



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



`Mult(00110010, 10011011)`



**Generic Group Model**



[Shop97]-Random Labels

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

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

$\text{Inv}(\tau(x)) \doteq \tau(-x)$ ,

001100010



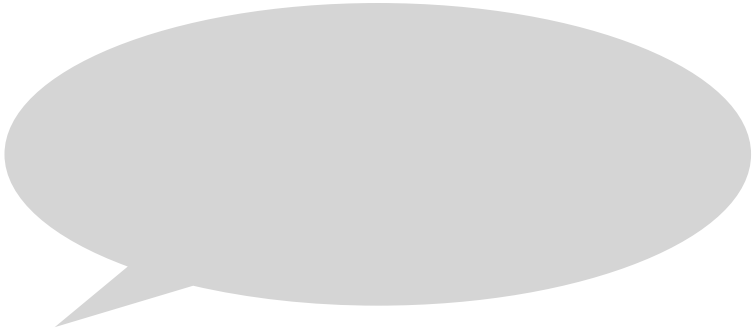
10011011







00111011



00111011