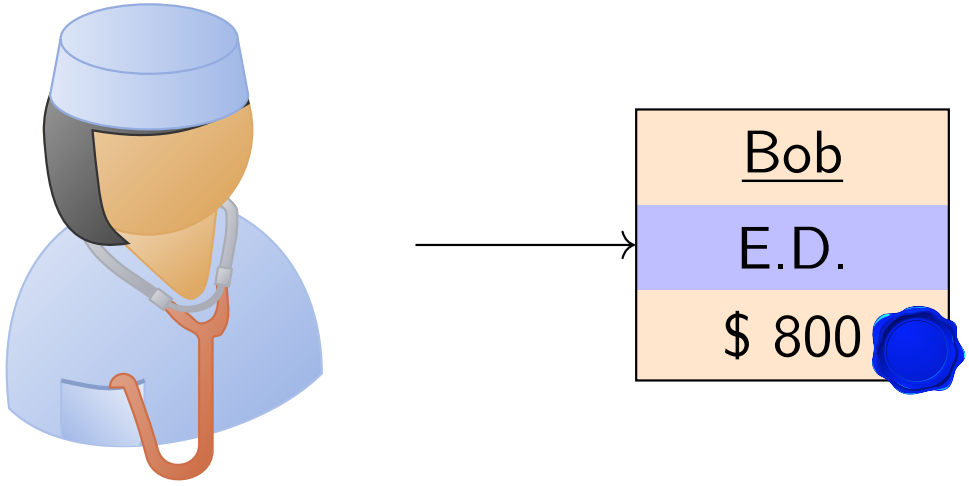
Efficient Unlinkable Sanitizable Signatures from Signatures with Re-Randomizable Keys

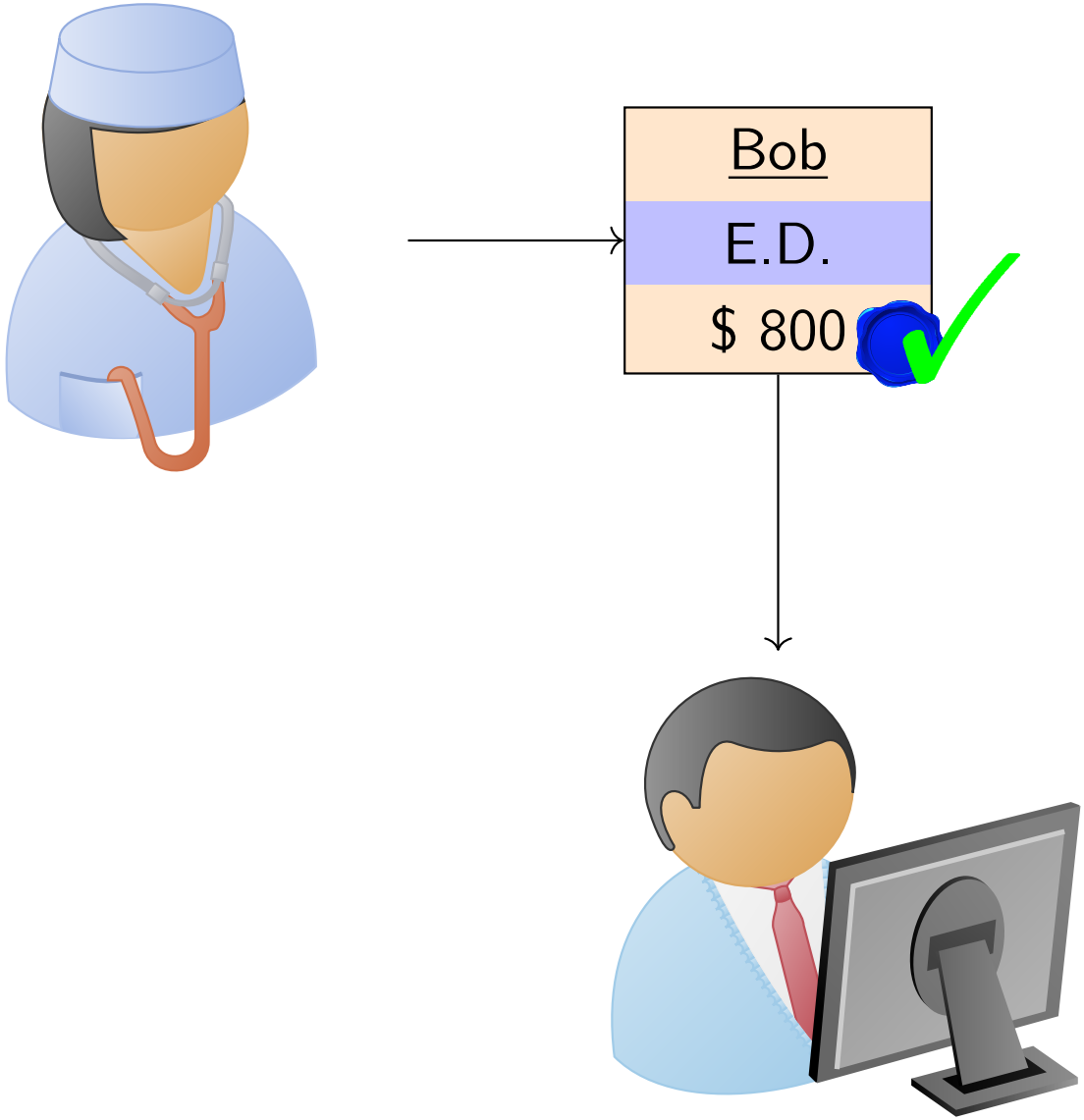
Nils Fleischhacker Johannes Krupp Giulio Malavolta
Jonas Schneider Dominique Schröder Mark Simkin

March 7, 2016

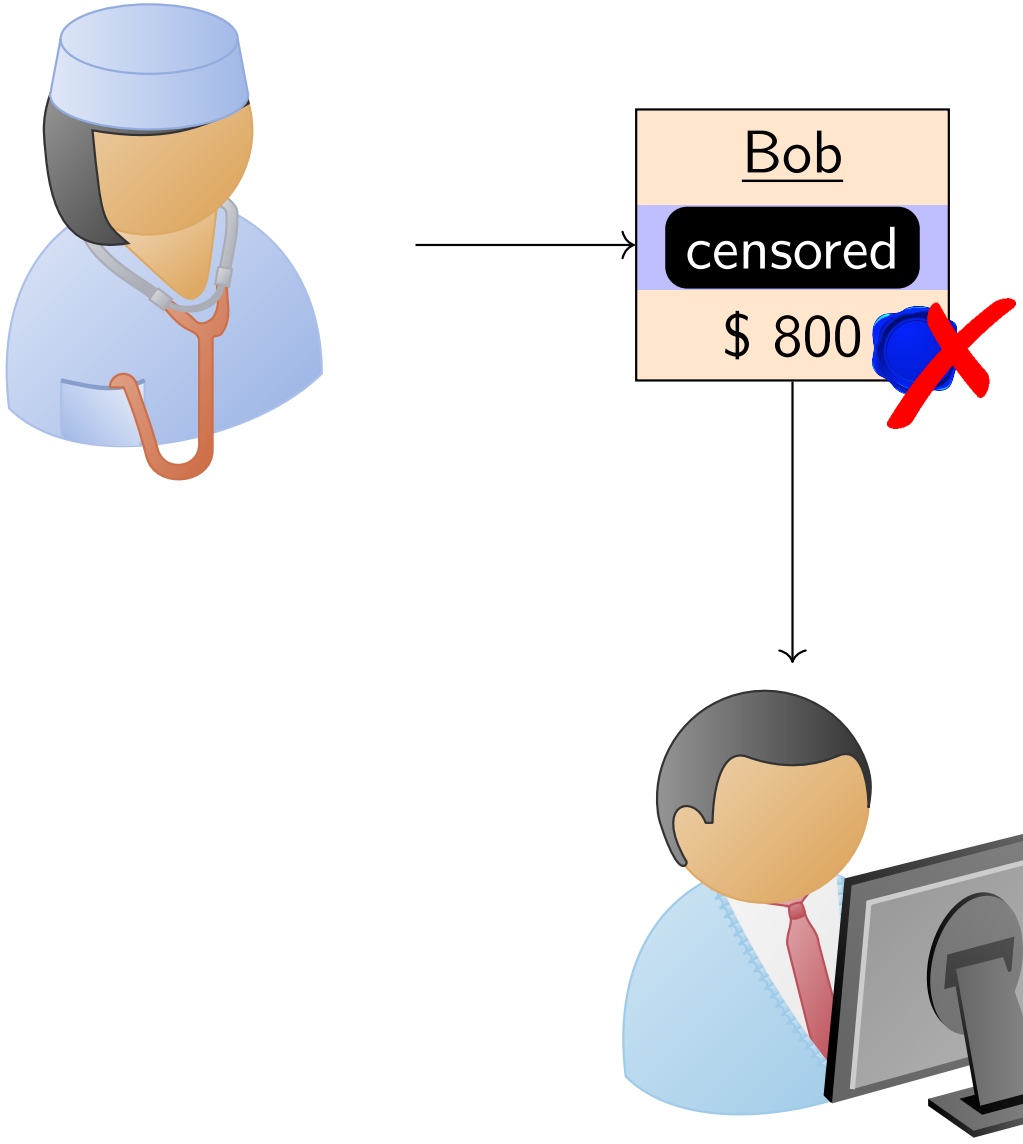
Sanitizable Signatures [ACdMT05]



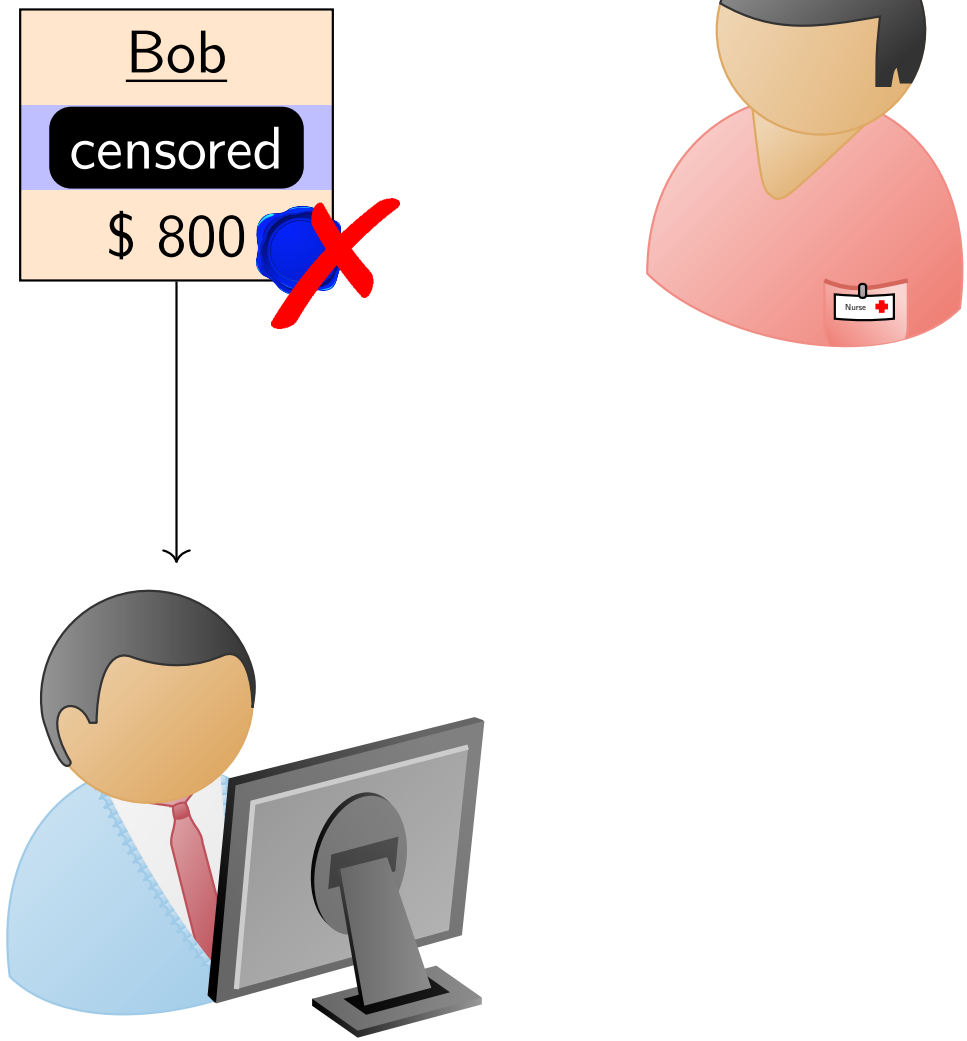
Sanitizable Signatures [ACdMT05]



