Multimodal Private Signatures

Khoa Nguyen, Fuchun Guo**,** Willy Susilo**,** Guomin Yang

University of Wollongong, Australia

CRYPTO 2022

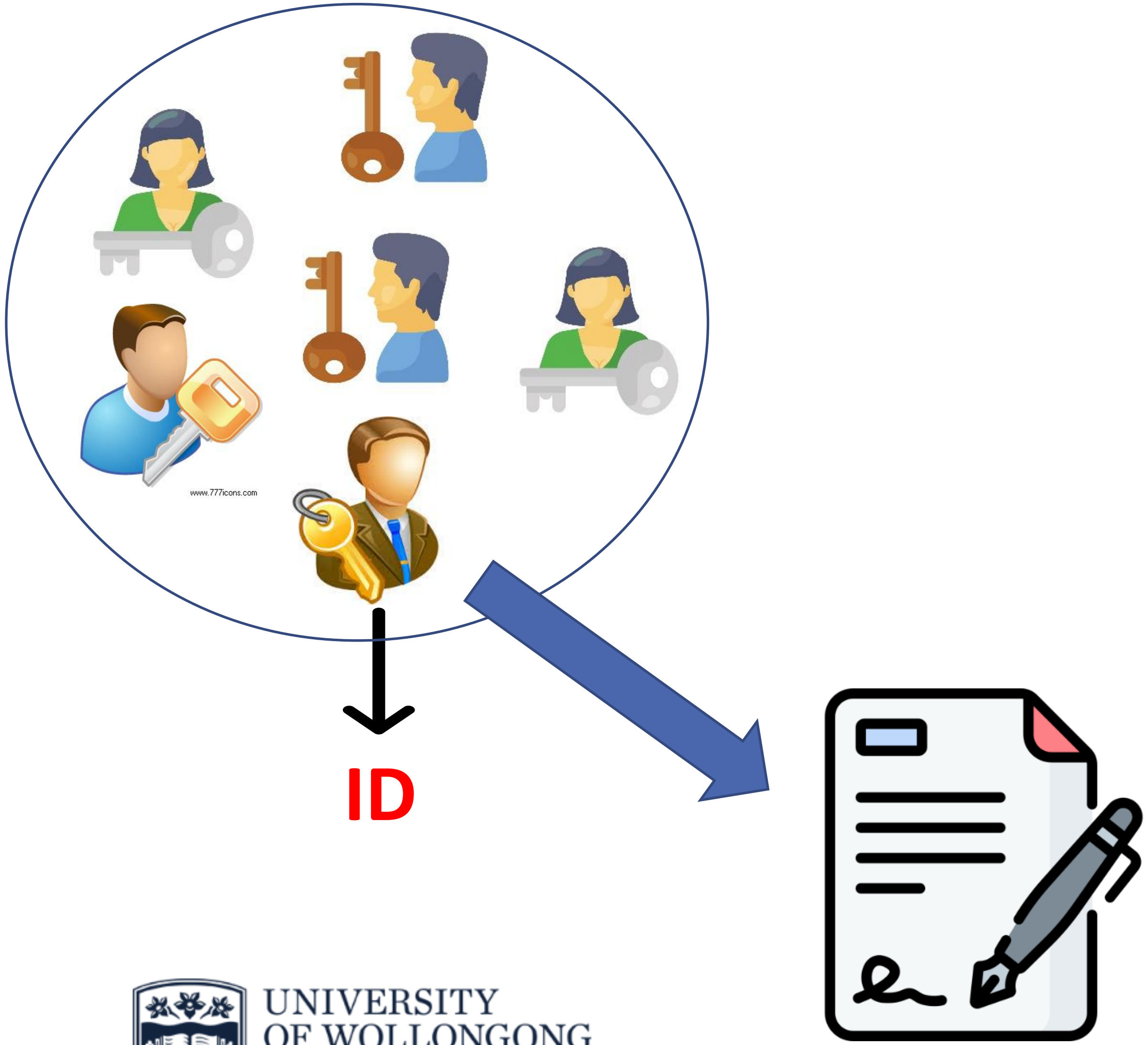
UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

