Advances in Applied Mathematics 应用数学进展, 2024, 13(12), 5164-5173
Published Online December 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.1312499

Hans汉斯

基于CRT和RSA的指定参与者的门限秘密共享方案

陈宇臻[1]，黄可可[2]，林昌露[1*]

[1]福建师范大学数学与统计学院，福建 福州
[2]福建师范大学计算机与网络空间安全学院，福建 福州

收稿日期：2024年11月20日；录用日期：2024年12月13日；发布日期：2024年12月23日

摘 要

针对医院间共享数据的实际需求，本文基于中国剩余定理结合RSA公钥加密分别设计了指定一个参与者和指定多个参与者的门限秘密共享方案，以实现医疗数据的安全共享。在秘密分发阶段，指定参与者可自主选择秘密份额，且无需在分发者与参与者之间建立安全信道；在秘密重构阶段，必须有特定的参与者参与才能成功恢复原始秘密。对方案的安全性与性能分析表明，所提出方案在效率和安全性上均优于现有方案。

关键词

门限秘密共享，指定参与者，中国剩余定理，RSA

Threshold Secret Sharing Scheme with Designated Participants Based on CRT and RSA

Yuzhen Chen[1], Keke Huang[2], Changlu Lin[1*]

[1]School of Mathematics and Statistics, Fujian Normal University, Fuzhou Fujian
[2]College of Computer and Cyber Security, Fujian Normal University, Fuzhou Fujian

Received: Nov. 20th, 2024; accepted: Dec. 13th, 2024; published: Dec. 23rd, 2024

Abstract

In order to meet the practical needs of sharing data between hospitals, this paper proposes a

*通讯作者。

文章引用: 陈宇臻, 黄可可, 林昌露. 基于 CRT 和 RSA 的指定参与者的门限秘密共享方案[J]. 应用数学进展, 2024, 13(12): 5164-5173. DOI: 10.12677/aam.2024.1312499

threshold secret sharing scheme for designating one participant and designating multiple participants based on the Chinese remainder theorem combined with RSA public key encryption, so as to realize the secure sharing of medical data. In the secret distribution phase, the designated participants can choose their own secret shares, and there is no need to establish a secure channel between the distributor and the participants; in the secret reconstruction phase, a designated participant must be involved in order to successfully recover the original secret. The analysis of the security and performance of the scheme shows that the proposed scheme is better than the existing scheme in terms of efficiency and security.

Keywords

Threshold Secret Sharing, Designated Participants, Chinese Remainder Theorem, RSA

1. 引言

在如今的信息时代，数据安全尤为重要，秘密共享能够将某个秘密信息分成多个秘密份额共享给方案中的参与者，使得只有达到特定数量的秘密份额才能够恢复出原始的秘密信息，是保护数据隐私性的重要密码技术之一。Shamir [1]和 Blakley [2]分别基于不同的工具提出了门限秘密共享方案，只有重构阶段的参与者提供的秘密份额数量等于或大于门限值时，可以重构得到秘密信息，否则这些参与者得不到关于秘密的任何信息。为了防止方案中的某些欺骗行为，1985 年，Chor 等人[3]提出了可验证秘密共享的概念。1987 年，Feldman [4]设计了一种非交互的可验证秘密共享方案，该方案基于循环群上的离散对数困难假设。1983 年，Asmuth 和 Bloom [5]提出了在整数环上基于中国剩余定理的门限秘密共享方案。在此基础上，Iftene [6]和 Qiong 等[7]基于中国剩余定理分别提出了一种可验证的秘密共享方案，但是这两种方案都无法阻止腐败的分发者分发不一致的份额给参与者。2010 年，Harn 和 Lin [8]提出了强的 t-一致性和强可验证秘密共享的定义并构造了强可验证秘密共享方案。2007 年，唐韶华[9]从电子招标系统的实际需求出发，采用多重门限的方法设计了指定人必须参与的秘密共享、以组为单位的秘密共享、指定组必须参与的秘密共享等算法解决了实际问题。2014 年，Subba 等[10]提出了基于中国剩余定理的多秘密共享方案，该方案是将多个秘密分发给不同的组，这样每个组都接收到为其准备的秘密，同时每个参与者的秘密份额可以重复使用。Harn 和 Miao [11]提出了基于中国剩余定理的带权重的秘密共享方案，该方案是一个门限秘密共享方案，同时每个参与者具有不同的权重，当参与重构的参与者的权重大于等于门限值才可以恢复秘密，小于门限值则无法恢复秘密，该方案通过对每个参与者的模数进行处理使得每个参与者的模数与其权重数相关。此外，Harn 和 Miao [12]提出了一种基于中国剩余定理的分层门限秘密共享方案，但是这个方案不是完备的，并且生成满足特定要求的素数成本较高。2015 年，Dong [13]利用中国剩余定理和 RSA 加密构造了秘密共享方案，该方案基于离散对数问题假设，不需要分发者和参与者的安全信道，同时参与者可以自行选择自己的秘密份额。2018 年，Ning 等[14]首次提出了基于多项式环的中国剩余定理的秘密共享方案，方案利用素性检测来查找两两互素的多项式作为参与者的模数，并且该方案是理想和完备的，该方案指出了 Shamir 的秘密共享方案是其方案的一个特例，将基于中国剩余定理的秘密共享方案和 Shamir 的秘密共享方案联系起来了。2022 年，Wu 等[15]指出 Ning 等[14]方案产生互素多项式非常耗时，导致效率低下。因此，Wu 等在不检查多项式不可约性的情况下，通过直接生成互素多项式构造了基于多项式环上的中国剩余定理的秘密共享方案，并利用公因子构建对称的安全信道并且实

