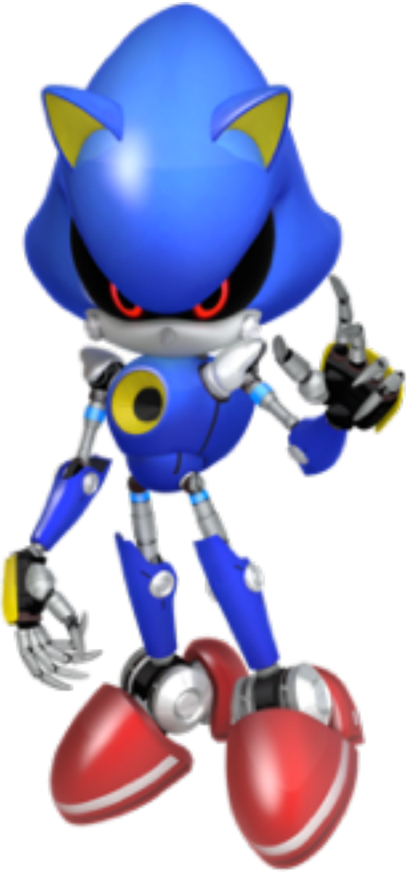
$\tau(1)$	000010100
$\tau(2)$	001100010
$\tau(3)$	100110011
$\tau(4)$	110111110
$\tau(5)$	001111011
$\cdots$	$\cdots$



Generic Group Model

11

[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:

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

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

Justification

- For certain elliptic curve groups, the best known attacks are all **generic**
- We can often get a **tighter** security bound **in the GGM**
- Counterexamples are **artificially crafted** [Den02]

$$\texttt{Mult}(101010010, 10011011)$$

10101010

$\perp$

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:

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

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

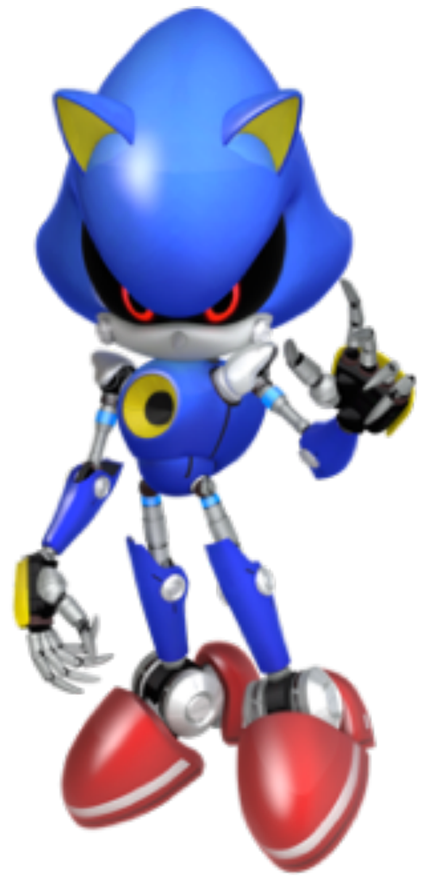
Justification

- For certain elliptic curve groups, the best known attacks are all **generic**
- We can often get a **tighter** security bound **in the GGM**
- Counterexamples are **artificially crafted** [Den02]

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

$\perp$

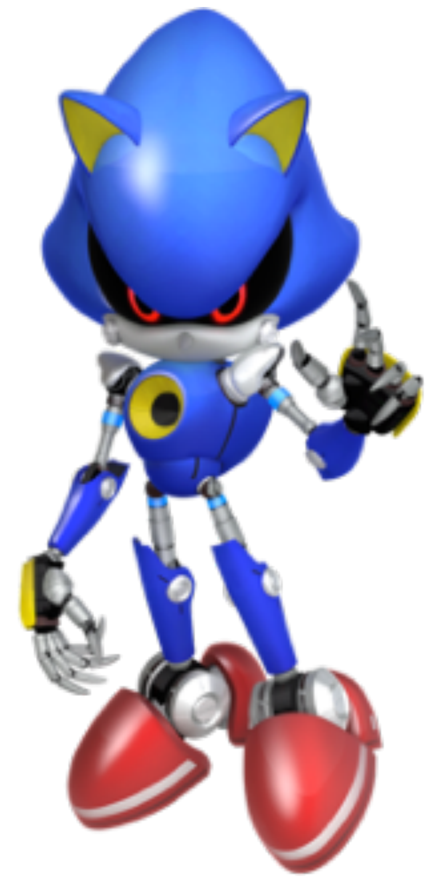
$\mathtt{Mult}(10101010, 10011011)$

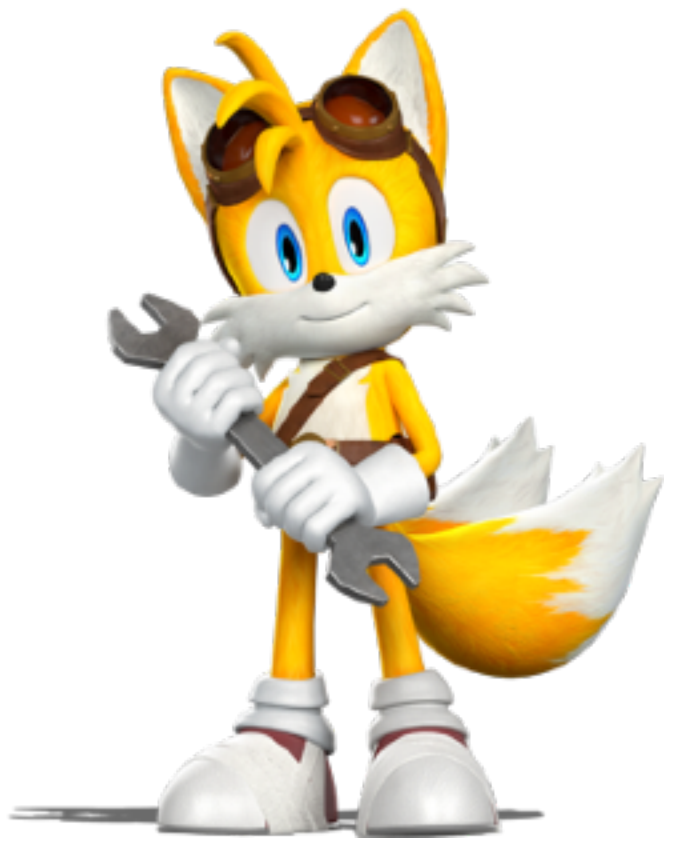


Bridge-Finding Game
In the Generic Group Model

(x_1, x_2, x_3)

$y = \vec{a} \cdot \vec{x} + b$





$\mathcal{L}$

$\tau(y)$	$\vec{a}$	b