Privacy Enhancing Cryptography

Luís T. A. N. Brandão · René Peralta · Angela Robinson

Cryptographic Technology Group, Computer Security Division, National Institute of Standards and Technology

Privacy-Enhancing Cryptography (PEC)

Goals:
- Follow the progress of emerging technologies in the area of PEC
- Promote the use of cryptographic protocols that enable privacy goals

Technical challenge: enable parties to interact meaningfully, towards achieving an application goal, without revealing unneeded private information to one another or to third parties, and enabling needed security and auditability.

Standardization challenge:
- Large variety of inter-dependent and connected components and techniques (e.g., circuit representation, underlying assumptions, ...)
- Active area of research, with sophisticated algorithms adapting every year

Base cryptographic techniques

The state-of-the-art in privacy-enhancing cryptography is developing rapidly as researchers find ways to implement these amazing techniques in practical ways. PEC is made possible by the following tools.

ZKPs	SMPC	FHE	Others
Zero-Knowledge Proofs	Secure Multiparty Computation	Fully Homomorphic Encryption	Identity-Based Encryption (IBE) Attribute-Based Encryption (ABE) Functional Encryption (FE), ...

Basic *gadgets* (building blocks)

Zero-knowledge proofs and other techniques are often composed by several basic building blocks (commonly referred to as gadgets). Some examples include:

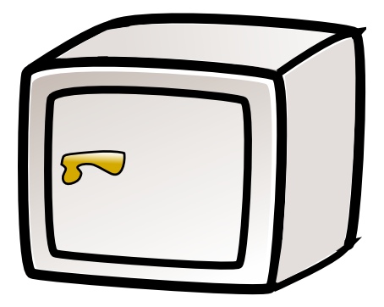
Encipher

Like a random-looking *scrambled text*. Needs a key to be read

Hash

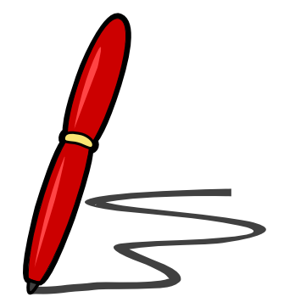
Like a *fingerprint* of data "unique" bit sequence (512 bits) looks random if source is unknown

Commitment



Like a *vault* that hides data, until it is open. Once closed one cannot change what is inside

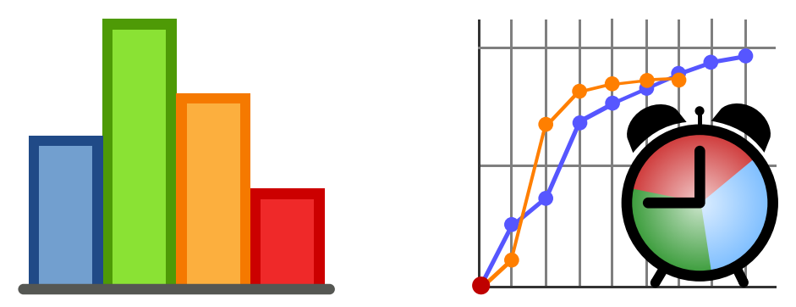
Sign



Like a physical signature, but cannot be forged. Not valid if copied to another document.

Vision and potential impact

- **The Reference Materials approach.** The high-level tools used in PEC are innovative technologies, though not yet widely adopted. The creation and dissemination of reference material is an important step for promoting the use of PEC. PEC applications include user identification and authentication, commercial transactions, private cloud storage and computation, among others.
- **Benchmarks.** We are proposing a benchmark suite to promote the experimentation and deployment of privacy-preserving applications. Potential benchmarks include:
  - Verification of allowed age
  - Private set intersection
  - Public auditability of randomized selections.