现消息验证，确保收到的消息是正确的。

另一方面，随着互联网 + 智慧医院的建设，医院业务架构愈加复杂，业务对接众多外部数据使用单位，存在有众多对外数据服务接口。由于医院数据中包含大量高价值、高敏感的个人隐私信息，例如某些病人的个人信息，病人的病历档案数据等。因此医院数据安全治理工作任务重、难度大。Health Level Seven International (HL7)定义了快速医疗保健互操作性资源(FHIR, Fast Healthcare Interoperability Resources)标准，以有效地交换和集成各种医疗机构(如诊所、初级保健医生、保险公司、医院等)之间的电子医疗保健数据[16]。2023 年，Yang 等[17]为解决在多医院环境中使用 FHIR 的安全性问题，分别提出了基于群组的秘密共享方案(GSS, Group-Based Secret Sharing)和基于指数的群组秘密共享方案(EGSS, Exponential-Based Group Secret Sharing Scheme)，方案基于多项式和 ElGamal 密码系统，在区块链上进行验证。但是该方案存在安全漏洞：在所提出的指定一个参与者的方案中，不需要指定的参与者，其他大于门限值的参与者可以合谋恢复原始秘密，无法达到声称的安全性。

因此，本文基于中国剩余定理与 RSA 加密方案，设计了两个指定参与者的秘密共享方案，其中方案一是指定一个参与者的秘密共享方案；方案二是指定多个参与者的秘密共享方案。 本文提出的方案可以用于下面场景：假设有一位病人甲，他因病到医院 A 就诊，完成诊疗后其病历数据由 A 医院保管并储存在 A 的病历数据库。但 A 医院 A 的医疗条件无法治愈甲的疾病，此时甲要去医院 B 和 C 进一步就诊治疗，由于甲先前在医院 A 就诊过，那么医院 B 和 C 可以将其在医院 A 就诊时的病历作为参考，即医院 B 和 C 需要访问医院 A 的数据库以获取甲的病历数据。当医院 B 和 C 想要访问甲的病历数据时医院 A 的授权，可以用秘密共享方案实现医院 B 和 C 对甲的病例数据的访问，但是为保护数据的隐私性，在共享时需要医院 A 的授权，也就是说，在秘密共享的重构阶段一定需要医院 A 的参与才可以使医院 B 和 C 得到甲的病例数据，即在重构阶段一定需要医院 A 的秘密份额才可以确保医院 B 和 C 恢复秘密。这是指定一个参与者(医院 A)的秘密共享方案的场景，当医院 B 和 C 获取了甲的病历数据时，当新的医院 D 想要获取甲的病历数据，在秘密共享方案的重构阶段就一定需要 A、B 和 C 的秘密份额才可以恢复秘密。因此，指定一个参与者的情况可以推广到指定多个参与者。

本文主要贡献如下所示：

1) 通过利用 RSA 加密算法，基于中国剩余定理分别构造了指定一个参与者和指定多个参与者的门限秘密共享方案，其中指定的参与者可自行选择值作为自己的私钥，不需要在分发者和参与者之间建立安全信道，并且在重构阶段其他参与者可以验证指定参与者的份额的正确性。

2) 通过对方案安全性与性能分析表明，该方案是安全的，能够同时具备可验证性、指定参与者参与重构的功能。

2. 预备知识

本节主要介绍中国剩余定理和 Asmuth-Bloom 的秘密共享方案。

2.1. 中国剩余定理(CRT, Chinses Remainder Theorem)

