



## 基于NTRUSign的电子现金方案

<http://www.firstlight.cn> 2010-01-01

基于NTRUSign数字签名方案构建一个新的电子现金方案，该方案的安全性基于格上的最近向量问题，并对该方案进行了详细的安全性分析。结果表明该方案满足一个电子现金方案应具有的性质，且实现速度快、占用资源少以及产生密钥容易，具有更高的实用性和安全性。

[存档文本](#)