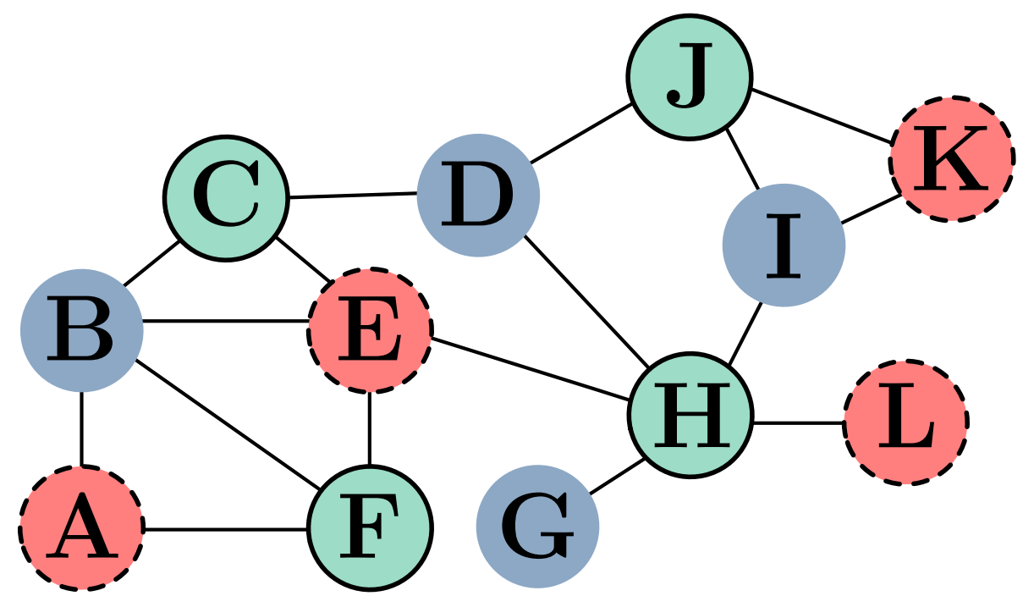


- **ZKProof:** ZKProof is an open initiative that is developing reference material to promote the secure, efficient and interoperable use of ZKPs technology. The **NIST-PEC team** is engaged in providing public feedback and collaborating in the development of useful reference material open to the public.

Zero-knowledge proofs (ZKPs)

ZKPs allow one party (the prover) to prove to another party (the verifier) that a given statement is true and/or that some mathematical solution is known to the prover.

Classic Example — Graph 3-colorability ([GMW'91])



