Computer Science and Application 计算机科学与应用, 2025, 15(2), 237-245
Published Online February 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.152051

Hans汉斯

基于NTRU可验证的秘密分享方案

宋怡浓[1]，梁碧滢[2]，李子臣[1*]

[1]北京印刷学院信息工程学院，北京
[2]北京信息科技大学计算机与通信工程学院，北京

收稿日期：2025年1月22日；录用日期：2025年2月21日；发布日期：2025年2月28日

摘　要

随着信息技术的快速发展，数据安全问题日益受到重视。本文提出了一种可验证的秘密分享方案，该方案基于Shamir秘密分享方案，并结合NTRU数字签名算法，增强方案的安全性。NTRU数字签名算法作为一种能够抵抗量子攻击的数字签名算法，有效防御了伪造和篡改攻击，确保了秘密恢复过程的可信度。本文详细分析了方案的正确性和安全性。

关键词

Shamir秘密分享，NTUR，数字签名，可验证秘密分享

A Verifiable Secret Sharing Scheme Based on NTRU

Yinong Song[1], Biying Liang[2], Zichen Li[1*]

[1]School of Information and Engineering, Beijing Institute of Graphic Communication, Beijing
[2]School of Computer and Communication Engineering, Beijing Information Science and Technology University, Beijing

Received: Jan. 22nd, 2025; accepted: Feb. 21st, 2025; published: Feb. 28th, 2025

Abstract

With the rapid development of information technology, data security issues are increasingly being taken seriously. This paper proposes a verifiable secret sharing scheme based on the Shamir secret sharing scheme and combined with the NTRU digital signature algorithm to enhance the security of the scheme. The NTRU digital signature algorithm, as a type of digital signature algorithm capable of resisting quantum attacks, effectively defends against forgery and tampering attacks, ensuring the credibility of the secret recovery process. This paper provides a detailed analysis of the correctness

*通讯作者。

文章引用: 宋怡浓, 梁碧滢, 李子臣. 基于 NTRU 可验证的秘密分享方案[J]. 计算机科学与应用, 2025, 15(2): 237-245.
DOI: 10.12677/csa.2025.152051

and security of the scheme.

Keywords

Shamir Secret Sharing, NTRU Encrypt, Digital Signature, Verifiable Secret Sharing

1. 引言

随着计算机和通信技术的迅速发展，秘密分享作为一种关键的密码技术逐渐被广泛应用。其基本思想是将一条秘密信息拆分成多个部分，将各部分分发给不同的成员，只有当足够多的成员合作时，才能重构出原始秘密。

1979 年，Shamir [1]基于拉格朗日多项式提出了经典的(t,n)阈值秘密分享方案。Shamir 的方案将秘密分割为 n 个部分，需要至少 t 个秘密才能恢复原始秘密。该方案因其简单而高效，成为密码学中的经典方法。秘密分享技术是一种用于划分秘密信息(如口令、密钥等)的加密技术。将秘密分成多个份额，只有在满足一定的门限条件时，才能重构出原始的秘密信息[2]-[4]。秘密分享为信息安全提供了强有力的保障，但也面临着一些挑战。目前，大多数秘密分享方案都是基于传统数学困难问题假设，如因子分解、离散对数等[5]-[7]。然而，随着 Shor [8]在 1994 年提出了一种量子算法来解决多项式内的因子分解问题，越来越多的学者提出了针对传统数学困难问题量子破解算法的研究，证明了基于传统数学困难问题方案的脆弱性。因此，迫切需要研究新的后量子方案。从实用的角度来看，基于格的秘密分享具有重要的研究意义和应用前景，特别是它的一些特殊性质，如可验证性、多秘密性等，从而拓宽了秘密分享在不同场景中的应用[9] [10]。1996 年，Hoffstein 等人提出了 NTRU 公钥加密方案[11]，并首次提出了 NTRU 假设。2000 年，NTRU 公钥加密方案的三位作者利用 NTRU 提出了 NSS 数字签名体制[12]，其安全性与在某个格中寻找短的向量有关。2003 年，Hoffstein 等人基于 NTRU 提出了签名方案[13]，作为 GGH 签名方案的高效实现。2014 年，Hoffstein 等人基于 NTRU 提出了 Hash And Sign 类型的签名方案[14]。国内学者也对 NTRU 签名算法进行了深入研究，并取得了显著成果。2006 年，杨真真等人结合格中的最近向量问题(CVP)和单向哈希函数的不可逆性，提出了一种基于 NTRU 的数字签名方案[15]。2008 年，胡予濮提出了一种新型的 NTRU 类数字签名方案[16]，该方案通过将公钥恢复私钥与格上的最小向量问题(SVP)等价，伪造签名与格上的最近向量问题(CVP)等价，但可能泄露私钥信息。2015 年，曹杰等人提出了一种新型基于 NTRU 的签名方案[17]，并对其安全性进行了全面分析，探讨了副本分析等攻击方法，同时优化了签名验证的速度。

