Recap

17

- **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**

Open Questions

	Security Bound
Key-Prefixed	$\varepsilon \leq \mathcal{O}\left(\frac{q^2 S \log p}{p} + \frac{q}{2^k}\right)$
Standar-dized	$\varepsilon \leq \mathcal{O}\left(\frac{q 2^k S}{p} + \frac{q}{2^k}\right)$

improved bound?

Can we use this technique to other cryptographic primitives? (e.g., Oblivious Transfer)

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**

Can we use this technique to other cryptographic primitives? (e.g., Oblivious Transfer)

Open Questions

	Security Bound
Key-Prefixed	$\varepsilon \leq \mathcal{O}\left(\frac{q^2 S \log p}{p} + \frac{q}{2^k}\right)$
Standar-dized	$\varepsilon \leq \mathcal{O}\left(\frac{q 2^k S}{p} + \frac{q}{2^k}\right)$

improved bound?

Thank you!