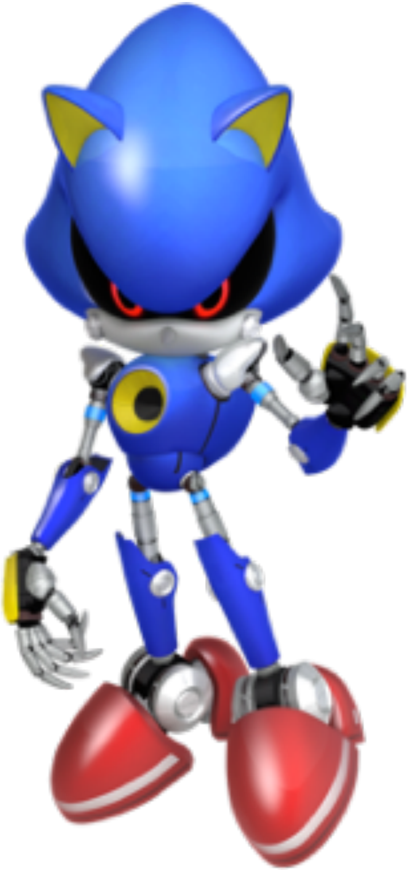
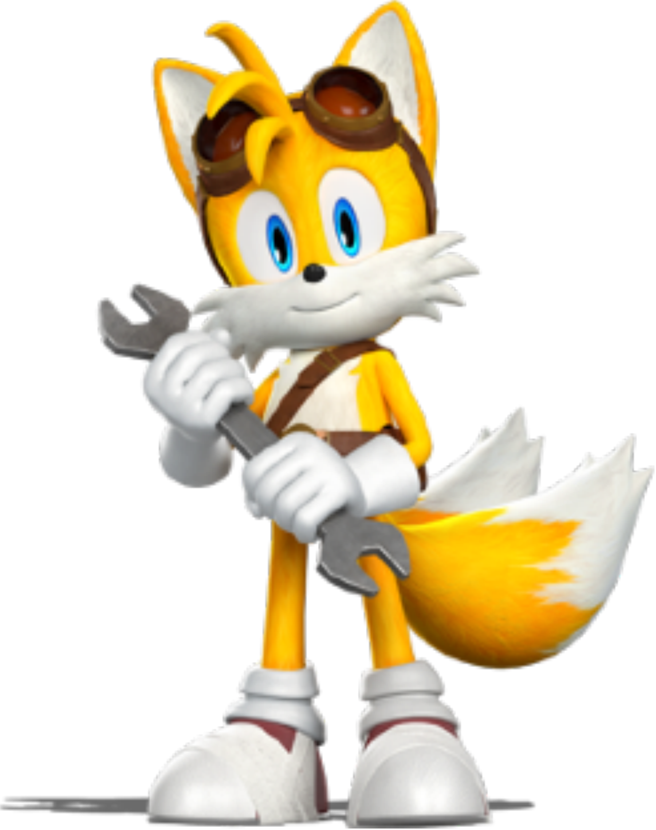
Bridge-Finding Game