定义 1 (中国剩余定理[18]) 随机选择两两互素的整数 $m_1, m_2, \cdots, m_n$，对于任意的整数 $a_1, a_2, \cdots, a_n$，满足 $a_i \in \mathbb{Z}_{m_i}$ $(i = 1, 2, \cdots, n)$，$\mathbb{Z}_{m_i}$ 为整数模 m_i 的剩余类环，则下列同余方程组

$$\begin{cases} X \equiv a_1 \left(\mathrm{mod}\, m_1\right), \\ X \equiv a_2 \left(\mathrm{mod}\, m_2\right), \\ \quad \vdots \\ X \equiv a_n \left(\mathrm{mod}\, m_n\right). \end{cases}$$

在模 $M=m_1\cdot m_2\cdots\cdots m_n$ 下有唯一解，解为 $X=\sum_{i=1}^{n}a_iM_iy_i\left(\mathrm{mod}\,M\right)$，其中 $M_i=M/m_i$，$y_i=M_i^{-1}\left(\mathrm{mod}\,m_i\right)$，$X=CRT\left(a_1,a_2,\cdots,a_n\right)$。

2.2. Asmuth-Bloom 的秘密共享方案

本小节介绍 Asmuth-Bloom 的 (t,n) 门限秘密共享方案，具体过程分为以下两个阶段：

- **秘密分发阶段**
  - D 选择两两互素的正整数 $m_0,m_1<m_2<\cdots<m_n$ 并且满足 $\prod_{i=0}^{t}m_i>m_0\prod_{i=1}^{t-1}m_{n-i+1}$。
  - D 选取秘密 $s\in\left(0,m_0-1\right)$，并选取随机的整数 p 使得 $s+pm_0\in\left(\prod_{i=n-t+2}^{n}m_i,\prod_{i=1}^{t}m_i\right)$。
  - D 计算 $s_i=s+pm_0\left(\mathrm{mod}\,m_i\right)$ 作为参与者 $P_i\left(i=1,2,\cdots,n\right)$ 的秘密份额，并通过安全信道发送给对应的参与者。
- **秘密重构阶段**
  - 假设进行重构的参与者为 $P_1,P_2,\cdots,P_t$，他们将各自的秘密份额集中起来可以得到下面的同余方程组

$$\begin{cases}X\equiv s_1\left(\mathrm{mod}\,m_1\right),\\X\equiv s_2\left(\mathrm{mod}\,m_2\right),\\\quad\vdots\\X\equiv s_t\left(\mathrm{mod}\,m_t\right).\end{cases}$$

  - 利用中国剩余定理可以得到在区间 $\left[0,\prod_{i=1}^{t}m_i-1\right]$ 内有唯一解，记为 x_0，又因为 $s+pm_0$ 同样满足上述的同余方程并且 $s+pm_0$ 也在区间 $\left[0,\prod_{i=1}^{t}m_i-1\right]$ 内，由解的唯一性可以得到 $s+pm_0=x_0$，并可以通过 $s=x_0\left(\mathrm{mod}\,m_0\right)$ 恢复出秘密。

3. Yang 等的方案和安全性分析

本节分析 Yang 等[17]的指定一个参与者的秘密共享方案，其中 3.1 节介绍具体方案，3.2 节对 Yang 等的指定一个参与者的秘密共享方案的安全性漏洞给出一个具体示例分析。

3.1. Yang 等方案回顾

Yang 等[17]方案中的指定一个参与者的秘密共享方案是一个 (t,n) 门限秘密共享方案，有 n 个参与者 $\left\{P_1,P_2,\cdots,P_n\right\}$，该方案在重构阶段需要指定参与者 P_{ID} 的参与才能够恢复秘密，否则就算多于 t 个参与者也无法恢复秘密，下面介绍方案的细节：

- **秘密分发阶段**
  - D 随机选取一个 $t-1$ 次多项式

$$f\left(x\right)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\left(\mathrm{mod}\,p\right),$$

其中秘密 $s=a_0$ 且 $a_1,a_2,\cdots,a_{t-1}\in\mathbb{F}_p$，$p$ 为一个素数。

  - 对于 $1\le i\le n$，当 $i=ID$ 时，D 计算秘密份额 $s_i=f\left(ID\right)$，当 $i\ne ID$ 时，D 计算秘密份额 $s_i=f\left(i\right)+f\left(ID\right)\left(\mathrm{mod}\,p\right)$，将 s_i 通过安全信道发给对应的参与者。

