## 环境与记号

* **群与配对**：设
* 为阶为 的乘法循环群，
* 为双线性配对函数，满足：
* 生成元：
* **哈希函数**：
* 为随机预言模型下的密码学哈希函数。
* **消息**：

## 用户秘钥

* **用户私钥**：，其中 , 。
* **用户公钥**：随机选取 $ h G^T $，公开公钥 $ = (h, h^{s-t}) $。
* **Nickname 生成**：用户随机选择 $ r $，计算：

$ = h^r, = h^{r(s-t)}. $

* **验证**：验证者检查是否成立：

$ ^{s-t}. $

* **隐私性**：其他人无法从 nickname 或 proof 推导出 $ s-t $，也无法将其关联到特定用户。

这样，用户的私钥差值 $ s-t $ 被有效隐藏，而 nickname 的归属权仅由用户和生成者知晓。

## 签名者说明

签名者定义：

对于合法签名者 ，若其由私钥 生成（即 , ），则存在秘密值

使得

本签名机制本质上是**证明签名者知道 使得**  的 Schnorr 类型零知识签名，并通过挑战 绑定消息 和昵称 ，防止重放攻击。

## 签名算法

**输入**：昵称 ，消息 。 **输出**：签名 。

**步骤**：

1. 计算：
2. 随机选取：
3. 生成承诺：
4. 计算挑战：
5. 利用私钥 计算：
6. 输出签名：

## 验签算法

**输入**： ，消息 ，签名 。 **输出**：（接受）或 （拒绝）。

**步骤**：

1. 获得签名：
2. 重新计算挑战（使用接收到的 ）：
3. 验证以下等式是否成立：
4. 若等式成立，则输出 ；否则输出 。

✅ **关键验签公式**：

## 正确性说明

若签名合法，则：

* ，
* ，
* ，

代入左边得：

因此验签等式成立。

## 安全性与绑定性

* **存在性安全**：只有知道 的用户才能生成有效签名。
* **不可伪造性**：攻击者无法在不知 的情况下通过挑战验证。
* **抗重放**：挑战 依赖于 、 、 和 ，确保签名与特定消息和昵称绑定。
* **零知识特性**：签名不泄露 本身，仅证明知识