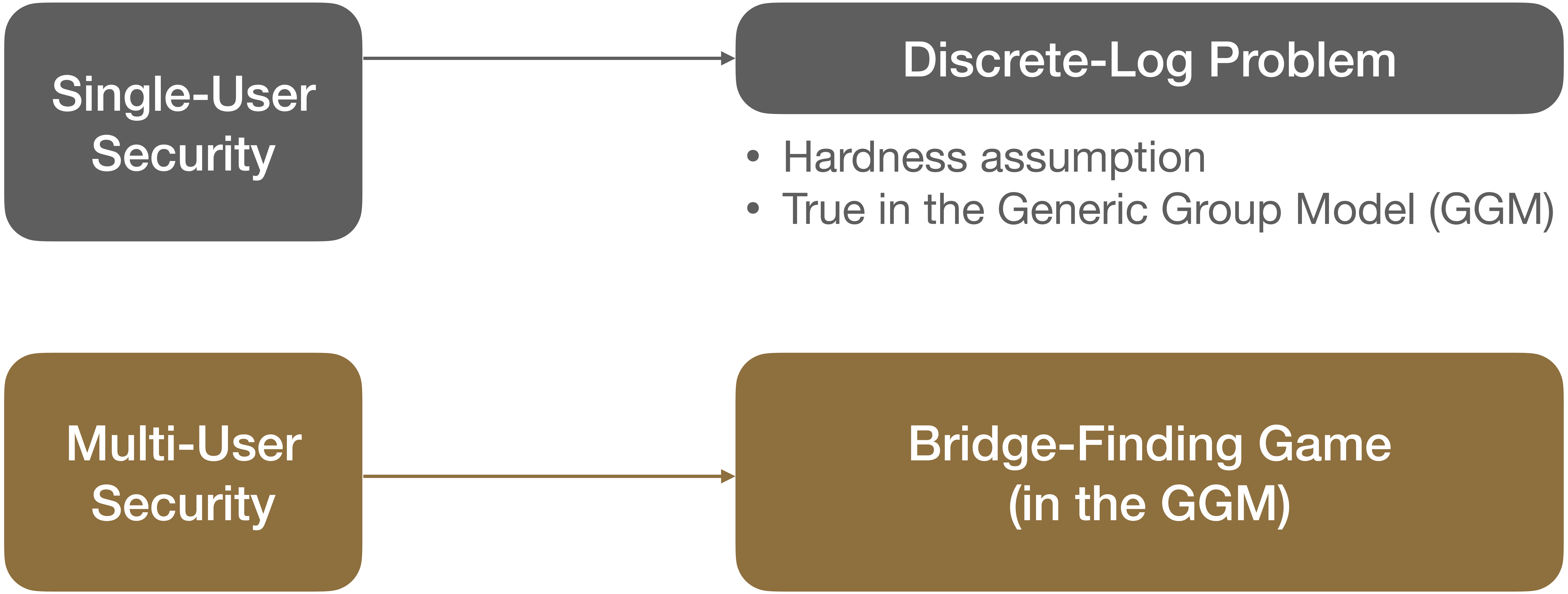
Reduction Idea

Multi-User Security of Short Schnorr Signatures



Single-User Security → Discrete-Log Problem

- Hardness assumption
- True in the Generic Group Model (GGM)

Multi-User Security → Bridge-Finding Game (in the GGM)

Generic Group Model

[Shoup 97] — Random Labels

- Models generic attacks in a cyclic group $G = \langle g \rangle$
- $\tau : \mathbb{Z}_p \to \mathbb{G} = \{0,1\}^m$ (random injection)
- Interpret $\tau(x)$ as g^x
- Oracles:

$$\texttt{Mult}(\tau(x), \tau(y)) \coloneqq \tau(x+y), \text{ and}$$

$$\texttt{Inv}(\tau(x)) \coloneqq \tau(-x),$$