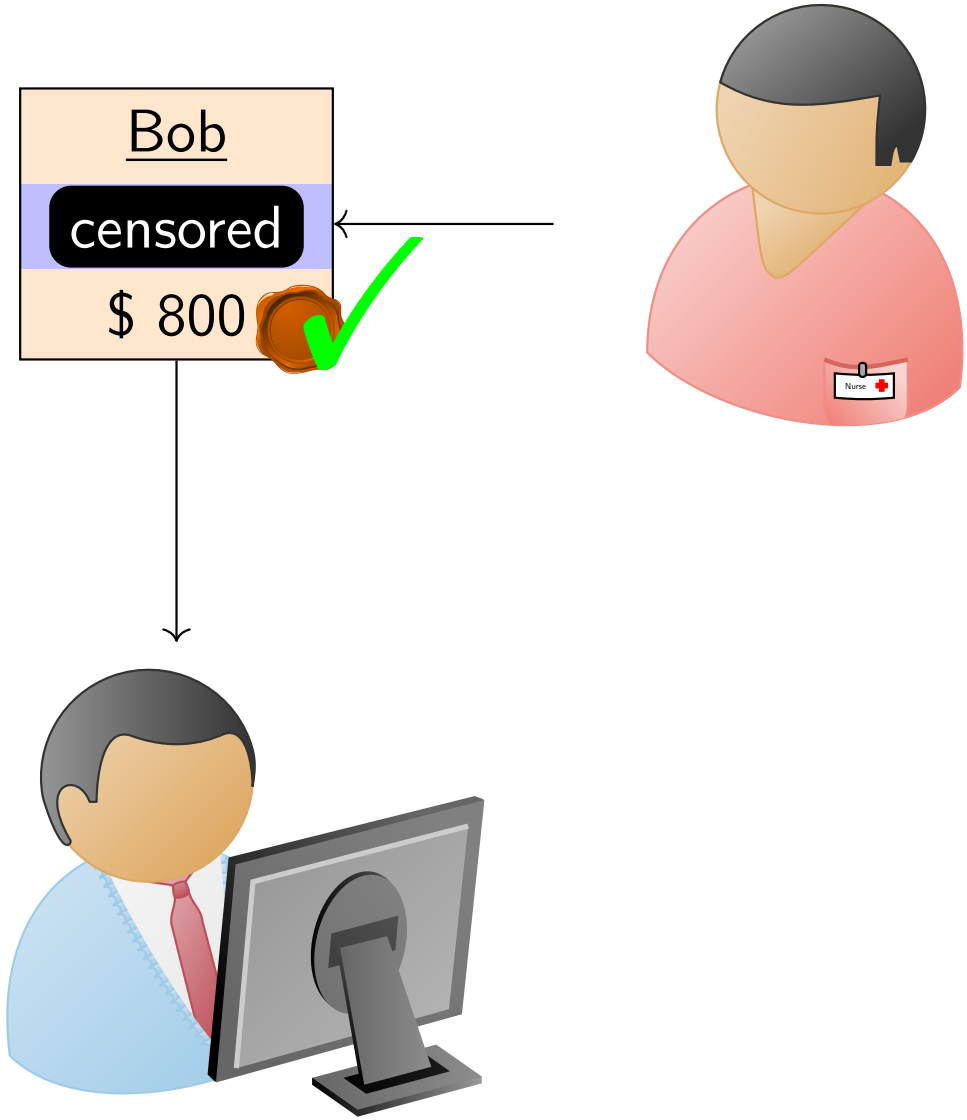
Sanitizable Signatures [ACdMT05]



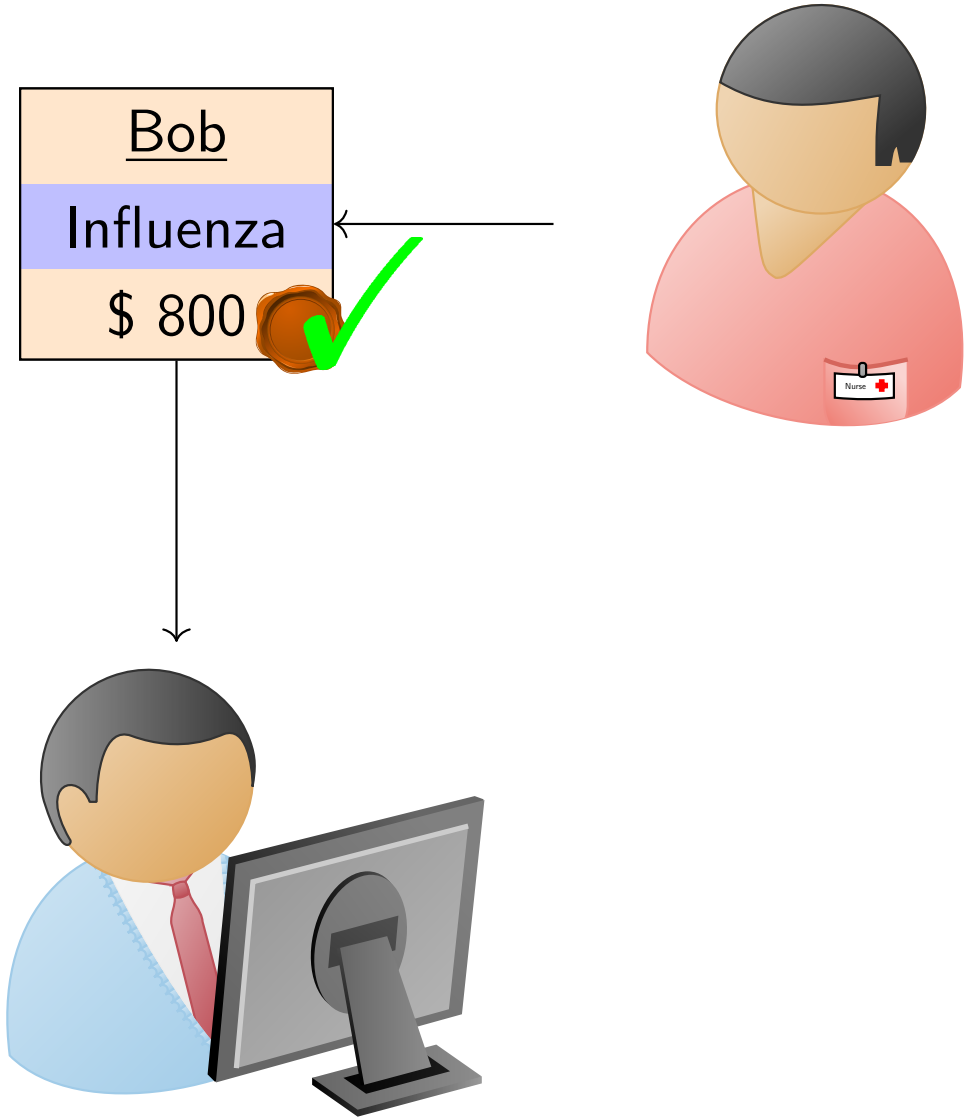
Sanitizable Signatures [ACdMT05]



Sanitizable Signatures [ACdMT05]



Sanitizable Signatures [ACdMT05]



Security of Sanitizable Signatures

- Formalized by Brzuska et al. [BFFLPSSV09]
  - Immutability
  - Sanitizer Accountability
  - Signer Accountability
  - Transparency
  - Unforgeability
  - Privacy
- Missing property identified by Brzuska et al. [BFLS10]
  - Unlinkability

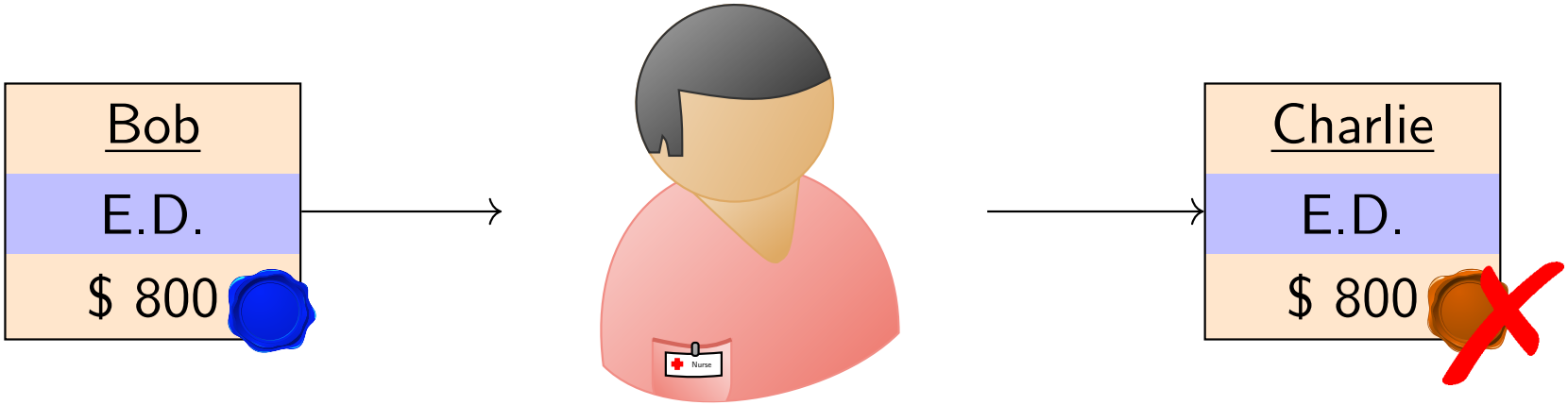
Security of Sanitizable Signatures

- Formalized by Brzuska et al. [BFFLPSSV09]
  - Immutability
  - Sanitizer Accountability
  - Signer Accountability
  - Transparency
  - ~~Unforgeability~~
  - ~~Privacy~~
- Missing property identified by Brzuska et al. [BFLS10]
  - Unlinkability

