Private Access Tokens Crypto

`draft-private-access-tokens-01`

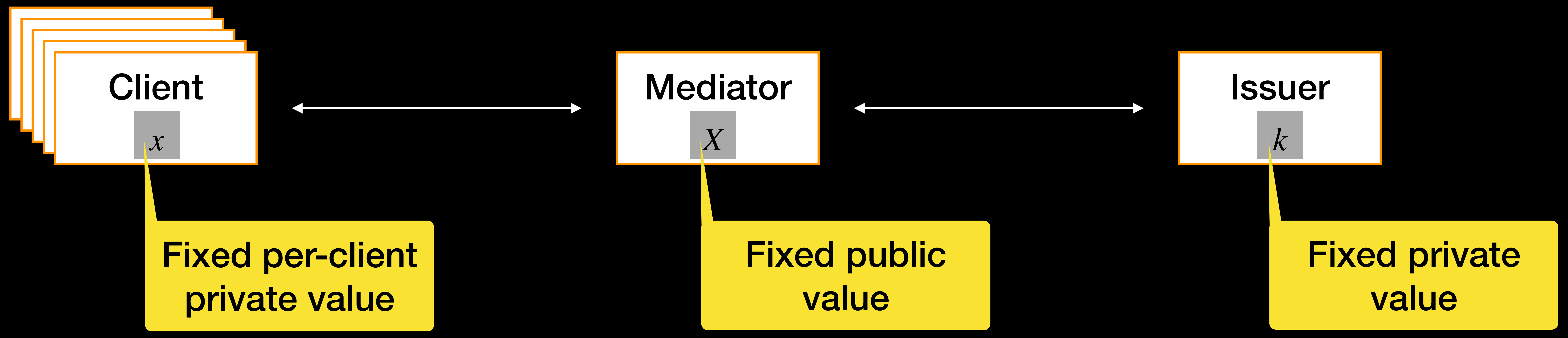
Hendrickson, Iyengar, Pauly, Valdez, Wood — IETF 112 Online— CFRG

Setting

Problem statement

Setting

Problem statement



Requirements

Problem statement

Compute deterministic value y over private client input x and private Issuer input k

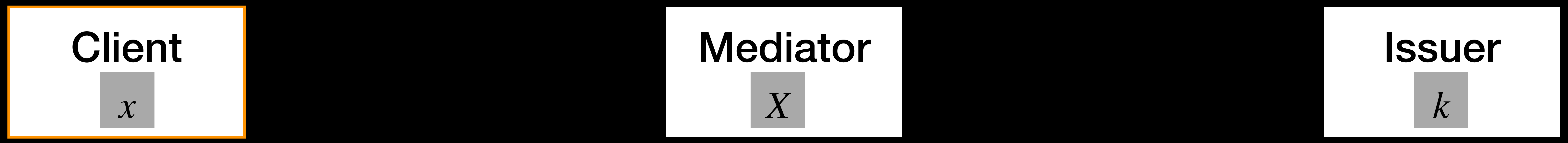
$$y = F(k, x)$$

Such that

- The Mediator only learns y if the client engages in the protocol with x;
- The Client cannot engage in the protocol for private input $x' \neq x$; and
- The Issuer does not learn x, nor when two requests have the same x.