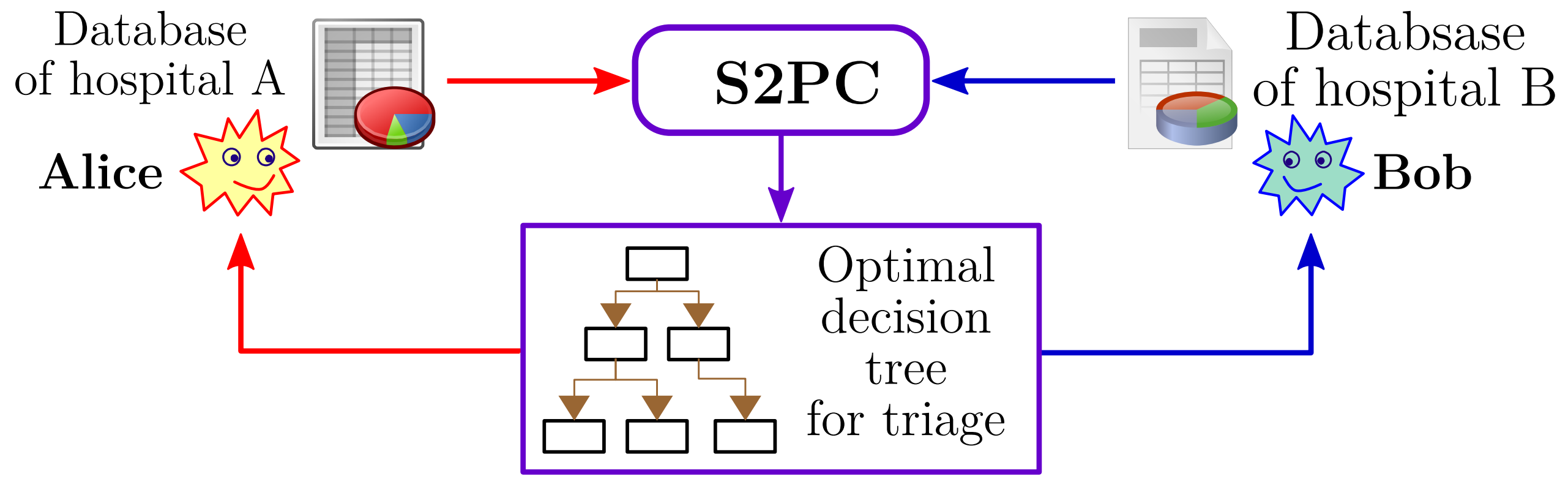
Example: a 3-colorable (3col) graph

- **What:** Prove knowledge of a 3-coloring of a graph (any two connected nodes have different colors), without revealing anything about the solution.
- **Why:** Any NP (non-deterministic polynomial) problem class can be reduced to graph 3-col, i.e., ZKPs can be applied to any practical problem.
- **Method:** Many iterations of the following:
  - The prover randomly permutes the colors (for example 🔴 🔵 🟢 → 🔵 🔴 🟢);
  - The prover commits to all the colors of all the vertices;
  - The verifier chooses one random edge and the verifier opens its two colors.

  The verifier accepts if and only if all edges have two different colors.

Secure multiparty computation (SMPC)

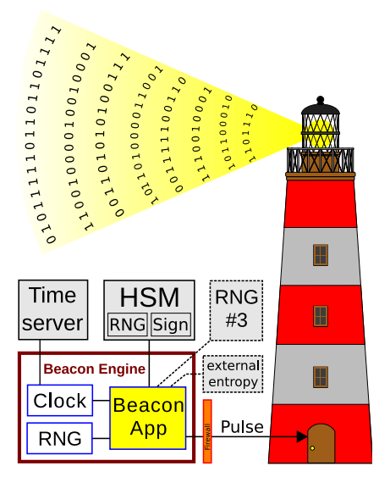
SMPC allows multiple (distrustful) parties to jointly compute a function of their distributed inputs, while retaining privacy and correctness of each input and output.



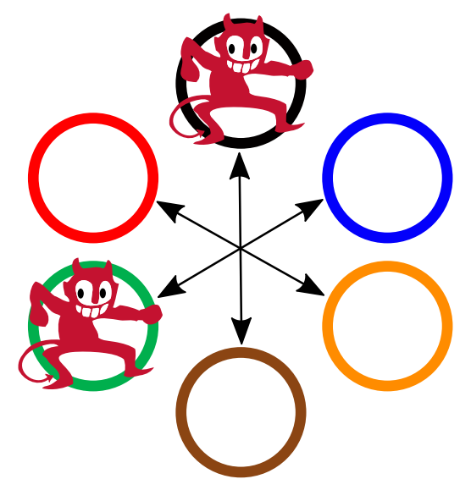
Some PEC project activities in 2019 (focus on ZKPs):

- April 2019: *NIST comments on the initial ZKProof documentation*
- April 2019: Talks at the 2nd ZKProof Workshop (Berkeley, USA)
- August 2019: Talk at the Advanced Cryptography Standardization (ACS'19) workshop
- October 2019: *NIST-PEC contributions to [...the] ZKProof Community Reference [...]*
- October 2019: Talk at the ZKProof Community Event (Amsterdam, Netherlands)
- (To appear) *Proposing a benchmark suite for Privacy-Enhancing Cryptography*

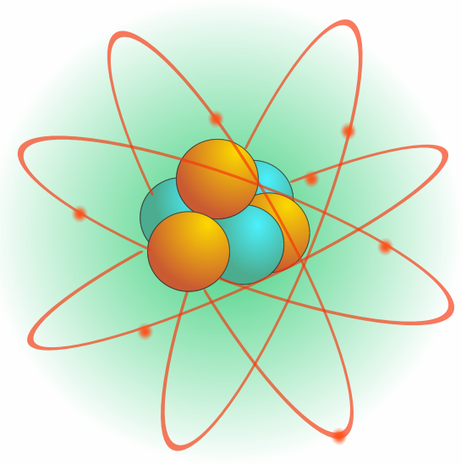
Foreseeable synergies with other projects:
- Privacy preserving public auditability, as enabled by **randomness beacons**
- SMPC is useful for **threshold cryptography** (compute on secret-shared key)
- Some **post-quantum** cryptographic schemes are based on PEC (and vice-versa)
- Efficient ZKPs and SMPC depend strongly on good **circuits** with low **complexity**