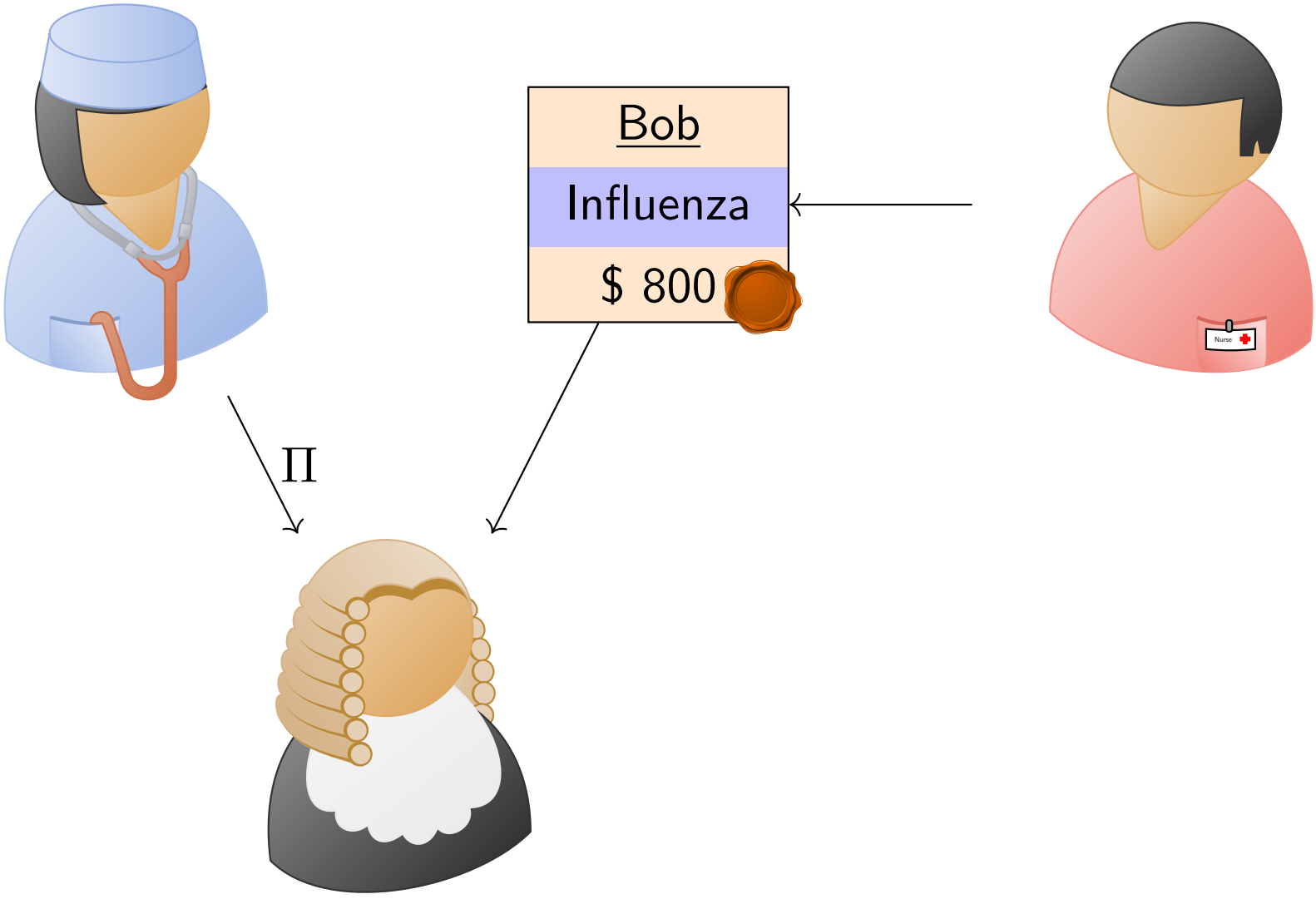
Security of Sanitizable Signatures

- Formalized by Brzuska et al. [BFFLPSSV09]
  - Immutability
  - Sanitizer Accountability
  - Signer Accountability
  - Transparency
  - ~~Unforgeability~~
  - ~~Privacy~~
- Missing property identified by Brzuska et al. [BFLS10]
  - Unlinkability

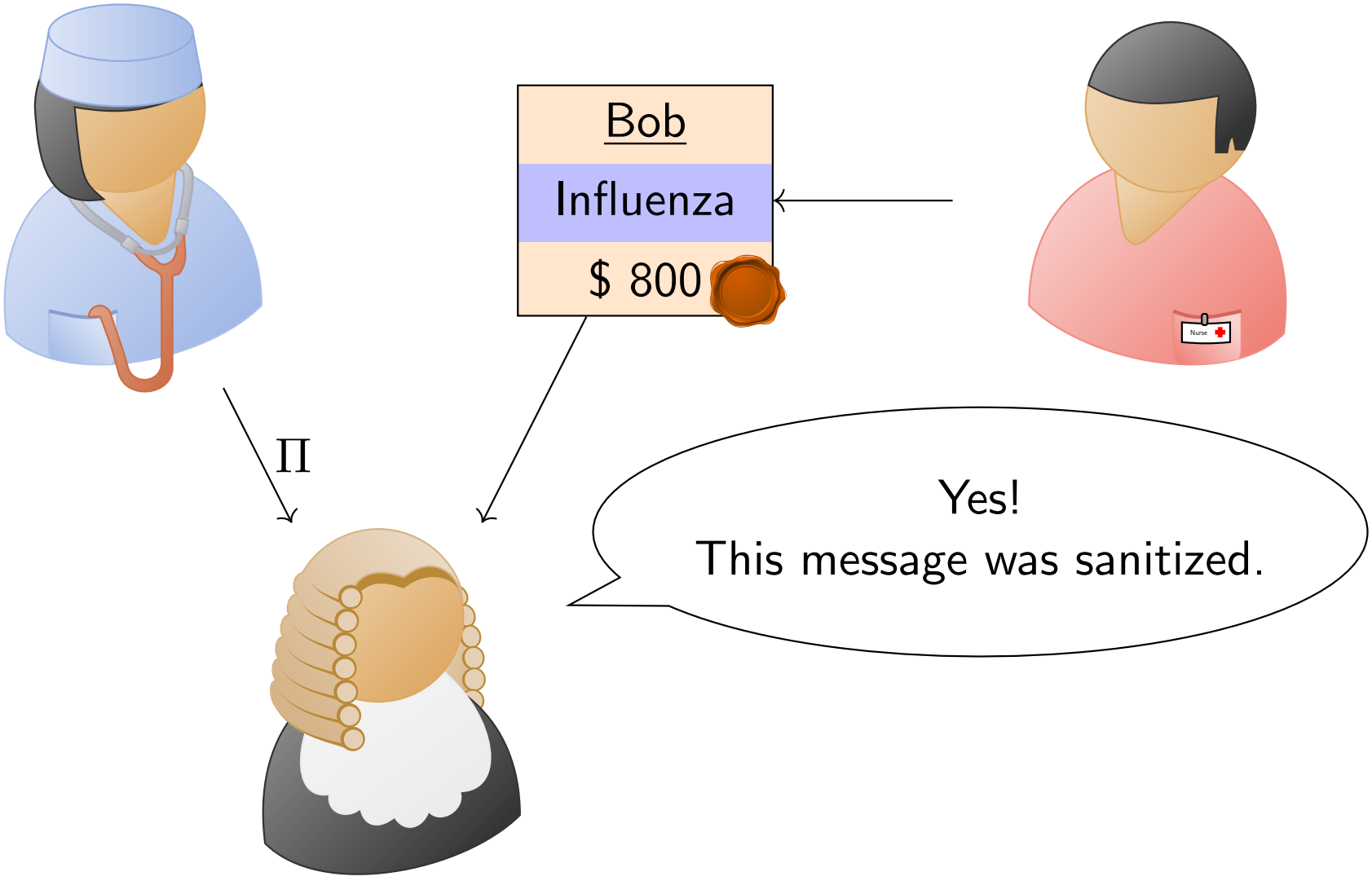
Immutability [ACdMT05][BFFLPSSV09]



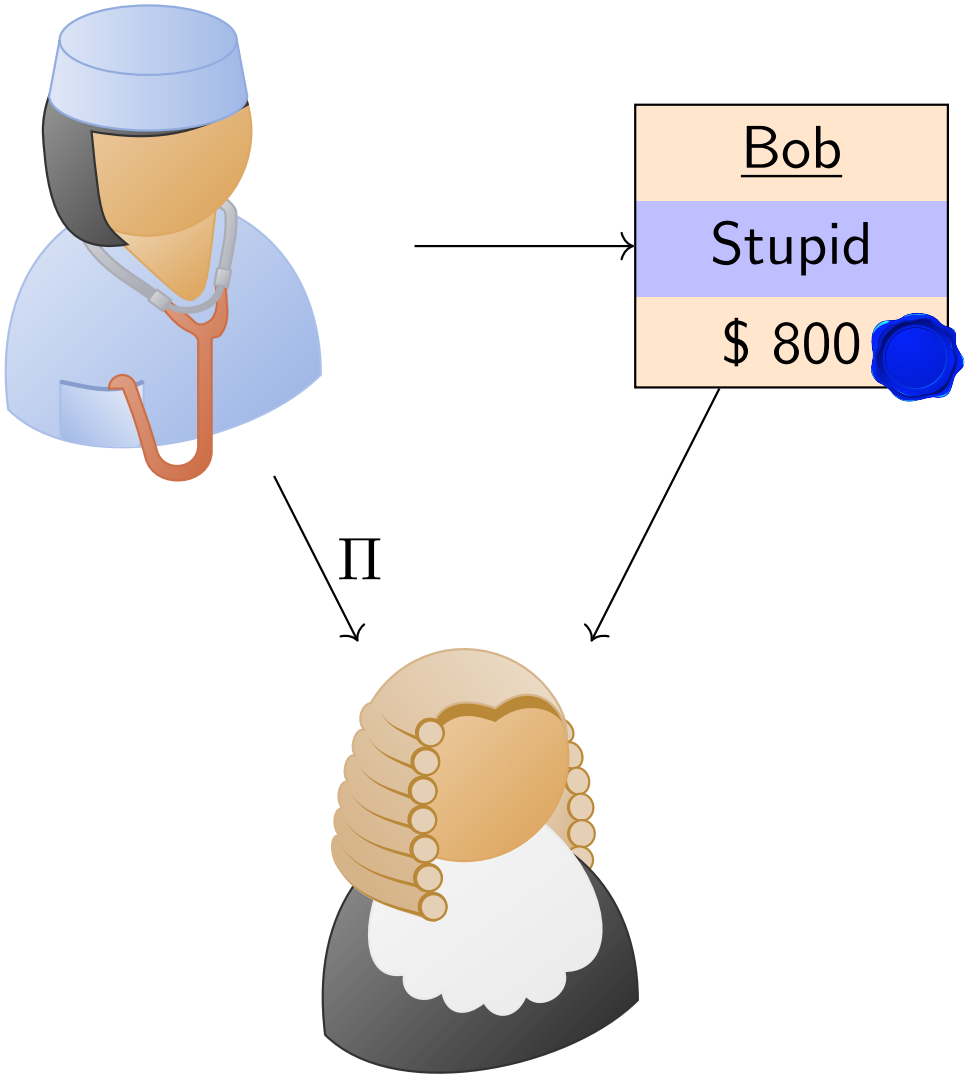
Sanitizer-Accountability [ACdMT05][BFFLPSSV09]