Building Blocks

Solution sketch



Assume prime-order group with generator G and order q, and

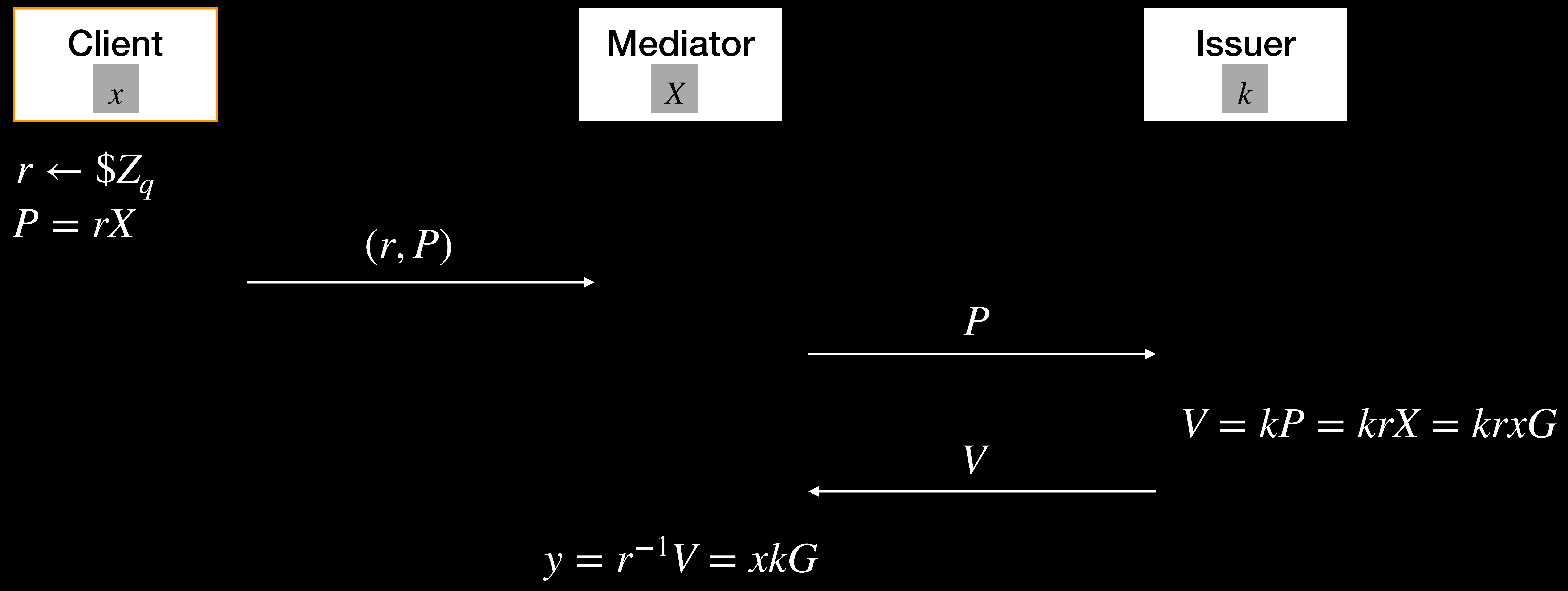
x and k are private scalars, and $X = xG$ a non-hiding commitment to x

$\pi = \text{NIZK}(\text{DL}(x, y) = z)$ is non-interactive Schnorr proof that $\log_z(x) = y$

$\text{VerifyNIZK}(x, y, \pi)$ outputs 1 for $\pi = \text{NIZK}(\text{DL}(x, y) = z)$, and 0 otherwise

