Bicameral and Auditably Private Signatures

Khoa Nguyen, Partha Sarathi Roy, Willy Susilo, **Yanhong Xu**

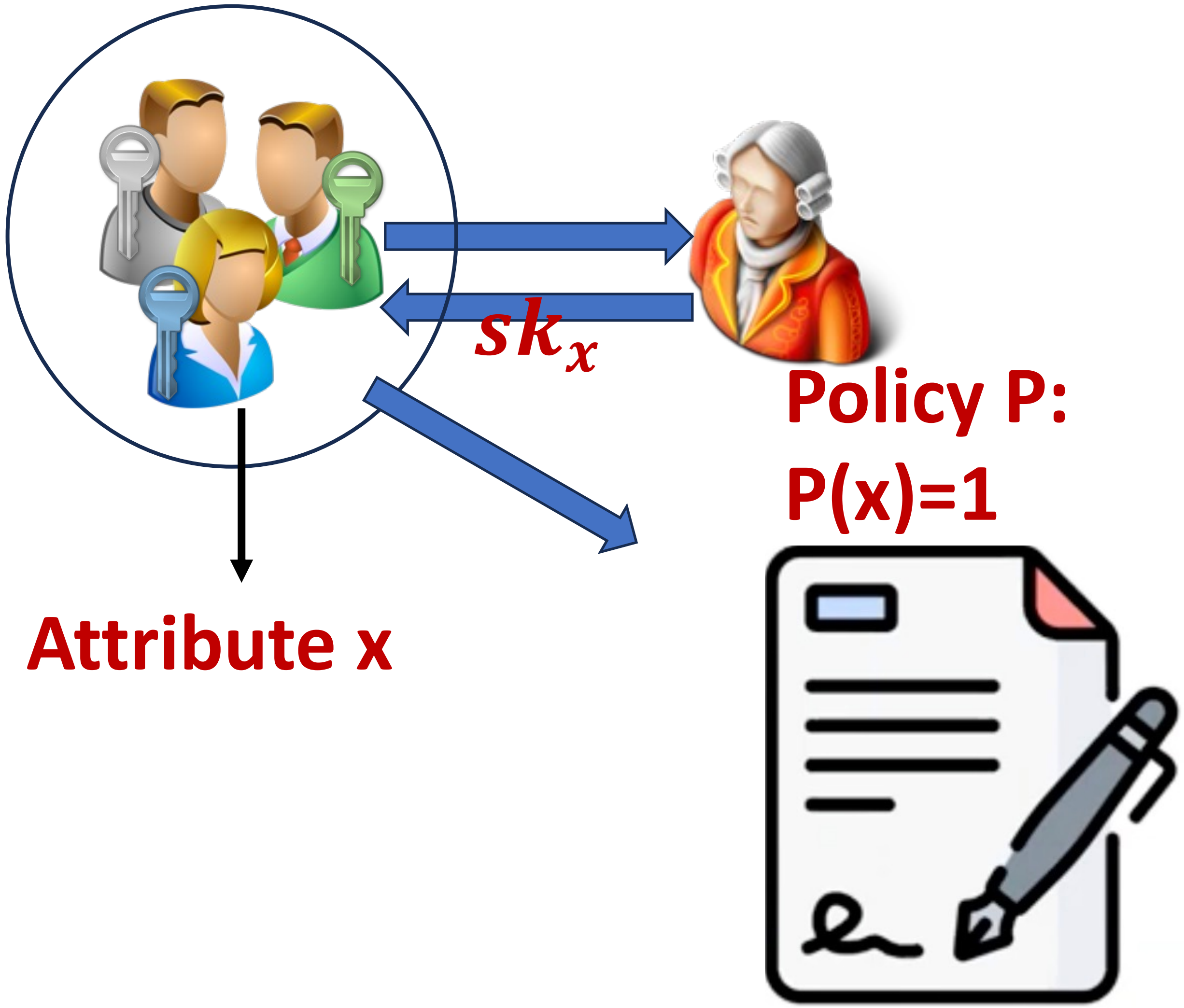
Dec 5, 2023

Guangzhou, China

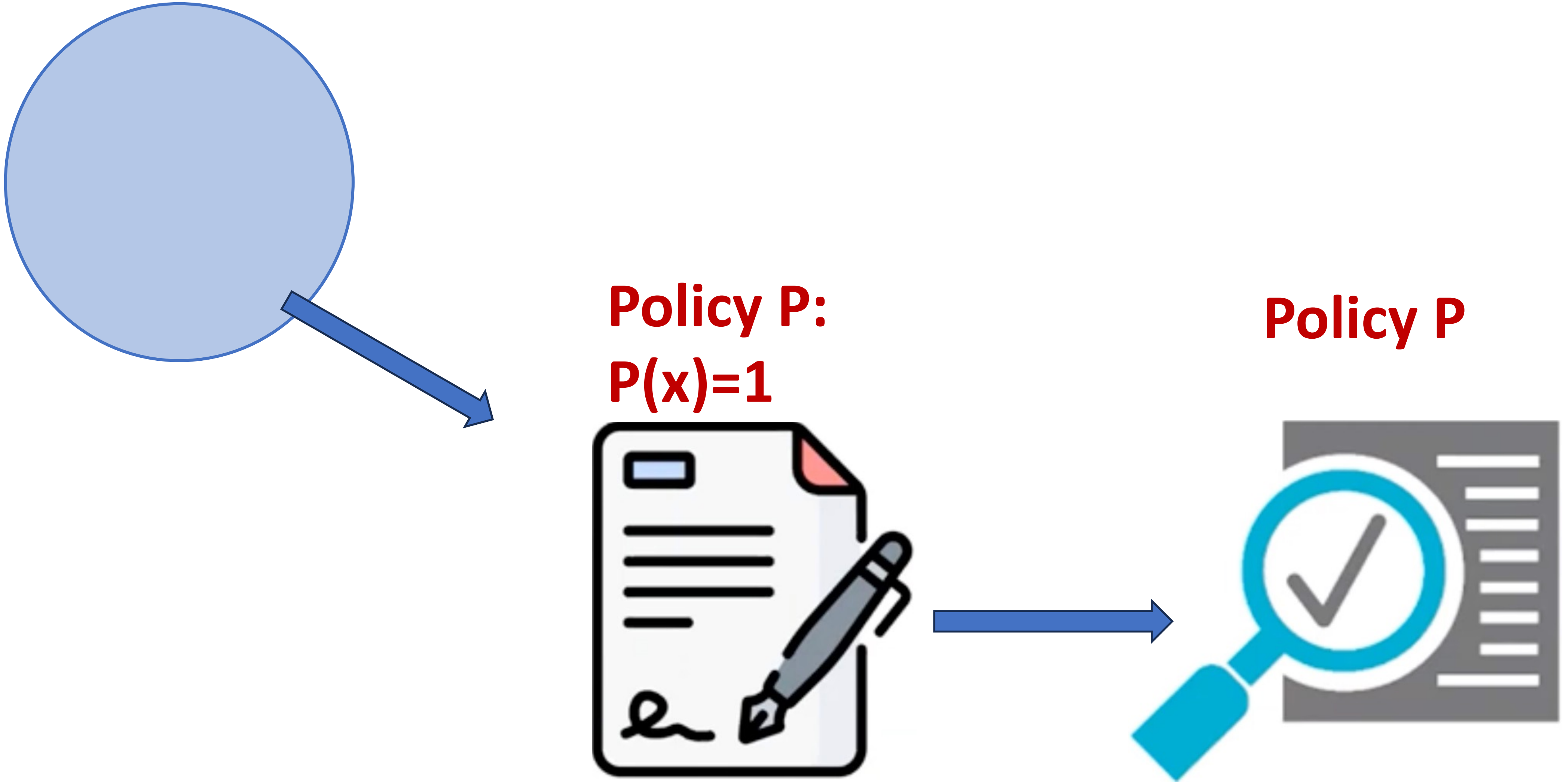
Outline

- Multi-User Private Signature Systems with Fine-Grained Controls
- Accoutable Privacy in Privacy-Preserving Signatures
- Bicameral and Auditably Private Signatures: Definitions and Constructions
- Open Questions