- **秘密重构阶段**
  - 在参与者收到对应的份额后，参与者 P_{ID} 和其他任意 $t-1$ 个参与者共同合作可以恢复秘密。P_{ID} 向其他参与重构的参与者发送秘密份额 $s_i = f(ID)$，其他参与者可以通过 $f(ID)$ 得到对应的 $f(i)$。
  - 参与者将得到的 $f(i)$ 集中起来利用拉格朗日插值公式(1)计算得到

$$f(x)=\sum_{i=1}^{t} s_i \prod_{j=1, j\neq i}^{t} (x-j)/(i-j) \pmod p,$$

从而得到秘密 $s = f(0) = a_0$。

3.2. Yang 等方案安全性分析

本节用一个简单的(2,3)门限秘密共享方案来说明 Yang 等[17]指定一个参与者的秘密共享方案的安全性漏洞。

假设有三个参与者，记为 A、B 和 C，并且假设 C 是指定的参与者，即重构时需要 C 的参与，否则 A 和 B 合谋无法恢复秘密，为说明 Yang 等[17]方案的安全隐患，给出 A、B 合谋而不需要 C 参与的情况下，成功恢复秘密的示例：

- 选取素数 p，假设生成的多项式为 $f(x) = a_0 + a_1 x \pmod p$，$C$ 作为指定参与者拿到的秘密份额为 $t_{ID} = f(3) = a_0 + 3a_1 \pmod p$，$A$ 拿到的秘密份额为 $s_1 = t_1 + t_{ID} = f(1) + f(3) = 2a_0 + 4a_1 \pmod p$，$B$ 拿到的秘密份额为 $s_2 = t_2 + t_{ID} = f(2) + f(3) = 2a_0 + 5a_1 \pmod p$。
- A 和 B 将他们的秘密份额集中起来，可以得到一个方程组

$$\begin{cases} 2a_0 + 4a_1 \pmod p = s_1, \\ 2a_0 + 5a_1 \pmod p = s_2. \end{cases}$$

将 $s_2 - s_1$ 就可以得到多项式的系数 a_1 再代入原方程组就可以得到秘密 a_0，重构过程不需要 C 的参与。即该方案无法达到所声明的安全性，无法满足指定参与者参与重构过程才能恢复原始秘密，因此 Yang 等[17]所构造的指定一个参与者的秘密共享方案存在安全隐患。

4. 方案设计

本节提出两个方案，方案一是指定一个参与者的秘密共享方案；方案二是指定多个参与者的秘密共享方案，两个方案都是 (t,n) 门限秘密共享，在初始化阶段，利用 RSA 公钥加密，由指定参与者选取自己的私钥并保管，计算公钥发送给分发者后由分发者公开相关参数，利用公开值，参与重构的参与者可以验证指定参与者的份额的正确性。

4.1. 方案一：指定一个参与者的秘密共享方案

- **初始化阶段**
  - 有 n 个参与者 $\{P_1, P_2, \cdots, P_n\}$，假设指定参与重构的参与者记为 P_Δ，$\Delta \in (1,2,\cdots,n)$，将 P_Δ 的份额记为 S_Δ。
  - D 选取两个大素数 $p = 2m+1$，$q = 2n+1$，其中 m 和 n 也都为素数，且任何人都不能有效地分解因式 $N = pq$，然后 D 选择整数 g 使得 $1 < g < N$，$(g,N) = 1$ 且 $(g \pm 1, N) = 1$，P_Δ 从 $[2,N]$ 中随机选取整数 s_Δ，计算 $R_\Delta = g^{s_\Delta} \pmod N$ 发送给 D。
  - D 选取整数 e 满足 $1 < e < \varphi(N) = (p-1)(q-1)$，使得 $(e, \varphi(N)) = 1$，D 计算 $S_0 = g^e \pmod N$，再用拓展的欧几里得算法计算唯一的整数 h，其中 $1 < h < \varphi(N)$，使得 $eh \equiv 1 \pmod{\varphi(N)}$，最后 D 公开

g，N，S_0，h，R_Δ。

- **秘密分发阶段**
  - D 选择两两互素的正整数 $m_0, m_1 < m_2 < \cdots < m_n$ 并且满足 $\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1}$。
  - D 选择秘密 $s \in (0, m_0 - 1)$，并选取随机的整数 p 使得 $s + pm_0 \in \left(\prod_{i=n-t+2}^{n} m_i, \prod_{i=1}^{t} m_i \right)$。
  - 对于 $1 \le i \le n$，当 $i = \Delta$ 时，D 计算份额 $S'_\Delta = (s + pm_0) (\mathrm{mod}\, m_\Delta) \oplus R_\Delta^e (\mathrm{mod}\, N)$，当 $i \ne \Delta$ 时，D 计算份额 $S'_i = (s + pm_0) (\mathrm{mod}\, m_i) \oplus R_\Delta^e (\mathrm{mod}\, N)$，其中 $\oplus$ 表示异或运算。将 S'_i 发给对应的参与者。