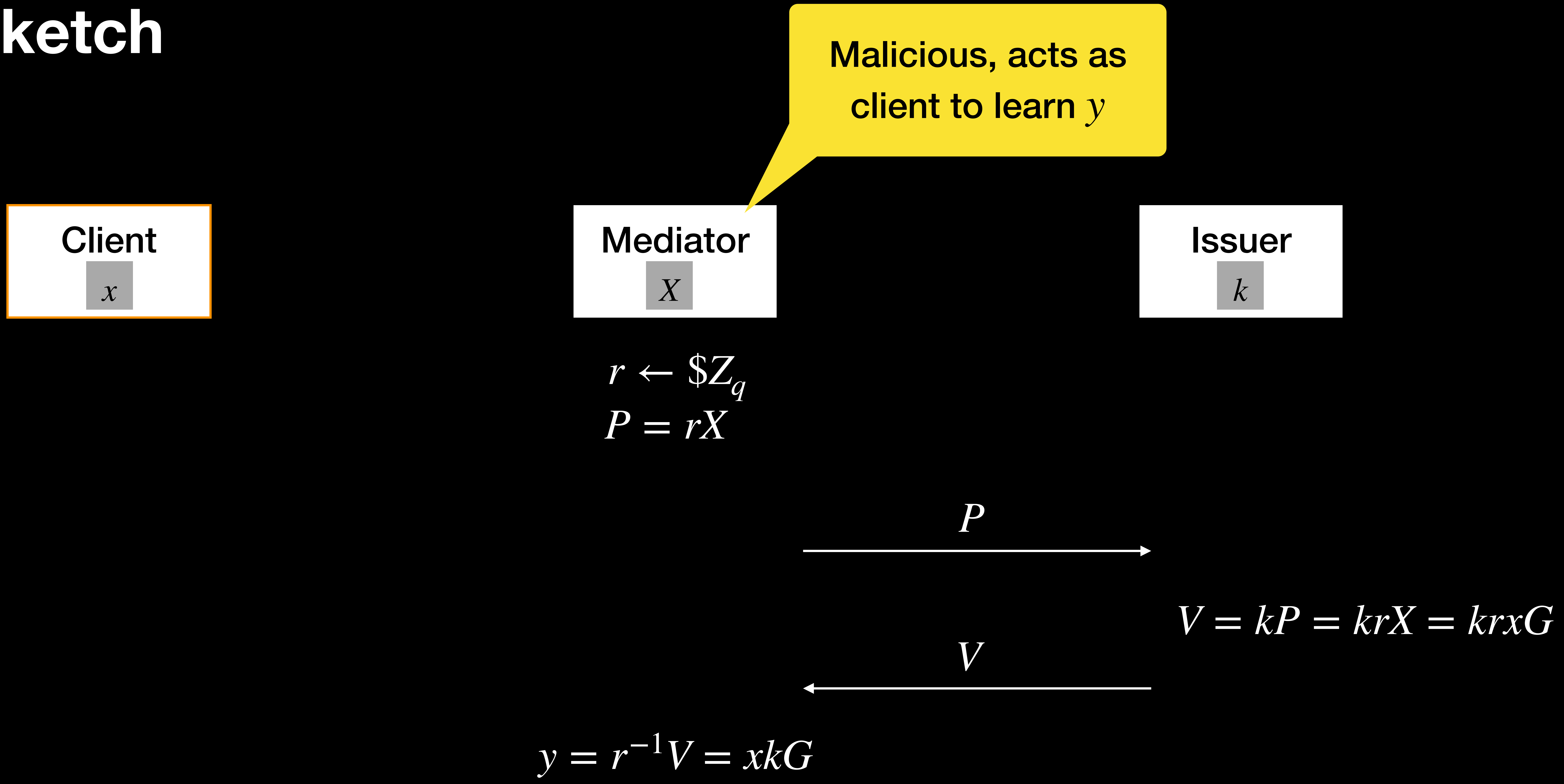
Protocol Overview

Solution sketch



Protocol Overview

Solution sketch



Protocol Overview

Solution sketch

Client (x) — **Mediator** (X) — **Issuer** (k)

Client:

$r \leftarrow \$ Z_q$

$P = rX$

$\pi = \text{NIZK}(\text{DL}(P, x) = rG)$

Client → Mediator: (r, π)

Mediator:

$\text{VerifyNIZK}(rG, P, \pi)$

Mediator → Issuer: (rG, P, π)

Issuer:

$\text{VerifyNIZK}(rG, P, \pi)$

$V = kP = krX = krxG$

Issuer → Mediator: V

$y = r^{-1}V = xkG$

Protocol Overview

Solution sketch

Client (x) — **Mediator** (X) — **Issuer** (k)

Client:

$r \leftarrow \$Z_q$

$P = rX$

$\pi = \text{NIZK}(\text{DL}(P, x) = rG)$

Client → Mediator: (r, π)

Mediator: $\text{VerifyNIZK}(rG, P, \pi)$

Mediator → Issuer: (rG, P, π)

Issuer:

$\text{VerifyNIZK}(rG, P, \pi)$

Only holder of x could have generated the request

$V = kP = krX = krxG$

Issuer → Mediator: V

$y = r^{-1}V = xkG$

Questions

Future work

Is the security model sensible?

Does the sketched protocol meet the desired security goals?

Does the protocol compute a PRF?