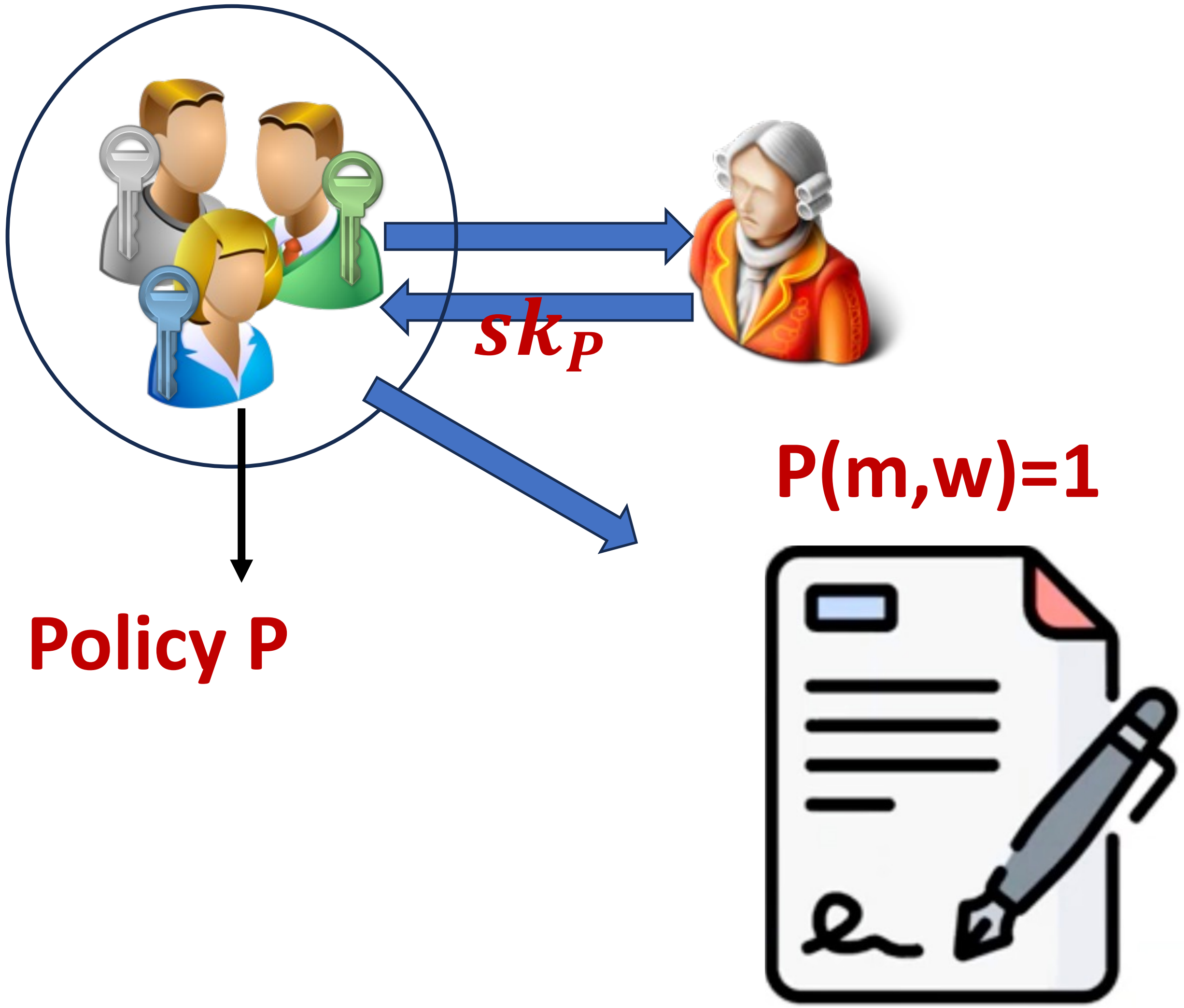
Attribute-Based Signatures [MPR11]



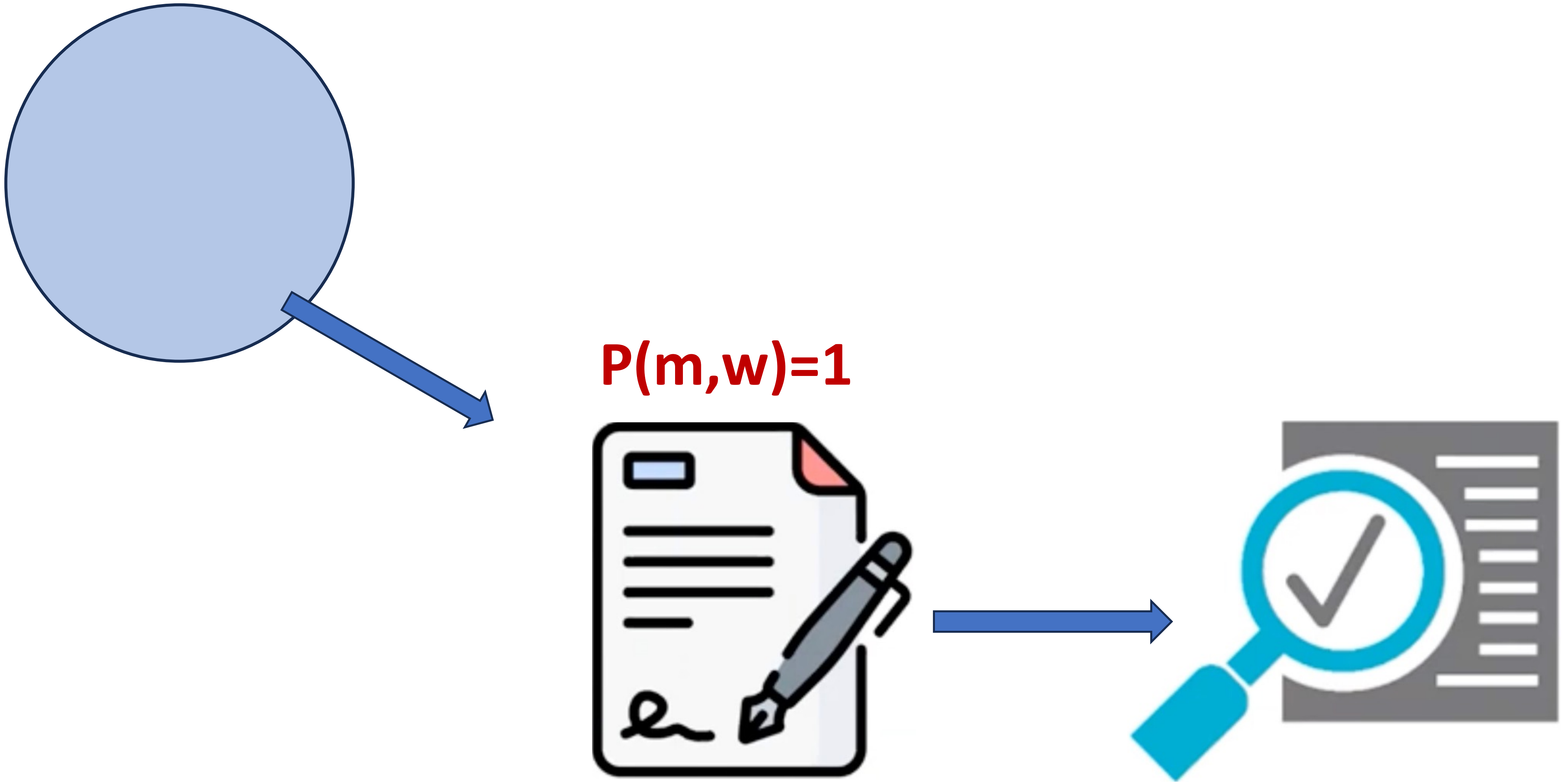
Attribute-Based Signatures [MPR11]



