Bridge-Finding Game

In the Bit-Fixing GGM

preprocessing phase

online phase

Fix

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

$\mathcal{L}$

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

$$(x_1, x_2, x_3)$$

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

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

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

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

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

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

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

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

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

$$\tau(y)$$

$$\vec{a}$$

b

$\tau(t_1)$

$$\tau(t_P)$$

$$(0,0,0)$$

$$(0, 0, 0)$$

t_1

t_P

• • •

• • •

• • •

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

$$\tau(x_1)$$

$\tau(x_2)$

$$\tau(x_3)$$

$$(1, 0, 0)$$

$$(0, 1, 0)$$

$$(0, 0, 1)$$

0

0

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

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

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

Restricted
Discrete-Log
Oracle

• • •

• • •

• • •

01101101

01101101

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

In the **Auxiliary-Input Model**, we have

Theorem (informal).

$$\Pr[\mathsf{BRIDGE}] \leq \mathcal{O}\left(\frac{q2^k S}{p}\right).$$

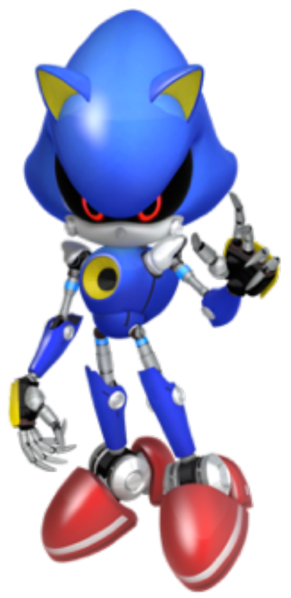
k-bit security: $p \approx 2^{2k} S$

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

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

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

$\tau(x_1 + x_2)$

$\mathcal{L}$

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

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

In the **Auxiliary-Input Model**, we have

Theorem (informal).

$$\Pr[\text{BRIDGE}] \leq \mathcal{O}\left(\frac{q2^k S}{p}\right).$$

k-bit security: $p \approx 2^{2k} S$

Multi-User Security Bound and Signature Length

"Short" Schnorr Signatures

		Security Bound	For k-bit Security	Signature Length
Without Preprocessing		$\varepsilon \leq \mathcal{O}\left(\frac{q^2+qN}{p}+\frac{q}{2^k}\right)$	$p \approx 2^{2k}$	$k+\log p \approx 3k$
With Preprocessing	Key-Prefixed	$\varepsilon \leq \mathcal{O}\left(\frac{q^2 S \log p}{p}+\frac{q}{2^k}\right)$	$p \approx 2^{2k} S \log p$	If $S = 2^{k/2}$ $\Rightarrow k+\log p \approx 3.5k$
	Standardized	$\varepsilon \leq \mathcal{O}\left(\frac{q 2^k S}{p}+\frac{q}{2^k}\right)$	$p \approx 2^{2k} S$	If $S = 2^{k/2}$ $\Rightarrow k+\log p \approx 3.5k$