- Privacy and Accountability in Multi-user Signatures
- Multimodal Private Signatures: Definitions and Constructions
- Open Questions

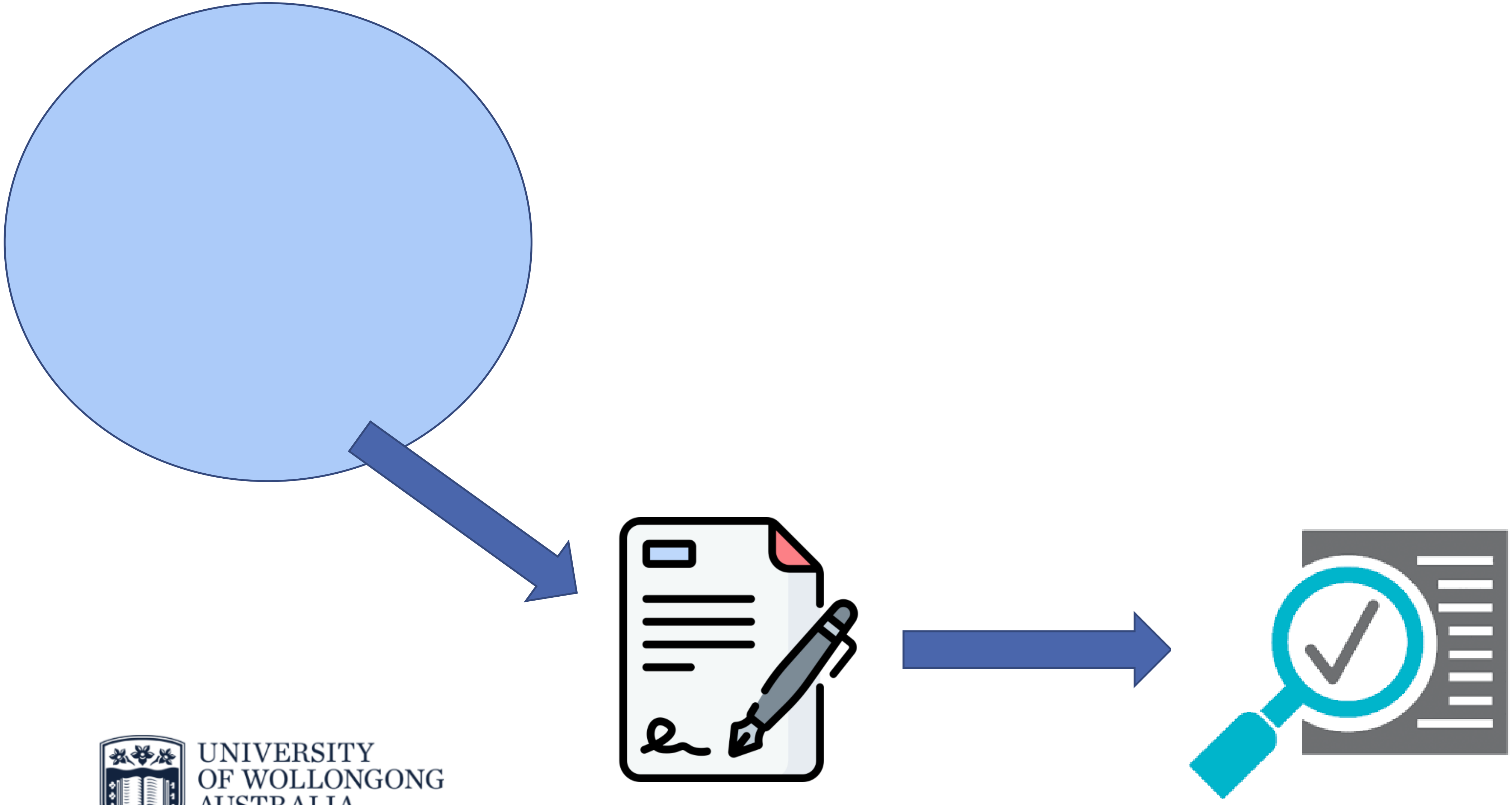
UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Ring Signatures [RST'01]



