doi:10.1631/FITEE.1500197

题目：NTRU 格上基于身份签名的高效方案

目的：众所周知，普通格上的基于身份的签名体制的公钥尺寸较大并且签名效率不甚令人满意，为提高格上的签名效率并且降低其公钥尺寸，本文设计了 NTRU 格上的基于身份的签名方案。

创新点：将抛弃采样技术扩展到 NTRU 格上，并利用 NTRU 格上的 SIS 问题构造了 NTRU 格上的首个可证安全的基于身份的签名方案，使得签名效率显著提高，并很大程度地降低了公钥尺寸。

方法：首先，明确 NTRU 格的定义，提出 NTRU 格上的小整数解问题（SIS），即定义 5，指出该困难问题在量子计算环境下是安全的。然后，将抛弃采样技术扩展到 NTRU 格上(算法 6)，利用扩展后的抛弃采样技术构造 NTRU 格上的基于身份的签名方案，详见算法 4-7。该方案的安全性依赖于所提出的 NTRU 格上的 SIS 问题，因而该方案在量子计算环境下仍然是安全的，并且其通信复杂度较低（详见表 1-2）。

结论：将抛弃采样技术扩展到 NTRU 格上，并构造了 NTRU 格上首个基于身份的签名方案，该签名方案与普通格上的基于身份的签名方案相比，效率更高，公钥尺寸更小。

关键词：身份；签名；NTRU 格；