基于多线性 Diffie-Hellman 问题的秘密共享方案

彭 巧[1,2],田有亮[2,3]
(1. 贵州大学数学与统计学院,贵州贵阳 550025;2. 贵州省公共大数据重点实验室,贵州贵阳 550025;
3. 贵州大学计算机科学与技术学院,贵州贵阳 550025)

摘 要: 秘密共享方案的信息率是衡量秘密共享通信效率的重要指标,鉴于已有的秘密共享方案效率不高的问题,本文基于多线性对提出了信息率为 $m/(m+1)$ 的可验证秘密共享方案. 方案中,共享秘密为 m 维向量,其可验证性可利用多线性映射的多线性性质来实现;同时,在多线性 Diffie-Hellman 问题下,方案是可证明安全的. 性能分析结果表明,与已有的相同安全级别下的秘密共享方案相比,该方案具有较高的通信效率,更适用于通信受限的数据容错的应用场景.

关键词: 可验证的秘密共享; 多线性映射; 信息率; 多线性 Diffie-Hellman 问题
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)01-0200-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.01.027

A Secret Sharing Scheme Based on Multilinear Diffie-Hellman Problem

PENG Qiao[1,2], TIAN You-liang[2,3]
(1. *College of Mathematics and Statistics, Guizhou University, Guiyang, Guizhou* 550025, *China*;
2. *Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang, Guizhou* 550025, *China*;
3. *College of Computer Science and Technology, Guizhou University, Guiyang, Guizhou* 550025, *China*)

Abstract: Information rate of secret sharing scheme is an important indicator to measure the communication efficiency of secret sharing, in view of the problem that the existing secret sharing schemes efficiency are not high, a verifiable secret sharing scheme with information rate for $m/(m+1)$ was proposed based on multiple linear. In this scheme, the shared secret is m dimensional vector, the verifiability can be achieved by using the multiple linear pair property of multilinear map. And, as well, the scheme is provably secure under the multilinear Diffie-Hellman problem. The performance analysis results show that this scheme has a higher communication efficiency compared with the existing secret sharing schemes under the same level of security, which is more suitable for those data fault-tolerant communication limited application scenarios.

Key words: verifiable secret sharing; multilinear map; information rate; multilinear Diffie-Hellman problem

1 引言

秘密共享是一种分发、保存以及恢复秘密密钥(或其他秘密信息)的方法. 首次提出秘密共享方案的是著名密码学家 Shamir[1] 和 Blakley[2] 分别基于拉格朗日插值多项式和射影几何理论提出的门限秘密共享方案,但该秘密共享方案中存在如下两个问题:(1)秘密分发者的诚实性:若分发者将错误的子秘密分发给部分或全部参与者,各参与者如何验证发送来的子秘密的真伪? (2)参与者的诚实性:在恢复秘密阶段,若某些恶意的参与者提供的是假的子秘密,那其他参与者如何鉴别? 对这两个问题的研究,就形成了可验证的秘密共享方案(简记为 VSS). 首次提出 VSS 来验证子秘密的真伪性这种思想的是文献[3],而 Feldman[4] 的工作则使 VSS 方案引起了众多密码研究者的重视.

然而,无论在 Shamir 等人的一般秘密共享方案中,还是在可验证秘密共享方案中,都需要假设秘密分发者和各参与者之间有秘密信道(private channel),以便分发子秘密,但文献[4]的研究存在诸多不足. 于是,随着双线性对技术的产生,文献[5]通过使用双线性映射

收稿日期:2015-06-24;修回日期:2016-08-29;责任编辑:马兰英
基金项目:国家自然科学基金(No.61363068, No. 61662009);中国博士后基金(No.2013M530705);贵州省自然科学基金(No.20132112);贵州大学博士基金(No.2012-024);贵州大学青年基金(No.201305);贵州大学研究生创新基金(No.2016016)

计算方程,提出了一种新的可验证的秘密共享方案,它更容易检测出分发者和参与者在共享份额时的欺骗行为[6],解决了上述方案的不足之处. 文献[7]基于椭圆曲线上的信息论安全设计的可验证秘密共享方案,利用双线性映射的双线性性质提高了方案中子秘密验证的有效性. 文献[8]基于双线性对提出公开可证明安全的秘密共享方案,但它需对每个共享秘密作与计算,因而计算量较大. 不过,上述方案的安全性都是基于传统的离散对数或大数分解的密码算法. 虽然在文献[9]中提出了基于 NTRU 算法的秘密共享方案,但该方案只能恢复单个秘密,存储量也比较大. 另外,许春香等人[10]将向量作为秘密,提出了预防欺诈的矢量空间秘密共享方案,其存储量较小,但该方案在初始化的子秘密更新阶段始终需要一位值得信赖的分发者参与,这在实际的网络环境中是不可能的.

随着多线性映射[11]在公钥密码方面的成功应用,如文献[12]利用多线性映射这一实用工具,使用一次签名算法提升了加密方案的安全性. 因而利用多线性映射构造秘密共享方案是一种新的尝试. 从已引用的文章可看出,为了构造出计算量小、通信量更低的算法又会导致方案的信息率相对降低,且已有的大多数文献的信息率为 1/2,文献[7]中最高达到了 2/3. 而信息率是度量秘密共享方案效率的一个至关重要的因素,因而构造出信息率渐进最优的秘密共享方案是一个挑战. 鉴于以上考虑,本文在文献[7]和文献[10]的基础上,将 m 维向量作为共享密钥,利用多线性映射的多线性对性质,基于求解多线性离散对数(MDL)和多线性计算性 Diffie-Hellman(MDH)问题提出了一个新的可验证秘密共享方案,其信息率为 $m/(m+1)$,达到了渐进最优. 本方案的优势在于秘密分发者不需为各位参与者计算相应的密钥,也不需要执行复杂的交互式协议,但信息率却可达到渐进最优. 另外,本方案仅应用多线性映射的多线性性质对子秘密的正确性进行验证,从而实现了秘密共享的可验证性功能. 相对于现有的基于传统的离散对数或大数分解的密码算法,该方案还具有设计合理、简单、计算量小的特性,与目前同类型的方案相比在信息率上具有较大的优越性.

