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
$\dots$	$\dots$	$\dots$

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

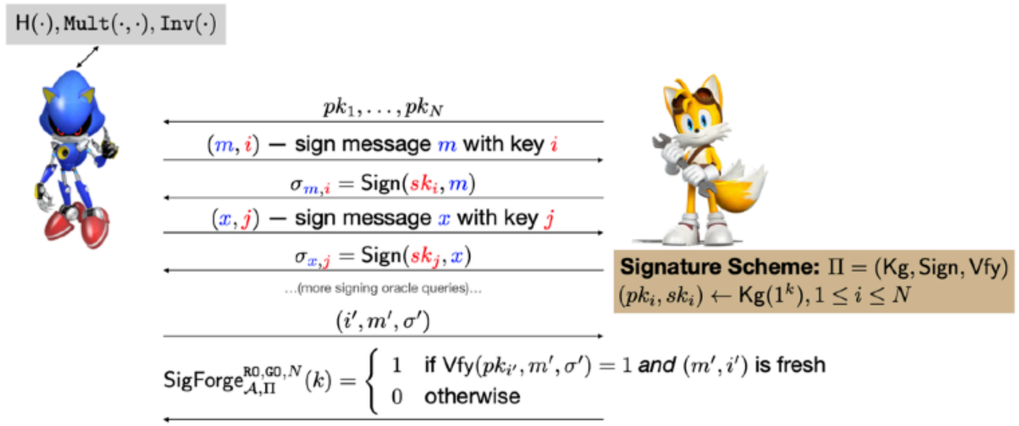
but $((-1,-1,0),0) \neq ((0,1,0),7)$

Then we learned

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

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

Multi-User Security of Short Schnorr Signatures
in the ROM+GGM



$$\Pr\left[\mathsf{SigForge}^{\mathtt{RO},\mathtt{GO},N}_{\mathcal{A},\Pi}(k) = 1\right] \le \Pr[\mathsf{BRIDGE}] + \Pr[\mathsf{Bad}]$$
$$\le \mathcal{O}\left(\frac{q^2 + qN}{p} + \frac{q}{2^k}\right)$$
$$\le \mathcal{O}\left(\frac{q+N}{2^k}\right),$$

where $p \simeq 2^{2k}$.