In the Generic Group Model

12





$\mathcal{L}$

$$\tau(y)$$

$\vec{a}$

b

$$\tau(1), \tau(x_1), \tau(x_2), \tau(x_3)$$

$$(x_1, x_2, x_3)$$

$\tau(1)$	$(0,0,0)$	1

$\tau(x_1)$	$(1, 0, 0)$	0
$\tau(x_2)$	$(0, 1, 0)$	0
$\tau(x_3)$	$(0, 0, 1)$	0

$$\xrightarrow{\texttt{Mult}(\tau(x_1),\tau(x_2))}$$

$\tau(x_1 + x_2)$	$(1, 1, 0)$	0

$$\xleftarrow{\tau(x_1 + x_2)}$$

$$\xrightarrow{\texttt{Inv}(\tau(x_1 + x_2))}$$

$$\xleftarrow{\tau(-x_1 - x_2)}$$

$\tau(-x_1 - x_2)$	$(-1,-1,0)$	0

$$\xrightarrow{\texttt{Mult}(\tau(x_1), \tau(1))}$$

$$\xleftarrow{\tau(x_1 + 1)}$$

$\tau(x_1 + 1)$	$(1, 0, 0)$	1

$$\xrightarrow{\hspace{2em}\texttt{Mult}(\tau(x_2), \mathfrak{h})\hspace{2em}}$$

$$\tau(x_2 + 7)$$

$\tau(x_2 + 7)$	$(0, 1, 0)$	7

$\cdots$

$\cdots \qquad \cdots \qquad \cdots$

Restricted Discrete-Log Oracle

$\mathfrak{y}$	$(0, 0, 0)$	7

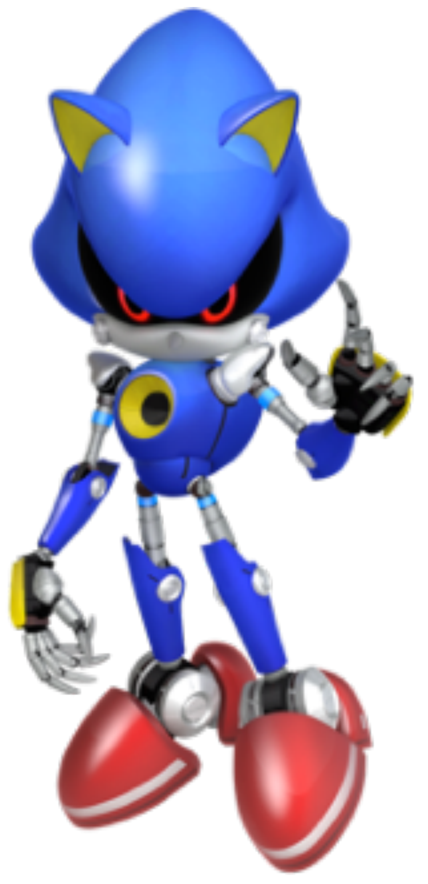
$$y = \vec{a} \cdot \vec{x} + b$$

Bridge-Finding Game

In the Generic Group Model

(x_1, x_2, x_3)

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



$\xleftarrow{\tau(1), \tau(x_1), \tau(x_2), \tau(x_3)}$

$\xrightarrow{\texttt{Mult}(\tau(x_1), \tau(x_2))}$

$\xleftarrow{\tau(x_1 + x_2)}$

$\xrightarrow{\texttt{Inv}(\tau(x_1 + x_2))}$

$\xleftarrow{\tau(-x_1 - x_2)}$

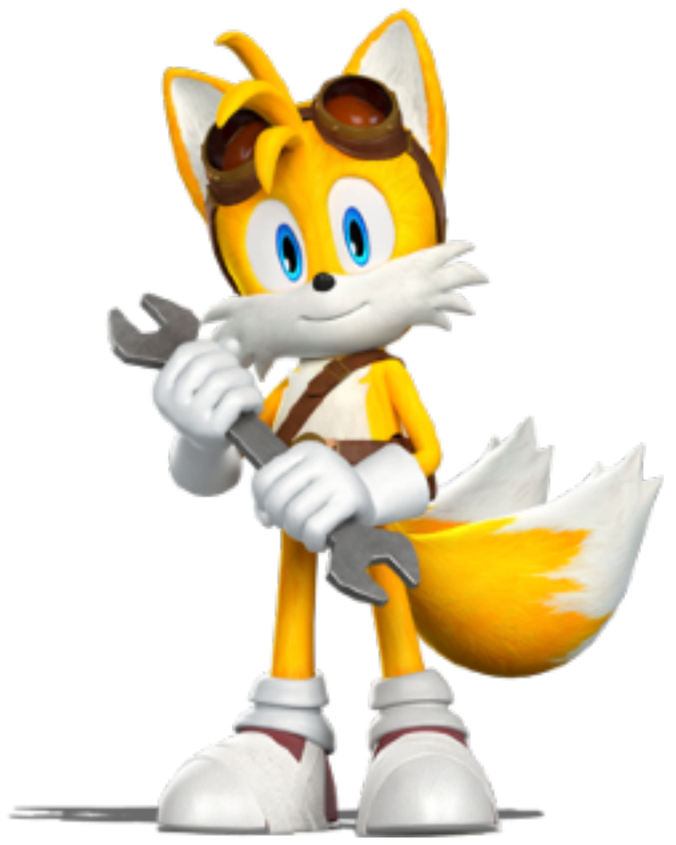
$\xrightarrow{\texttt{Mult}(\tau(x_1), \tau(1))}$