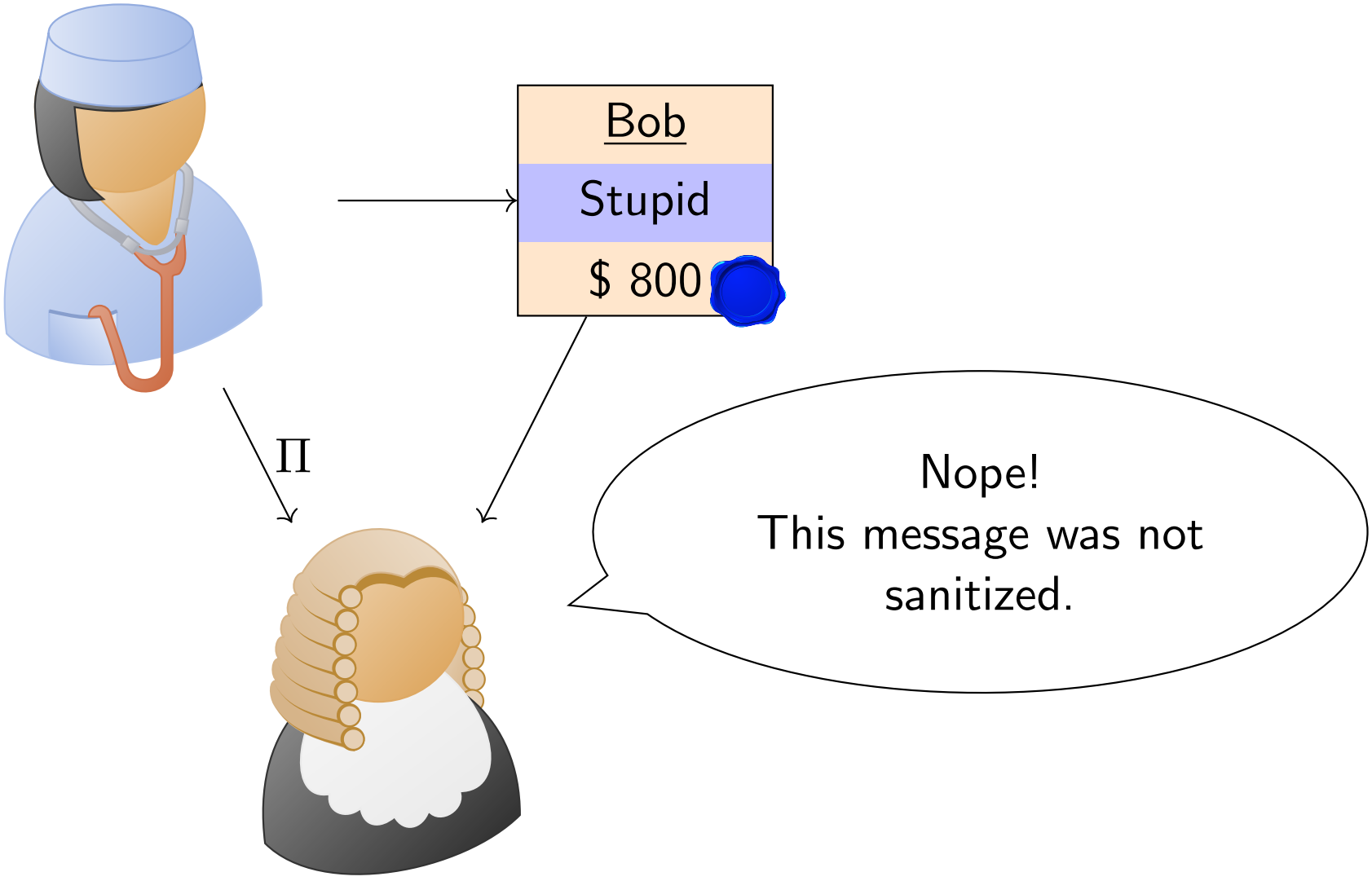
Sanitizer-Accountability [ACdMT05][BFFLPSSV09]



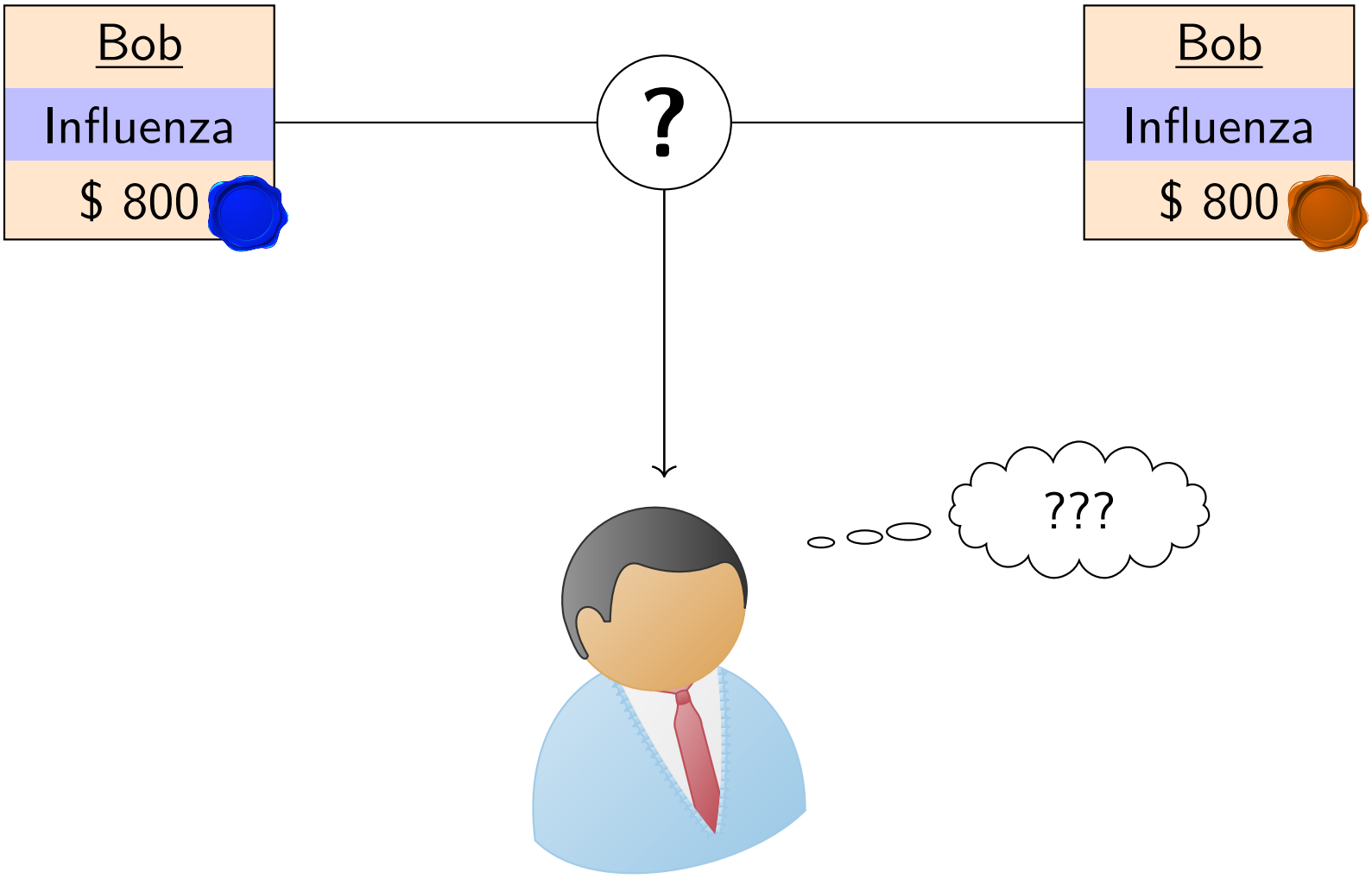
Signer-Accountability [ACdMT05][BFFLPSSV09]



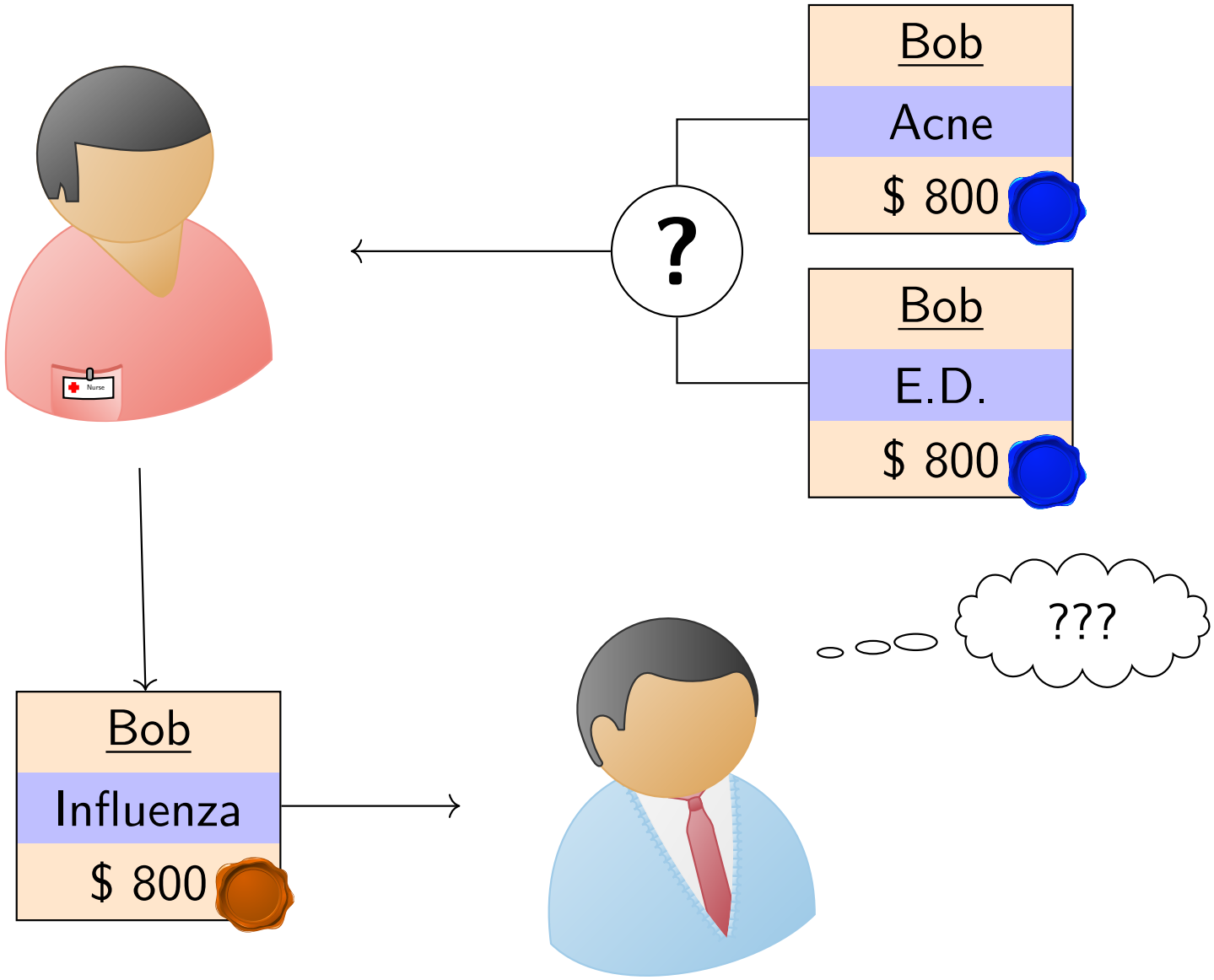
Signer-Accountability [ACdMT05][BFFLPSSV09]