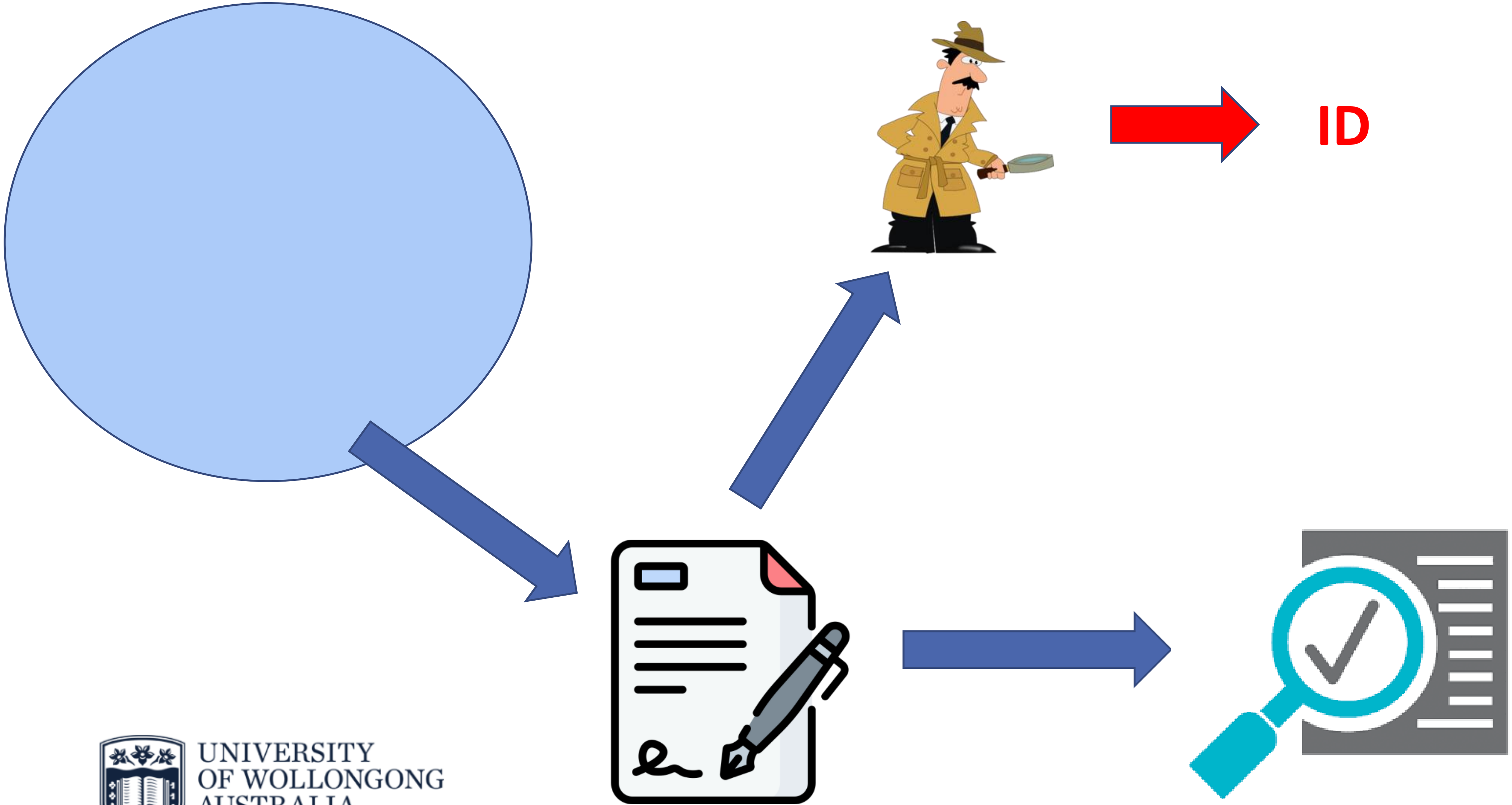
UNIVERSITY OF WOLLONGONG AUSTRALIA

Ring Signatures [RST’01]