2　预备知识

2.1　多线性映射

定义 1　设$(G_1,+)$,$(G_2,\cdot)$分别是阶为 q 的循环加法群和循环乘法群,其中 q 为素数. 则多线性映射 e_n: $G_1^n\to G_2$有以下性质:

(1)多线性:对所有 $g_1,g_2,\cdots,g_n\in G_1$ 和 $a_1,a_2,\cdots,a_n\in \boldsymbol{Z}_q^*$,有 $\boldsymbol{e}_n(\boldsymbol{a}_1\boldsymbol{g}_1,\boldsymbol{a}_2\boldsymbol{g}_2,\cdots,\boldsymbol{a}_n\boldsymbol{g}_n)=\boldsymbol{e}_n(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n)^{\boldsymbol{a}_1\boldsymbol{a}_2\cdots\boldsymbol{a}_n}$.

(2)非退化性:若元素 $\boldsymbol{g}\in\boldsymbol{G}_1$ 是 $\boldsymbol{G}_1$ 的一个生成元,则 $\boldsymbol{e}_n(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n)$是 $\boldsymbol{G}_2$ 的生成元.

(3)可计算性:对所有 $\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n\in\boldsymbol{G}_1$,存在一个有效的算法计算 $\boldsymbol{e}_n(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n)$,称映射 $\boldsymbol{e}_n(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n)$为多线性映射.

2.2　计算性 Diffie-Hellman 问题

计算性 Diffie-Hellman 问题可如下定义:对于加法循环群 $G=<g>$,已知 G 中两个元素 $g_1=ag$ 和 $g_2=bg$ 以及 G 的生成元 g,但不知道 a 和 b,计算 $g_3=abg$ 是困难的.

2.3　复杂性假设

定义 2　多线性离散对数问题(*MDL*):设 G 是 q 阶有限循环群,对所有 $k>1$,$1\leqslant i\leqslant k$ 以及 $g_i\in G$,给定(i,g_i,ag_i),对任意的 $a\in Z_q^*$,求解 a 是困难的.

定义 3　n 阶多线性计算 Diffie-Hellman(n-MDCH 或 n-MDH)问题[13]:在(G_1,G_2,e)中,其中 G_1,G_2 均是阶为 p 的群,随机选取 $a_1,a_2,\cdots,a_n\in Z_p$ 对于给定的 P,$a_1P,a_2P,\cdots,a_nP$ 计算 $e_n(P,P,\cdots,P)^{a_1a_2\cdots a_n}\in G_2$.

MDH 假设可描述为:算法 A 在概率多项式时间内,以不可忽略的优势求解 MDH 问题是困难的.

3　本文提出的秘密共享方案

3.1　方案描述

假设有秘密分发者 D 需在 n 个参与者 $U=\{P_1,P_2,\cdots,P_n\}$ 间共享秘密向量 $\boldsymbol{S}=(\boldsymbol{S'}_1,\boldsymbol{S'}_2,\cdots,\boldsymbol{S'}_m)\in\boldsymbol{G}_1$,$S'_i\in Z_q^*$,$i=1,2,\cdots,m$. 仅当 t 个或 t 个以上的参与者联合起来才能恢复共享秘密,任意 $t-1$ 或者更少的参与者既无法重构出秘密也得不到关于秘密的任何信息.

具体方案包括以下 4 个部分:系统初始化、秘密分发阶段、子密钥的验证阶段和秘密恢复阶段.

系统初始化　设$(G_1,+)$是阶为素数 q 的加法循环群,$(G_2,\cdot)$是 q 阶乘法循环群,P 为 G_1 的生成元;且它们之间存在多线性映射 e_m:$G_1^m\to G_2$能被有效计算;假设 $\boldsymbol{G}_1$ 和 $\boldsymbol{G}_2$ 上的离散对数都是难解的;设 m 维向量构成的共享秘密记作 $\boldsymbol{S}=(\boldsymbol{S'}_1,\boldsymbol{S'}_2,\cdots,\boldsymbol{S'}_m)\in\boldsymbol{G}_1$,$S'_i\in Z_q^*$,$i=1,2,\cdots,m$.

秘密分发阶段　分发协议包括以下 5 个步骤.

(1)秘密分发者 D 公布秘密 $\boldsymbol{S}$ 的承诺:$C_0=e(r_0P,\boldsymbol{S})=e_{m+1}(r_0P,\boldsymbol{S'}_1,\boldsymbol{S'}_2,\cdots,\boldsymbol{S'}_m)$,$\forall r_0\in Z_q^*$.

