# Anonymous Cred

/!\ Authentication happen before each signature

## General idea:

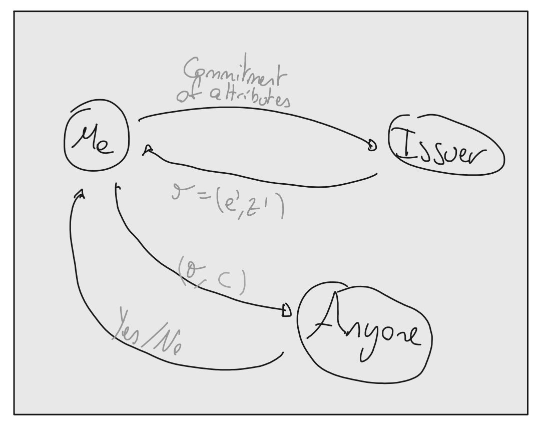
→ Generate anonymous credentials where:

i) User holds secret attributes (age, secret key (to be sure it is me), ...)

ii) Issuer certifies these attributes by issuing a signature

iii) The issuer:
- → Does not learn the secret attributes
- → Cannot, later, link a credential to a signature

iv) the user:
- → Can randomize credentials
- → Can prove possession of a credential using ZK proof




## Building Blocks

↳ Note See Chaum Peterson in Voting

### NI Schnorr - Samir Signature

Idea: P must prove he has $x$ st $h = g^x$; his sk. We link a signature to that key $x$ for a msg $m$

How it works

↳ We use $H(\dots)$ to make a signature of $m$.

$P$ = Issuer $\quad\quad V$ = me

$y \xleftarrow{\$} \mathbb{Z}_q$

$\xrightarrow{a := g^y}$

$\xleftarrow{e = H(a, h, m)}$

$\xrightarrow{z = y + ex}$

Then a valid signature is $\sigma = (a, z)$ for $m$:

i) Recompute $c = H(a, h, m)$

ii) Check $g^z \overset{?}{=} a \cdot h^e$

## Issue:

if Issuer is the verifyer (or they collide) he will be able to track the signature he issued

### Non interactive Divertible Schnorr Proofs (and Sign)

This is all "me"

$P$ = Issuer $\quad\quad$ $D$ = Me

$y \xleftarrow{\$} \mathbb{Z}_q$ $\quad \xrightarrow{a := g^y}$ $\quad$ $w, y' \xleftarrow{\$} \mathbb{Z}_q$ $\quad \xrightarrow{a' := a^w g^{y'}}$

$\xleftarrow{e = e' \cdot w^{-1}}$ $\quad\quad \xleftarrow{e' := H(g, h, a', m)}$

$\xrightarrow{z = e \cdot x + y \bmod (q)}$ $\quad\quad \xrightarrow{z' = w \cdot z + y'}$

Then a signature is $\sigma = (e', z')$:

Check that $e' = H(g, h, \underbrace{g^{z'}/h^{e'}}_{= a'}, m)$

Note: $(a, e, z) \perp\!\!\!\perp (a', e', z')$ donc lorsqu'on (ni P) voit une signature on ne sait pas qui l'a issued

P is signing a msg he has no control over

⇒ will use commitments

### Multi Pedersen commitment:

- $pk = (G, q, g_1, \dots, g_\ell, h)$
- $\mathrm{Com}_{pk}(m_1, \dots, m_\ell; r) = g_1^{m_1} \cdots g_\ell^{m_\ell} h^r$

⇒ We can create another commitment by:

$c' = c \cdot h^{r'}$ : Perfectly unlinkable with initial $c$.

## Final

Idea:

→ We will sign the randomized commitment of all attributes (given to P with $\pi$ proving the commitment): $c = u_1^{m_1} \cdot u_2^{m_2} \cdots u_\ell^{m_\ell} \cdot \boxed{u_0^r}$

→ P computes $d = c^x$ and proofs knowledge of:

$$\log_g(h) = x = \log_c(d)$$ (ensures sign tied to commitment)

For this we use CP (non interactive!)

→ Adapt $(c, d)$ into $(c', d')$ such that the signature:

$\sigma = (e', z')$ is valid for

$$\log_g h = x = \log_{c'} d'$$

⇒ P will provide $v_0 = u_0^x$ to help me compute:

$$d' = d \cdot v_0^{r'} = (c \cdot u_0^{r'})^x = (c')^x$$

### Full Scheme

$$pk = (g, h, u_0, v_0, \{u_i\}_{i=1}^{\ell})$$

Signer $\quad\quad\quad\quad$ User

Picks $y \xleftarrow{\$} \mathbb{Z}_q$ $\quad\quad$ Picks $r, r', w, y' \xleftarrow{\$} \mathbb{Z}_q$

$d = c^x$ $\quad \xleftarrow{c,\ \pi \text{ can proof I have } m}$ $\quad c = u_1^{m_1} \cdots u_\ell^{m_\ell} u_0^r$ ($u_1^{m_1}$ is my key)

For CP: $a = g^y$, $b = c^y$, $a_0 = u_0^y$ $\quad \longrightarrow$ $\quad$ compute:
- $c' = c \cdot u_0^{r'}$
- $d' = d\, v_0^{r'}$ (see previously why)
- $a' = a^w g^{y'}$ (for Divertible)
- $b' = (b \cdot a_0^{r'})^w \cdot (c u_0^{r'})^{y'}$ (for Divertible)

} CP

$\xleftarrow{e = e' \cdot w^{-1}}$ $\quad$ Get its challenge: $e' = H(g, h, c', d', a', b')$

$z = ex + y$ $\quad \xrightarrow{z}$

A signature is $(e', z')$ on $(c, d)' = (c, d)(u_0, v_0)^{r'}$

Verifying as: $e' = H(g, h, c', d', g^{z'}/h^{e'}, (c')^{z'}/(d')^{e'})$

Which says:
- → $c$ Signed by P (with $x$)
- → P knew what he was signing
- → randomized by sender to avoid tracking