注意，由于指定参与者 P_Δ 与分发者 D 在初始化阶段利用 RSA 加密使得方案的原始秘密份额 S_i 和 S_i 被隐藏在秘密份额 S'_i 和 S'_Δ，所以此方案在秘密分发阶段不需要安全信道。

- **秘密重构阶段**
  - 假设参与者 $P_1, P_2, \cdots, P_{t-1}, P_\Delta$ 参与重构阶段想要恢复秘密，P_Δ 利用公开值 S_0 和自己的私钥 s_Δ 计算 $R_\Delta^e = S_0^{s_\Delta}$ 向其他参与者公开值 R_Δ^e。
  - 验证阶段：其他参与者收到值 R_Δ^e 后可以验证式子 $R_\Delta^{eh} \equiv R_\Delta (\mathrm{mod}\, N)$ 是否成立，若成立，则进行下一步，若不成立，则停止重构。
  - 所有参与者验证通过后，将份额 S'_i 与公开值 R_Δ^e 做异或运算并将 t 个参与者的份额集中起来可以得到下面的同余方程组

$$\begin{cases} x \equiv S'_1 \oplus R_\Delta^e (\mathrm{mod}\, N) (\mathrm{mod}\, m_1), \\ x \equiv S'_2 \oplus R_\Delta^e (\mathrm{mod}\, N) (\mathrm{mod}\, m_2), \\ \quad \vdots \\ x \equiv S'_\Delta \oplus R_\Delta^e (\mathrm{mod}\, N) (\mathrm{mod}\, m_\Delta). \end{cases}$$

  - 利用中国剩余定理可以得到在区间 $\left[0, \prod_{i=1}^{t} m_i - 1 \right]$ 内有唯一解，记为 x_0，又因为 $s + km_0$ 同样满足上述的同余方程并且 $s + km_0$ 也在区间 $\left[0, \prod_{i=1}^{t} m_i - 1 \right]$ 内，由解的唯一性可以得到 $s + km_0 = x_0$，并可以通过 $s = x_0 (\mathrm{mod}\, m_0)$ 恢复出秘密。

4.2. 方案二：指定k个参与者的秘密共享方案

下面将指定一个参与者的方案推广到指定 $k (2 \le k \le t-1)$ 个参与者，具体过程如下：

- **初始化阶段**
  - 有 n 个参与者 $\{P_1, P_2, \cdots, P_n\}$，假设指定参与重构的参与者记为 $P_{\Delta_1}, P_{\Delta_2}, \cdots, P_{\Delta_k}$，$\Delta_i \in (1, 2, \cdots, n), (i = 1, 2, \cdots, t)$，将 P_{Δ_i} 的份额记为 S_{Δ_i}。
  - D 选取两个大素数 $p = 2m + 1$，$q = 2n + 1$，其中 m 和 n 也都为素数，且任何人都不能有效地分解因式 $N = pq$，然后 D 选择整数 g 使得 $1 < g < N$，$(g, N) = 1$ 且 $(g \pm 1, N) = 1$，P_Δ 从 $[2, N]$ 中随机选取整数 s_{Δ_i}，计算 $R_{\Delta_i} = g^{s_{\Delta_i}} (\mathrm{mod}\, N)$ 发送给 D，D 在收到 R_{Δ_i} 后要确保对于 $i \ne j$ 时，$R_{\Delta_i} \ne R_{\Delta_j}$，否则需要指定参与者重新选择直到 $R_{\Delta_i} \ne R_{\Delta_j}$ 为止。
  - D 选取整数 e 满足 $1 < e < \varphi(N) = (p-1)(q-1)$，使得 $(e, \varphi(N)) = 1$，D 计算 $S_0 = g^e (\mathrm{mod}\, N)$，再用拓展的欧几里得算法计算唯一的整数 h，其中 $1 < h < \varphi(N)$，使得 $eh \equiv 1 (\mathrm{mod}\, \varphi(N))$，最后 D 公开 g，N，S_0，h，R_Δ。

