Security reduction of FO transform and variations

Ganyu (Bruce) Xu

University of Waterloo

April, 2024

Outline

- Some preliminaries
- FO Transform in 1999
- IND-CCA KEM in 2017

Fujisaki-Okamoto Transformation, 1999

Inputs:

- Public-key encryption scheme (KeyGen, E^{asym}, D^{asym})
- Symmetric encryption scheme (E^{sym}, D^{sym})
- A hash function $G : \mathcal{M}^{\text{asym}} \to \mathcal{K}^{\text{sym}}$ (aka a KDF)
- A hash function $H : \{0,1\}^* \to \text{Coin}^{\text{asym}}$

Fujisaki-Okamoto Transformation, 1999 cont'

$E^{\mathsf{hy}}(\mathsf{pk}, m \in \mathcal{M}^{\mathsf{sym}})\ \sigma \leftarrow \mathcal{M}^{\mathsf{asym}}$

$a \leftarrow G(\sigma)$