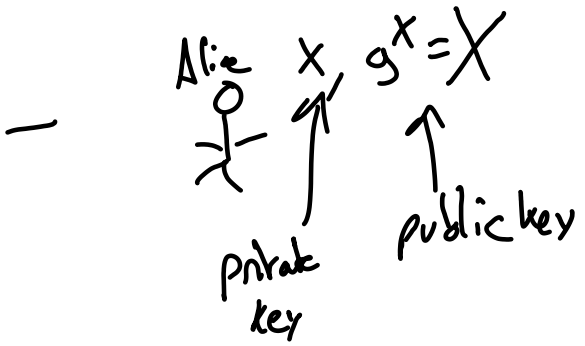
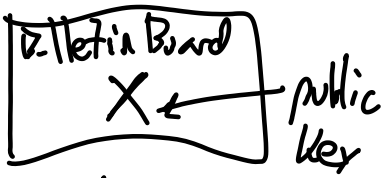
Zero Knowledge Proofs

Monday, September 27, 2021 4:40 PM

Zero Knowledge Proofs notation





"no one can compute x from X by DLOG"

ZKP is Alice can say: "I know my secret key x s.t. $X = g^x$"

w/o revealing x

ZKP $\{(x) : X = g^x\}$

- witness
- statement
- relation / predicate

$X = g^x$

Alice sends $y = F_k(1)$

Can bob check y is actual $F_k(1)$ w/o knowing k?

Where's Waldo ZKP.