(2)秘密分发者 D 选取 $G_1[x]$上的次数不超过 $t-1$ 的秘密多项式 $\boldsymbol{F}(\boldsymbol{x})=\boldsymbol{F}_0+\boldsymbol{F}_1\boldsymbol{x}+\boldsymbol{F}_2\boldsymbol{x}^2+\cdots+\boldsymbol{F}_{t-1}\boldsymbol{x}^{t-1}$,满足 $\boldsymbol{S}=\boldsymbol{F}_0=\boldsymbol{F}(0)=(\boldsymbol{S'}_1,\cdots,\boldsymbol{S'}_m)$,多项式系数为向量 $\boldsymbol{F}_1=(\boldsymbol{f}_{1,1},\boldsymbol{f}_{1,2},\cdots,\boldsymbol{f}_{1,m})$,$\boldsymbol{F}_2=(\boldsymbol{f}_{2,1},\boldsymbol{f}_{2,2},\cdots,\boldsymbol{f}_{2,m})$,$\cdots,\boldsymbol{F}_{t-1}=(\boldsymbol{f}_{t-1,1},\boldsymbol{f}_{1,t-2},\cdots\boldsymbol{f}_{t-1,m})$,$\boldsymbol{f}_{i,j}\in Z_q^*$ 其中 $i\in\{1,\cdots,t-1\}$,$j\in\{1,2,\cdots,m\}$,接下来计算秘密份额 $\boldsymbol{S}_i=$

$(\boldsymbol{S}_{i1},\boldsymbol{S}_{i2},\cdots,\boldsymbol{S}_{im})=\boldsymbol{F}(i)$,$S_{ij}\in Z_q^*$,其中 $i=1,\cdots,n$,$j=1,\cdots,m$.

(3)秘密分发者 D 随机选取 $g_1,\cdots,g_{t-1}\in_R Z_q^*$,并广播承诺 $C_j=e(g_jP,\boldsymbol{F}_j)=e_{m+1}(g_jP,f_{j1},f_{j2},\cdots,f_{jm})$,其中 $j=1,\cdots,t-1$.

(4)设 $t-1$ 次多项式 $g(x)=r+r_1x+\cdots+r_{t-1}x^{t-1}$,其中 $r=r_0$,D 计算 $r_i=g(i)\in Z_q^*$,$i=1,2,\cdots,n$.

(5)秘密分发者 D 秘密发送子密钥$(\boldsymbol{S}_i,\boldsymbol{r}_i)$(其中 $\boldsymbol{S}_i=(\boldsymbol{S}_{i1},\boldsymbol{S}_{i2},\cdots,\boldsymbol{S}_{im})$)给 P_i,$i=1,2,\cdots,n$.

子密钥的验证阶段 参与者 P_i 接收到$(\boldsymbol{S}_i,\boldsymbol{r}_i)$后,可通过下式(1)来验证接收到的子秘密的正确性:

$$e(r_iP,\boldsymbol{S}_i)=e_{m+1}(r_iP,\boldsymbol{S}_{i1},\boldsymbol{S}_{i2},\cdots,\boldsymbol{S}_{im})=\sqrt{C_i^t\cdot\prod_{j=0}^{t-1}C_j^{(i^j)^{m+1}}} \tag{1}$$

秘密恢复阶段 当至少 t 个参与者 $P_i(i\in N$ 且 $|N|\geqslant t)$拿出他们各自拥有的正确子秘密$(\boldsymbol{S}_i,r_i)$后,即可利用 Lagrange 插值多项式来恢复秘密 $\boldsymbol{S}$ 和 r:

$$\begin{cases}\boldsymbol{S}=\sum\limits_{i\in N}L_{Ni}(i)\cdot\boldsymbol{S}_i\\ r=\sum\limits_{i\in N}L_{Ni}(i)\cdot\boldsymbol{r}_i\end{cases} \tag{2}$$

其中 $L_{Ni}(i)$为插值系数,且 $L_{Ni}(x)=\prod\limits_{j\in N\backslash|i|}\dfrac{x-x_j}{x_i-x_j}$,向量 $\boldsymbol{S}_i=(\boldsymbol{S}_{i1},\boldsymbol{S}_{i2},\cdots,\boldsymbol{S}_{im})$,$i=1,2,\cdots,n$.

随后即可利用公开信息 C_0 来验证$(\boldsymbol{S}_i,r_i)$的正确性:$C_0=e(rP,\boldsymbol{S})=e_{m+1}(r_0P,\boldsymbol{S}'_1,\boldsymbol{S}'_2,\cdots,\boldsymbol{S}'_m)$.

3.2 正确性和安全性分析

本小节给出了所提出的可验证秘密共享方案的正确性和安全性的分析过程.

3.2.1 正确性分析

引理 1 首先证明式(1)的正确性.

证明 因为 $\boldsymbol{S}_i=\boldsymbol{F}(i)$,$C_0=e(r_0P,\boldsymbol{S})$,及 $C_j=e(g_jP,\boldsymbol{F}_j)=e_{m+1}(r_jP,\boldsymbol{f}_{j,1},\boldsymbol{f}_{j,2},\cdots,\boldsymbol{f}_{j,m})$,所以有下面的式(3)

$$\begin{aligned}e(r_iP,\boldsymbol{S}_i)&=e_{m+1}(r_iP,\boldsymbol{S}+\boldsymbol{F}_1i+\cdots+\boldsymbol{F}_{t-1}i^{t-1})\\&=e(r_iP,\boldsymbol{S})\cdot e(r_iP,\boldsymbol{F}_1i)\cdots e(r_iP,\boldsymbol{F}_{t-1}t^{i-1})\end{aligned} \tag{3}$$

以及下面的式(4)

$$\begin{aligned}e(r_iP,\boldsymbol{S}_i)&=e_{m+1}(r_0P+r_1iP+\cdots+r_{t-1}i^{t-1}P,\boldsymbol{S}_i)\\&=e(r_0P,\boldsymbol{S}_i)\cdot e(r_1iP,\boldsymbol{S}_i)\cdots e(r_{t-1}i^{t-1}P,\boldsymbol{S}_i)\end{aligned} \tag{4}$$