本文提出了一种基于 NTRU 数字签名算法的(t,n)秘密分享方案，从理论上对方案的安全性和正确性进行了证明。利用 NTRU 数字签名算法，有效防止了恶意解码和篡改。

本文第 2 节介绍了秘密分享的基本概念，格理论的相关知识，以及 NTRU 公钥加密算法的核心原理，为理解本文提出的方案打下基础。第 3 节详细描述了该方案的设计和实现过程，包括参数设置、方案初始化、秘密分享过程和秘密重建过程。此部分重点阐述了如何结合 NTRU 算法和 Shamir 的阈值方案，以实现高效且安全的秘密分享。第 4 节对提出的方案进行了详细的正确性和安全性分析。通过定理的证明，验证了方案的理论可行性和安全性保障。第 5 节总结了本文的主要贡献，并提出了未来的研究方向和改

进建议。

2. 基础知识

2.1. 秘密分享

Shamir 秘密分享是一种将秘密分割成多个份额的方法[18]，使得只有当一定数量的份额组合在一起时，原始秘密才能被恢复。这个过程可以用以下步骤描述：

1) 秘密分发：设有 n 个参与者进行秘密分享，存在可信方为管理者，秘密为 S，管理者选择一个足够大的素数 q，构造多项式 $s(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\left(\mathrm{mod}\,q\right)$ 其中 $a_0=S$，$a_1,\cdots,a_{t-1}$ 是随机生成的系数，t 是恢复秘密所需的最小份额数。

2) 生成份额：对于 $i=1,2,\cdots,n$，管理者计算 $s(x_i)$，其中 x_i 是为每个参与者生成的随机值；每个 $(x_i,s(x_i))$ 称为一个份额，其中 i 是份额的索引，$s(x_i)$ 是份额的值。

3) 秘密恢复：t 个参与者通过拉格朗日插值法恢复多项式 $s(x)$，恢复多项式后，可以通过计算 $s(0)$ 来恢复秘密 S。

2.2. 偏差

定义 1 (偏差) 给定两个多项式 $a(X)$ 和 $b(X)$，首先将它们的系数模 q 约简到区间 $\left[-\frac{q}{2},\frac{q}{2}\right]$，再将它们的系数模 p 约简到区间 $\left[-\frac{p}{2},\frac{p}{2}\right]$，化简后的多项式分别为：

$$\overline{a}(X)=\overline{a}_0+\cdots+\overline{a}_{N-1}X^{N-1}$$

$$\overline{b}(X)=\overline{b}_0+\cdots+\overline{b}_{N-1}X^{N-1}$$

偏差是两个多项式在模 p 情况下的不同系数的位置的数量：

$$Dev(a,b)=\#\left\{i:\overline{a}_i\neq\overline{b}_i\bmod p\right\}$$

其中 # 表示集合的元素个数。偏差是验证签名的核心指标，用于确保签名 s 和秘密 m 的关联性，其中 $D_{\min}$ 和 $D_{\max}$ 控制允许的偏差范围。通过偏差验证，可以在签名和消息之间引入一定的“容忍度”，既保证签名有效性，又增强安全性。实际计算中，多项式的卷积和模运算可能引入小的系数偏差。偏差允许一定程度的误差，而不影响签名的真实性。

