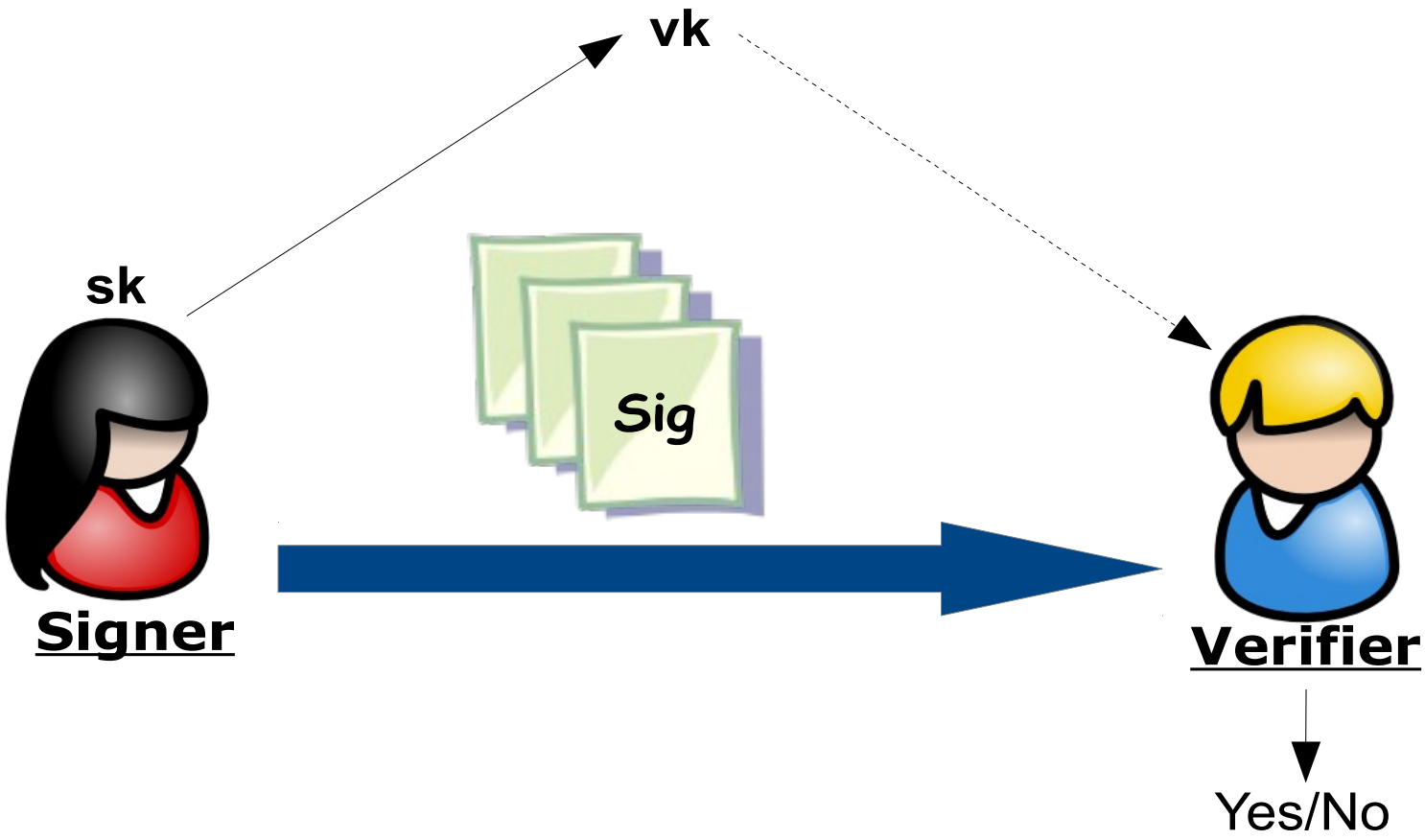
Traceable Attribute-Based Signatures

Dr. Essam Ghadafi

University College London
e.ghadafi@ucl.ac.uk

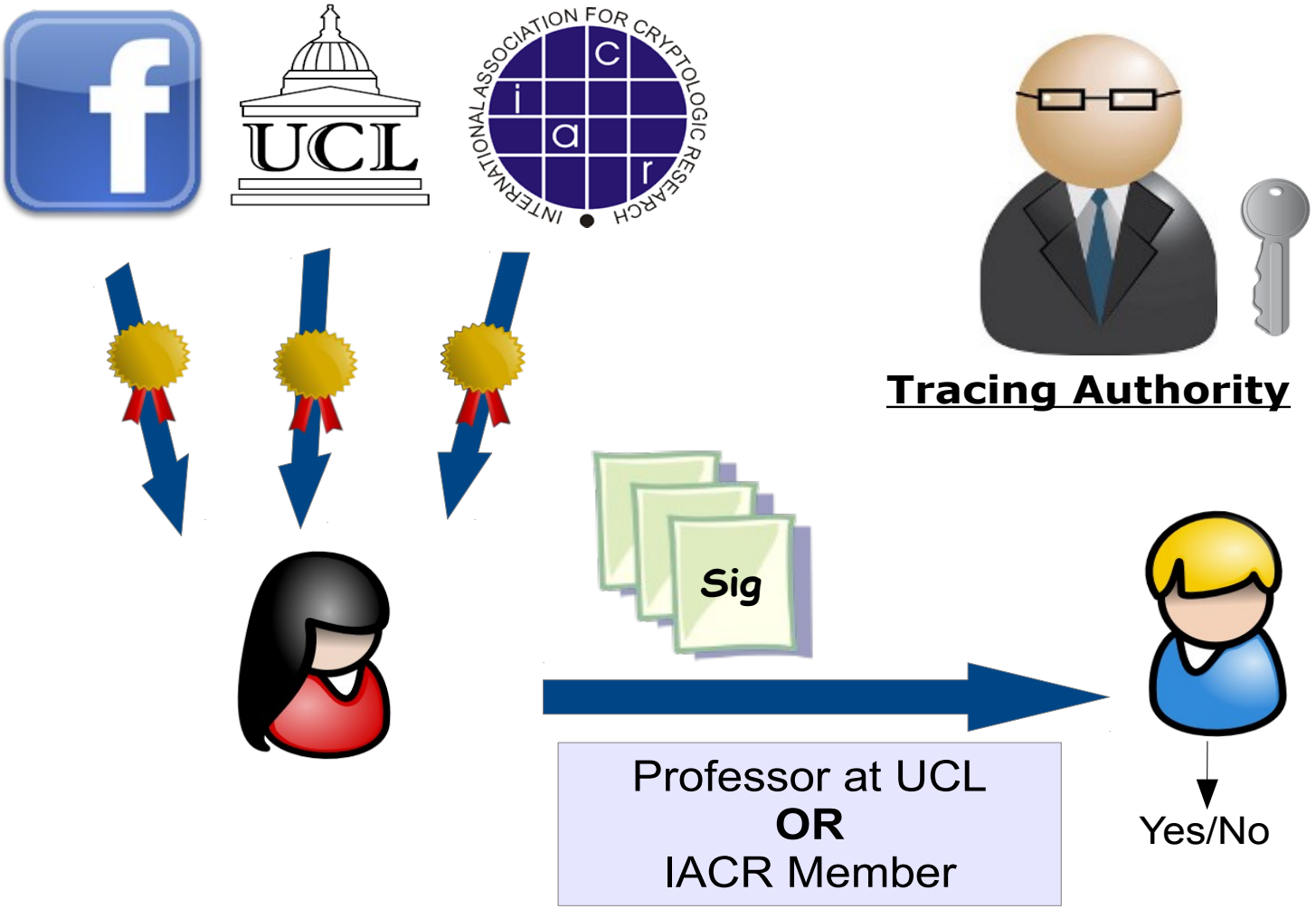
Digital Signatures



Unforgeabiltiy: You can only sign messages if you have the signing key.

Attribute-Based Signatures [Maji et al. 2008]:

- Users have attributes ("Manager", "Finance Department", etc.).
- User with attributes $\mathcal{A}$ can sign messages w.r.t. policy $\mathbb{P}$ if $\mathbb{P}(\mathcal{A}) = 1$.
- Verifier only learns that the signature produced by someone with sufficient attributes to satisfy $\mathbb{P}$.


UCL
INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
Tracing Authority
Sig
Professor at UCL
OR
IACR Member
Yes/No

Project I

- **Project:** Efficient Instantiations of Traceable Attribute-Based Signatures.
- **Aim of the Project:** Design an efficient instantiation of traceable attribute-based signatures in the Random Oracle Model.
- **Project Type:** 100% Research.
- **The Student:**
  - Background and interest in Cryptography, e.g. done well and enjoyed the Intro to Crypto course (and maybe is taking the Cryptanalysis course).
  - Some mathematical background.

PROJECT II

- **Project:** Traceable Attribute-Based Signatures with Threshold Opening.

- **Aim of the Project:** Extend existing models and constructions to the threshold opening setting where opening signatures is only possible if an authorized subset of openers (rather than a single one) act collectively.

- **Project Type:** 100% Research.

- **The Student:**
  - Background and interest in Cryptography, e.g. done well and enjoyed the Intro to Crypto course (and maybe is taking the Cryptanalysis course).
  - Some mathematical background.

The End

Questions?