$\xleftarrow{\tau(x_1 + 1)}$

$\xrightarrow{\texttt{Mult}(\tau(x_2), \mathfrak{y})}$

$\xleftarrow{\tau(x_2 + 7)}$

$\ldots$



Restricted Discrete-Log Oracle

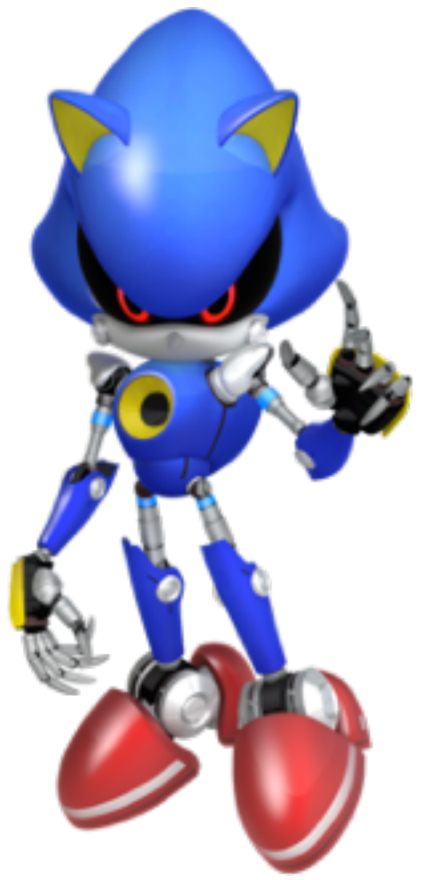
$\mathcal{L}$

$\tau(y)$	$\vec{a}$	b
$\tau(1)$	$(0, 0, 0)$	1
$\tau(x_1)$	$(1, 0, 0)$	0
$\tau(x_2)$	$(0, 1, 0)$	0
$\tau(x_3)$	$(0, 0, 1)$	0
$\tau(x_1 + x_2)$	$(1, 1, 0)$	0
$\tau(-x_1 - x_2)$	$(-1, -1, 0)$	0
$\tau(x_1 + 1)$	$(1, 0, 0)$	1
$\mathfrak{y}$	$(0, 0, 0)$	7
$\tau(x_2 + 7)$	$(0, 1, 0)$	7
$\ldots$	$\ldots$	$\ldots$

Bridge-Finding Game
in the Generic Group Model

(x_1, x_2, x_3)

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



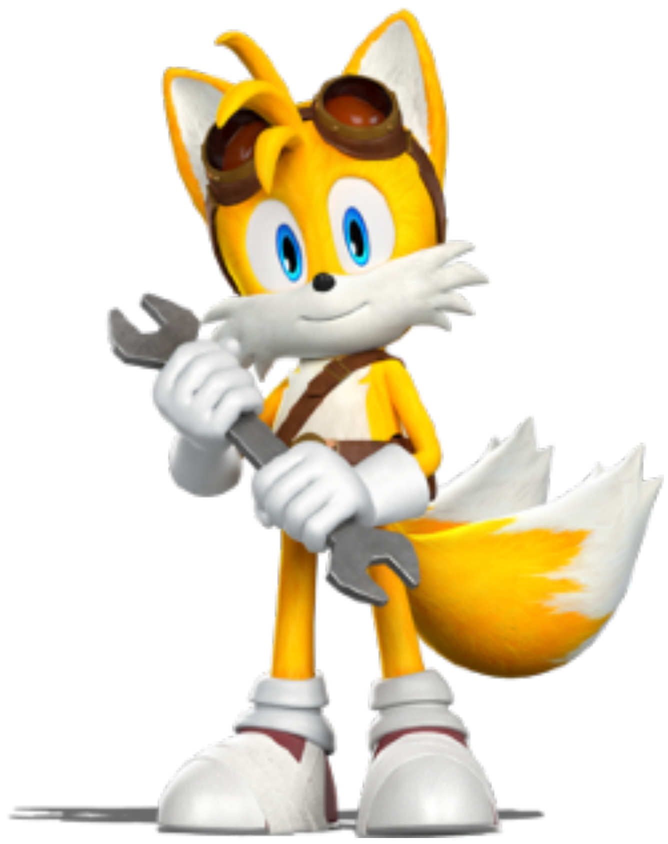
$\tau(1), \tau(x_1), \tau(x_2), \tau(x_3)$

$\texttt{Mult}(\tau(x_1), \tau(x_2))$

$\tau(x_1 + x_2)$

$\texttt{Inv}(\tau(x_1 + x_2))$

$\tau(-x_1 - x_2)$



$\mathcal{L}$

$\tau(y)$	$\vec{a}$	b
$\tau(1)$	$(0,0,0)$	1
$\tau(x_1)$	$(1,0,0)$	0
$\tau(x_2)$	$(0,1,0)$	0
$\tau(x_3)$	$(0,0,1)$	0
$\tau(x_1 + x_2)$	$(1,1,0)$	0
01101101	$(-1,-1,0)$	0
$\tau(x_1 + 1)$	$(1,0,0)$	1
$\mathfrak{y}$	$(0,0,0)$	7
01101101	$(0,1,0)$	7
$\cdots$	$\cdots$	$\cdots$

Bridge event since $\tau(-x_1 - x_2) = \tau(x_2 + 7) = 01101101$

but $((-1,-1,0),0) \neq ((0,1,0),7)$

Then we learned

$$-x_1 - x_2 = x_2 + 7$$

Theorem (informal). $\Pr[\text{BRIDGE}] \leq \mathcal{O}\left(\frac{q^2 + qN}{p}\right).$