DOI:10.3969/j.issn.1003-5060.2025.04.018

一种可验证的(k,n)门限多秘密共享方案

张宏图, 胡 航, 李富林
(合肥工业大学 数学学院,安徽 合肥 230601)

摘 要:基于排列和Diffie-Hellman问题,文章提出一种可验证的(k,n)门限多秘密共享方案。该方案中排列的使用确保了计算生成的秘密份额的安全性,在Diffie-Hellman问题的假设下,各参与者的伪份额均由自己生成,基于相关等式是否成立实现了方案的可验证性。各参与者只需维护1个彼此不同的伪份额即可根据门限值k进行多个秘密的重构。结果表明,该方案不需要安全信道,各参与者的伪份额可重复使用,且可以抵抗合谋攻击和外部攻击。

关键词:多秘密共享;门限恢复;可验证性;排列;Diffie-Hellman问题
中图分类号:TN918.1 **文献标志码**:A **文章编号**:1003-5060(2025)04-0544-05

A verifiable (k,n) threshold multi-secret sharing scheme

ZHANG Hongtu, HU Hang, LI Fulin
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

Abstract: Based on the permutation and Diffie-Hellman problem, a verifiable (k,n) threshold multi-secret sharing scheme is proposed. In the scheme, the application of the permutation ensures the security of the secret shares generated by calculation. Under the assumption of the Diffie-Hellman problem, participants' pseudo-shares are generated by themselves. The verifiability of the scheme is achieved based on whether the relevant equation holds. Each participant only needs to maintain a pseudo-share that is different from each other to reconstruct multiple secrets according to the threshold value k. Further analysis shows that the scheme does not need a secure channel, the pseudo-share of each participant can be reused, and it can resist collusion and external attacks.

Key words: multi-secret sharing; threshold recovery; verifiability; permutation; Diffie-Hellman problem

0 引 言

秘密共享技术在网络通信等领域中扮演着至关重要的角色,可以利用它将秘密信息共享给其他人。就秘密共享方案而言,门限秘密共享方案是普遍的。文献[1-2]最早提出了门限秘密共享方案,该方案的主要思想是将共享的秘密划分为若干个伪份额,此后只要有不少于门限个数的有效伪份额就可以恢复共享的秘密。

随着对门限秘密共享方案性能要求的提高,研究者们发现了该方案的一些不足之处。基于此,文献[3]提出一种多秘密共享方案;文献[4]介绍了一种理想的多秘密共享方案,该方案在秘密恢复后,每个参与者各自保存的伪份额仍可再使用;文献[5]提出一种各参与者都能验证伪份额的一致性的秘密共享方案,且还能验证秘密分发者的欺骗行为;文献[6]构造了可抵抗秘密分发者的欺骗、可对参与者的诚实性进行检验的秘密共享

收稿日期:2022-05-05;**修回日期**:2022-11-09
基金项目:国家自然科学基金资助项目(12171134);国家自然科学基金联合基金资助项目(U21A20428)
作者简介:张宏图(1997—),男,安徽合肥人,合肥工业大学硕士生;
李富林(1979—),男,安徽巢湖人,博士,合肥工业大学副教授,硕士生导师.

方案，但该方案中各参与者的伪份额不具有可重复使用性；文献[7]研究了一种高效的、可验证的多秘密共享方案，为了验证秘密共享是否有效，各参与者必须检验多个方程；文献[8-9]提出门限可验证的多秘密共享方案，在秘密重构阶段，恢复秘密的参与者可以有效地验证其他参与者的伪份额的一致性，即可以有效地抵抗合谋攻击；文献[10]提出门限多秘密共享方案，该方案通过在参与者之间构造会话密钥，以此形成一个安全的通信环境，有效地抵抗外部攻击；文献[11]提出可以在异步环境下对多个秘密进行恢复的秘密共享方案，并证明了文献[10]在 1 个秘密被恢复后，剩下未被恢复的秘密均可由 $k-1$ 个参与者重构得到，解决了安全性有限的问题。然而，如果参与者发送与其合谋参与者的伪份额给诚实参与者，那么诚实参与者的秘密恢复过程会被阻止，因此不能抵抗合谋攻击[11]。此外，为了恢复共享的秘密，各参与者均需要保存不止一个数据，增加了参与者的存储负担[10-11]。