又因为

$$e(r_iP,\boldsymbol{S})\cdot e(r_0P,\boldsymbol{S}_i)=e(r_iP,\boldsymbol{S}_i)\cdot e(r_0P,\boldsymbol{S})=C_i\cdot C_0$$

$$\begin{aligned}&e(r_iP,\boldsymbol{F}_1i)\cdot e(r_1iP,\boldsymbol{S}_i)=e(r_iP,\boldsymbol{S}_i)\cdot e(r_1iP,\boldsymbol{F}_1i)\\&=C_i\cdot e_{m+1}(r_1iP,\boldsymbol{f}_{1,1}i,\boldsymbol{f}_{1,2}i,\cdots,\boldsymbol{f}_{1,m}i)\\&=C_i\cdot e_{m+1}(r_1P,\boldsymbol{f}_{1,1},\boldsymbol{f}_{1,2},\cdots,\boldsymbol{f}_{1,m})^{i^{m+1}}\\&=C_i\cdot C_1^{(i)^{m+1}}\\&\vdots\\&e(r_iP,\boldsymbol{F}_{t-1}i^{t-1})\cdot e(r_{t-1}i^{t-1}P,\boldsymbol{S}_i)\\&=e(r_iP,\boldsymbol{S}_i)\cdot e(r_{t-1}i^{t-1}P,\boldsymbol{F}_{t-1}i^{t-1})\\&=C_i\cdot e_{m+1}(r_{t-1}i^{t-1}P,\boldsymbol{f}_{t-1,1}i,\boldsymbol{f}_{t-1,2}i,\cdots,\boldsymbol{f}_{t-1,m}i)\\&=C_i\cdot C_{t-1}^{(i^{t-1})^{m+1}}\end{aligned}$$

则用式(3)式(4)得

$$\begin{aligned}&e(r_iP,\boldsymbol{S}_i)\cdot e(r_iP,\boldsymbol{S}_i)\\&=[e(r_iP,\boldsymbol{S})\cdot e(r_0P,\boldsymbol{S}_i)]\cdot[e(r_iP,\boldsymbol{F}_ii)\cdot e(r_1iP,\boldsymbol{S}_i)]\\&\cdots[e(r_iP,\boldsymbol{F}_{t-1}i^{t-1})\cdot e(r_{t-1}i^{t-1}P,\boldsymbol{S}_i)]\\&=(C_i\cdot C_0)\cdot(C_i\cdot C_1^{(i^{m+1})^1})\cdots(C_i\cdot C_{t-1}^{(i^{m+1})^{t-1}})\\&=C_i^t\cdot\prod_{j=0}^{t-1}C_j^{(i^{m+1})^j}\end{aligned}$$

则 $e(r_iP,\boldsymbol{S}_i)=\sqrt{C_i^t\cdot\prod\limits_{j=0}^{t-1}C_j^{(i^{m+1})^j}}$,其中 $\boldsymbol{S}_i=(\boldsymbol{S}_{i1},\cdots,\boldsymbol{S}_{im})$,证毕.

3.2.2 安全性分析

下面我们将通过引理 2 和引理 3 阐述本方案的安全性基于计算性多线性 Diffie-Hellman(MDH)问题的难解性.

引理 2 该秘密共享方案中,群 G_1 上的秘密多项式 $\boldsymbol{F}(\boldsymbol{x})$的系数 $\boldsymbol{F}_0,\boldsymbol{F}_1,\cdots,\boldsymbol{F}_{t-1}$的承诺值 $C_0,C_1,\cdots,C_{t-1}$是安全的⇔假设 MDH 成立.

证明 (1)⇒反证法. 假设该方案中的承诺算法是安全的,但 MDH 假设不成立. 由 MDH 假设不成立知,存在算法 A:对于 G_1 中已知的 $\boldsymbol{P},a_1\boldsymbol{P},\cdots,a_m\boldsymbol{P}(a_1,a_2,\cdots,a_m\in_R Z_q^*)$算法 A 能以不可忽略的优势 ε 计算出 $e_m(P,P,\cdots,P)^{a_1a_2\cdots a_m}$. 下证此承诺算法能被算法 A 攻破. 要攻破上述承诺算法,只需从承诺 C_i 中计算出 F_i 即可. 为此,在 Z_q^* 中随机选取 $2m$ 个元素 $\alpha_1,\alpha_2,\cdots,\alpha_m,\alpha'_1,\alpha'_2,\cdots,\alpha'_m$,然后分别向 A 提供输入$(\boldsymbol{P},\boldsymbol{\alpha}_1\boldsymbol{P},\boldsymbol{\alpha}_2\boldsymbol{P},\cdots,\boldsymbol{\alpha}_m\boldsymbol{P})$及$(\boldsymbol{P},\boldsymbol{\alpha}'_1\boldsymbol{P},\boldsymbol{\alpha}'_2\boldsymbol{P},\cdots,\boldsymbol{\alpha}'_m\boldsymbol{P})$. 由于该输入是随机选取的,因而由假设知 A 将以优势 ε 分别输出 $e_m(P,P,\cdots,P)^{\alpha_1\alpha_2\cdots\alpha_m}$和 $e_m(P,P,\cdots,P)^{\alpha_1'\alpha_2'\cdots\alpha_m'}$.

又因为 $C_i=e_m(P,\cdots,P)^{\alpha_1\alpha_2\cdots\alpha_m}\cdot e_m(P,\cdots,P)^{\alpha'_1\alpha'_2\cdots\alpha'_m}$,则由多线性映射的多线性可得 $e_m((\alpha_1\alpha_2\cdots\alpha_m)P,P,\cdots,P)=C_i/e_m(P,P,\cdots,P)^{\alpha_1\cdot\alpha_2\cdots\alpha'_m}$,从而可得出系数向量 F_i. 这与承诺算法是安全的相矛盾,因而假设不成立,从而承诺算法是安全的,必有 MDH 假设成立.

