Generic Group Model

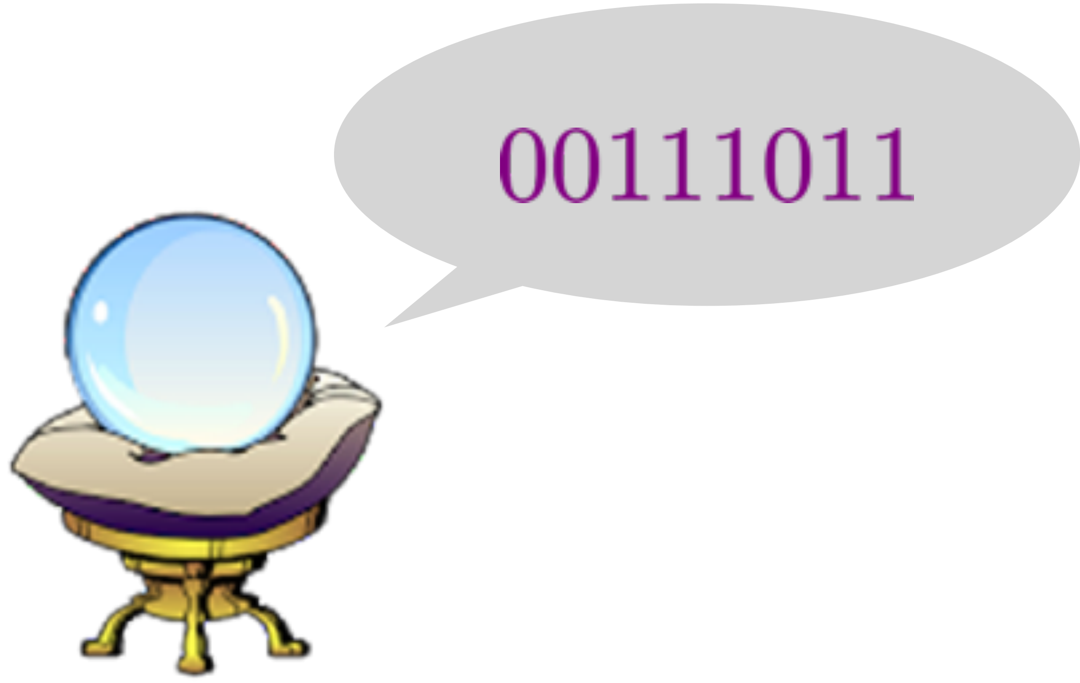
[Shoup 97] — Random Labels

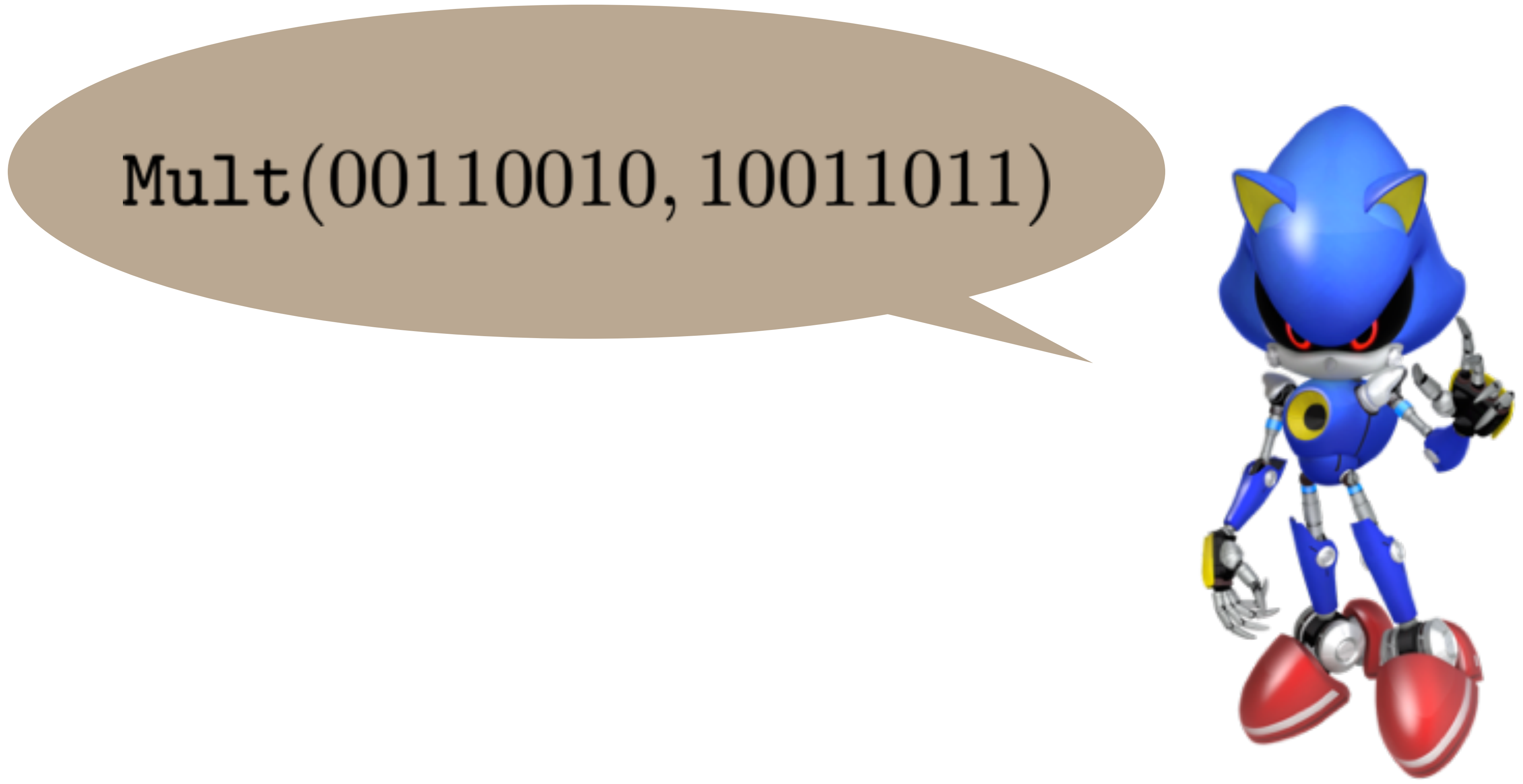
- ▷ Models generic attacks in a cyclic group $G = \langle g \rangle$
- ▷ $\tau : \mathbb{Z}_p \to \mathbb{G} = \{0,1\}^m$ (random injection)
- ▷ Interpret $\tau(x)$ as g^x
- ▷ Oracles:

$$\texttt{Mult}(\tau(x), \tau(y)) := \tau(x+y), \text{ and}$$

$$\texttt{Inv}(\tau(x)) := \tau(-x),$$

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





Generic Group Model

[Shoup 97] — Random Labels

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

$$\texttt{Mult}(\tau(x), \tau(y)) := \tau(x+y), \text{ and}$$

$$\texttt{Inv}(\tau(x)) := \tau(-x),$$

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

$\texttt{Mult}(10101010, 10011011)$