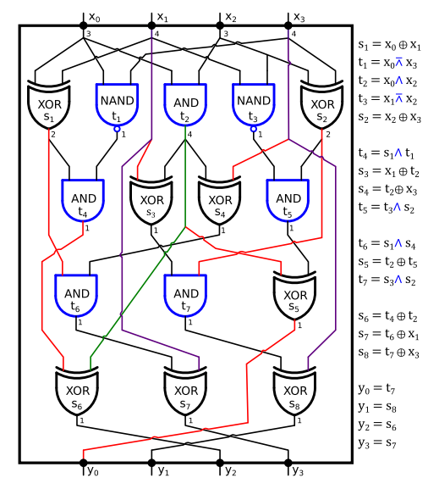
Randomness Beacons



Threshold Cryptography



Post-Quantum Cryptography



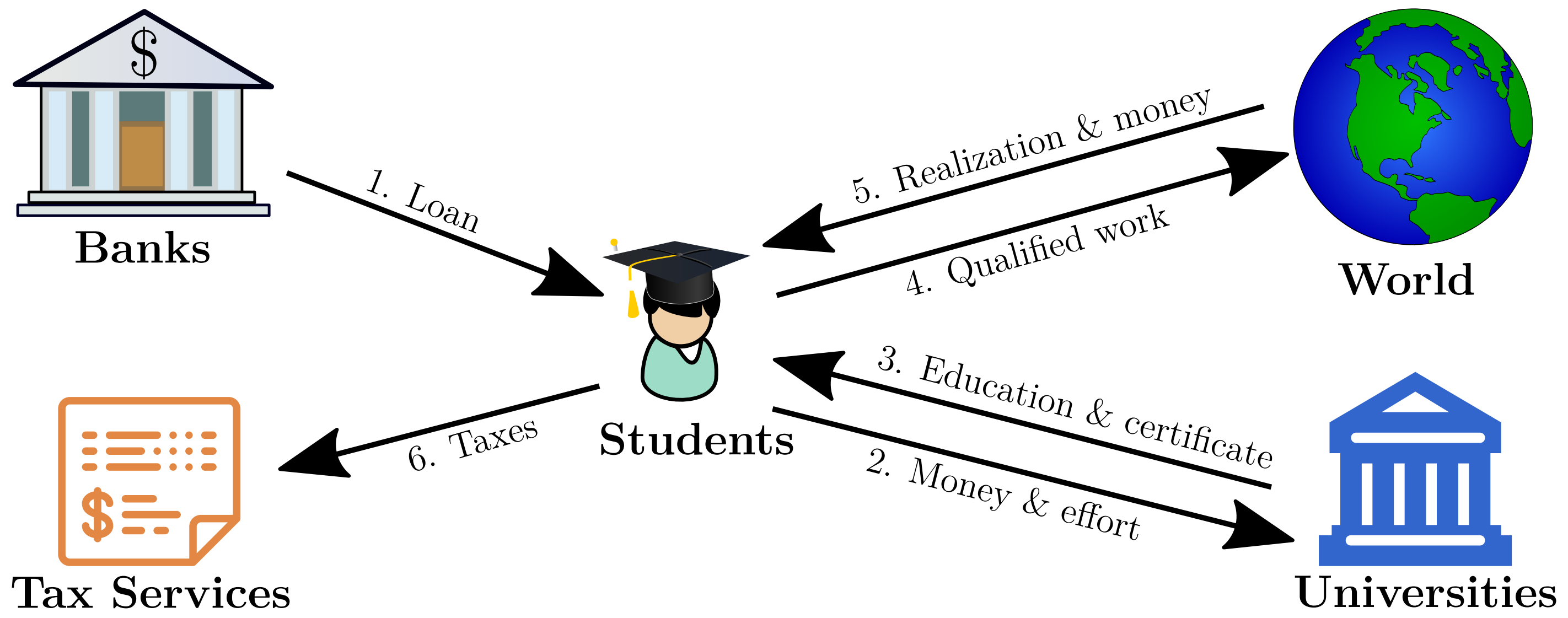
Circuit Complexity

Students Right to Know

A U.S. Congress bill (2019) mandates the use of SMPC (or equivalent) to estimate the return on investment by students on their college education.

https://www.congress.gov/bill/116th-congress/house-bill/1565

- The data are distributed across several entities: SSA, Treasury, VA, Universities.
- Due to privacy concerns, these entities cannot share their data.