本文基于 Diffie-Hellman 问题和排列设计了一种可验证的(k,n)门限多秘密共享方案。秘密分发者计算得到的秘密份额的安全性可以通过使用排列的方法来确保，各参与者分别选择自己的份额。基于 Diffie-Hellman 问题的假设，各参与者的伪份额均由他们各自生成，且与秘密分发者之间不需要安全信道进行伪份额的传输。任何参与者均可利用相关等式是否成立来验证其他参与者以及秘密分发者的诚实性。在秘密恢复阶段，基于异或运算以及 Diffie-Hellman 问题的假设，参与者之间可以安全地进行伪份额的交互，以使得外部攻击可以被阻止。最后，只要有不少于 k 个不同的正确的伪份额，多个共享的秘密(s 个秘密)就可以被恢复。特别地，各参与者分别只需存储 1 个自选的份额即可共享这 s 个秘密，且在共享秘密改变后各参与者的伪份额均可再使用。结果表明，本文提出的方案可以抵抗合谋攻击。

1　基础知识

1.1　Diffie-Hellman 问题

定义 1[12]　设 G 是一个 p 阶循环加法群，S 是群 G 的一个生成元，其中 p 是一个大素数。

1) DL(discrete logarithm)问题。对于给定的 S,$Q\in G$，使 $a\in Z_p^*$ 满足 $Q=aS$ 是困难的。

2) CDH(computational Diffie-Hellman)问题。对于 a,$b\in Z_p^*$，给定 S、aS、bS，计算 abS 是困难的。

1.2　排列

定义 2　排列是指从确定个数的元素集合中取出目标个数的元素，再对取出的元素进行排序。具体来说，假设从 n 个不同元素中任取 m($m\leqslant n$，m 与 n 均为自然数，下同)个不同的元素，并按照一定的顺序排列。此外，从 n 个不同元素中取出 m($m\leqslant n$)个元素的所有排列的个数，称作从 n 个不同元素中取出 m 个元素的排列数，用符号 $A(n,m)$表示，其中，$A(n,m)=n(n-1)\cdots(n-m+1)$。特别地，本文规定 $0!=1$。

2　本文方案

本文做以下规定：

1) n 个参与者 $P_1,P_2,\cdots,P_n$；

2) k($k<n$)个需要共享的秘密 $S_1,S_2,\cdots,S_k$；

3) 假设本文中 n 的选择需要满足 $n!>2^{256}$；

4) 本文方案需要一个 NB 公告牌，秘密分发者 D 公布的信息都会被记录在该公告牌上，并且只有 D 可以修改、更新公告牌上的内容，其他人只能阅读或者下载；

5) 本文方案出现的“+”运算均表示为模 p 的加法运算，其中 p 是一个大素数。

本文方案主要由初始化阶段、构造阶段、验证阶段、恢复阶段 4 个重要阶段组成。

2.1　初始化阶段

D 公布参数(p,G,S)，其中 p 是一个大素数，G 是有限域 GF(p)上的一个加法循环群，S 是 G 的一个生成元。

参与者 P_i 先为自己选择一个份额 $r_i\in Z_p^*$，并计算 $R_i=r_iS$，然后隐私保存 r_i，最后将 R_i 发送给 D，其中 $i=1,2,\cdots,n$。

D 需要确保 R_i 的唯一性，即需要判断 $R_i\neq R_t\Leftrightarrow r_iS\neq r_tS$ 是否成立，其中 $i,t=1,2,\cdots,n$，且 $i\neq t$。如果不成立，那么 D 必须要求这些参与者重新选择并发送它们的 R_i，直到 R_i 彼此互不相同为止。如果 R_i 彼此互不相同，那么 D 在 NB 公告牌上公布信息(x_i,R_i)，其中 x_i 代表参与者 P_i 的唯一身份信息，$x_i\in Z_p^*$，$i=1,2,\cdots,n$。

