

*Project21: Schnorr Bacth

说明:

Schnorr Signature

- Key Generation
 - $P = dG$
- Sign on given message M
 - randomly k , let $R = kG$
 - $e = \text{hash}(R||M)$
 - $s = k + ed \bmod n$
 - Signature is : (R, s)
- Verify (R, s) of M with P
 - Check sG vs $R + eP$
 - $sG = (k + ed)G = kG + edG = R + eP$

根据以上 Schnorr 签名方案实现基础的 Schnorr 签名以及认证。实现 Schnorr 签名的批量验签。

批量验证的原理:

给定有 n 个公钥、消息和签名元组 $(P_i, m_i, (R_i, s_i))$, 验证者生成 n 个随机数 a_1, \dots, a_n , 来计算 n 个挑战哈希值 $e_i = H(P_i, R_i, m_i)$, 然后检查:

$(a_1s_1 + a_2s_2 + \dots + a_ns_n) \cdot G = a_1 \cdot R_1 + a_2 \cdot R_2 + \dots + a_n \cdot R_n + (a_1e_1) \cdot P_1 + (a_2e_2) \cdot P_2 + \dots + (a_ne_n) \cdot P_n$, 如果相等则通过验证。

运行结果:

```
Microsoft Visual Studio 调试 × + ∨
对消息的签名为: [(7, 16), 2]
对消息的签名为: [(7, 16), 18]
对消息的签名为: [(7, 1), 2]
对消息的签名为: [(7, 1), 14]
对以上4个签名分别进行验证.....
签名验证成功!
签名验证成功!
签名验证成功!
签名验证成功!
对以上4个签名批量验签:
签名验证成功!
```

实现方法：

本项目使用 C 语言编程实现

分工： 自己独立完成