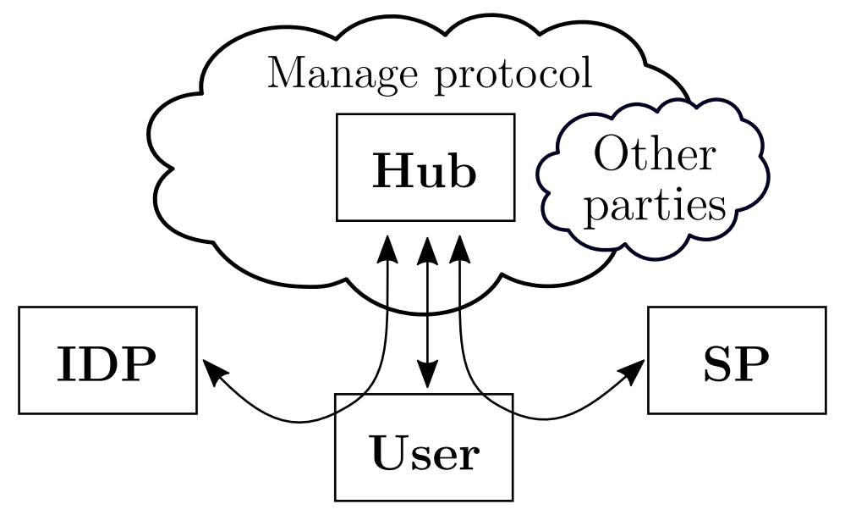
Approach

- Data holders encrypt the relevant data.
- Data holders participate in an SMPC that calculates aggregate statistics. This requires they link, in a privacy preserving way, data pertaining to the same student.

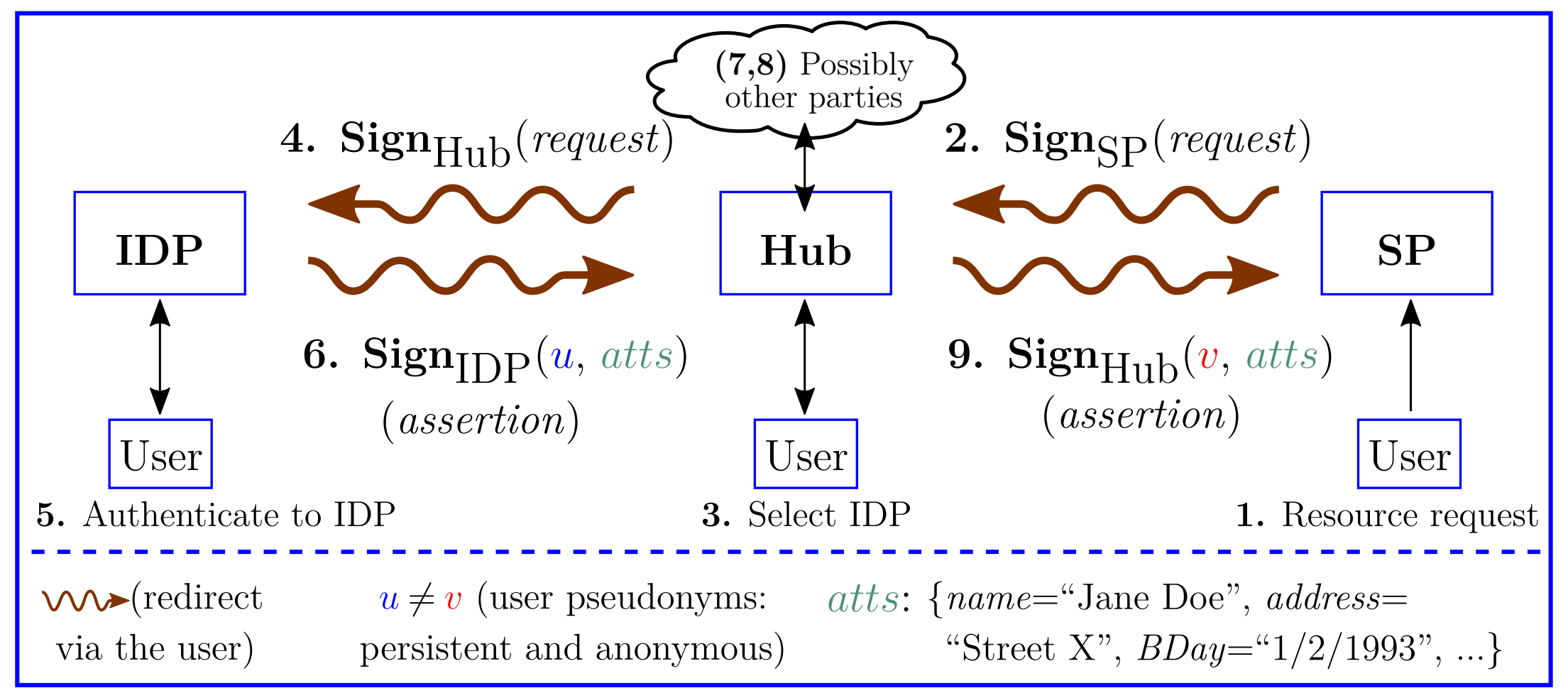
Result: Estimated return on investment while complying with privacy regulations.