偏差范围的设置避免了直接解码攻击：如果没有偏差 $D_{\min}=D_{\max}=0$，攻击者可以通过多次观察完全恢复私钥。偏差的存在迫使攻击者处理更高维度的格问题，显著增加破解难度。

偏差范围的选择直接影响安全性和签名验证速度：较大的 $D_{\max}$ 提高了效率，但降低安全性。较小的 $D_{\max}$ 增强了安全性，但增加了计算开销。

2.3. NTRU 格

定义 2 (NTRU 格)给定环 $R_q=\mathbb{Z}_q[x]/(X^N-1)$，$q$ 是素数，N 是 2 的幂，设 $f,g\in R_q$ (f 存在逆元 $f^{-1}\in R_q$)，$h=f^{-1}\cdot g\bmod q$。则 NTRU 格由 q 和 h 定义为：

$$\Lambda_{h,q}=\left\{(u,v)\in R^2\mid u+vh=0\bmod q\right\}$$

2.4. NTRU 数字签名

NTRU 数字签名的核心思想是利用公共和私有密钥对，这些密钥的形式与 NTRU 公钥密码体系中使

用的密钥相同。公钥是一个多项式 h，私钥是一个多项式 f。签名过程涉及选择一个多项式 w，它与消息 m 和私钥 f 相乘，生成签名 s。验证过程需要检查 s 与 m 的偏差是否在允许的范围内，以及使用公钥 h 计算出的多项式 c 与另一个多项式 $g_0 \cdot m$ 的偏差是否也在允许的范围内。NTRU 数字签名方案介绍见表 1：

Table 1. NTRU lattice-based signature scheme
表 1. NTRU 数字签名方案

步骤 1：密钥生成	NTRU 数字签名方案涉及五个参数 $(N, p, q, D_{\min}, D_{\max})$。选择两个多项式 f 和 g，计算 f 在模 q 情况下的逆元 f^{-1}，然后计算公钥 $h \equiv f^{-1} \cdot g \pmod{q}$
步骤 2：签名过程	构造一个掩码多项式 w，然后对消息 m 计算签名 $s \equiv f \cdot w \pmod{q}$，则签名是 (m, s)
步骤 3：验证过程	检查 $s \neq 0$ 并验证两个条件：s 和 $f_0 \cdot m$ 的偏差是否在 $D_{\min}$ 和 $D_{\max}$ 之间，以及 $c \equiv h \cdot s \bmod q$ 和 $g_0 \cdot m$ 的偏差是否在 $D_{\min}$ 和 $D_{\max}$ 之间

3. 基于 NTRU 可验证的秘密分享方案设计

文献[19]-[21]介绍了格理论在秘密共享技术中的应用，在本节将详细介绍基于 NTRU 数字签名算法的可验证秘密分享方案的设计，包括参数设置、方案初始化、秘密分享过程和秘密重建过程，首先，参数设置部分见表 2。

3.1. 参数设置

Table 2. Parameter settings
表 2. 参数设置

N	NTRU 中使用的多项式的最高次数，通常作为素数
q	NTRU 中的最大模数，通常为正整数
p	NTRU 中的最小模数，通常为小的正整数或低次幂的多项式
f, g	NTRU 中生成密钥的多项式
f^{-1}	f 模 p 下的逆元
w	NTRU 中用于加密的随机多项式