- **秘密分发阶段**
  - D 选择两两互素的正整数 $m_0, m_1 < m_2 < \cdots < m_n$ 并且满足 $\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1}$。
  - D 选择秘密 $s \in (0, m_0 - 1)$，并选取随机的整数 p 使得 $s + pm_0 \in \left(\prod_{i=n-t+2}^{n} m_i, \prod_{i=1}^{t} m_i \right)$。
  - 对于指定参与者 $P_{\Delta_1}, P_{\Delta_2}, \cdots, P_{\Delta_k}$，$\Delta_i \in (1,2,\cdots,n), (i = 1,2,\cdots,t)$，$D$ 计算秘密份额 $S'_{\Delta_i} = (s + p \cdot m_0) \left(\mathrm{mod}\, m_{\Delta_i}\right) \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)$，对于剩下的参与者，$D$ 计算秘密份额 $S'_i = (s + p \cdot m_0) \left(\mathrm{mod}\, m_i\right) \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)$，其中 $\oplus$ 表示异或运算。将 S'_{Δ_i} 和 S'_i 发给对应的参与者。

注意，由于指定参与者 P_{Δ_i} 与分发者 D 在初始化阶段利用 RSA 加密使得方案的原始秘密份额 S_i 和 S_Δ 被隐藏在秘密份额 S'_i 和 S'_{Δ_i} 中，所以此方案在秘密分发阶段不需要安全信道。

- **秘密重构阶段**
  - 假设指定的 k 个参与者 $P_{\Delta_1}, P_{\Delta_2}, \cdots, P_{\Delta_k}$ 和剩下的任意 $t-k$ 个参与者一起参与重构。每个指定参与者利用公开值 S_0 和各自的私钥 s_{Δ_i}，分别计算 $R^e_{\Delta_i} = S_0^{s_{\Delta_i}}$，并向其他参与者公开值 $R^e_{\Delta_i}$。
  - 验证阶段：其他参与者收到值 $R^e_{\Delta_i}$ 后，通过验证 $R^{eh}_{\Delta_i} \equiv R_{\Delta_i} \left(\mathrm{mod}\, N\right)$ 是否成立，若成立，则进行下一步；若不成立，则停止重构。
  - 所有参与者通过验证后，将份额 S'_i 与所有公开值 $R^e_{\Delta_i}$ 作异或运算并将 t 个参与者的份额集中起来可以得到同余方程组

$$\begin{cases} x \equiv S'_{\Delta_1} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{\Delta_1}\right), \\ x \equiv S'_{\Delta_2} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{\Delta_2}\right), \\ \quad \vdots \\ x \equiv S'_{\Delta_k} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{\Delta_k}\right), \\ x \equiv S'_{i_1} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{i_1}\right), \\ x \equiv S'_{i_2} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{i_2}\right), \\ \quad \vdots \\ x \equiv S'_{i_{t-k}} \oplus R^e_{\Delta_1} \oplus R^e_{\Delta_2} \oplus \cdots \oplus R^e_{\Delta_k} \left(\mathrm{mod}\, N\right)\left(\mathrm{mod}\, m_{i_{t-k}}\right). \end{cases}$$

  - 利用中国剩余定理可以得到在区间 $\left[0, \prod_{i=1}^{t} m_i - 1\right]$ 内有唯一解，记为 x_0，又因为 $s + km_0$ 同样满足上述的同余方程并且 $s + km_0$ 也在区间 $\left[0, \prod_{i=1}^{t} m_i - 1\right]$ 内，由解的唯一性可以得到 $s + km_0 = x_0$，并可以通过 $s = x_0 \left(\mathrm{mod}\, m_0\right)$ 恢复出秘密。

5. 方案分析

本节对第 4 节提出的方案进行安全性分析，由于方案二可以看作是方案一的一般情况，所以只对方案二进行安全性分析。

定理 **1** 若方案二中参与重构的参与者数量大于等于 t 并且包含指定的 k 个参与者 P_{Δ_i}，则参与重构的参与者按照重构阶段步骤可以恢复秘密。

证明：该方案的秘密重构过程主要分为两个步骤，第一步由指定参与者 P_{Δ_i} 向其他参与重构的参与者公开值 $R^e_{\Delta_i}$，其他参与重构的参与者收到公开值后，验证式子 $R^{eh}_{\Delta_i} \equiv R_{\Delta_i} \left(\mathrm{mod}\, N\right)$ 是否成立来确保 P_{Δ_i} 没有欺