Use-case: brokered identification

Problem: The "National Strategy for Trusted Identities in Cyberspace" (NSTIC) required privacy properties for **mediated** identification transactions on the Internet:

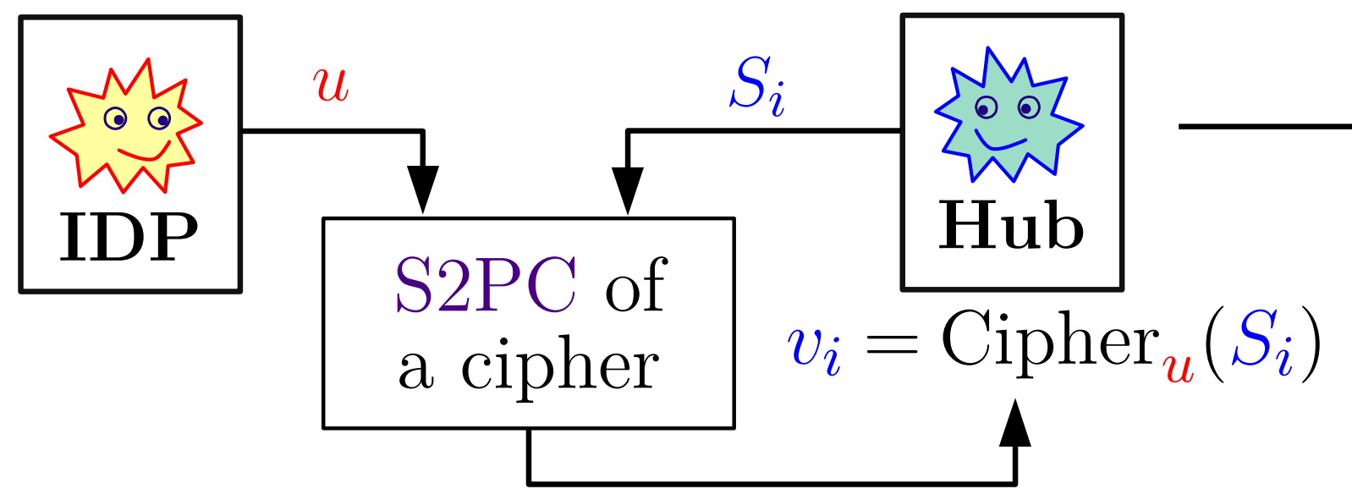


Legend:
- IDP (**Id**entity **P**rovider);
- SP (**S**ervice **P**rovider)


(7,8) Possibly other parties
4. $\text{Sign}_{\text{Hub}}(request)$
2. $\text{Sign}_{\text{SP}}(request)$
IDP
Hub
SP
6. $\text{Sign}_{\text{IDP}}(u, atts)$ (assertion)
9. $\text{Sign}_{\text{Hub}}(v, atts)$ (assertion)
User
User
User
5. Authenticate to IDP
3. Select IDP
1. Resource request
(redirect via the user)
$u \neq v$ (user pseudonyms: persistent and anonymous)
$atts$: {name="Jane Doe", address="Street X", BDay="1/2/1993", ...}

Example challenge: how to prevent the Hub from profiling user transactions?

Solution approach for unlinkability: Transform the pseudonyms using an S2PC:



- v_i is pseudo-random
- The Hub learns nothing about u
- THe IDP learns nothing about S_i and v_i

When the same user accessed different SPs, the Hub sees different pseudonyms, thus **avoiding linkability** of transactions of the same user to different SPs.

The PEC Project/Team contact: crypto-privacy@nist.gov

Webpage: https://csrc.nist.gov/Projects/Privacy-Enhancing-Cryptography

Poster produced for: NIST-ITL Science Day 2019 — November 06, 2019 (Gaithersburg, USA)