(2)⇐反证法. 假设 MDH 假设成立,但所提方案中的承诺算法是不安全的. 那么由承诺算法的不安全性知,存在算法 B:当向算法 B 输入群 G_1 中的任何 $m+1$ 个随机元素 $Q_1,Q_2,\cdots,Q_{m+1}$时,系数 $\boldsymbol{F}_i$ 就能被算法 B 以不可忽略的优势 ε 计算出来,并且系数 $\boldsymbol{F}_i$ 满足下面

的等式: $C_i = e(F_i, r_iP) = e_{m+1}(Q_1, \cdots, Q_m, Q_{m+1})$.

若设 $\boldsymbol{F}_i = (\boldsymbol{\beta}_1\boldsymbol{P}, \boldsymbol{\beta}_2\boldsymbol{P}, \cdots, \boldsymbol{\beta}_m\boldsymbol{P})$, $\beta_i \in Z_q^*$, $i = 1, 2, \cdots, m$ 及 $Q_1 = \boldsymbol{\beta}_1'\boldsymbol{P}, \boldsymbol{Q}_2 = \boldsymbol{\beta}_2'\boldsymbol{P}, \cdots, \boldsymbol{Q}_{m+1} = \boldsymbol{\beta}_{m+1}'\boldsymbol{P}$, 其中 $\beta_j \in_R Z_q^*$, $j = 1, \cdots, m+1$. 则算法 B 能以不可忽略的优势 ε 计算出的系数向量 $\boldsymbol{F}_i$ 将满足 $\boldsymbol{e}_{m+1}(\boldsymbol{\beta}_1'\boldsymbol{P}, \boldsymbol{\beta}_2'\boldsymbol{P}, \cdots, \boldsymbol{\beta}_{m+1}'\boldsymbol{P}) = \boldsymbol{e}_{m+1}(\boldsymbol{\beta}_1\boldsymbol{P}, \boldsymbol{\beta}_2\boldsymbol{P}, \cdots, \boldsymbol{\beta}_m\boldsymbol{P}, \boldsymbol{r}_i\boldsymbol{P})$. 由多线性映射的多线性性可得 $e_{m+1}(P, P, \cdots, P)^{\beta\beta_2\cdots\beta_{m+1}'} = e_{m+1}(P, P, \cdots, P)^{\beta\beta_2\cdots\beta_m r_i} \Rightarrow e_{m+1}(P, P, \cdots, P)^{\beta\beta_2\cdots\beta_m r_i \cdot (\beta\beta_2\cdots\beta_{m+1}')^{-1}} = e_{m+1}(P, P, \cdots, P)$

整理上式可得 $e_{m+1}(P, P, \cdots, P)^{(\beta\beta_1'^{-1})\cdot(\beta_2\beta_2'^{-1})\cdots(\beta_m\beta_{m+1}'^{-1})(r\beta_{m+1}'^{-1})} = e_{m+1}(P, P, \cdots, P)$. 令 $\boldsymbol{b}_1 = \boldsymbol{\beta}_1\boldsymbol{\beta}_1'^{-1}, \boldsymbol{b}_2 = \boldsymbol{\beta}_2\boldsymbol{\beta}_2'^{-1}, \cdots, \boldsymbol{b}_m = \boldsymbol{\beta}_m\boldsymbol{\beta}_m'^{-1}, \boldsymbol{b}_{m+1} = \boldsymbol{r}_i\boldsymbol{\beta}_{m+1}'^{-1}$ 则有 $e_{m+1}(P, P, \cdots, P)^{b_1b_2\cdots b_{m+1}} = e_{m+1}(P, P, \cdots, P)$, 这表明算法 B 对于 G_1 中给定的 $\boldsymbol{P}, \boldsymbol{b}_1\boldsymbol{P}, \cdots, \boldsymbol{b}_m\boldsymbol{P}, \boldsymbol{b}_{m+1}\boldsymbol{P}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_{m+1} \in_R Z_p^*)$, 它都能够以不可忽略的优势计算出 $e_{m+1}(P, P, \cdots, P)^{b_1b_2\cdots b_{m+1}}$. 因此 MDH 假设不成立, 即它与上述假设矛盾. 所以, 若 MDH 假设成立, 则上述方案中的承诺算法就是安全的.

综合(1)和(2), 根据反证法可证得, 所提方案中的承诺算法是安全的⇔MDH 假设成立.

引理 3　在所提秘密共享方案中, 若 MDH 假设成立, 则 $t-1$ 个参与者的任意组合都不能恢复出共享秘密 $\boldsymbol{S}$.

证明　用反证法. 假设 $t-1$ 个参与者组合能够恢复出秘密 $\boldsymbol{S}$. 不失一般性, 记这 $t-1$ 个参与者为 $P_1, \cdots, P_{t-1}$. 下面证明, 对任意给定的 $\boldsymbol{cP}, \boldsymbol{d}_1\boldsymbol{P}, \boldsymbol{d}_2\boldsymbol{P}, \cdots, \boldsymbol{d}_m\boldsymbol{P}$, 其中 $\boldsymbol{c}, \boldsymbol{d}_1, \boldsymbol{d}_2, \cdots, \boldsymbol{d}_m \in \boldsymbol{Z}_p^*$, 存在攻击者 Λ 利用这 $t-1$ 个参与者作为预言机(Oracle), 就能将 $\boldsymbol{e}_{m+1}(\boldsymbol{P}, \boldsymbol{P}, \cdots, \boldsymbol{P})^{\boldsymbol{cd}_1\boldsymbol{d}_2\cdots\boldsymbol{d}_m}$ 计算出. 不妨设 $d_1, d_2, \cdots, d_m, c$ 是随机元素, 否则就用与之不同的元素 $\boldsymbol{c}', \boldsymbol{d}'_1, \boldsymbol{d}'_2, \cdots, \boldsymbol{d}'_m$ 对 $cP, d_1P, d_2P, \cdots, d_mP$ 进行随机化.