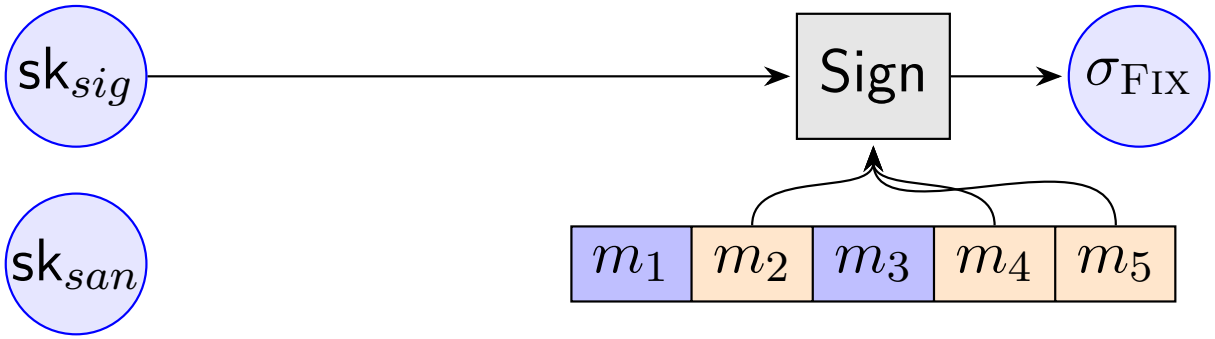
Transparency [ACdMT05][BFFLPSSV09]



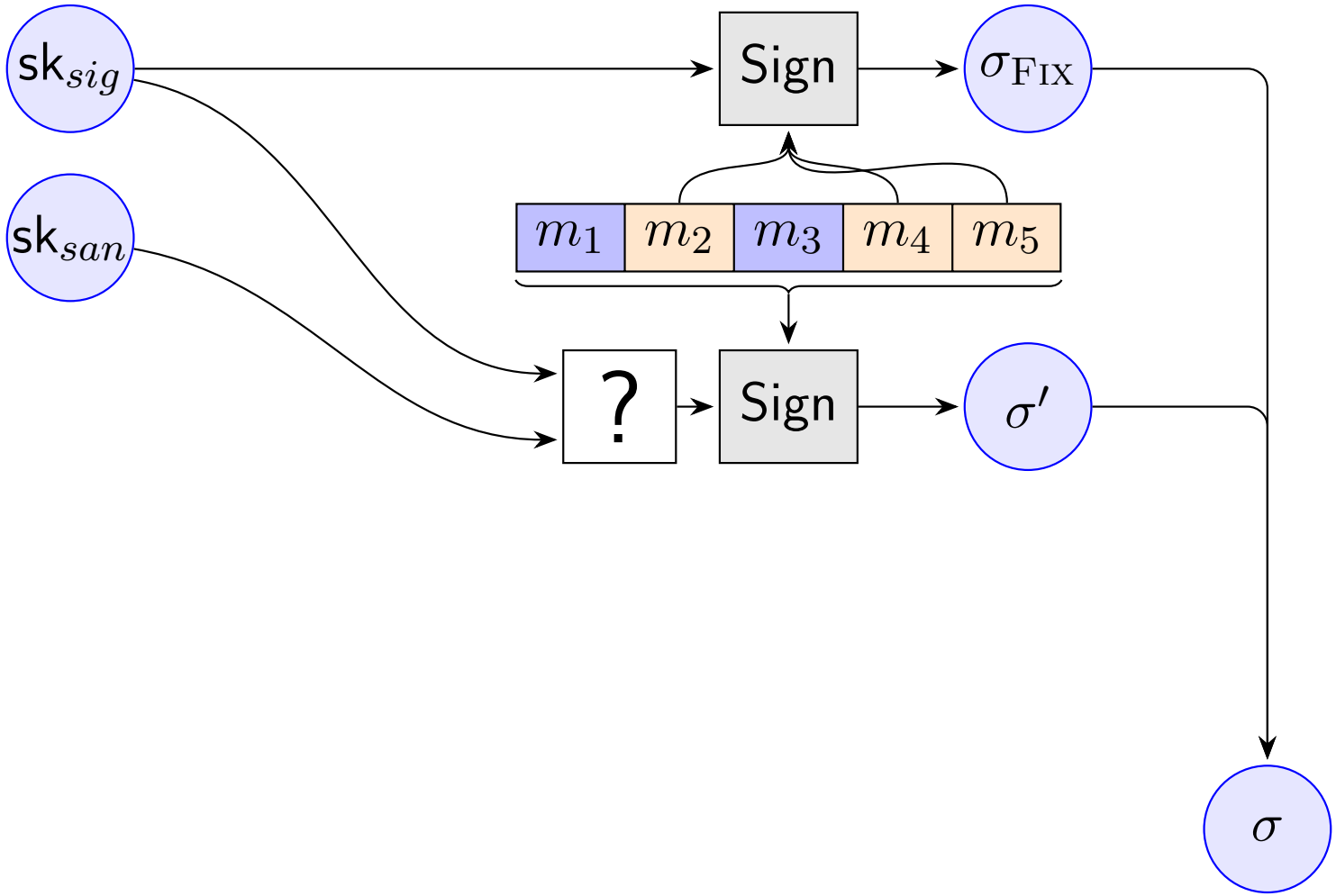
Unlinkability [BFLS10]