3.2. 秘密分享过程

管理员生成参数 (N, p, q)，选择可逆私有多项式 f 和多项式 g，形如：

$$f = f_0 + pf_1$$

$$g = g_0 + pg_1$$

其中 f_0, g_0 是固定的多项式，f_1, g_1 是具有小系数的随机多项式，从多项式集合 F_f 和 F_g 中选取，p 是一个小整数。计算多项式 f^{-1}，通过扩展欧几里得算法满足下式：

$$f^{-1} \cdot f \equiv 1 \pmod{q}$$

计算公钥如下式所示：

$$h \equiv f^{-1} \cdot g \pmod{q}$$

私钥为 (f, g)，公钥为 h，管理员将秘密转换为对应的十进制数，作为多项式 $sk(x)$ 中的常数项 m 进行计算，如下式所示：

$$sk(x)=m+\sum_{i=1}^{t-1}a_i x^i$$

3.3. 签名过程

计算 $sk_i=sk(x_i)$，$(i=1,2,\cdots,n)$。构造随机掩码 w_i，如下式：

$$w_i=sk_i+w'+pw''$$

其中 sk_i 为每位参与者所持有的份额，i 为每位参与者的 ID，w',w'' 是具有小系数的随机多项式。使用私钥多项式 f，计算签名：

$$s_i\equiv f\cdot w_i\pmod q$$

则签名结果为 (sk_i,s_i)，将 (x_i,sk_i,s_i) 作为份额通过安全信道传送给子份额持有者

3.4. 验证过程

文献[22]-[25]介绍了多种秘密共享份额验证方法，本文采用偏差(Deviation)概念[12]，用于衡量两个多项式在模 p 的情况下的不同程度。为了排除伪造的零签名，首先确保 $s_i\neq 0$，然后验证以下两个条件：

验证条件(A)：比较 s_i 和 $f_0\cdot m$ 的偏差：

$$D_{\min}\le Dev(s_i,f_0\cdot m)\le D_{\max}$$

验证条件(B)：使用公钥 h，计算 $c_i\equiv h\cdot s_i\pmod q$，比较 c_i 和 $g_0\cdot sk_i$ 的偏差

$$D_{\min}\le Dev(c_i,g_0\cdot sk_i)\le D_{\max}$$

如果验证条件(A)和(B)均满足，则签名有效，可进行秘密重建过程，否则，可通过对应未通过验证份额的索引 i 获得欺骗者的 ID。

3.5. 秘密重构过程

验证签名通过，可进行秘密重构，通过拉格朗日插值法对原始多项式进行重建，如下式所示：

$$sk(x)=\sum_{i=1}^{t}\left(sk_i\sum_{1\le j\le t}^{j\neq i}\frac{x-x_i}{x_j-x_i}\right)$$

当 $x=0$ 时，可得到 $sk(0)=m$。

4. 方案分析

4.1. 正确性分析

定理 1 本方案满足至少 t 个参与者可恢复秘密信息。

证明：本方案中秘密分发以及重建过程应用 Shamir 多项式和拉格朗日插值法，与文献[1]类似，并在此基础上增加了安全验证过程，保证可成功重建秘密的条件并且增加了更多的安全性。

定理 2 在 NTRU 签名方案中，如果私钥 f 和掩码多项式 $w_i=sk_i+w'+pw''$ 被正确选择，那么由 f 生成的签名 (sk_i,s_i) 必定能够通过验证条件 A 和 B。

证明：根据 NTRU 签名方案，签名 s 的生成公式为：

$$\begin{aligned}s_i&\equiv f\cdot w_i \bmod q\\&\equiv f_0\cdot sk_i+f_0\cdot w'+pf_0\cdot w''+pf_1\cdot w_i \bmod q\end{aligned}$$

上式可以分为主项 $f_0 \cdot m$、修正项 $f_0 \cdot w'$ 和随机项 $pf_0 \cdot w'' + pf_1 \cdot w_i$。

