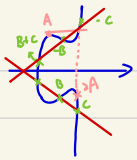


$(B+C)+(-B)=C$

EC point addition

加上反元素

DLP

$f(g, g^{\alpha}) \to \alpha$, g is generator is $\mathbb{Z}_g$ (同樣意義 αP，不同表示方法)

Vrfy (vk, m, σ)

$\sigma_2 \cdot \sigma_1 =?$ (vk)

$(H(m)+\alpha u)P = H(m)P + u(\alpha P)$

↳ $H(\sigma_1, vk, m)$

=> 代表所有人都可以驗證

if $\sigma_2 \cdot \sigma_1 == H(m)P + u(\alpha P)$: return True

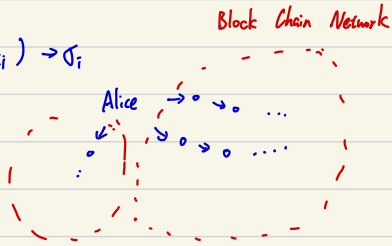
else : return False

$\sigma_1 = rP$

$\sigma_2 = r^{-1}(H(m) + \alpha \cdot u)$ => α 相同的机率很，所以数字又有自己做得出来

Alice ⟼ Bob
tx_i

$Sign(sk_{Alice}, tx_i) \to \sigma_i$



如果兩筆交易 剛好 r 用了同一個，那麼就可以得知該人的 α，導致帳號被盜

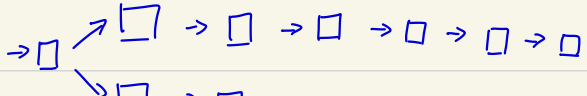
所以 現在自用找零錢包，多個錢包，用了就走，就不用到同一個 α

when r 用到相同，σ_1 就會相同

① $\sigma_2 = r^{-1}(H(m) + \alpha \cdot u)$

② $\sigma_2 = r^{-1}(H(m) + \alpha \cdot u)$

=> 則可得 α 值 (極度危險!!)



長鏈：以 Bitcoin 為例，A tx is complete if tx is with 6 confirmations (包含自己)

短鏈：旨被無視，上面的交易指在鏈上

正常來說，大家都跟著最長的鏈做題目

Byzantin Generals Problem (1982 Lamport et al.)

① 假設 n 個將軍，有一個發指令的將軍，

② 向此時他要發 (0 or 1) 的指令給所有將軍

1. 所有的好人都指往相同的方向

2. 如果發指令將軍是好人，所有好人都會聽他的 (CG)

Example. We can know CG is 100% loyal,

Byzantine Broadcast became trivial

Example We can know CG is 100% traitor

我 retreat 我好了

BB Problem Definition

- Entities : nodes (generals), sender

  (node 1 is the sender)

- $[n] = \{1, \cdots, n\}$ denotes the set of all nodes

  - Honest nodes
  - Corrupted nodes (a subset of nodes) Controlled by an adversary (對手)

    ① send / transmit arbitrary messages

    ② share info or coordinated attack

    ③ stop

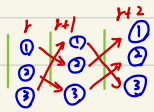
    ④ incorrect step

[Static Corruption model

Adversary decides corrupted nodes at beginning]

Synchronous network

If an honest node send a msg
in round r to an honest recipient
the recipient gets it at the begining of $r+1$



Def of BB

Consistency : If two honest node output b_1, b_2, then $b_1 = b_2$

Validity : If S is honest with input b
then all honest ones output b'
s.t. $b' = b$