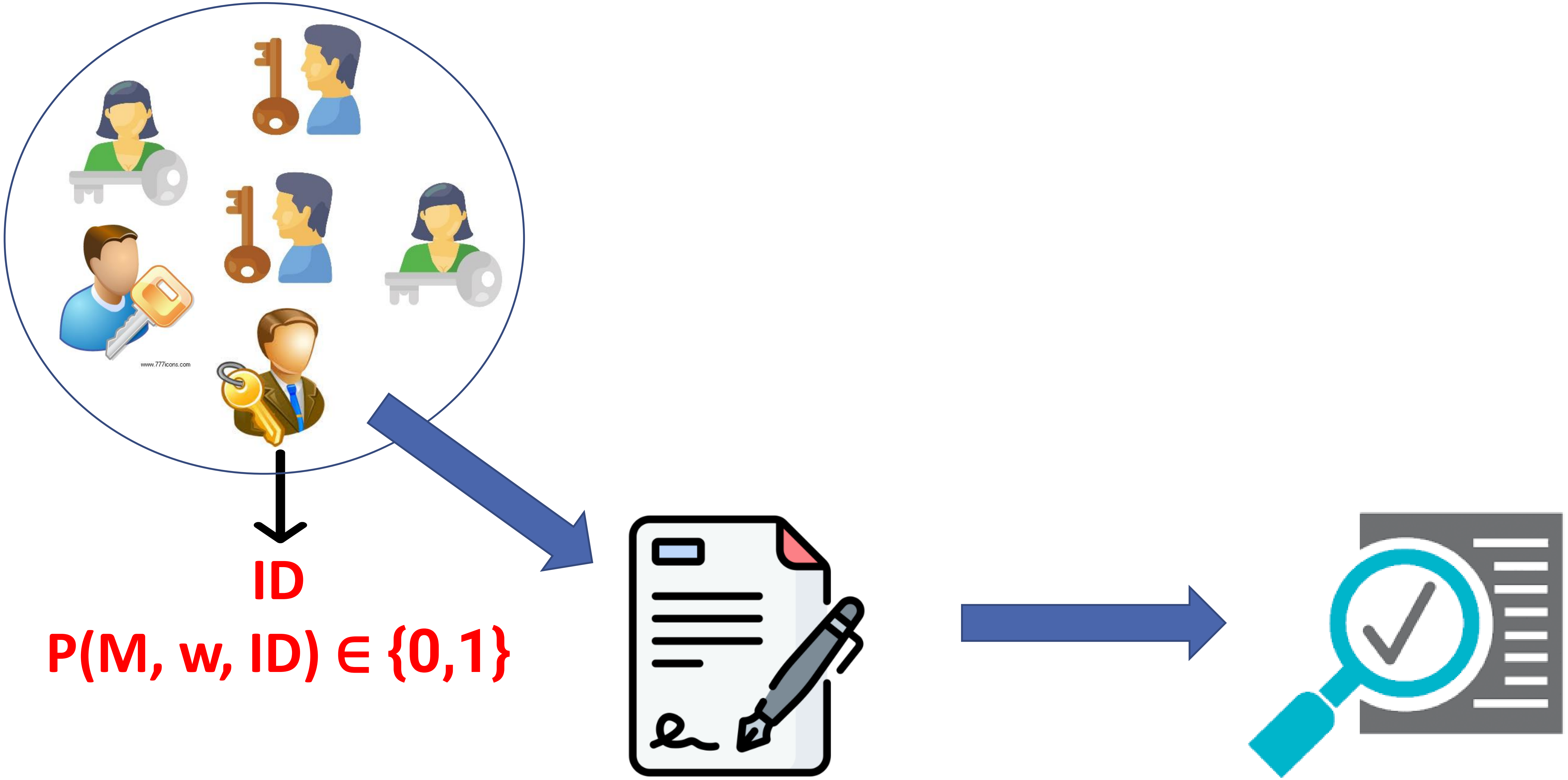
UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Group Signatures [CvH’91]

