

**Prover**

$(g, q, y, \alpha)$

---

$$r \in_R \mathbb{Z}_q$$

$$t := g^r$$

$$s := r - c\alpha \bmod q$$

**Verifier**

$(g, q, y)$

---

$$c \in_R \{0, 1\}^k$$

$$t \stackrel{?}{=} g^s y^c$$

$t$



Diagram illustrating a decommitment protocol:

- The Prover (left) has parameters  $(g, q, y, \alpha)$  and a secret  $r$ .
- The Prover computes  $t := g^r$ .
- The Verifier (right) has parameters  $(g, q, y)$  and a commitment  $c$ .
- The Prover sends  $t$  to the Verifier.
- The Verifier sends  $c$  back to the Prover.
- The Prover computes  $s := r - c\alpha \bmod q$ .
- The Prover sends  $s$  to the Verifier.
- The Verifier checks if  $t \stackrel{?}{=} g^s y^c$ .

$c$

$s$