学与信息安全、视觉密码。

刘新（1983-），男，山西山阴人，陕西师范大学博士生、讲师，主要研究方向为多方保密计算。

（上接第 138 页）

[17] EDWARDS H M. A normal form for elliptic curves[J]. Bulletin of the American Mathematical Society, 2007,44(3):393-422.

[18] BERNSTEIN D J, LANGE T. Faster Addition and Doubling on Elliptic Curves[M]. Heidelberg Springer Berlin, 2007.29-50.

[19] PBC Library[EB/OL]. http://crypto.stanford.edu/pbc/.

作者简介：

杨玉龙（1988-），男，湖北襄阳人，贵州大学硕士生，主要研究方向为密码学与可信计算。

彭长根[通信作者]（1963-），男，侗族，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为密码学、信息安全。E-mail：sci.cgpeng@gzu.edu.cn。

周洲（1989-），女，湖北潜江人，贵州大学硕士生，主要研究方向为密码学与可信计算。

张晓培（1979-），男，河南鹤壁人，博士，贵州大学讲师，主要研究方向为计算机网络通信与安全。