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 $S = 2^{k/2}$ $\Rightarrow k + \log p \approx 3.5k$

Recap

- ▷ **Short Schnorr signatures** achieve k bits of **multi-user security** (of length $3k$ bits)
- ▷ **Key-prefixed** short Schnorr signatures achieve k bits of multi-user security against **preprocessing attacks** (of length $3k + \log S$ bits)
- ▷ **Standardized implementations** of short Schnorr signatures achieve k bits of multi-user security against **preprocessing attacks** (of length $3k + \log S$ bits)
- ▷ We extend Coretti et al.'s BF-to-AI technique to work in **multiple idealized models**