Idemix verification equation

$$\tilde{A}^e = \frac{Z}{S^{\tilde{v}} R_0^{a_0} R_1^{a_1} \cdots R_i^{a_i}} \bmod n$$

public key: $(Z, S, R_0 \cdots R_i, n)$

private key: primes p, q for $n = pq$

issued signature: (A, e, v)

disclosed signature: $(\tilde{A}, e, \tilde{v})$

a_0 as holder secret

$a_1 \cdots a_i$ as attributes

$\tilde{A}, S^{\tilde{v}}$ for unlinkability

$\tilde{A} = AS^r \bmod n$ and

$\tilde{v} = v - er$

Diploma

secret: **xxxxxxxx**,

name: **xxxxxxxx**,

title: **PhD**

A, e, v

Schnorr's Zero Knowledge protocol

given $H = R^a$

choose random t

$U = R^t \bmod n$	$\xrightarrow{U}$		**commitment**
	$\xleftarrow{c}$	choose random c	**challenge**
$r = t + ca$	$\xrightarrow{r}$	$R^r H^{-c} \stackrel{?}{=} U \bmod n$	**response**