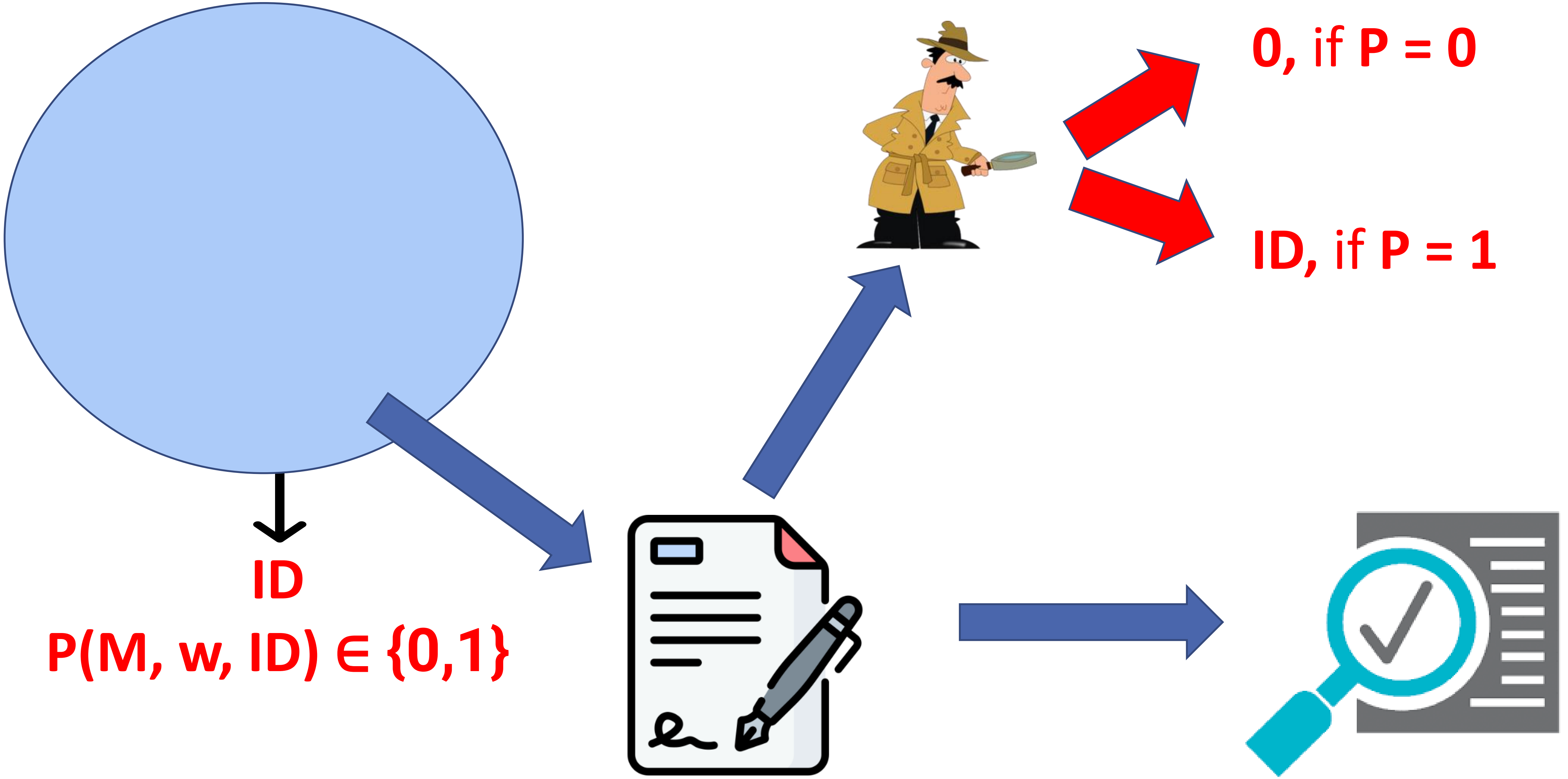


UNIVERSITY OF WOLLONGONG AUSTRALIA

Bifurcated Anonymous Signatures (BiAS) [LNPY'21]