目标 1：证明 s_i 和 $f_0 \cdot m$ 的偏差满足 $Dev(s_i, f_0 \cdot sk_i) \le D_{\max}$。$w'$ 的设计是为了减少 s_i 和 $f_0 \cdot sk_i$ 的偏差；通过遍历每个系数位置，调整 w' 使偏差最小化。p 的选择限制了随机项的幅度；随机掩码 w'' 的稀疏性(例如，非零系数有限)确保随机项引入的噪声有限。

多项式 $f \cdot w_i$ 的系数在模 q 下可能出现截断。根据小系数多项式的性质，卷积的无穷范数满足：

$$\|f \cdot w_i\|_\infty \approx \gamma \cdot \|f\| \cdot \|w_i\|$$

其中 $\gamma < 0.15$ 是经验值，只要 $\gamma \cdot \|f\| \cdot \|w\| < q/2$，模 q 化简不会显著增加偏差。因此通过合理参数选择和 w', w'' 的设计，可以保证偏差 $Dev(s_i, f_0 \cdot sk_i)$ 满足条件。

目标 2：证明 c_i 和 $g_0 \cdot sk_i$ 的偏差满足 $Dev(c_i, g_0 \cdot sk_i) \le D_{\max}$。根据验证公式，$c_i$ 的计算为：

$$\begin{aligned} c_i &\equiv h \cdot s_i \bmod q = g \cdot w_i \bmod q \\ &\equiv g_0 \cdot sk_i + g_0 \cdot w' + pg_0 \cdot w'' + pg_1 \cdot w_i \bmod q \end{aligned}$$

主项 $g_0 \cdot sk_i$ 在模 p 下，理论上应与 c_i 的主要部分一致。修正项 $g_0 \cdot w'$ 和随机项 $pg_0 \cdot w'' + pg_1 \cdot w_i$ 的分析与目标 1 类似。模 q 化简得影响由 $g \cdot w_i$ 得无穷范数控制，通过参数设置可以确保截断误差不会引入额外偏差。

通过以上分析和推导，已证明本方案中签名方案的正确性。只要参数选择合理(如 $q, p, N, D_{\min}, D_{\max}$)，并正确生成签名 (sk_i, s_i)，签名将通过验证条件(A)和(B)。

4.2. 安全性分析

定理 3 本方案安全性基于格上最短向量困难问题。

证明：给定公钥 $h = f^{-1} \cdot g \bmod q$，攻击者希望通过 NTRU 格恢复私钥 (f, g)。令 NTRU 格为 L_{NTRU} 是一个 $2N$−维格，生成矩阵为：

$$B = \begin{bmatrix} I & H \\ 0 & qI \end{bmatrix}$$

其中 I 是 $N \times N$ 单位矩阵，H 是公钥 h 的循环矩阵。攻击者需要在格 L_{NTRU} 中找到短向量 (f, g)，使得：

$$f \cdot h \equiv g \bmod q$$

假设攻击者使用格约简算法(如 LLL 或 BKZ)，其复杂度与格的维度和最短向量长度密切相关。根据高斯启发式，L_{NTRU} 中最短向量长度为：

$$\lambda \approx \sqrt{\frac{q}{2\pi e}} \cdot N^{1/4}$$

如果私钥向量的欧几里得范数 $(\|f, g\|)$ 远小于 λ，则格约简攻击可能恢复私钥。因此本方案中推荐参数选取 $N = 251, q = 128$ 确保 $\|f, g\| \gg \lambda$。

定理 4 本方案随机搜索给定消息上的有效签名的概率是可忽略的。

证明：设想一名攻击者企图随机挑选出一条消息的有效签名[26]。他首先随机挑选一个符合条件(A)的 s 值，这一步相对容易，接着尝试找到一个符合条件(B)的 c_i 值。一旦找到，攻击者便伪造了签名；如果没找到，攻击者就更换 s 值重试。我们需要评估一个随机选择的、符合条件(A)的 s 值生成一个符合条件(B)的 c_i 值的几率。s 值的条件(A)对最终的 c_i 值没有实质影响，因为 c_i 值是通过 s 值乘以 h 并对 q 取模数得到的，而 h 的值在模 q 下接近于均匀分布。简而言之，我们是在计算一个随机选择的系数在 $-q/2$ 到