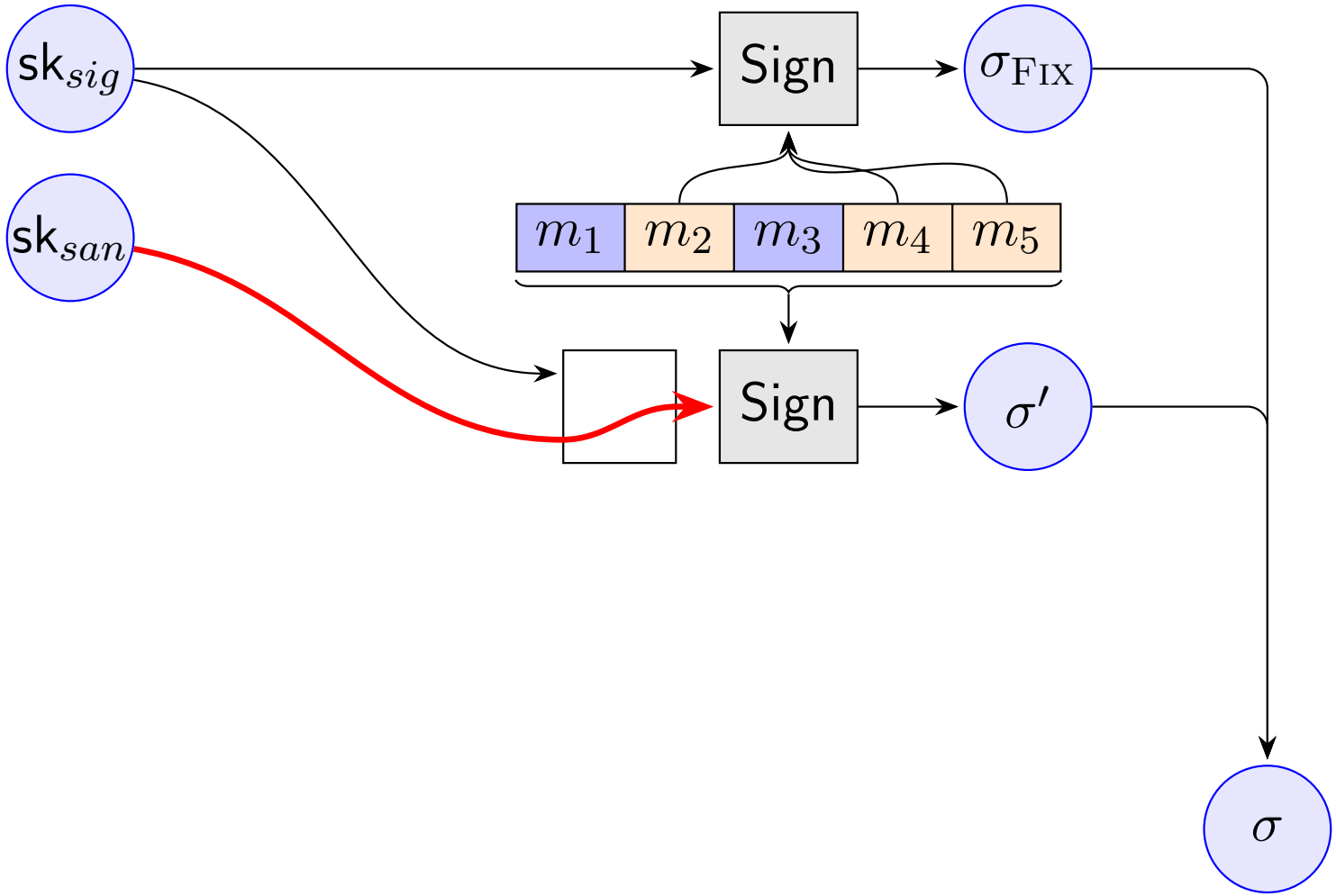
The General Idea



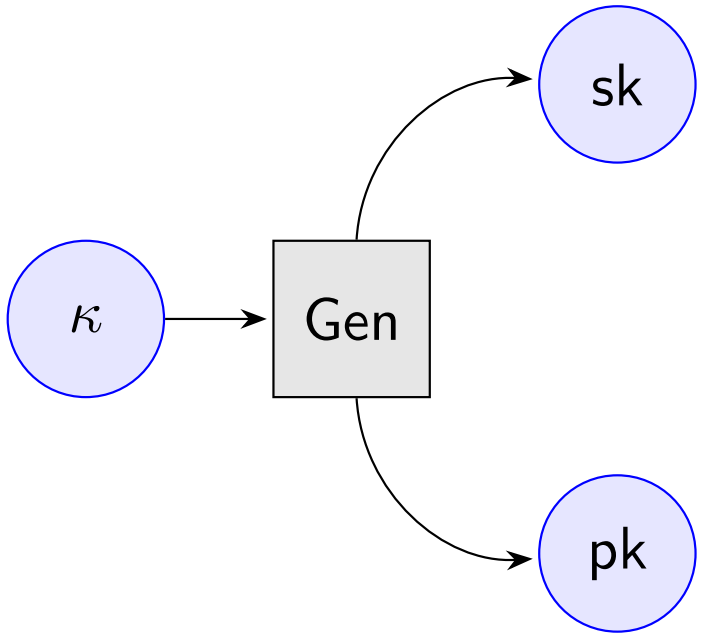
The General Idea



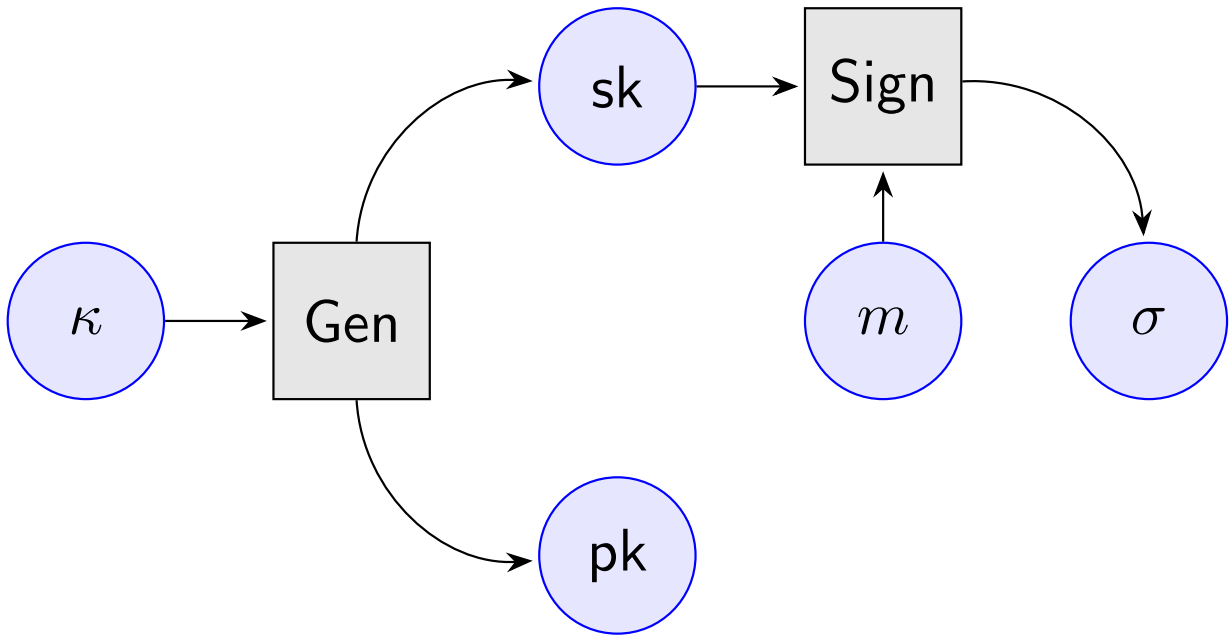
The General Idea



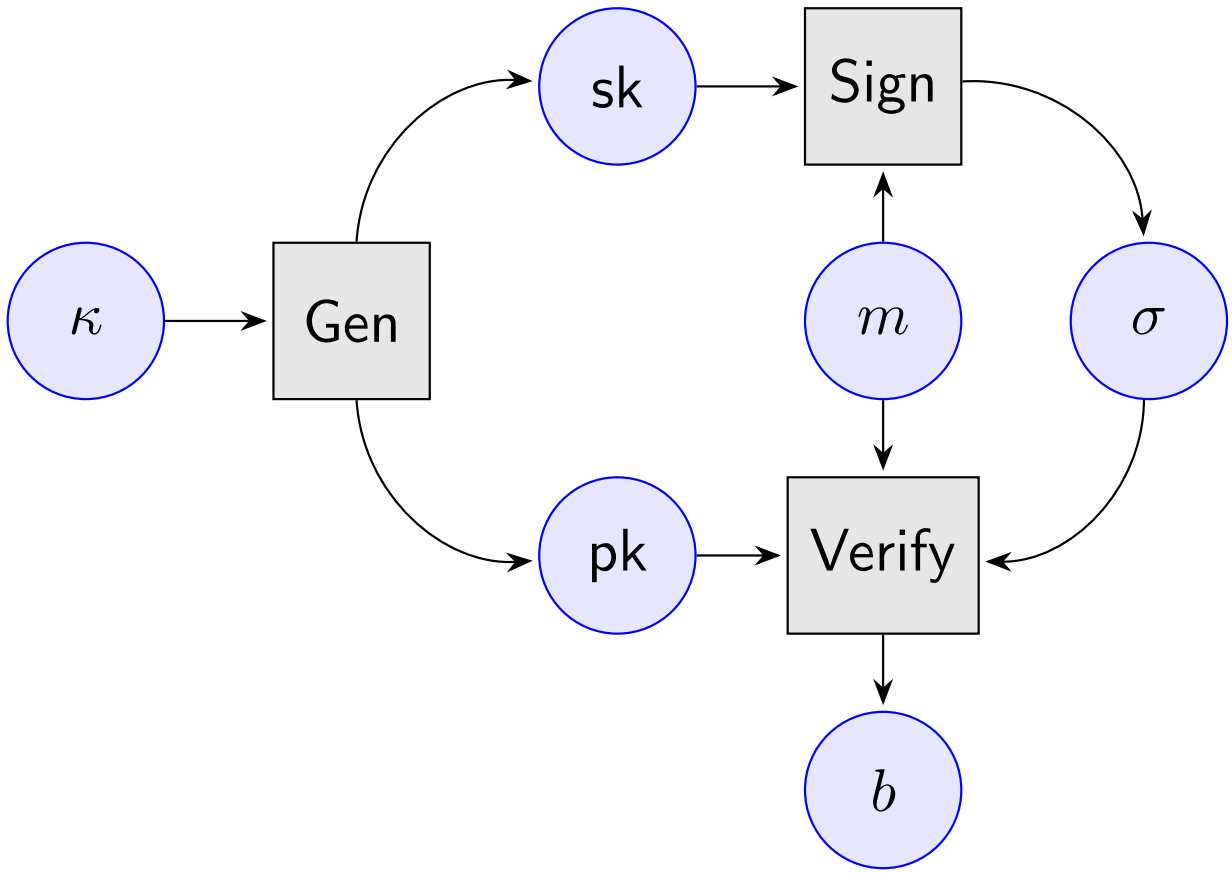
Signatures with Re-Randomizable Keys



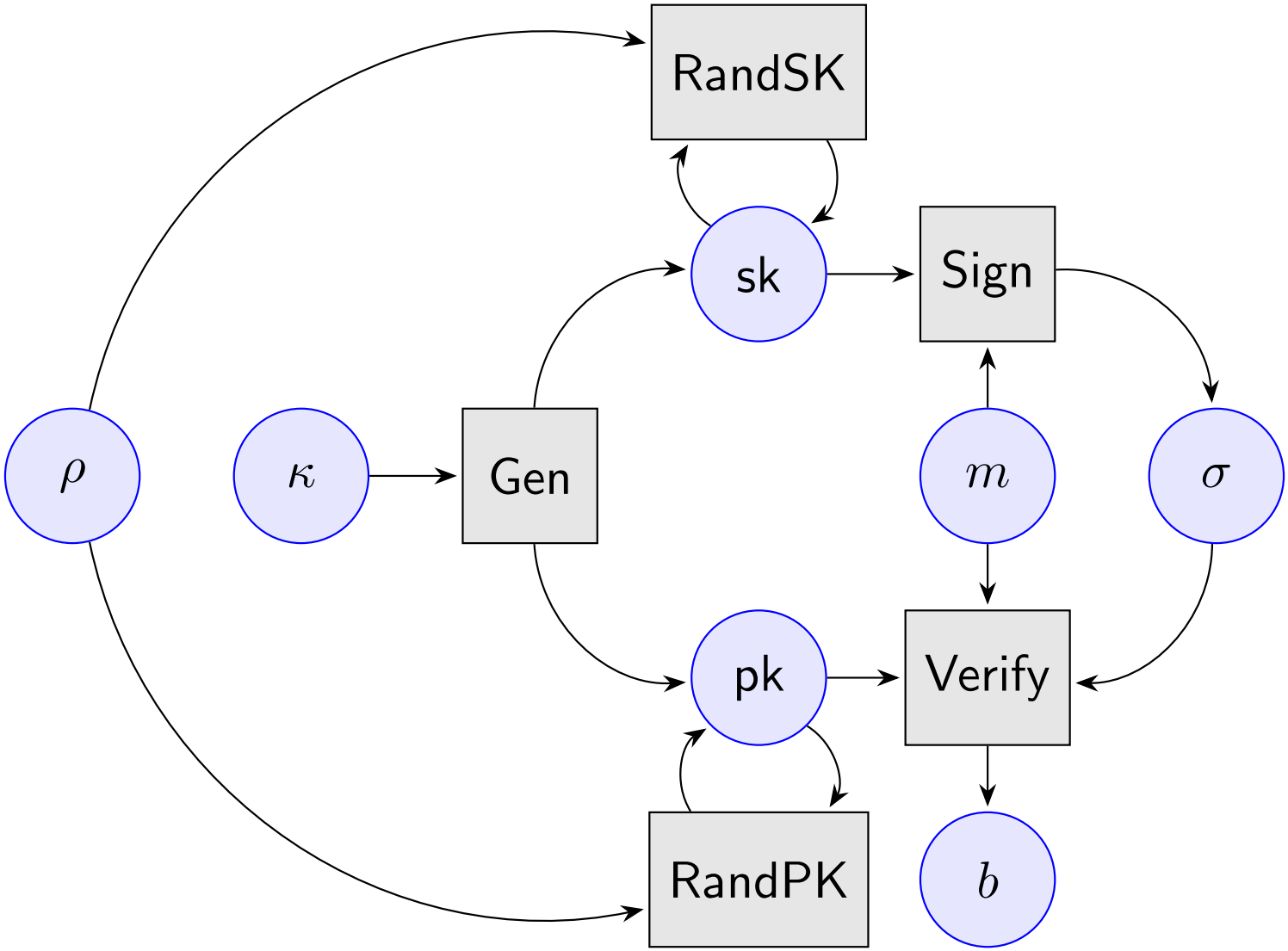
Signatures with Re-Randomizable Keys



Signatures with Re-Randomizable Keys



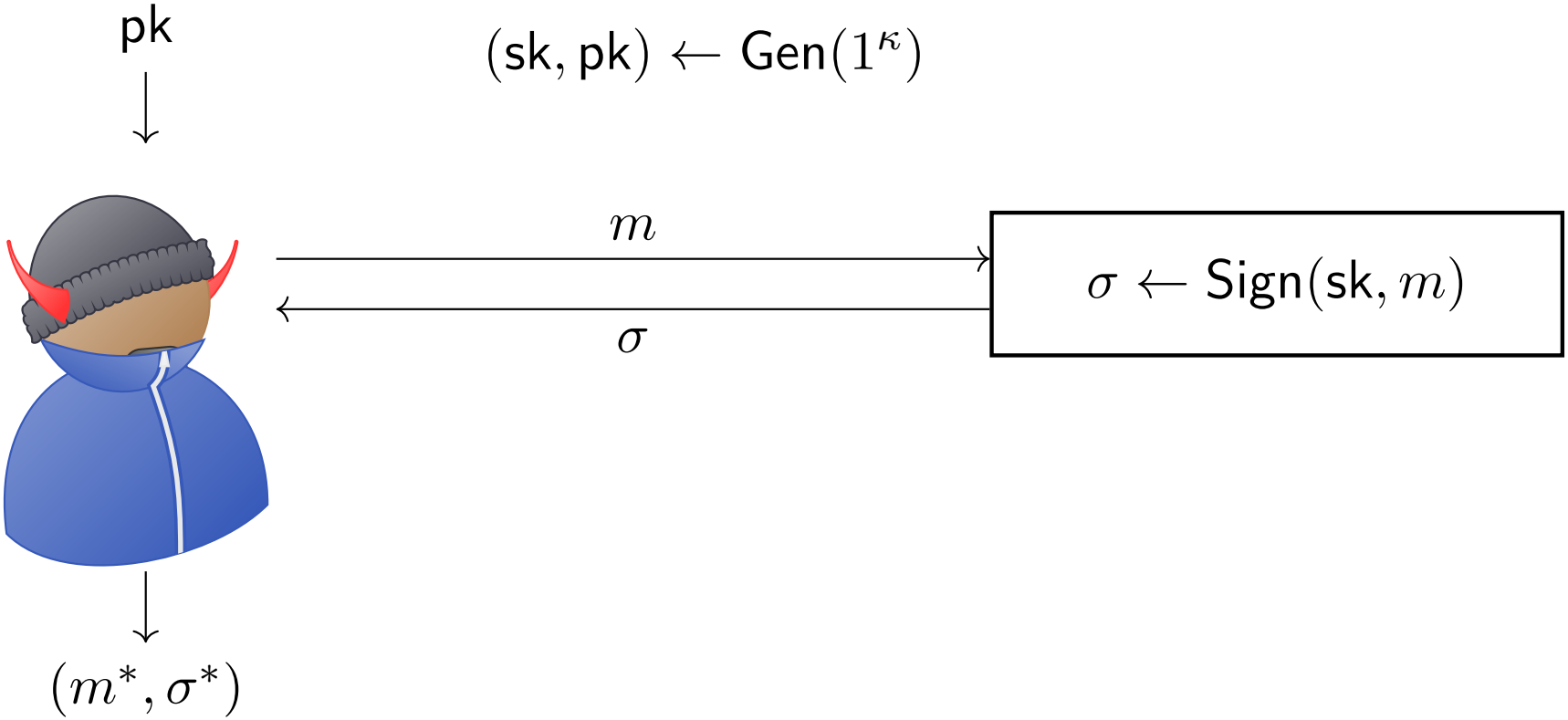
Signatures with Re-Randomizable Keys



Unforgeability under Re-Randomized Keys

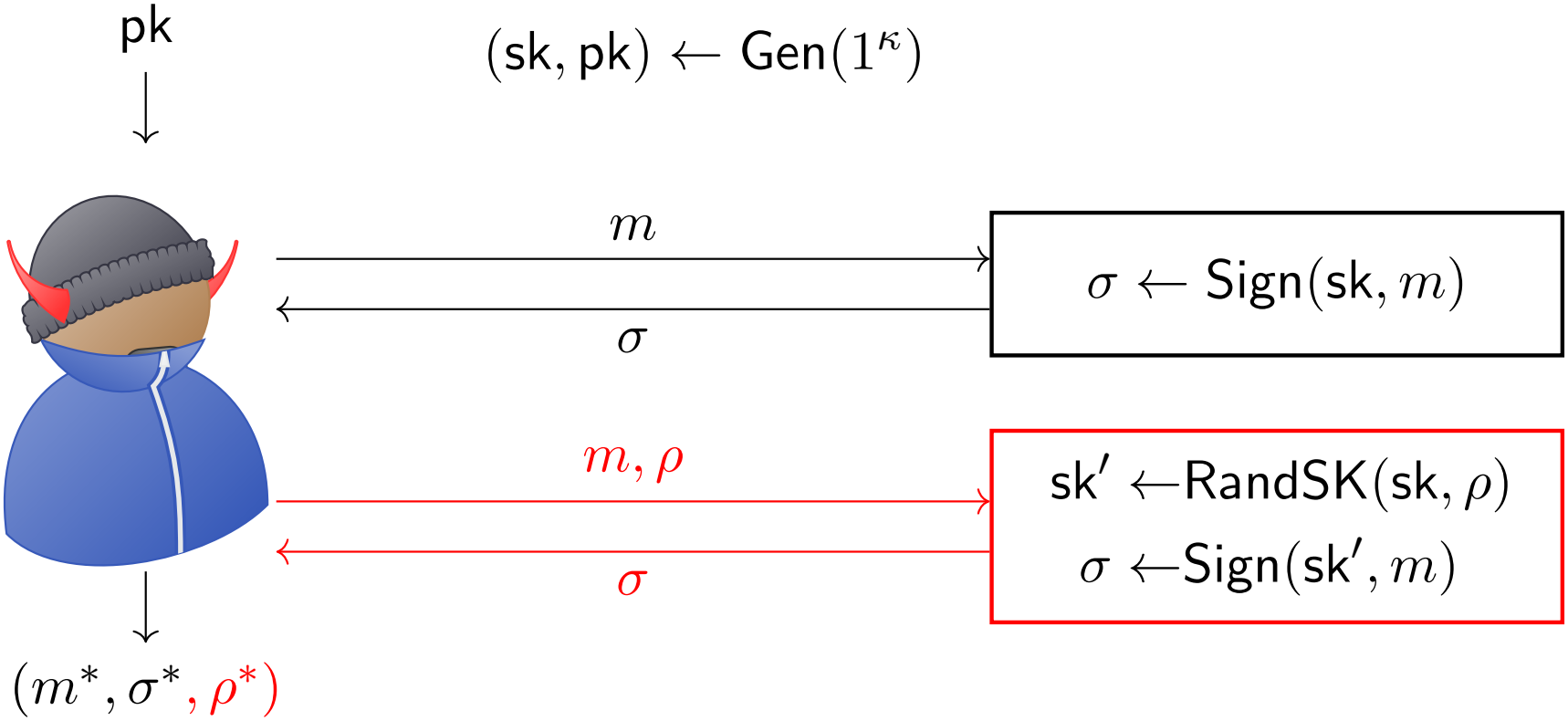
$$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^\kappa)$$

Unforgeability under Re-Randomized Keys



The attacker wins if $\mathsf{Verify}(\mathsf{pk}, m^*, \sigma^*) = 1$ and $m \neq m^*$

Unforgeability under Re-Randomized Keys



The attacker wins if $\mathsf{Verify}(\mathsf{pk}, m^*, \sigma^*) = 1$ and $m \neq m^*$