骗行为，所有重构的参与者通过验证后，进行重构的第二步，参与者将自己的秘密份额 S_i' 与所有的公开值 $R_{\Delta_i}^e$ 做异或运算后，可以得到原始的秘密份额，得到原始秘密份额后，大于等于 t 个参与者将他们的秘密份额集中起来，基于 Asmuth-Bloom 的门限秘密共享方案和中国剩余定理可以恢复出秘密 s。

定理 **2** 若方案二中参与重构的参与者数量大于等于 t，但不全包含指定的 k 个参与者 P_{Δ_i}，则参与重构的参与者无法恢复秘密。

证明：不妨假设有 $k-1$ 个指定参与者属于参与重构的参与者子集中，则剩下的参与者数量大于等于 $t-k+1$，也大于等于 $t-k$，这里不妨假设第 k 个指定的参与者 P_{Δ_k} 不属于参与重构的参与者子集中，由于 P_{Δ_k} 没有参与重构，则其他参与者无法得到公开值 $R_{\Delta_k}^e$，另一方面，又因为大整数的素因子分解是困难的，所以参与者无法从公开值 N 中得到系统参数 e，从而也无法得到公开值 $R_{\Delta_k}^e$，而得不到公开值 $R_{\Delta_k}^e$ 就无法计算得到每个参与者的原始秘密份额，也就无法恢复秘密 s。

定理 **3** 若方案二中重构阶段参与者数量小于 t，则参与重构的参与者无法恢复秘密。

证明：记参与者重构的参与者子集为 Γ，考虑两种情况：

- 情况 1：指定参与者 $P_{\Delta_1}, P_{\Delta_2}, \cdots, P_{\Delta_k} \in \Gamma$，由于指定的 k 个参与者都参与重构，从而参与重构的参与者可以利用公开值 $R_{\Delta_i}^e$ 计算出原始的秘密份额，但由于参与重构的参与者数量小于 t，不妨假设由 $t-1$ 个参与者参与重构，则他们在得到原始秘密份额后，利用中国剩余定理可以得到在模 $t-1$ 个模数 m_i 下的唯一解，记为 x_0，但是根据 $\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1}$，可以得到秘密 s 为 x_0 的正整数倍并且这 $t-1$ 个参与者恢复秘密的概率为 $\frac{1}{m_0}$。
- 情况 2：指定参与者 $P_{\Delta_1}, P_{\Delta_2}, \cdots, P_{\Delta_k}$ 不全属于 Γ 不妨假设有 $k-1$ 个指定参与者属于参与重构的参与者子集中，则根据定理 2，参与重构的参与者无法恢复秘密 s。

综上所述，少于 t 个参与者参与重构无法恢复秘密。

6. 方案对比

本节将本文方案二与文献[9]方案和文献[17]方案进行对比，后者两个方案都是基于多项式构造，方案二基于中国剩余定理构造。文献[9]方案对指定 k 个参与者和剩下的 $n-k$ 个参与者分别构造 (k,k) 和 $(t-k,n-k)$ 门限方案，通过将两个方案的秘密相关联达到指定参与者的目的。文献[17]方案利用秘密共享方案的同态性，让每个参与者作为分发者向其他参与者分发秘密份额，其他参与者的秘密份额中包含指定参与者的秘密份额，以达到指定参与者的目的，份额的验证在区块链上进行。但文献[9]方案和文献[17]方案都需要分发者和参与者间的安全信道。

表 1 给出了三个方案的安全属性对比，本文方案二利用 RSA 公钥加密验证指定参与者的份额，在分发阶段指定参与者与分发者交互生成私钥，所以在分发阶段不需要参与者和分发者的安全信道，并且可以满足安全性。

Table 1. Security property comparisons among the secret sharing with the designed multiple participants
表 1. 指定多个参与者的秘密共享方案的安全属性比较

方案	可验证	安全信道	安全性
唐韶华方案[9]	×	需要	√
Yang 等方案[17]	√	需要	×
本文方案二	√	不需要	√

符号说明：√表示具备性质；×表示不具备性质。

表 2 给出了三个方案的效率对比，由于在重构阶段要解同余方程组，所以方案二的计算复杂度为$O\left(tm^2\right)$，其中 m 为每个参与者模数的大小。但方案二的公开值个数比文献[9]方案和文献[17]方案的公开值更少。

Table 2. Efficiency comparisons among the secret sharing with the designed multiple participants
表 2. 指定多个参与者的秘密共享方案的效率比较