下面为攻击者 Λ 构建一个模拟的 VSS 系统, 使得当用 $P_1, \cdots, P_{t-1}$ 作为预言机时, 可得出 $e_{m+1}(P, P, \cdots, P)^{cd_1d_2\cdots d_m}$. 构建模拟的 VSS 系统分为以下 5 个步骤:

构建模拟的 VSS 系统分为以下 5 个步骤:

(1) 攻击者 Λ 设定 $\boldsymbol{C}_0 = \boldsymbol{e}_{m+1}(\boldsymbol{cP}, \boldsymbol{d}_1\boldsymbol{P}, \boldsymbol{d}_2\boldsymbol{P}, \cdots, \boldsymbol{d}_m\boldsymbol{P})$; 通过对 C_0 作这样的设定, $\boldsymbol{F}(0) = (\boldsymbol{d}_1\boldsymbol{P}, \boldsymbol{d}_2\boldsymbol{P}, \cdots, \boldsymbol{d}_m\boldsymbol{P})$ 以及 $g(0) = \boldsymbol{c}$ 就可以被确定.

(2)在 $G_1 \times Z_q^*$ 中随机选取 $t-1$ 组 $m+1$ 维向量 $(\boldsymbol{F}(1), \boldsymbol{g}(1)), (\boldsymbol{F}(2), \boldsymbol{g}(2)), \cdots, (\boldsymbol{F}(t-1), \boldsymbol{g}(t-1))$, 则由(1)中确定的 $\boldsymbol{F}(0)$ 和 $g(0)$ 的值, 多项式 $\boldsymbol{F}(\boldsymbol{x})$ 和 $g(x)$ 就可以被固定.

(3)攻击者 Λ 计算前 $t-1$ 个多线性对 $e(r_iP, \boldsymbol{S}_i) = e_{m+1}(r_iP, \boldsymbol{S}_{i1}, \boldsymbol{S}_{i2}, \cdots, \boldsymbol{S}_{im})$, $i = 1, 2, \cdots, t-1$ 的值.

(4)因为 $\boldsymbol{F}(0)$ 和 $g(0)$ 的值是隐藏在承诺值 C_0 中的, 所以 $(\boldsymbol{F}(i), g(i))$, $i = t, t+1, \cdots, n$ 的值无法被攻击者 Λ 计算出来; 但是, 攻击者 Λ 可以根据 Lagrange 插值公式计算出余下的 $n-t+1$ 个 $e(r_iP, \boldsymbol{S}_i)$ 的值, 其 $i = t, t+1, \cdots, n$.

(5)攻击者 Λ 计算承诺 C_i $(i = 1, 2, \cdots, t-1)$. 已知多项式 $\boldsymbol{F}(\boldsymbol{x}) = \boldsymbol{S} + \sum_{i=1}^{t-1} \boldsymbol{F}_i\boldsymbol{x}^i$ 和 $g(x) = r + \sum_{i=1}^{t-1} g_ix^i$, 故可以得到如下方程组:

$$\begin{cases} e(rP, \boldsymbol{S})^1 \cdot e(g_1P, \boldsymbol{F}_1)^{0^2} \cdots e(g_{t-1}P, \boldsymbol{F}_{t-1})^{q^{2(t-1)}} \\ \quad = e(g(0)P, \boldsymbol{F}(0)) \\ e(rP, \boldsymbol{S})^1 \cdot e(g_1P, \boldsymbol{F}_1)^{1^2} \cdots e(g_{t-1}P, \boldsymbol{F}_{t-1})^{1^{2(t-1)}} \\ \quad = e(g(1)P, \boldsymbol{F}(1)) \\ e(rP, \boldsymbol{S})^1 \cdot e(g_1P, \boldsymbol{F}_1)^{2^2} \cdots e(g_{t-1}P, \boldsymbol{F}_{t-1})^{2^{2(t-1)}} \\ \quad = e(g(2)P, \boldsymbol{F}(2)) \\ \qquad\qquad \vdots \\ e(rP, \boldsymbol{S})^1 \cdot e(g_1P, \boldsymbol{F}_1)^{(t-1)^2} \cdots e(g_{t-1}P, \boldsymbol{F}_{t-1})^{(t-1)^{2(t-1)}} \\ \quad = e(g(t-1)P, \boldsymbol{F}(t-1)) \end{cases}$$

在上述 $t-1$ 个方程中, 攻击者 Λ 只知道 $m+1$ 维向量 $(\boldsymbol{F}(1), \boldsymbol{g}(1)), (\boldsymbol{F}(2), \boldsymbol{g}(2)), \cdots, (\boldsymbol{F}(t-1), \boldsymbol{g}(t-1))$ 的值, 而 $\boldsymbol{F}(0)$ 和 $\boldsymbol{g}(0)$ 的值是未知的, 因此它无法求出向量 $\boldsymbol{S}, \boldsymbol{F}_1, \cdots, \boldsymbol{F}_{t-1}$ 及未知量 $r, g_1, \cdots g_{t-1}$ 的值. 但是对于攻击者来说, 承诺值 C_0 是已知的, 故 Λ 利用 C_0 和上述方程组可以求出承诺值 C_i $(i = 1, 2, \cdots, t-1)$.