Policy-Based Signatures [BF14]



Policy-Based Signatures [BF14]



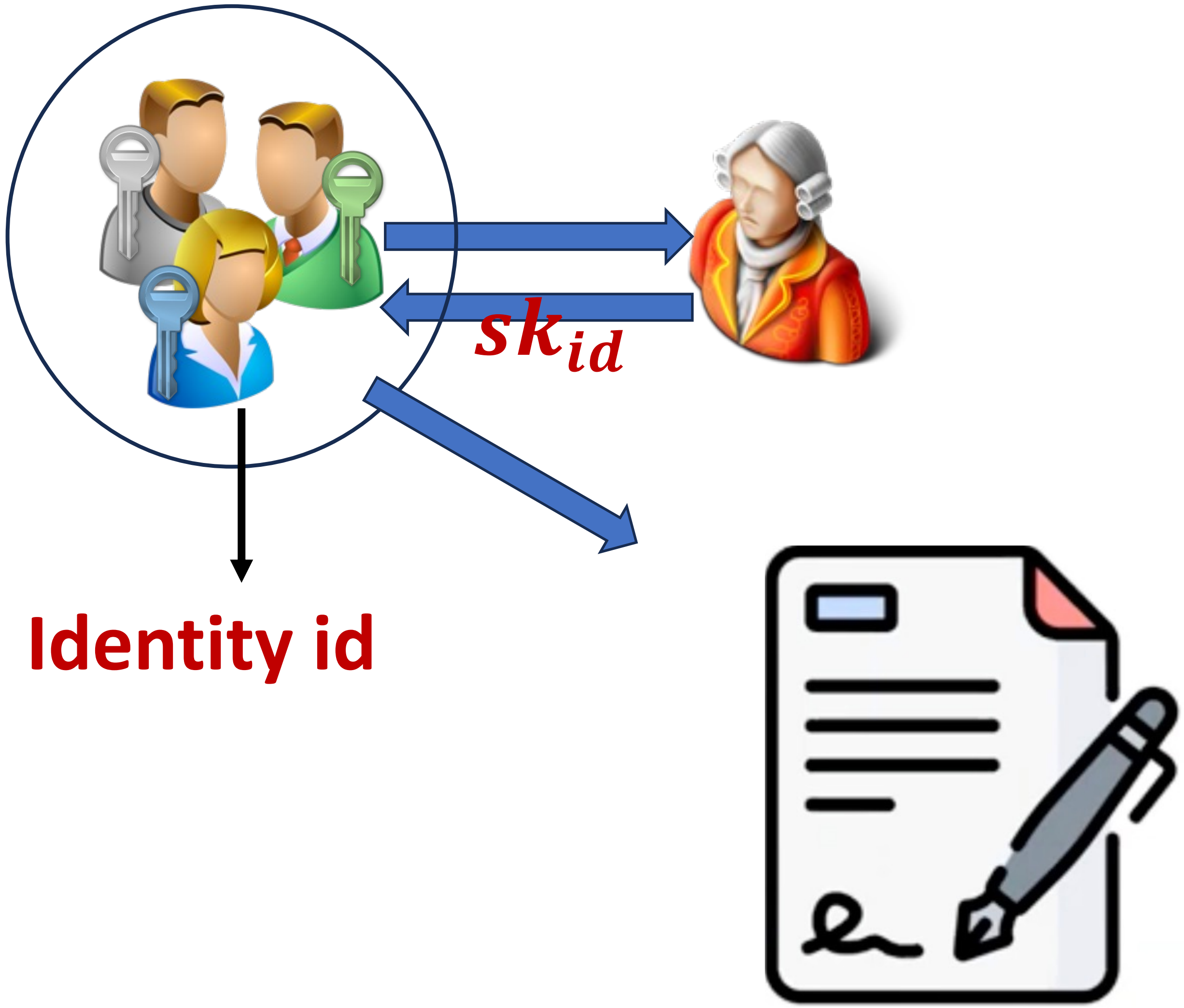
State-of-the-Affairs

References	Attribute	Policy/functions	To sign a message m
ABS [MPR11]	secret	public	P(x)=1
PBS [BF14] FS [BGI14]	NA	secret	P(m,w)=1 P(m)=1
PS [AHY15]	public	secret	P(x)=1
MPS [NGSY22]	secret (id)	public	P(m,id,w) !=0