$q/2$ 区间内的多项式 c_i 满足条件(B)的概率。这个概率可以通过基础概率论来估算。

随机挑选的 c_i 的系数可以看作是 N 个独立的随机变量，它们的值在模 q 下均匀分布。sk_i 的系数是固定的目标值在模 p 下。我们需要计算随机挑选的 N 个整数元组在模 q 下的坐标至少为 $D_{\min}$ 且不超过 $D_{\max}$ 等于在模 p 下到固定目标值的概率。如果 q 远大于 p，那么这个概率可以近似为：

$$P\left(D_{\min} \le Dev\left(c_i, g_0 \cdot sk_i\right) \le D_{\max}\right) \approx \frac{1}{p^N} \sum_{d=D_{\min}}^{D_{\max}} \binom{N}{d} (p-1)^d$$

注意，对于条件(B)，概率是 p^{-N}，因为 $c_i \pmod p$ 的所有 N 个“随机”系数必须匹配 $g_0 \cdot sk_i$。所以使用随机选择的 s 成功伪造的概率可忽略。

定理 5 本方案可抵抗 NTRU 格结构及其针对公钥的格攻击。

证明：攻击者可以尝试从公钥 h 中提取私钥 f，无论是否有一长串真实签名。或者，他可以尝试在不知道 f 的情况下伪造签名，只使用 h。攻击者希望通过格约简算法从公钥中获得私钥。与 NTRU 密码系统的情况一样，通过这种方式恢复私钥相当于解决某类最短或最接近向量问题。

设 L 是一个行列式为 d，维数为 n 的格。设 v_0 表示给定的固定向量，可能是原点。设 r 表示一个给定的半径，并考虑定位一个向量 $v \in L$ 的问题，使得 $\|v - v_0\| < r$。对于大的 n，解决这个问题的难度与数量有关，κ 值是衡量格中最短向量与目标向量之间距离的一个指标：

$$\kappa = \kappa(L, r) = \frac{r}{d^{1/n}\sqrt{n/(2\pi e)}}$$

这里的分母是高斯启发式算法预测 L 中最短预期向量的长度。如果 $\kappa < 1$，那么高斯启发式表明，如果存在解决方案，那么解决方案可能是唯一的。κ 越接近 0，使用格约简方法找到唯一解决方案就越容易。当 κ 接近 1 时，格约简方法变得越无效。例如，设 $(L_n, r_n, v_{0,n})$ 是一系列格、半径和目标向量，其维度 n 不断增加，包含目标向量(即，满足 $|v_n - v_{0,n}| < r_n$)，且其 κ 值满足：

$$\kappa_n = \kappa(L_n, r_n) = b/\sqrt{n}$$

对于常数 b，格点归约方法找到目标向量 v_n 所需的时间像 $e^{\alpha n}$ 一样增长，α 的值大致与 b 成正比。类似地，如果 $\kappa \ge 1$，那么方程的解可能不是唯一的，但当 κ 接近 1 时，找到解会变得越来越困难。

由于本方案中的公钥与 NTRU 公钥的形式非常相似，因此可以使用基于最短向量的 $2N$ 维格攻击来尝试从 h 导出 f 和 g。$2N$ 维 NTRU 格 L^{NT} 由集合中的 $2N$ 个向量的线性组合组成：

$$\left\{\left(X^i, X^i \cdot h\right) : 0 \le i \le N\right\} \cup \left\{\left(0, qX^i\right) : 0 \le i \le N\right\}$$

