Schnorr signatures

basic version non-blind:

1. Setup: choose $p$ - prime (bitlenght $\lambda$ !)

$\mathbb{G}$ - group (multiplikative) of order $p$

$G$ - generator in this group

$H: \{0,1\}^* \to \mathbb{Z}_p$ hash function

$par := (p, \mathbb{G}, G, H)$

2. Key generation: choose random number $x \in \mathbb{Z}_p = \{0, \dots, p-1\}$ with mod

$X := x \cdot G$

$sk := (par, x)$ signing key $\quad pk := (par, X)$ public key of the signer

3. Sign: choose random $r \in \mathbb{Z}_p$

message $m$ $\quad R := r \cdot G$

$c := H(R \| m)$

concatenation

$s := (r + cx) \bmod p$

return $\sigma := (R, s)$

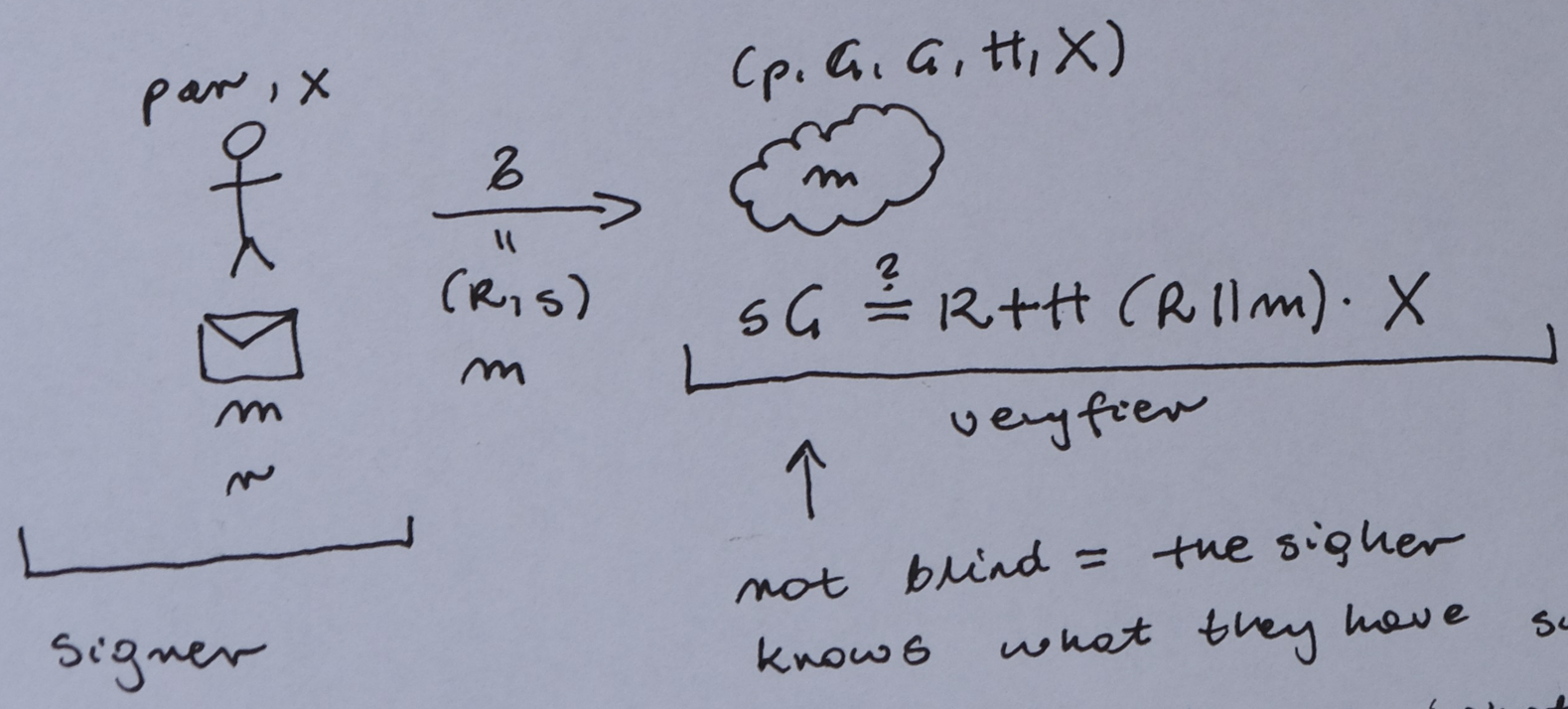
4. Verify: take $(p, \mathbb{G}, G, H, X)$, $\sigma$

$c' = H(R \| m)$

return $(sG = R + c'X)$

if true signature is valid

if false — " — is not valid




not blind = the signer knows what they have signed !!!

the verifier knows what message they are verifying and who signed it

Schnorr blind signature - is obtained from non-blind by replacing signing step 3. with the interactive protocol

the signer out = 1 if the interaction is valid, and $\perp$ if not
the user output is a signature $\sigma$ if interaction terminates correctly and $\perp$ if not

for a 2-round protocol the interaction is as follows:

1. initiation $(msg_{u,0}, state_{u,0}) := ((\ ), (pk, m))$ $\}$ $User_0(pk, m)$
2. 2nd round $(msg_{s,1}, state_s) \leftarrow Sign_1(sk, msg_{u,0})$

$(msg_{u,1}, state_{u,1}) \leftarrow User_1(state_{u,0}, msg_{s,1})$

$(msg_{s,2}, b) \leftarrow Sign_2(state_s, msg_{u,1})$

$\sigma \leftarrow User_2(state_{u,1}, msg_{s,2})$

Verification: the deterministic verification algorithm takes a public key $pk$, a message $m$, and signature $\sigma$ and returns 1 if $\sigma$ is valid on $m$ under $pk$,
" " 0 if is not valid

Blindness = a signer cannot link a message/signature pair to a particular execution of the signing protocol: we may chosse two messages $m_1, m_0$ and even if we run the signining process on them, given two signatures $\sigma_0, \sigma_1$ we cannot determine whitch signature belongs to message $m_0$

| | | |
|---|---|---|
| $Sign((p, \mathbb{G}, G, H), x)$ | | $User((p, \mathbb{G}, G, H, X), m)$ |
| $r \in \mathbb{Z}_p$ random, $R := rG$ | $\xrightarrow{R}$ | $\alpha, \beta \in \mathbb{Z}_p$ random |
| | | $R' := R + \alpha G + \beta \cdot X$ |
| | | $c' := H(R' \Vert m)$, $c := (c' + \beta) \bmod p$ |
| $s := (r + cx) \bmod p$ | $\xleftarrow{c}$ | |
| | $\xrightarrow{s}$ | if $sG \neq R + cX$ return $\perp$ |
| return 1 | | $s' := (s + \alpha) \bmod p$ |
| | | return $\sigma := (R', s')$ |

signer$(p, \mathbb{G}, G, H), x)$ $\xleftarrow{R}$ $\xrightarrow{c}$ $\xleftarrow{s}$ user$((p, \mathbb{G}, G, H, X), m)$

return 1 return $z = (R', s')$

$z$

verification$((p, \mathbb{G}, G, H, X), z)$

return valid / not valid

digital cash, voting protocols