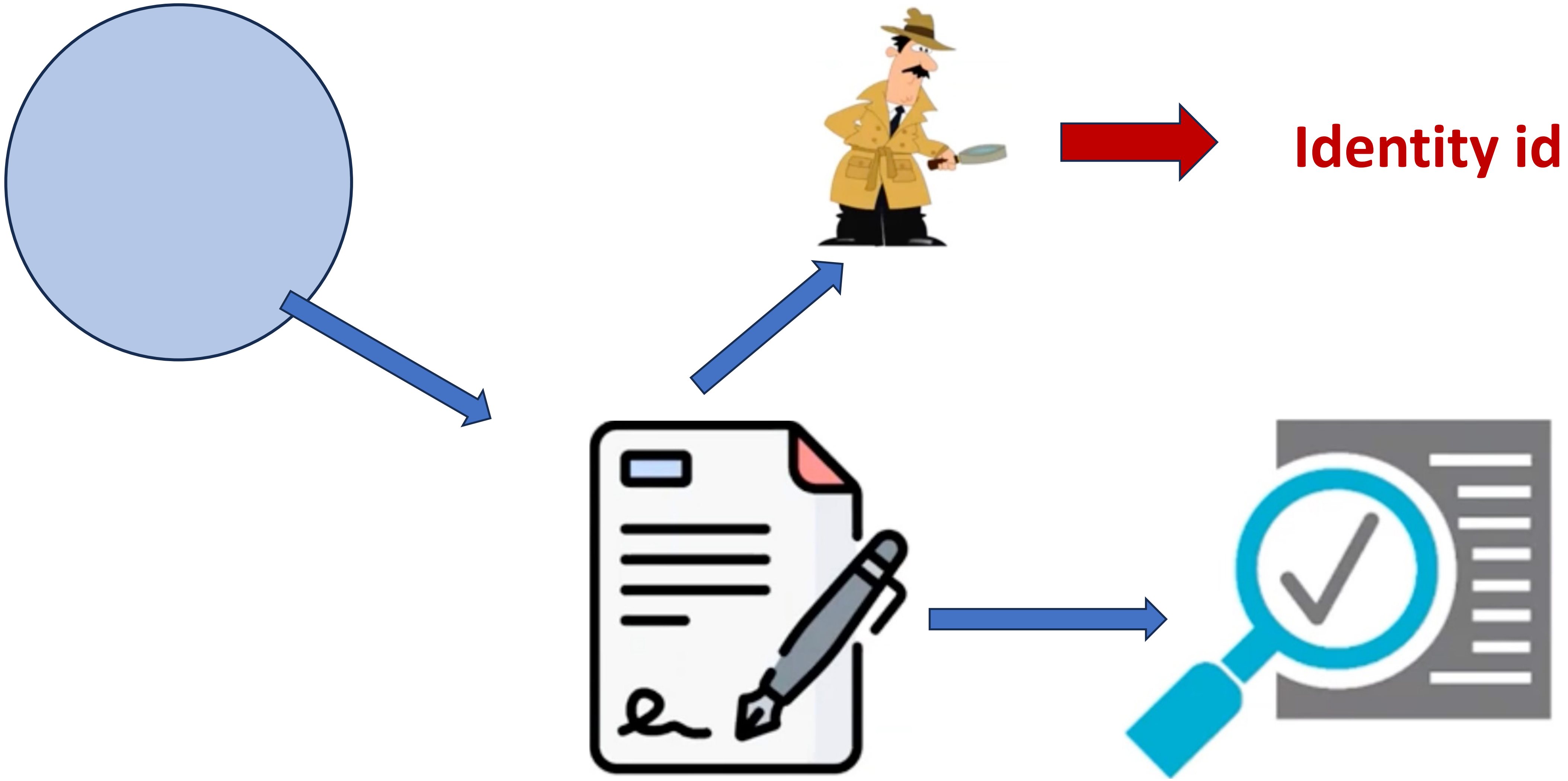
Outline

- Multi-User Private Signature Systems with Fine-Grained Controls
- Accoutable Privacy in Privacy-Preserving Signatures
- Bicameral and Auditably Private Signatures: Definitions and Constructions
- Open Questions

Group Signatures [CvH91]



Group Signatures [CvH91]



State-of-the-Affairs

References	Fine-Grained tracing	
[KTY04] [SEH+12]	user-specific trapdoor msg-specific trapdoor	Who can trace
[KM15]	Traceable sk/non-traceable sk	Whether to trace
[CHL06] [FS07]	Double spend/sign the same event twice	When to trace
[LNPY21] [NGSY22]	All or nothing (id or 0)/ trace to Gi(id)	What to trace