Bifurcated Anonymous Signatures (BiAS) [LNPY'21]



Total Tracing vs. Privacy

Total tracing VS **Privacy**

All identifying info of the traced users must be disclosed

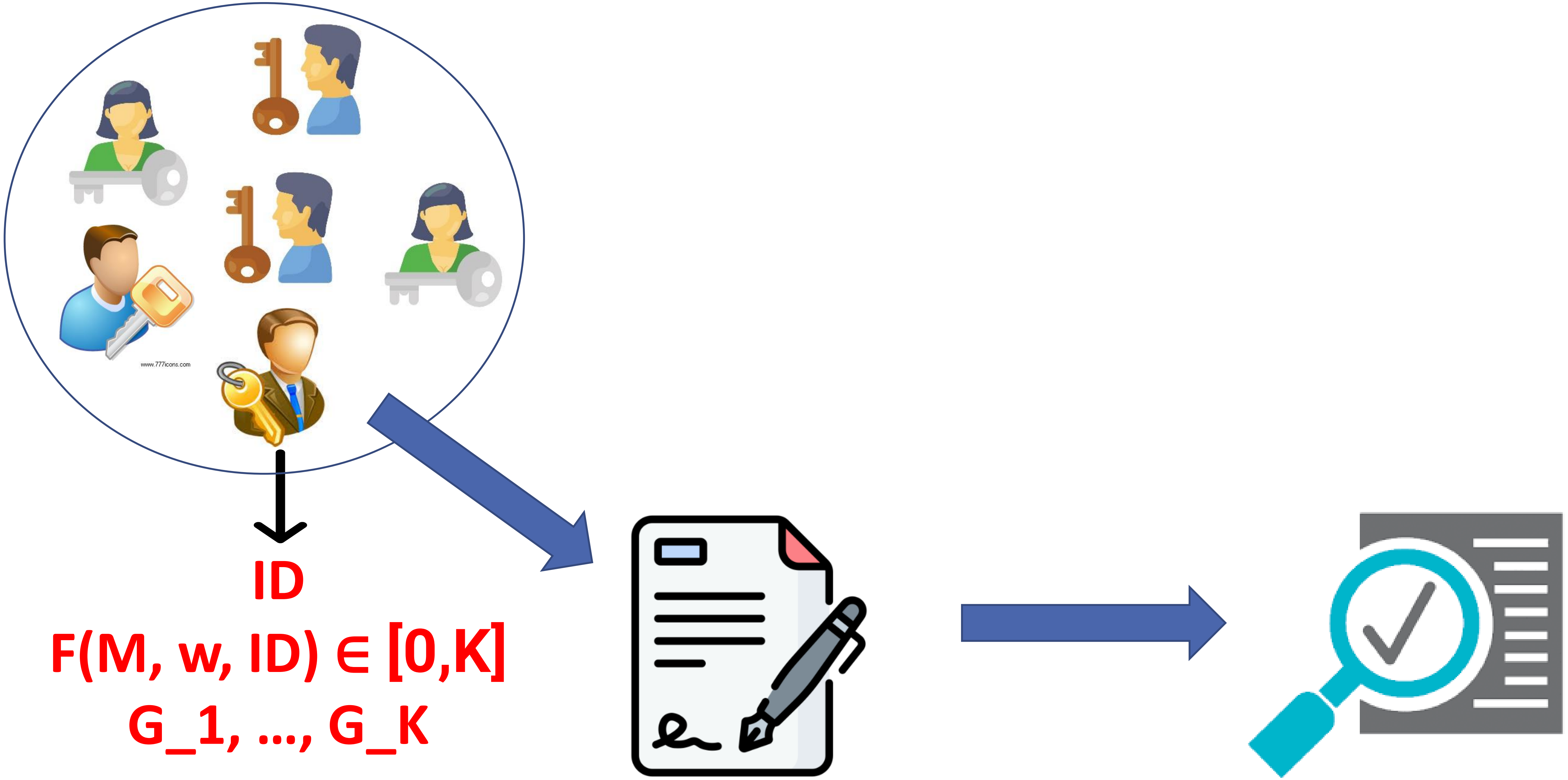
The right of an individual to control with info can be disclosed