因此, 构建出了攻击者 Λ 的模拟的 VSS 系统. 当 Λ 向 $t-1$ 个参与者 P_i $(i = 1, 2, \cdots, t-1)$ 提供这一系统的相关信息时, 这些参与者的个人观察是相互一致的. 那么根据假设知这 $t-1$ 个参与者可以恢复出共享秘密向量 $\boldsymbol{S} = \boldsymbol{F}(0)$ 且它满足 $e_{m+1}(\boldsymbol{cP}, \boldsymbol{d}_1\boldsymbol{P}, \boldsymbol{d}_2\boldsymbol{P}, \cdots, \boldsymbol{d}_m\boldsymbol{P}) = e(g(0)P, \boldsymbol{F}(0))$ 由多线性映射的多线性性质得 $e_{m+1}(P, P, \cdots, P)^{cd_1d_2\cdots d_m} = e(g(0)P, \boldsymbol{F}(0))$ 由于多线性对在这个模拟的 VSS 系统中可以被有效的计算, 这表明 MDH 问题能被这 $t-1$ 个参与者求解, 这与 MDH 假设成立相矛盾, 从而引理得证.

定理 1　该秘密共享方案的安全性基于 MDL 和 MDH 的难解性.

证明　(1)由引理 2 及其证明知对密钥及其份额的承诺 $C_0, C_1, \cdots, C_{t-1}$ 是安全的, 是基于 MDH 假设成立这一前提.

(2)在秘密分发阶段, 假设存在攻击者欲从公布的承诺 $C_0, C_1, \cdots, C_{t-1}$ 中获取 $\boldsymbol{F}_0, \boldsymbol{F}_1, \cdots, \boldsymbol{F}_{t-1}$ 和 $r_0, r_1, \cdots, r_{t-1}$, 则他必须要求解 MDL 和 MDH.

(3)由引理 3 知, 对 $t-1$ 参与者联合不能恢复共享秘密 $\boldsymbol{S}$ 这一引理的证明也是基于多线性对的 MDH 的难解性.

(4)攻击者欲从验证式(1)中求解子秘密 $(\boldsymbol{S}_i, r_i)$ 也必须求解 MDL 和 MDH. 综上所述, 本方案的安全性是

基于 MDL 和 MDH 的难解性的.

3.3 信息率

本节主要考虑方案的信息率. 我们知道信息率是衡量协议效率的一个重要因素,信息率越高,秘密共享体制的数据扩散程度越小,协议安全性就越高,所以我们希望能构造出信息率渐进最优的秘密共享方案. 而在本方案中,由于其共享秘密为 m 维向量 $\boldsymbol{S}=(\boldsymbol{S}'_1,\cdots,\boldsymbol{S}'_m)$,$\boldsymbol{S}'_i\in G_1$,$i=1,\cdots,m$,所以 $|\boldsymbol{S}|=m\cdot|q|$;方案中子秘密为 $(\boldsymbol{S}_i,r_i)$,其中 $\boldsymbol{S}_i=(\boldsymbol{S}_{i1},\cdots,\boldsymbol{S}_{im})\in G_1$,且 $r_i\in Z_q^*$.

因此,$|(\boldsymbol{S}_i,r_i)|=|\boldsymbol{S}_i|+|r_i|=m\cdot|q|+|q|$. 所以根据信息率的定义知,本方案的信息率为:

$$IR_{SS}=\frac{|\boldsymbol{S}|}{|(\boldsymbol{S}_i,r_i)|}=\frac{m\cdot|q|}{m\cdot|q|+|q|}=\frac{m}{m+1}\to 1$$

由此可见,本文方案的信息率达到了渐进最优.

3.4 性能分析

(1)从计算量上来看. 本文方案的秘密分发者 D 不需为各位参与者计算相应的子密钥,而文献[14]和文献[15]以及文献[16]中均需要为各参与者计算相应的子密钥,因而本方案在子密钥的产生上节省了计算开销. 在秘密分发阶段,秘密分发者需要为每一个参与者计算群 G_1 上的多线性对次数是 $2t$ 次,且所需的主要运算和参与者数目 n 成线性关系;子秘密的验证阶段需要 m 次多线性对运算和 m 次数乘运算,因此本方案较文献[15]和文献[16]在计算量上有明显的优势,对份额验证的不足之处是采用等式(1),基于多线性对的计算相对于数乘、点乘等运算没有什么优势,但是利用多线性映射对其信息率进行优化,能有效提高此方案在云计算、大数据安全存储等应用中效率;在秘密恢复阶段,计算量为群 G_1 上 t 次数乘运算. 另外,本文方案的主要运算开销与参与者数目成线性关系,而且在秘密分发阶段中我们对有些计算可以作预处理,这样可以大大提高秘密分发的效率.

(2)从信息率上来看. 文献[15]和文献[17]中方案的信息率都是 1/2;文献[16]和文献[7]的信息率分别是 1/5、2/3;而本方案中应用多线性映射的多线性构造的方案其信息率几乎为 1,达到了渐进最优. 可见本方案在相同的安全级别下有较高的信息率,其秘密共享体制的数据扩散程度较小,安全性相对较高,因而本方案在信息率上具有明显的优势,能更好地满足那些对通信效率要求更高的应用场景. 另外,本文是基于多线性映射这一实用工具,将一个 m 维向量作为共享密钥而构造的可验证方案,这是构造秘密共享方案的一个新的尝试.

(3)从存储量上来看. 本方案的存储花费主要包括秘密信息的存储和公开信息的存储. 对于秘密分发者来说,需要保密的信息为 $t-1$ 次秘密多项式 $\boldsymbol{F}(x)$,其长度为 mt,而文献[18]中需要存储的是 n 次多项式的长度,存储量明显比本方案大;对于参与者来说,需要对子秘密 $(\boldsymbol{S}_i,r_i)$ 进行保密,它是 $m+1$ 维向量,其长度为 $m+1$,与已存在方案的存储量相差不大;公开信息的存储就是对承诺值的存储,其大小与参与者数目成线性比例,由于公开信息的泄露不会对系统造成任何影响,因此,可以将这些信息由一个或多个参与者共同存储,以便合理利用系统,不会给系统造成过重的存储负担.

