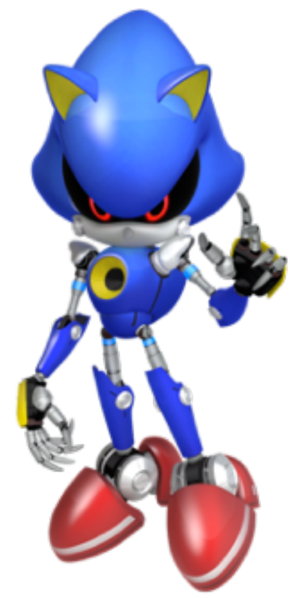
Bridge-Finding Game

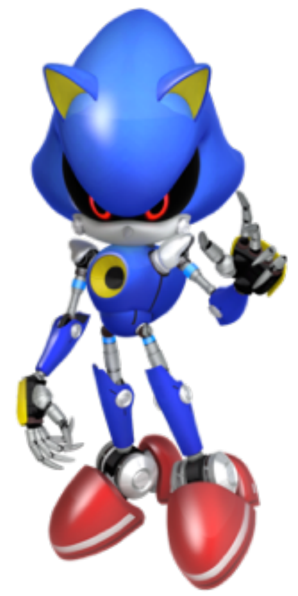
In the Bit-Fixing GGM



Fix $(t_1, \tau(t_1)), \ldots, (t_P, \tau(t_P))$

preprocessing phase

online phase



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

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

$\leftarrow \tau(x_1 + x_2)$

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

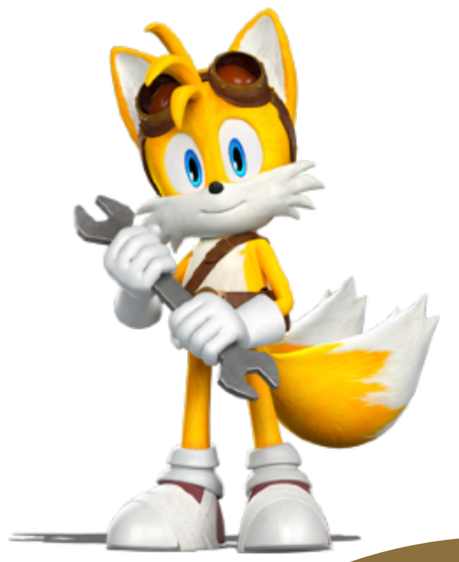
$\leftarrow \tau(-x_1 - x_2)$

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

$\leftarrow \tau(x_1 + 1)$

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

$\leftarrow \tau(x_2 + 7)$



Restricted Discrete-Log Oracle

(x_1, x_2, x_3)

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

$\mathcal{L}$

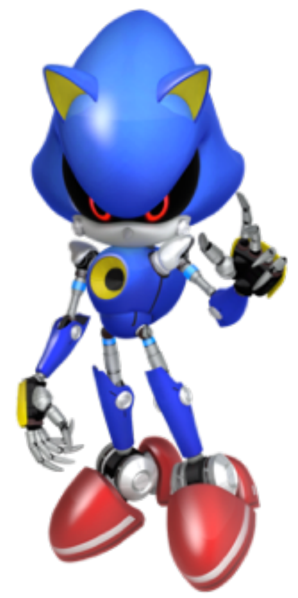
$\tau(y)$	$\vec{a}$	b
$\tau(t_1)$	$(0,0,0)$	t_1
$\cdots$	$\cdots$	$\cdots$
$\tau(t_P)$	$(0,0,0)$	t_P
$\tau(1)$	$(0,0,0)$	1
$\tau(x_1)$	$(1,0,0)$	0
$\tau(x_2)$	$(0,1,0)$	0
$\tau(x_3)$	$(0,0,1)$	0
$\tau(x_1 + x_2)$	$(1,1,0)$	0
$\tau(-x_1 - x_2)$	$(-1,-1,0)$	0
$\tau(x_1 + 1)$	$(1,0,0)$	1
$\mathfrak{y}$	$(0,0,0)$	7
$\tau(x_2 + 7)$	$(0,1,0)$	7
$\cdots$	$\cdots$	$\cdots$

Bridge-Finding Game

In the Bit-Fixing GGM

(x_1, x_2, x_3)

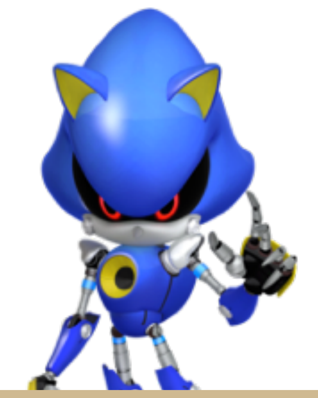
$\tau(y) = \vec{a} \cdot \vec{x} + b$



Fix $(t_1, \tau(t_1)), \ldots, (t_P, \tau(t_P))$

preprocessing phase

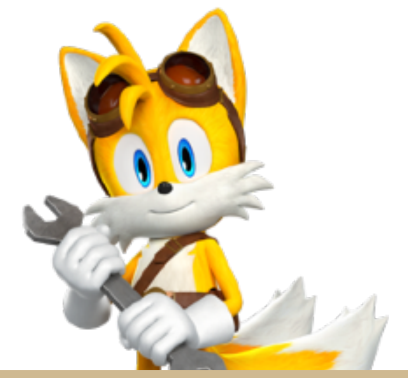
online phase



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

$\mathtt{Mult}(\tau(x_1), \tau(x_2))$ →

$\tau(x_1 + x_2)$



$\mathcal{L}$

$\tau(y)$	$\vec{a}$	b
$\tau(t_1)$	$(0,0,0)$	t_1
$\cdots$	$\cdots$	$\cdots$
01101101	$(0,0,0)$	t_P
$\tau(1)$	$(0,0,0)$	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
$\tau(x_2 + 7)$	$(0,1,0)$	7
$\cdots$	$\cdots$	$\cdots$

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

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

Then we learned

$$x_1 + x_2 + t_P = 0$$

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