Generic Group Model

[Shoup 97] — Random Labels

- \triangleright Models generic attacks in a cyclic group $G = \langle g \rangle$
- $\triangleright \ \tau : \mathbb{Z}_p \to \mathbb{G} = \{0,1\}^m \text{ (random injection)}$
- \triangleright Interpret $\tau(x)$ as g^x
- ▷ Oracles:

$$\operatorname{Mult}(\tau(x), \tau(y)) \coloneqq \tau(x+y), \text{ and }$$

$$\operatorname{Inv}(\tau(x)) \coloneqq \tau(-x),$$

au(1)	00010100
$\tau(2)$	00110010
$\tau(3)$	10011011
au(4)	11011110
$\tau(5)$	00111011
• • •	• • •



Mult(00110010, 10011011)



Generic Group Model

[Shoup 97] — Random Labels

- \triangleright Models generic attacks in a cyclic group $G = \langle g \rangle$
- $\triangleright \ \tau : \mathbb{Z}_p \to \mathbb{G} = \{0,1\}^m$ (random injection)
- \triangleright Interpret $\tau(x)$ as g^x
- ▷ Oracles:

$$\operatorname{Mult}(\tau(x), \tau(y)) \coloneqq \tau(x+y)$$
, and

$$Inv(\tau(x)) := \tau(-x),$$

$\tau(1)$	00010100
$\tau(2)$	00110010
au(3)	10011011
au(4)	11011110
au(5)	00111011
• • •	



Mult(10101010, 10011011)