更有效的攻击是利用对 f_0, g_0 的了解，在同一个 $2N$ 维格上对 f_1, g_1 进行最近向量攻击。目标是在 L^{NT} 中找到最接近向量 $\left(0, (g_0 - f_0 \cdot h)p'\right)$ 的向量，其中 $pp' \equiv 1 \pmod q$。如果成功，这次攻击会产生一个小型 F，使得 $G \equiv F \cdot h - (g_0 - f_0 \cdot h)p' \pmod q$ 也很小。然后 $(f_0 + pF, g_0 + pG)$ 要么是原始密钥，要么是一个有用的替代品。采用这种方法，在平衡格后，我们得到方程中的常数 c 的以下估计：

$$b > \frac{2\pi e \|f_1\| \cdot \|g_1\|}{q}$$

由于更大的 b 值会产生更长的求解运行时间，所以 N, F_f, F_g 被选择为使得 $\|f_1\|, \|g_1\|$ 可以给出足够大的 b 值则可防御格攻击。

5. 总结

本文提出了一种基于 NTRU 签名算法可验证的秘密分享方案。该方案通过利用 NTRU 数字签名的高

效性和抗量子性，结合随机掩码，防止了成员之间的欺骗行为和密码分享份额的恶意篡改，从而提升了整体安全性。与传统基于离散对数和大数分解的方案相比，NTRU 基于格的安全性提供了更强的防御能力，尤其在量子计算环境中具有较强的抗攻击能力。该方案不仅有效提升了秘密分享的安全性，还具有较强的灵活性和可扩展性，适应现代信息保护和共享的多样化需求。

基金项目

国家自然科学基金(62472040)；中国版权保护中心版权研究课题(BQ2024017)；北京市教委科研计划资助(No. KM202110015004)；北京市高等教育学会 2022 年立项面上课题(MS2022093)；北京市教育委员会科学研究计划项目资助(KM202310015002)。

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] Tassa, T. (2007) Hierarchical Threshold Secret Sharing. *Journal of Cryptology*, **20**, 237-264. https://doi.org/10.1007/s00145-006-0334-8

[3] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T. (2008) A New (*k*,*n*)-Threshold Secret Sharing Scheme and Its Extension. In Wu, T.C., Lei, C.L., Rijmen, V. and Lee, D.T., Eds., *Lecture Notes in Computer Science*, Springer, 455-470. https://doi.org/10.1007/978-3-540-85886-7_31

[4] Kumar, P., Banerjee, K., Singhal, N., Kumar, A., Rani, S., Kumar, R., *et al.* (2022) Verifiable, Secure Mobile Agent Migration in Healthcare Systems Using a Polynomial-Based Threshold Secret Sharing Scheme with a Blowfish Algorithm. *Sensors*, **22**, Article 8620. https://doi.org/10.3390/s22228620

[5] Hazay, C., Mikkelsen, G.L., Rabin, T., Toft, T. and Nicolosi, A.A. (2018) Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting. *Journal of Cryptology*, **32**, 265-323. https://doi.org/10.1007/s00145-017-9275-7

[6] Velumani, R., Sudalaimuthu, H., Choudhary, G., Bama, S., Jose, M.V. and Dragoni, N. (2022) Secured Secret Sharing of QR Codes Based on Nonnegative Matrix Factorization and Regularized Super Resolution Convolutional Neural Network. *Sensors*, **22**, Article 2959. https://doi.org/10.3390/s22082959

[7] Yuan, J. and Li, L. (2019) A Fully Dynamic Secret Sharing Scheme. *Information Sciences*, **496**, 42-52. https://doi.org/10.1016/j.ins.2019.04.061

[8] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings* 35*th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, 20-22 November 1994, 124-134. https://doi.org/10.1109/sfcs.1994.365700

[9] Tang, G., Pang, B., Chen, L. and Zhang, Z. (2023) Efficient Lattice-Based Threshold Signatures with Functional Interchangeability. *IEEE Transactions on Information Forensics and Security*, **18**, 4173-4187. https://doi.org/10.1109/tifs.2023.3293408

[10] Rajabi, B. and Eslami, Z. (2019) A Verifiable Threshold Secret Sharing Scheme Based on Lattices. *Information Sciences*, **501**, 655-661. https://doi.org/10.1016/j.ins.2018.11.004

[11] Hoffstein, J., Pipher, J. and Silverman, J.H. (1996) NTRU: A New High Speed Public Key Cryptosystem. Technical Report, presented at the rump session of Annual International Cryptology Conference (CRYPTO).