A Short Summary So Far

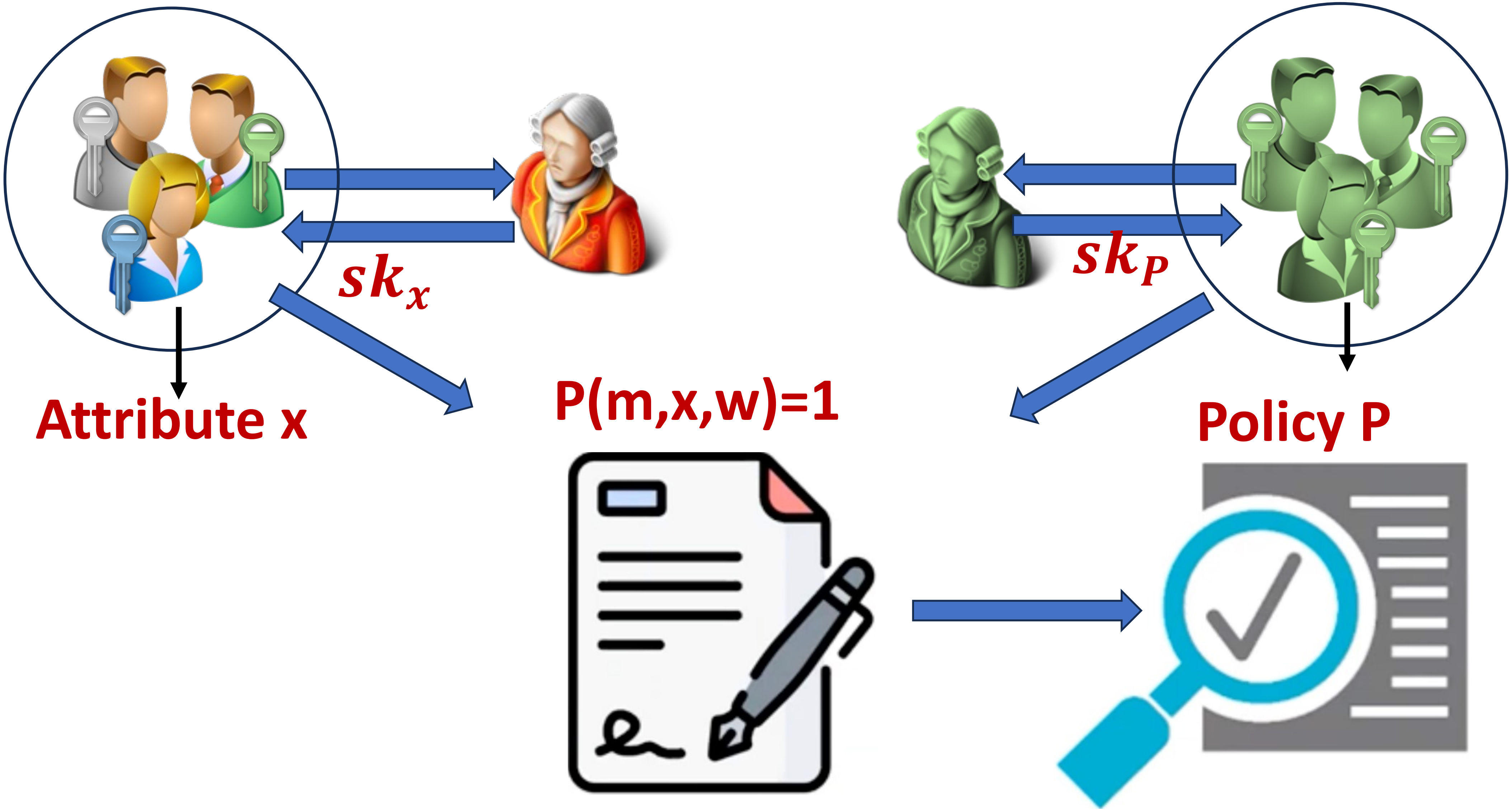
- In the field of multi-user private signatures

Current state	problems
Involving policies and/or attributes	But only employ one authority, and protect one of them
Achieves accountable privacy	Users have no control over the private information after outputting signatures