or $\mathsf{Verify}(\mathsf{pk}', m^*, \sigma^*) = 1$ and $m \neq m^*$ with $\mathsf{pk}' \leftarrow \mathsf{RandPK}(\mathsf{pk}, \rho^*)$

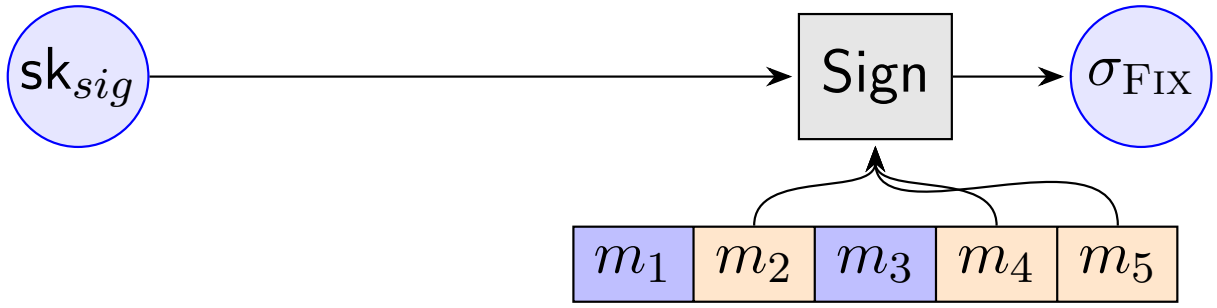
Unforgeability under Re-Randomized Keys

- Nontrivial Property
  - Does not follow from standard unforgeability.
  - Many schemes with re-randomizable keys not unforgeable under re-randomized keys
  - e.g. Boneh-Boyen, Camenisch-Lysyanskaya
- Instantiations in ROM and Standard Model
  - Schnorr
  - Hofheinz-Kiltz

Unforgeability under Re-Randomized Keys

- Nontrivial Property
  - Does not follow from standard unforgeability.
  - Many schemes with re-randomizable keys not unforgeable under re-randomized keys
  - e.g. Boneh-Boyen, Camenisch-Lysyanskaya
- Instantiations in ROM and Standard Model
  - Schnorr
  - Hofheinz-Kiltz