2.2　构造阶段

D 选择 $t_1,t_2,\cdots,t_k\in Z_p^*$，并使用 k($k<n$)个数对(t_1,S_1)，(t_2,S_2)，…，(t_k,S_k)构造一个 $k-1$ 次多项式：

$$E(x)=e_0+e_1x+\cdots+e_{k-1}x^{k-1}(\mathrm{mod}\ p)\qquad(1)$$

其中，第 $k-1$ 次项的系数需要满足 $e_{k-1}\neq 0$。

利用式(1)以及参与者的身份信息 x_i,D 计算并获得 n 个不同的点 $\boldsymbol{v}_i=(x_i,y_i)$,记 $y_i=E(x_i)$为秘密份额,计算并且公布$(x_i,H(y_i))$,其中 $H(y_i)$为 y_i 的哈希值,$i=1,2,\cdots,n$。

根据计算得到的秘密份额 $y_1,y_2,\cdots,y_n$,D 构造一个排列随机数 $T=e_1|e_2|\cdots|e_n$,其中:$e_t=y_i;i,t=1,2,\cdots,n$。排列随机数 T 是由秘密份额 y_i 随机排列产生的,此时只有 D 知道 y_i 的排列顺序,且排列的情况有 $A(n,n)=n!$ 种。

假设 $n=4$,D 计算得到的 4 个秘密份额分别为 $y_1=456,y_2=36,y_3=12,y_4=4$。$D$ 对这 4 个不同的秘密份额进行随机排列,若此时 $e_1=4=y_4,e_2=12=y_3,e_3=456=y_1,e_4=36=y_2$,则 D 公布的排列随机数 $T=41\ 245\ 636$。D 设秘密份额 y_i 的第 1 位数在 T 中所在的位置为 t_i,若 $y_1=456,y_2=36,y_3=12,y_4=4$,且排列随机数 $T=41\ 245\ 636$,则 $t_1=4,t_2=7,t_3=2,t_4=1$,其中,i、$t=1,2,\cdots,n$。

D 设秘密份额 y_i 的长度为 u_i,若 $y_1=456,y_2=36,y_3=12,y_4=4$,则 $u_1=3,u_2=2,u_3=2,u_4=1$,其中,$i=1,2,\cdots,n$。

D 选择一个私钥 $r\in Z_p^*$,再结合公开值 S,计算并公布 $R=rS$,其中生成的 R 需要确保 $R,R_1,R_2,\cdots,R_n$ 彼此互不相同。

参与者 P_i 与 D 互相确定参与者 P_i 的伪份额为 $\alpha_i=rR_i=rr_iS=r_iR=r_irS,i=1,2,\cdots,n$。

D 利用 n 个不同的点$(\alpha_1,t_1),(\alpha_2,t_2),\cdots,(\alpha_n,t_n)$构造一个 $n-1$ 次多项式 $E_1(x)$,记

$$E_1(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}(\mathrm{mod}\ p) \tag{2}$$

D 利用 n 个不同的点$(\alpha_1,u_1),(\alpha_2,u_2),\cdots,(\alpha_n,u_n)$构造一个 $n-1$ 次多项式 $E_2(x)$,记

$$E_2(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}(\mathrm{mod}\ p) \tag{3}$$

D 计算 A_i 和 M,$i=1,2,\cdots,n$,其中

$$A_i=(E_2(\alpha_i)+ME_1(\alpha_i))(\mathrm{mod}\ p) \tag{4}$$

$$M=H\left(S_1\|S_2\|\cdots\|S_k\right) \tag{5}$$

$H(\cdot):\{0,1\}^*\to Z_p^*$ 是一个合适的单向抗碰撞哈希函数。

2.3 验证阶段

对于恢复秘密的参与者 P_t,其他恢复秘密的参与者 P_i 会给 P_t 发送(x_i,T_i),其中,$T_i=\alpha_i\oplus\beta_{i\to t}$记为伪秘密份额,$\beta_{i\to t}=r_iR_t,1\leqslant i\leqslant n,1\leqslant t\leqslant n$;$P_t$ 会结合 r_t 和 R_i 解密 T_i,获得伪份额 α_i,P_t 通过判断式(6)是否成立来确定 P_i 的诚实性。式(6)如下:

$$A_i=\sum_{w=0}^{n-1}c_w(\alpha_i)^w(\mathrm{mod}\ p) \tag{6}$$

其中,$c_w=b_w+Ma_w(\mathrm{mod}\ p)$。

如果式(6)成立,那么说明 P_i 是诚实的,即此时 P_t 获得的伪份额 α_i 是正确且有效的。P_t 重复如上的验证工作,以此获得所有正确的伪份额。如果式(6)不成立,那么 P_t 选择与其他诚实的恢复秘密的参与者继续进行伪份额的交换,以此获得不少于 k 个不同的正确的伪份额来恢复共享的秘密。假设 F 表示所有欺骗者组成的集合,若 $n-|F|<k$,则停止秘密的恢复,其中 $|F|$ 表示集合 F 中欺骗者的个数。