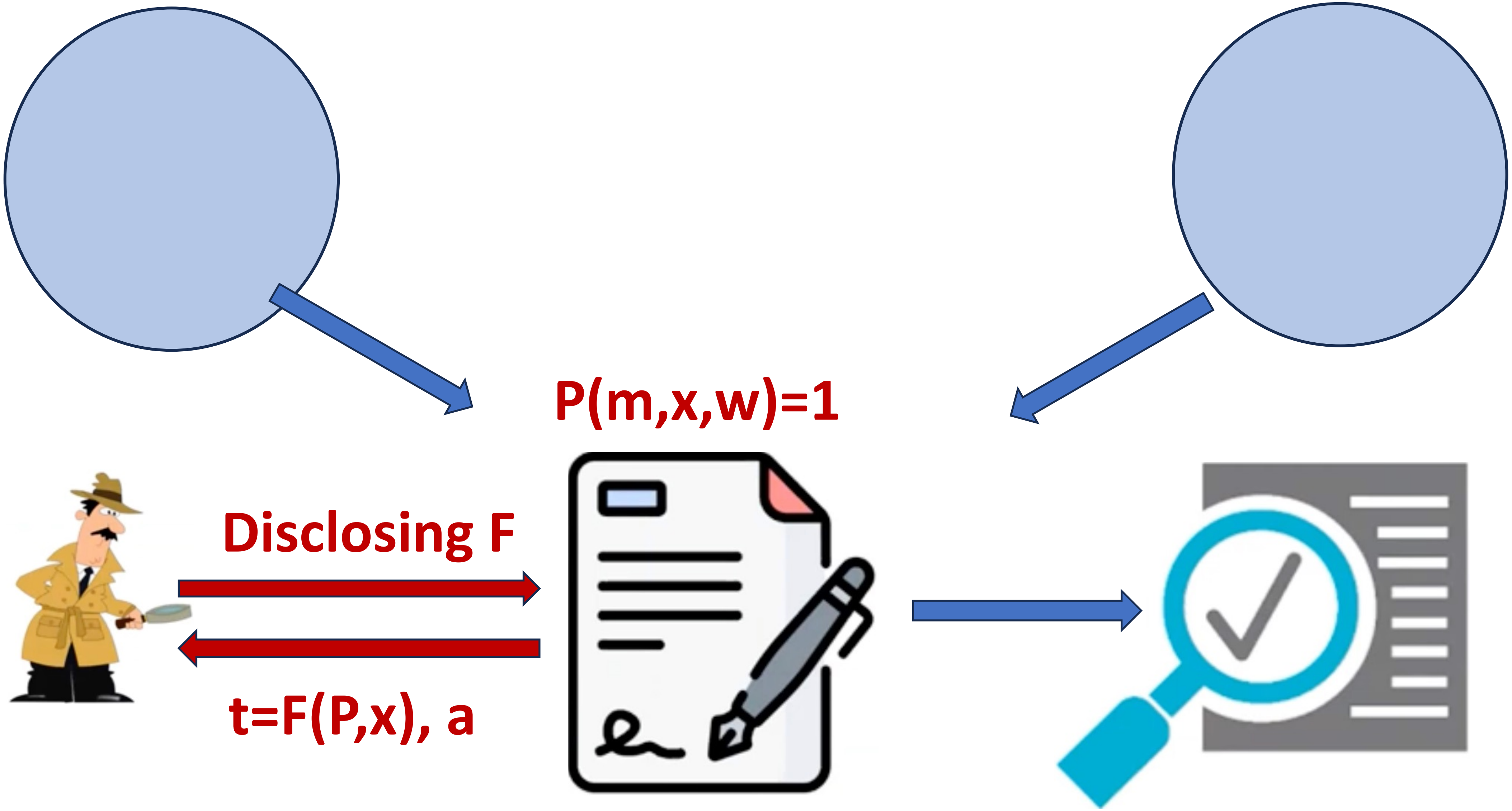
Outline

- Multi-User Private Signature Systems with Fine-Grained Controls
- Accoutable Privacy in Privacy-Preserving Signatures
- Bicameral and Auditably Private Signatures: Definitions and Constructions
- Open Questions