Authorities could only be interested in whether a user

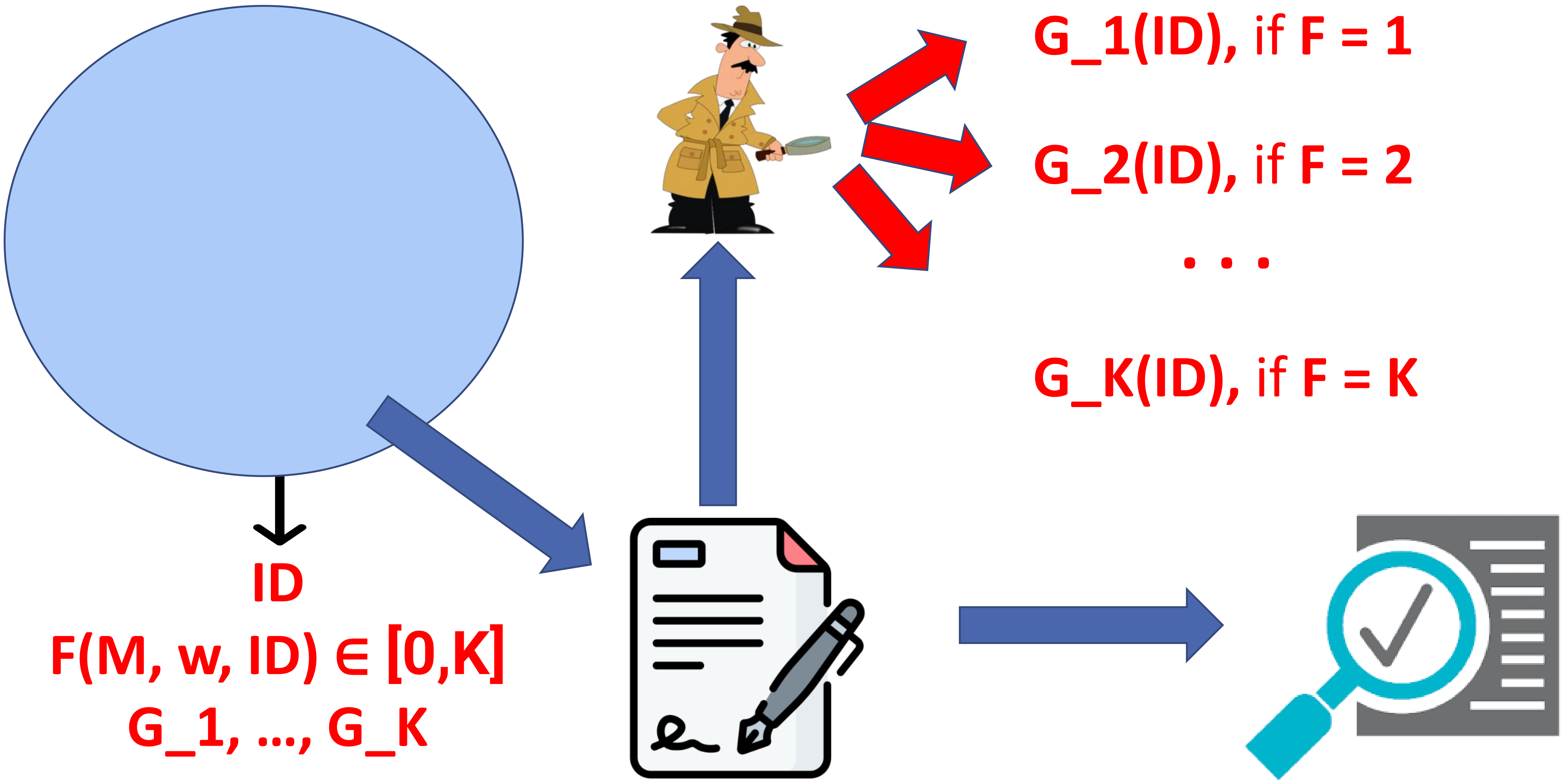
- **Is > 18**
- **Works in company X**
- **Lives at city Y**
- **Has annual income > Z**
- **Has been fully vaccinated**
- **Etc.**