方案	公开值个数	计算复杂度
唐韶华方案[9]	$2n+4$	$O\left(t^2\right)$
Yang 等方案[17]	$nk-n$	$O\left(t^2\right)$
本文方案二	$n+k+5$	$O\left(tm^2\right)$

符号说明：t 为方案门限值；m 为每个参与者模数的大小。

7. 总结

本文基于中国剩余定理和 RSA 公钥密码系统，提出了两个指定参与者必须参与重构的秘密共享方案。方案一是指定一个参与者的秘密共享方案，方案二是指定多个参与者的秘密共享方案。与其他方案相比，本文方案利用 RSA 公钥加密实现在分发阶段不需要参与者和分发者间的安全信道和在重构阶段可验证参与者份额的功能。本文方案能满足病人病历在医院间数据库安全共享的实际应用需求。

基金项目

福建省高校产学合作科技计划项目(2023H6012)。

参考文献

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[2] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. 1979 *International Workshop on Managing Requirements Knowledge* (*MARK*), New York, 4-7 June 1979, 313-318. https://doi.org/10.1109/mark.1979.8817296

[3] Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B. (1985) Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. 26*th Annual Symposium on Foundations of Computer Science* (*SFCS* 1985), Portland, 21-23 October 1985, 383-395. https://doi.org/10.1109/sfcs.1985.64

[4] Feldman, P. (1987) A Practical Scheme for Non-Interactive Verifiable Secret Sharing. 28*th Annual Symposium on Foundations of Computer Science* (*SFCS* 1987), Los Angeles, 12-14 October 1987, 427-438. https://doi.org/10.1109/sfcs.1987.4

[5] Asmuth, C. and Bloom, J. (1983) A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, **29**, 208-210. https://doi.org/10.1109/tit.1983.1056651

[6] Iftene, S. (2007) Secret Sharing Schemes with Applications in Security Protocols, Technical Report. University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science.

[7] Li, Q., Wang, Z.F. and Niu, X.M. (2005) A Non-Interactive Modular Verifiable Secret Sharing Scheme. 2005 *Proceedings on Communications, Circuits and Systems*, Hong Kong, 27-30 May 2005, 84-87.

[8] Harn, L. and Lin, C. (2010) Strong (n, t, n) Verifiable Secret Sharing Scheme. *Information Sciences*, **180**, 3059-3064. https://doi.org/10.1016/j.ins.2010.04.016

[9] 唐韶华. 特殊门限秘密共享方法及其应用[J]. 华南理工大学学报(自然科学版), 2007(10): 168-171+177.

[10] Subba, R.Y.V. and Bhagvati, C. (2014) CRT Based Threshold Multi Secret Sharing Scheme. *International Journal of Network Security*, **16**, 249-255.

[11] Harn, L. and Miao, F.Y. (2013) Weighted Secret Sharing Based on the Chinese Remainder Theorem. *International Journal of Network Security*, **2013**, 420-425.

[12] Harn, L. and Fuyou, M. (2014) Multilevel Threshold Secret Sharing Based on the Chinese Remainder Theorem. *Information Processing Letters*, **114**, 504-509. https://doi.org/10.1016/j.ipl.2014.04.006

[13] Dong, X.D. (2015) A Multi-Secret Sharing Scheme Based on the CRT and RSA. *International Journal of Electronics and Information Engineering*, **2**, 47-51.

[14] Ning, Y., Miao, F., Huang, W., Meng, K., Xiong, Y. and Wang, X. (2018) Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem. In: *Lecture Notes in Computer Science*, Springer 310-331. https://doi.org/10.1007/978-3-030-03332-3_12

[15] Wu, L., Miao, F., Meng, K. and Wang, X. (2021) A Simple Construction of CRT-Based Ideal Secret Sharing Scheme and Its Security Extension Based on Common Factor. *Frontiers of Computer Science*, **16**, 1-9. https://doi.org/10.1007/s11704-021-0483-9

[16] Vorisek, C.N., Lehne, M., Klopfenstein, S.A.I., Mayer, P.J., Bartschke, A., Haese, T., *et al*. (2022) Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review. *JMIR Medical Informatics*, **10**, e35724. https://doi.org/10.2196/35724

[17] Yang, C., Li, P., Cheng, H., Kuo, H., Lu, M. and Xiong, L. (2024) A Security Model of Multihospital FHIR Database Authorization Based on Secret Sharing and Blockchain. *IEEE Internet of Things Journal*, **11**, 10325-10335. https://doi.org/10.1109/jiot.2023.3328989

[18] Cohen, H. (2013) A Course in Computational Algebraic Number Theory. Springer Science & Business Media.