2.4 恢复阶段

各参与者 P_i 计算各自的伪份额 $\alpha_i=r_iR$,$i=1,2,\cdots,n$。各参与者之间进行伪份额 α_i 的交互。在进行伪份额 α_i 的交互时,恢复秘密的参与者 P_i 给恢复秘密的参与者 P_t 发送$(x_i,T_i=\alpha_i\oplus\beta_{i\to t})$,而不是直接发送$(x_i,\alpha_i)$,其中,$\beta_{i\to t}=r_iR_t=R_ir_t$。

参与者 P_t 对接收到的(x_i,T_i)进行验证。参与者 P_t 结合自选的份额 r_t 以及公开的(x_i,R_i),计算得到 $\beta_{i\to t}=r_tR_i$,计算获得伪份额 $\alpha_i=T_i\oplus\beta_{i\to t}$,结合上述验证阶段对计算得到的 α_i 进行验证,进而判断 P_i 的诚实性。

不失一般性,假设此时有 k 个诚实的参与者 $P_1,P_2,\cdots,P_k$ 参与秘密的恢复,即此时每个恢复秘密的参与者 P_t 均可获得 k 个正确的伪份额 $\alpha_1,\alpha_2,\cdots,\alpha_k,1\leqslant t\leqslant k$。

恢复秘密的参与者 P_t 均可将 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 分别代入式(2)和式(3)中,计算得到 $t_i=E_1(\alpha_i)$和 $u_i=E_2(\alpha_i)$,$i=1,2,\cdots,k,1\leqslant t\leqslant k$;其次,$P_t$ 均可利用计算得到的 t_i、u_i 以及公开的排列随机数 T 获得 y_i,进而获得 k 个不同的有效的点 $\boldsymbol{v}_i=(x_i,y_i)$,$i=1,2,\cdots,k$;恢复秘密的参与者 P_t 可利用 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_k$ 重构多项式 $E(x)$,结合重构的 $E(x)$ 以及公开的 $t_1,t_2,\cdots,t_k$,共享的秘密 $S_1=E(t_1)$,$S_2=E(t_2),\cdots,S_k=E(t_k)$均可被恢复。

综上所述,只要有不少于 k 个诚实的参与者参与秘密共享,那么共享的多个秘密都可以被恢复。

3 安全性分析

为了便于分析,本文给出了以下 5 个命题以

及相应的证明。

命题 1　在参与者诚实并正确地执行本文方案的基础上，任意合法的授权集合均可成功恢复所共享的秘密。

证明　设$\gamma=\{P_1,P_2,\cdots,P_k\}$是一个最小授权集合。首先，恢复秘密的参与者$P_t$从NB公告牌上查获$R=rS$，并计算自己的伪份额$\alpha_t=r_tR$，$1\leqslant t\leqslant k$；随后，参与者$P_t$需要验证$D$的诚实性，在确定自己的伪份额$\alpha_t$是正确的基础上才会与其他恢复秘密的参与者$P_u(1\leqslant u\leqslant k)$互换伪份额，假设参与者$P_t$已经验证了$D$是诚实的，且获得了$k$个正确的伪份额$\alpha_1,\alpha_2,\cdots,\alpha_k$，则参与者$P_t$会将$\alpha_i$分别代入多项式$E_1(x)$和$E_2(x)$，计算得到$t_i$和$u_i$；再结合公开的排列随机数$T$获得$y_i$，$i=1,2,\cdots,k$，参与者$P_t$可以获得$k$个不同的有效的点$\boldsymbol{v}_i=(x_i,y_i)$，$i=1,2,\cdots,k$；利用拉格朗日插值公式和$k$个点$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_k$，参与者$P_t$可以重构多项式$E(x)$，进而结合公开的数$t_1,t_2,\cdots,t_k$恢复共享的秘密$S_1=E(t_1)$，$S_2=E(t_2)$，$\cdots$，$S_k=E(t_k)$。综上所述，$S_1,S_2,\cdots,S_k$可被任意合法的授权集$\gamma$恢复。