4 结束语

在秘密共享方案的研究中,为了实现可验证性,并构造出信息论安全且信息率为 1 的秘密共享方案一直是一个挑战. 本文基于多线性映射,构造了一个信息率渐进最优的可验证秘密共享方案. 在此方案中,首先,利用多线性映射这一工具和拉格朗日插值的方法构造了 (t,n) 门限秘密共享方案,使得至少 t 个参与者合作才能重构出秘密;其次,通过多线性映射的多线性性质对子秘密进行验证,从而实现了秘密共享方案的可验证性功能;最后,性能分析结果表明所提方案是高效且信息论安全的.

参考文献

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[A]. Proceedings of the National Computer Conference[C]. Germany:Springer-Verlag,1979,48:313-317.

[3] CHOR B,DOLDWASSER S,MICALI S,et al. Presence of faults[A]. Proc 26th IEEE Symposium on Foundations of Computer Sciences (FOCS′85)[C]. Los Angeles,1985. 383-395.

[4] Feldman P. A practical scheme for non-interactive verifiable secret sharing[A]. Proc 28th IEEE Symposium on Foundations of Computer Sciences(FOCS′87)[C]. Los Angeles, 1987. 427-438.

[5] Heidarvand S,Villar J L. Public verifiability from pairings in secret sharing schemes[A]. International Workshop on Selected Areas in Cryptography (SAC 2008)[C]. Springer Berlin Heide-lberg,2008. 294-308.

[6] MTOPA H. How to share a secret with cheaters[J]. Journal of Cryptology,1988,1(2):133-138.

[7] 田有亮,马建峰,彭长根. 椭圆曲线上的信息论安全的可验证秘密共享方案[J]. 通信学报,2011,32(12):96-102.
Tian Y L,Ma J F,Peng C G. Information-theoretic secure verifiable secret sharing scheme on elliptic curve group[J]. Journal on Communications,2011,32(12):96-102. (in Chinese)

[8] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM, J Compute, 2003, 32(3): 586 – 615.

[9] BAI F, et al. The IMPORTANT framework for analyzing the impact of mobility on performance of routing for Ad Hoc networks[J]. Ad Hoc Networks, 2003, 1(4): 383 – 403.

[10] 许春香,傅小彤,肖国镇. 预防欺诈的矢量空间秘密共享方案[J]. 西安电子科技大学学报:自然科学版,2002,29(4):527 – 529.
XU C X, FU X T, XIAO G Z. A vector space secret sharing scheme against cheating[J]. Journal of Xidian University: Natural Science, 2002, 29(4): 527 – 529. (in Chinese)

[11] CORON J S, LEPOINT T, TIBOUCHI M. Practical multilinear maps over the integers[A]. Advances in Cryptology-Crypto[C]. BERLIN: SPINGER-VERLAG, 2013. 476 – 493.

[12] 张敏情,张腾飞,王绪安. 基于多线性映射的可公开验证加密[J]. 武汉大学学报,2014,60(6):507 – 512.
Zhang M Q, Zhang T F, Wang X A. Publicly verifiable encryption in multilinear maps[J]. Journal of Wuhan University, 2014, 60(6): 507 – 512. (in Chinese)

[13] Coron J S, Lepoint T, Tibouchi M. Practical Multilinear Maps Over the Integers[A]. Advances in Cryptology-CRYPTO 2013[M]. Berlin Heidelberg Springer, 2013, 476 – 493.

[14] 田有亮,彭长根. 基于双线性对的可验证秘密共享方案[J]. 计算机应用,2007,27(B12):125 – 127.
Tian Y L, Peng C G. Verifiable secret sharing scheme based on bilinear pairing[J]. Computer Applications, 2007, 27(B12): 125 – 127. (in Chinese)

[15] 田有亮,彭长根. 基于双线性对的可验证秘密共享方案及其应用[J]. 计算机工程,2009,35(10):158 – 161.
Tian Y L, Peng C G. Verifiable secret sharing and its applications based on bilinear pairings[J]. Computer Engineering, 2009, 35(10): 158 – 161. (in Chinese)

[16] 李慧贤,庞辽军. 基于双线性变换的可证明安全的秘密共享方案[J]. 通信学报,2008,29(10):45 – 49.
Li H X, Pang L J. Provably secure secret sharing scheme based on bilinear maps[J]. Journal on Communications, 2008, 29(10): 45 – 49. (in Chinese)

[17] PEDERSON T P. Non-interactive and information theoretic secure verifiable secret sharing[A]. Cryptology-CRYPTO' 91[C]. Berlin: Springer-Verlag, 1992. 129 – 140.

[18] 庞辽军,王育民. 基于 RSA 密码体制(t,n)门限秘密共享方案[J]. 通信学报,2005,26(6):70 – 73.
Pang L J, Wang Y M. Secret sharing scheme based on RSA cryptosystem(T, n) threshold[J]. Journal on Communications, 2005, 26(6): 70 – 73. (in Chinese)

作者简介

彭　巧　女,1991 年生于湖北孝感. 贵州大学数学与统计学院信息安全硕士生. 研究方向为信息安全和云计算上的隐私保护、大数据及其密码应用.
E-mail: 1107304865@qq.com

田有亮(通信作者)　男,1982 年生于贵州六盘水. 贵州大学教授,博士生导师,贵州省公共大数据重点实验室学术带头人,贵州大学密码学与数据安全研究所副所长. 研究方向为博弈论、密码学、信息安全.
E-mail: youliangtian@163.com