UNIVERSITY OF WOLLONGONG AUSTRALIA

Our Proposal



Our Proposal



Example: Anonymous Financial Transactions

X: transaction amount

$X < 100$	• Anonymity against everyone
$100 \leq X < 1K$	• Authority can learn sender's country
$1K \leq X < 10K$	• Authority can learn sender's country and organization
$10{,}000 \leq X$	• Authority can learn sender's full identity

UNIVERSITY OF WOLLONGONG AUSTRALIA

Our Contributions

- **New concept**: Multimodal Private Signatures (MPS)
  - Novel approach for addressing the "privacy vs accountability" tension
  - Anonymous signatures can be opened to some partial info **op** of **ID**
  - **op** can be flexibly defined based on a set of disclosing functions
  - **Privacy**: signer can decide whether to disclose **op**
  - **Accountability**: authority can learn **op** if needed.

Our Contributions

- **Formalizations of MPS:**
  - Syntax
  - Security definitions

- **Constructing MPS:**
  - Generic construction based on commonly used building blocks.
  - Concrete constructions: pairing-based (SM), lattice-based (ROM)

Security of MPS

- **Privacy:** each party in the system can only learn the piece of signer's information which the signer intends to disclose.

    1. Without OA's opening key, one can learn nothing about the signer's private information (akin to CCA-anonymity in GS).
    2. Even the OA can additionally learn only the value of $\boldsymbol{G_j(ID)}$.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Security of MPS

- **Unforgeability:**

1. If $\boldsymbol{j = F(M, w, ID) = 0}$, then $\boldsymbol{\Sigma}$ should not be valid.
2. It should be infeasible to mislead the opening (traceability in GS)
3. No one can frame an honest user (non-frameability in GS)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Generic Construction

- Modular design for arbitrary signing/disclosing functions
  - Building blocks: ordinary signatures + PKE + NIZK
  - Realizable in the standard model from pairings and from lattices

- "Sign-then-encrypt-then-prove" paradigm
  - **GS**: encrypt **ID**
  - **BiAS**: encrypt ``**ID** or **0**''
  - **Here**: encrypt $\mathbf{op} = G_{F(M,w,\mathrm{ID})}(\mathbf{ID})$ and prove well-formedness.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Lattice-Based and Pairing-Based Instantiations

- Consider the setting with 1 signing function and 4 disclosing functions
  - Let $M = Com(w)$, define $j = F(M, w) \in [0, 4]$ based on integer ranges.
  - Define G_1, G_2, G_3, G_4 as linear transformations: $G_j(ID) = H_j \cdot ID$
- **Pairing-based building blocks:** Pedersen com, Kiltz et al.'s SPS (C'15), Boneh-Boyen sig (EC'04), Kiltz's PKE (TCC'06), GS proofs (EC'08)
- **Lattice-based building blocks:** KTX com (AC'08), Libert et al.'s sig (AC'16), PKE from GPV IBE (STOC'08) + CHK (EC'04), Stern-like ZKP (C'93, AC'17)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Some Open Questions

1. Practical MPS schemes with expressive signing functions and disclosing functions
2. Efficient MPS schemes with post-quantum security
3. Theoretical connections between MPS and FE
4. MPS with additional functionalities, e.g., verifiable opening, user revocations

UNIVERSITY
OF WOLLONGONG
AUSTRALIA