命题 2　各参与者均可验证秘密分发者D是否诚实。

证明　各参与者的份额均由其各自选择和生成，即在此处D不存在欺骗。

参与者P_t计算自己的伪份额$\alpha_t=r_tR$，并计算$t_t=E_1(\alpha_t)$和$u_t=E_2(\alpha_t)$，根据t_t、u_t以及公开的T得出y_t'，通过判断等式$H(y_t')=H(y_t)$是否成立来确定秘密分发者D的诚实性，$1\leqslant t\leqslant n$。若该式成立，则说明D是诚实的（此时说明参与者P_t的伪份额α_t是有效的）；否则说明D存在欺骗行为。

命题 3　在秘密恢复阶段，各恢复秘密的参与者均可验证其他恢复秘密的参与者的诚实性。

证明　在秘密恢复阶段，各恢复秘密的参与者P_t在验证秘密分发者D是诚实的基础上，通过判断等式$A_u=\sum_{w=0}^{n-1}c_w(\alpha_u^*)^w(\bmod p)$是否成立来确定其他恢复秘密的参与者$P_u$是否诚实，其中，$\alpha_u^*$是由$P_u$发送给$P_t$的伪份额，$1\leqslant t\leqslant n$，$1\leqslant u\leqslant n$。若该式成立，则说明$P_u$是诚实的；否则说明$P_u$存在欺骗行为。

命题 4　若没有份额r_i以及私钥r，则外部攻击者不可能从公开的信息（或者截获的信息T_i）中解密获得α_i和y_i，$1\leqslant i\leqslant n$，即本文可抵抗外部攻击。

证明　在排列以及$n!>2^{256}$的假设下，攻击者不可能通过公开的排列随机数T得到对应的秘密份额y_i。此外，在Diffie-Hellman问题的假设下，攻击者不可能通过公开的R_i、R得到对应参与者的份额r_i和秘密分发者D的私钥r，进而不可能通过截获T_i得到对应参与者的伪份额α_i，即不可能通过公开的多项式$E_1(x)$、$E_2(x)$得到对应的t_i、u_i，进而不能获得y_i。

命题 5　在秘密恢复阶段，本文可抵抗合谋攻击。

证明　在秘密恢复阶段，各参与者之间进行(x_u,T_u)的交互（本文假设x_u不能被篡改），然后恢复秘密的参与者P_t会结合r_t、(x_u,T_u)、$(A_1,A_2,\cdots,A_n)$以及$E_1(x)$、$E_2(x)$和M对其他恢复秘密的参与者P_u的诚实性进行验证，$1\leqslant t\leqslant n$，$1\leqslant u\leqslant n$。如果P_u给P_t发送$T_u=\alpha_i\oplus\beta_{u\to t}$，那么$P_t$会利用等式$A_u=\sum_{w=0}^{n-1}c_w(\alpha_i)^w(\bmod p)$不成立来确定$P_u$发送的伪份额不满足一致性，其中$\alpha_i$为参与者$P_u$通过与参与者$P_i$合谋获得的伪份额，$1\leqslant i\leqslant n$。

4　结　　论

本文介绍了一种可验证的(k,n)门限多秘密共享方案。各参与者自选自己的份额，并且基于Diffie-Hellman问题的假设，用于恢复共享秘密的伪份额都由各参与者自己生成，其优点是避免了由分发份额或者伪份额产生的秘密分发者的欺骗行为，实现了各参与者的伪份额可重复使用，且还实现了各参与者分别只需维护1个份额即可实现多个秘密的安全共享。此外，在秘密构造阶段，本文利用排列将秘密分发者计算生成的秘密份额构造成一个公开的排列随机数，且在秘密恢复阶段，各参与者之间进行伪秘密份额的交互，而不是直接进行伪份额的交互，其优点是可以抵抗外部攻击。

与此同时，恢复秘密的参与者均可通过判断相关等式是否成立来验证对应参与者的伪份额的一致性，其优点是可以及时验证对应参与者的诚实性以及抵抗参与者之间的合谋攻击。本文主要贡献在于，从排列和Diffie-Hellman问题的角度出发，设计了一种不需要安全信道且可抵抗合谋攻击以及外部攻击的可验证的(k,n)门限多秘密共享方案。

[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[C]// 1979 International Workshop on Managing Requirements Knowledge (MARK). New York:IEEE,1979:313-318.