[12] Hoffstein, J., Pipher, J. and Silverman, J.H. (2001) NSS: An NTRU Lattice-Based Signature Scheme. In: Pfitzmann, B., Ed., *Lecture Notes in Computer Science*, Springer, 211-228. https://doi.org/10.1007/3-540-44987-6_14

[13] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H. and Whyte, W. (2003) NTRUSign: Digital Signatures Using the NTRU Lattice. In: Joye, M., Ed., *Lecture Notes in Computer Science*, Springer, 122-140. https://doi.org/10.1007/3-540-36563-x_9

[14] Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H. and Whyte, W. (2014) Transcript Secure Signatures Based on Modular Lattices. In: Mosca, M., Ed., *Lecture Notes in Computer Science*, Springer International Publishing, 142-159. https://doi.org/10.1007/978-3-319-11659-4_9

[15] 杨真真, 蔺大正, 张东巍, 等. 一种基于 NTRU 的数字签名方案[C]//通信理论与技术新进展——第十一届全国青年通信学术会议论文集. 2006.

[16] 胡予濮. 一个新型 NTRU 类数字签名方案[J]. 计算机学报, 2008, 31(9): 1661-1665.

[17] 张卷美, 曹杰, 刘年义, 等. 一种基于 NTRU 新型签名方案的设计[J]. 四川大学学报(工程科学版), 2015, 47(1):

49-53.

[18] Bogdanov, D. (2007) Foundations and Properties of Shamir's Secret Sharing Scheme Research Seminar in Cryptography. University of Tartu, Institute of Computer Science.

[19] Khorasgani, H.A., Asaad, S., Eghlidos, T. and Aref, M. (2014) A Lattice-Based Threshold Secret Sharing Scheme. 2014 11*th International ISC Conference on Information Security and Cryptology*, Tehran, 3-4 September 2014, 173-179. https://doi.org/10.1109/iscisc.2014.6994043

[20] Asaad, S., Khorasgani, H.A., Eghlidos, T. and Aref, M. (2014) Sharing Secret Using Lattice Construction. 7*th International Symposium on Telecommunications* (*IST*'2014), Tehran, 9-11 September 2014, 901-906. https://doi.org/10.1109/istel.2014.7000831

[21] Steinfeld, R., Pieprzyk, J. and Wang, H. (2007) Lattice-based Threshold Changeability for Standard Shamir Secret-Sharing Schemes. *IEEE Transactions on Information Theory*, **53**, 2542-2559. https://doi.org/10.1109/tit.2007.899541

[22] Amroudi, A.N., Zaghain, A. and Sajadieh, M. (2017) A Verifiable (k,n,m)-Threshold Multi-Secret Sharing Scheme Based on NTRU Cryptosystem. *Wireless Personal Communications*, **96**, 1393-1405. https://doi.org/10.1007/s11277-017-4245-9

[23] Ogata, W. and Araki, T. (2017) Computationally Secure Verifiable Secret Sharing Scheme for Distributing Many Secrets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **100**, 103-114. https://doi.org/10.1587/transfun.e100.a.103

[24] 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*, Portland, 21-23 October 1985, 383-395. https://doi.org/10.1109/sfcs.1985.64

[25] Stadler, M. (1996) Publicly Verifiable Secret Sharing. In: Maurer, U., Ed., *Lecture Notes in Computer Science*, Springer, 190-199. https://doi.org/10.1007/3-540-68339-9_17

[26] Albrecht, M. and Ducas, L. (2021) Lattice Attacks on NTRU and LWE: A History of Refinements. https://eprint.iacr.org/2021/799