Our Proposal – Bicamerality, Signability, Privacy



Our Proposal – Disclosures and Auditable Privacy



Our Contributions

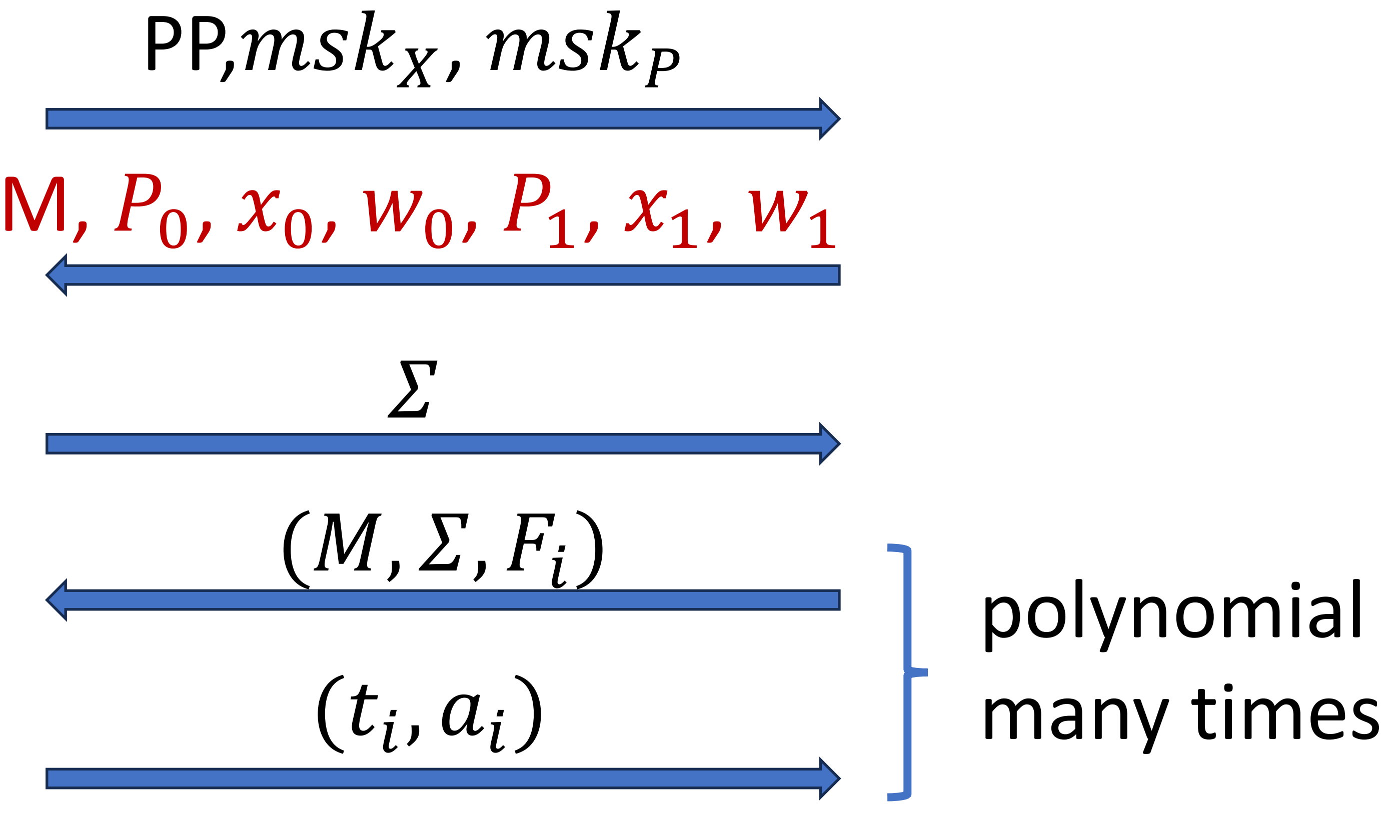
- **New concept:** Bicameral and Auditably Private Signatures (BAPS)
  - **Bicamerality and Privacy:** Simultaneously protect policies and attributes
  - Securely disclose private information after signing
  - **Auditable privacy: the signer disclose t=F(P,x) only when asked to do so**

Our Contributions

- **Formalization of BAPS:**
  - **Syntax**
  - **Security definitions:** privacy and auditable privacy, soundness, unforgeability
- **Constructions of BAPS:**
  - **Generic construction** based on commonly used building blocks
  - **Concrete construction** based on lattice assumptions in ROM (bucket search, quadractic disclosing functions)

Security of BAPS -- Privacy and Auditable Privacy

- Sample a bit b
- Compute $\Sigma \leftarrow Sign(P_b, x_b, w_b, sk_{x_b}, sk_{P_b}, \mathrm{M})$
- Compute $(t_i, a_i) \leftarrow Disclose\ (M, \Sigma, P_b, x_b, F_i)$



$$\boldsymbol{F_i(P_0, x_0) = F_i(P_1, x_1)}$$

Security of BAPS -- Privacy and Auditable Privacy (cont)

- If $\boldsymbol{F_i}$ is the identity function, then the above definition is trivial
- Resort to **simulatability-based notion**
  - Define simulated algorithms
  - Privacy and auditable privacy requires that: adv could not tell whether it is interacting with real algorithms or simulated algorithms

Security of BAPS – Unforgeability

1) No one can sign a valid Σ, if **P(x,m,w)=0**
2) No one can sign valid signatures **without possessing a valid attribute certificate**
3) No one can sign valid signatures **without possessing a valid policy certificate**
4) **t=F(P,x)**, if (P,x) is the underlying policy-attribute of sigma

Generic Construction of BAPS

- **Modular design for arbitrary policies and disclosing functions**
  - **Building blocks:** ordinary signatures + NIZK + commitment
  - Realizable in the **standard model** from pairings and lattices
- "Sign-then-commitment-then-prove" paradigm
  - **Sign** x and P, obtaining sk_{x_b}, sk_{P_b}
  - **Commit** to x and P, obtaining com_x, com_P
  - **Prove** knowledge of x, P, sk_{x_b}, sk_{P_b} when signing, and **t=F(P,x)** when disclosing

A Lattice-Based Instantiation of BAPS

- Consider a setting with
  - ✓ **arbitrary polynomial-size circuits representing policies**
  - ✓ **quadratic disclosing functions:** $t = G_1 \cdot (b \otimes b) + G_2 \cdot b \ mod\ 2$
- "Sign-then-commitment-then-prove" paradigm
  - ✓ a new approach to prove circuit satisfiability for a hidden-yet-certified circuit
  - ✓ a dedicate ZK handling quadratic relations

Outline

- Multi-User Private Signature Systems with Fine-Grained Controls
- Accoutable Privacy in Privacy-Preserving Signatures
- Bicameral and Auditably Private Signatures: Definitions and Constructions
- Open Questions

Open Questions

1) Practically efficient lattice-based BAPS

2) Efficient BAPS without ZK

3) BAPS with additional functionalities