[3] HE J,EDWARD D. Multistage secret sharing based on one-way function [J]. Electronics Letters, 1994, 30 (19): 1591-1592.

[4] JACKSON W A,MARTIN K,O'KEEFE C M,et al. Ideal secret sharing schemes with multiple secrets[J]. Journal of Cryptology,1996,9(4):233-250.

[5] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proceedings of the 26th IEEE Symposium on Foundations of Computer Science. Portland: IEEE, 1985: 383-395.

[6] CHEN D,LU W,XING W W,et al. An efficient verifiable threshold multi-secret sharing scheme with different stages [J]. IEEE Access,2019,7:107104-107110.

[7] HARN L. Efficient sharing (broadcasting) of multiple secrets[J]. IEEE Proceedings-Computers and Digital Techniques,1995,142(3):237-240.

[8] MARYAM S G,MOJTABA B,CHRISTOPHE D. Threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem[J]. IET Information Security,2019,13(3):278-284.

[9] WANG N,CAI Y Y,FU J S,et al. Information privacy protection based on verifiable (t,n)-threshold multi-secret sharing scheme[J]. IEEE Access,2020,8:20799-20804.

[10] HARN L,HSU C F. (t,n) Multi-secret sharing scheme based on bivariate polynomial[J]. Wireless Personal Communications,2017,95(2):1495-1504.

[11] ZHANG T,KE X Z,LIU Y X. (t,n) Multi-secret sharing scheme extended from Harn-Hsu's scheme[J]. EURASIP Journal on Wireless Communications and Networking, 2018,2018(1):1-4.

[12] DIFFIE W,HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory,1976, 22(6):644-654.

(责任编辑 闫杏丽)

(上接第543页)

[参 考 文 献]

[1] 吴梁玉,陈永平,施明恒,等. 流动聚焦微通道中双重乳液乳化行为研究[J]. 工程热物理学报,2014,35(6):1167-1169.

[2] 吴梁玉. 双乳液的制备及其流体动力学行为研究[D]. 南京:东南大学,2016.

[3] UTADA A S,LORENCEAU E,LINK D R,et al. Monodisperse double emulsions generated from a microcapillary device[J]. Science,2005,308(5721):537-541.

[4] PAN D,CHEN Q,CHEN S,et al. Experimental study on millimeter-scale W1/O/W2 compound droplets formation in a co-flowing device with two-step structure[J]. Chemical Engineering Science,2020,216:115493.

[5] LU P,WU L,LIU X. Visualization study of oil-in-water-in-oil (O/W/O) double emulsion formation in a simple and robust co-flowing microfluidic device [J]. Micromachines, 2017,8(9):268.

[6] ZHOU C,YUE P,FENG J J. Formation of simple and compound drops in microfluidic devices[J]. Physics of Fluids, 2006,18(9):092105.

[7] 刘赵淼,杜宇,逄燕. W/O/W型双乳液滴在微通道内生成过程的研究[J]. 分析化学,2018,46(3):324-331.

[8] NABAVI S A,VLADISAVLJEVIĆ G T,GU S,et al. Double emulsion production in glass capillary microfluidic device: parametric investigation of droplet generation behaviour [J]. Chemical Engineering Science,2015,130:183-196.

[9] LIU X,WU L,ZHAO Y,et al. Study of compound drop formation in axisymmetric microfluidic devices with different geometries[J]. Colloids and Surfaces A (Physicochemical and Engineering Aspects),2017,533:87-98.

[10] MICHELON M,LEOPÉRCIO B C,CARVALHO M S. Microfluidic production of aqueous suspensions of gellan-based microcapsules containing hydrophobic compounds [J]. Chemical Engineering Science,2020,211:115314.

(责任编辑 胡亚敏)