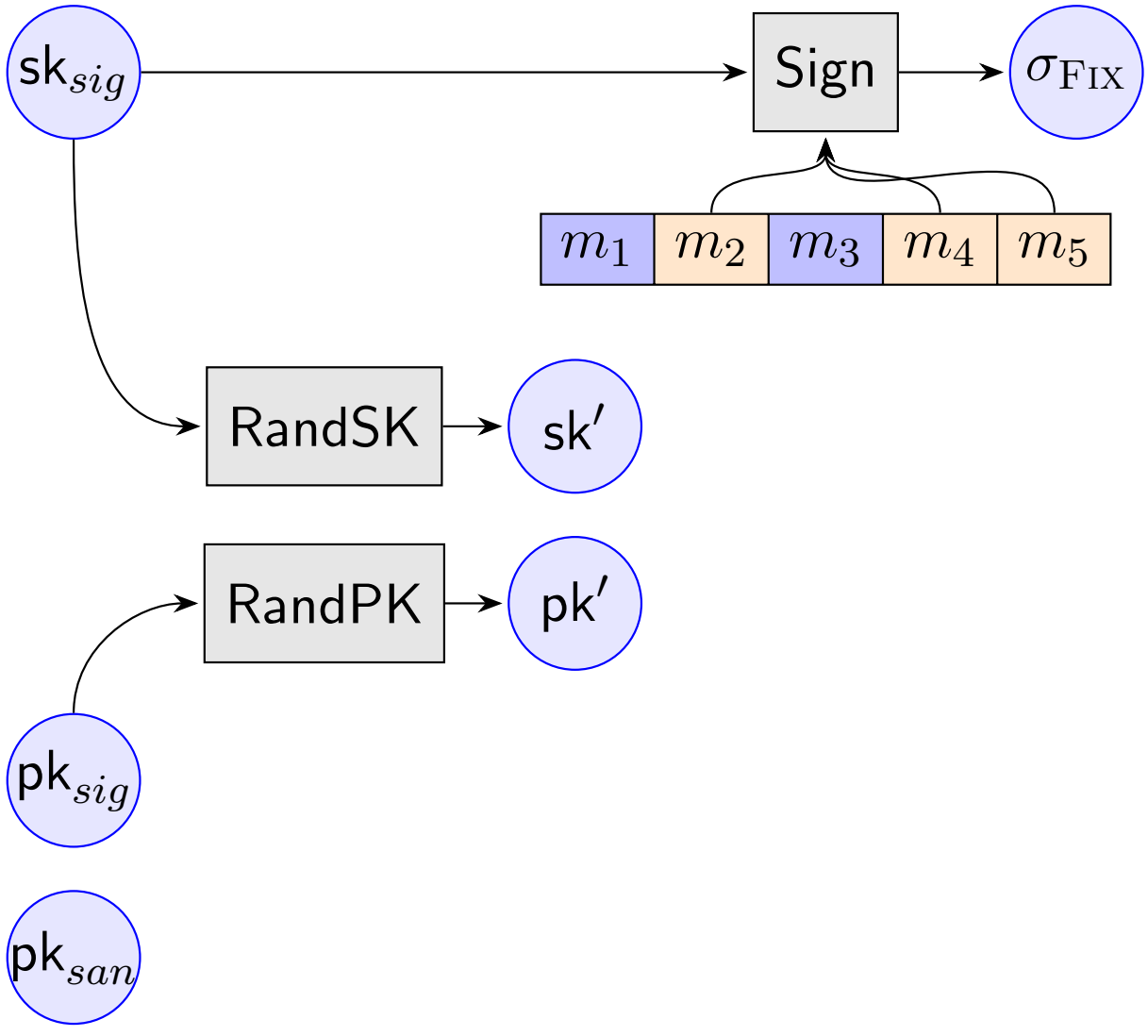
Our Construction



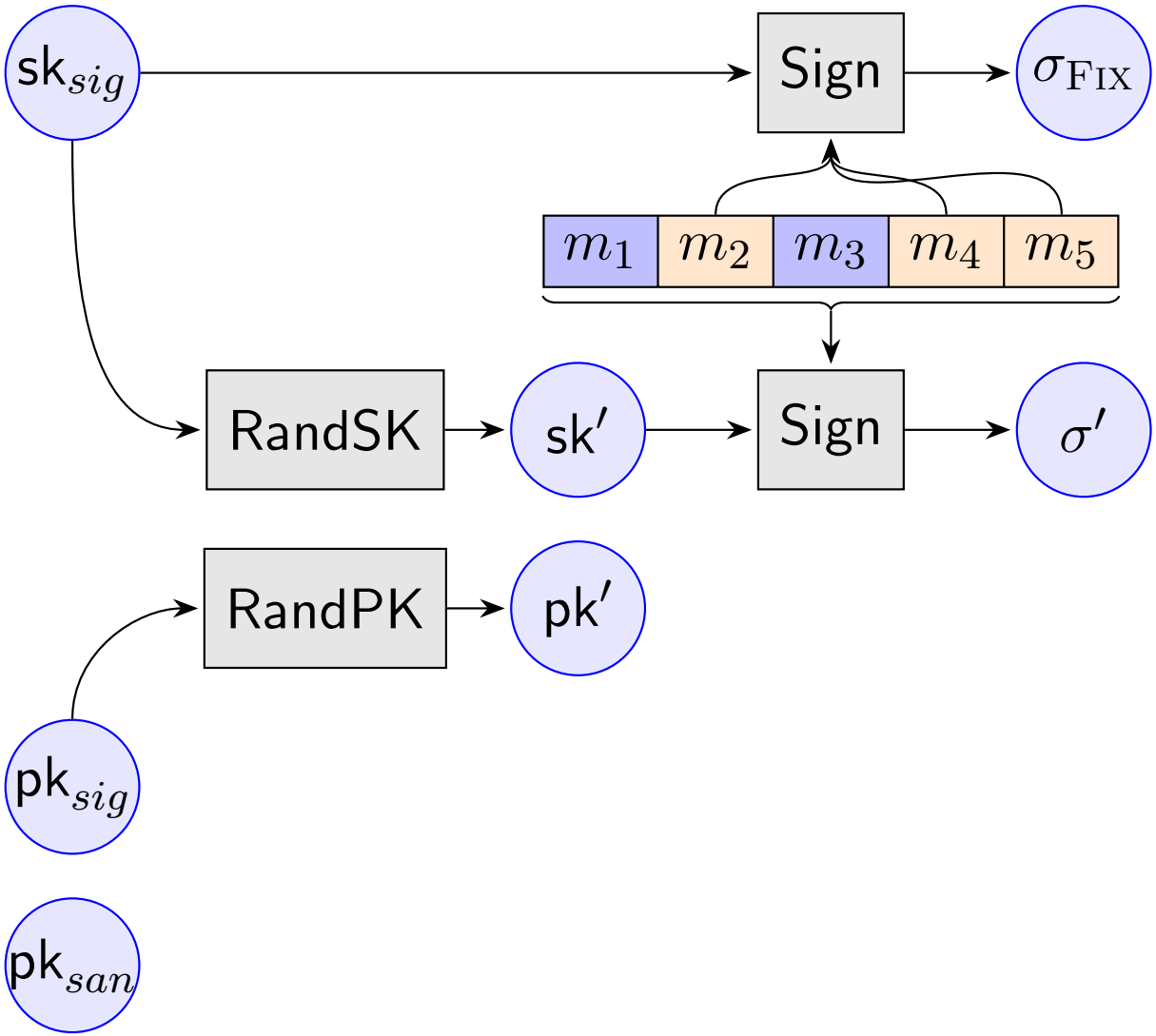
pk_{sig}

pk_{san}

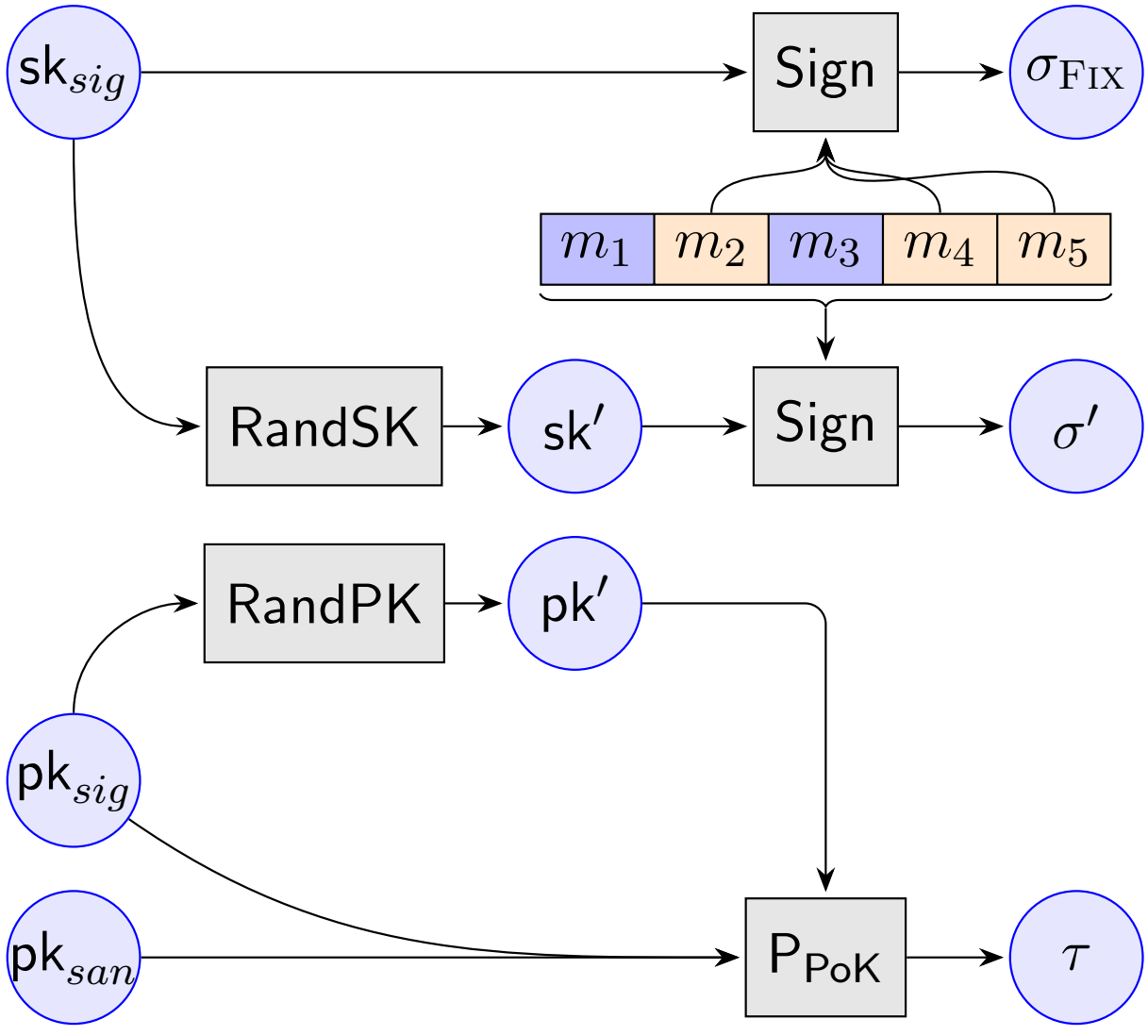
Our Construction



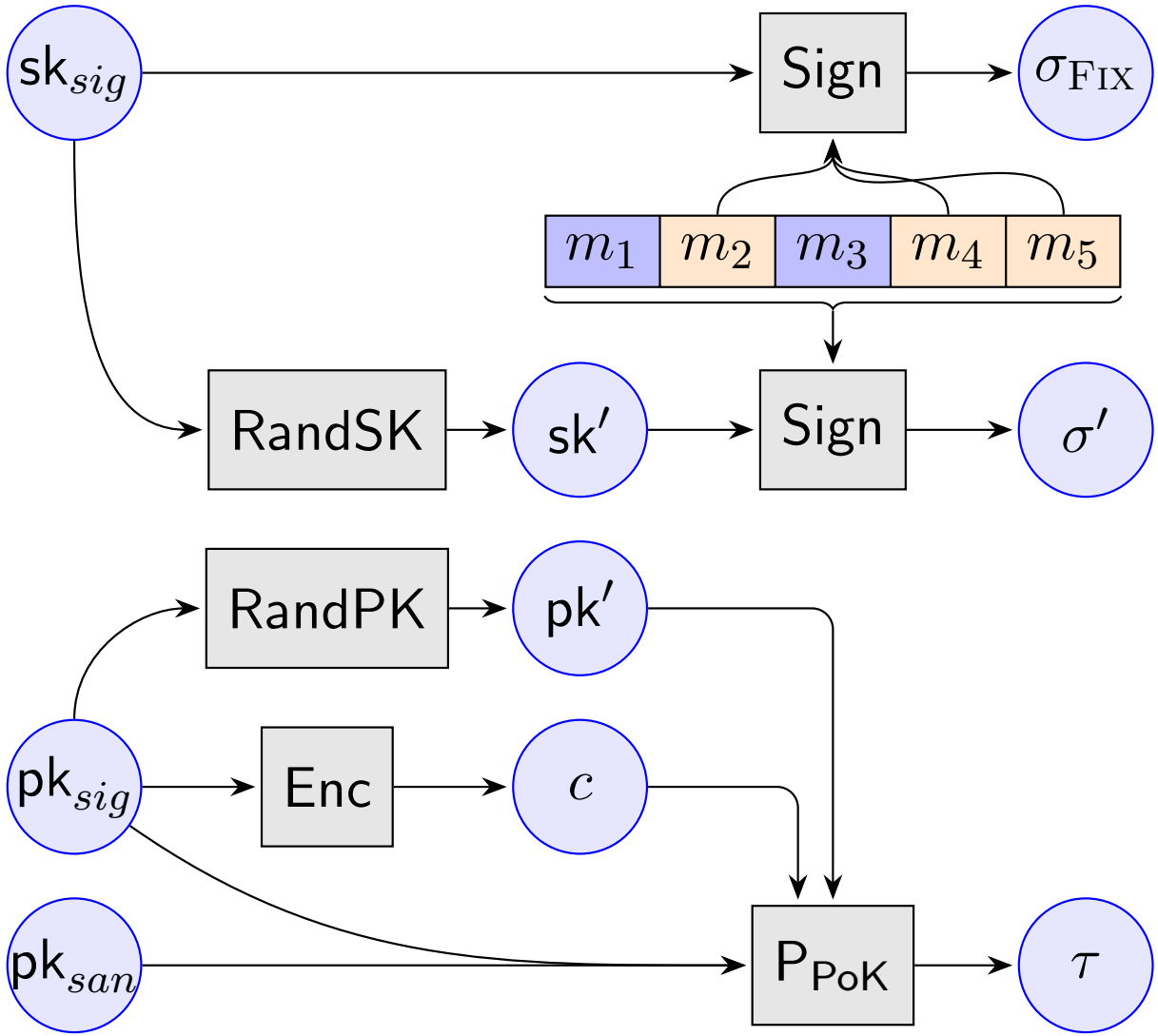
Our Construction



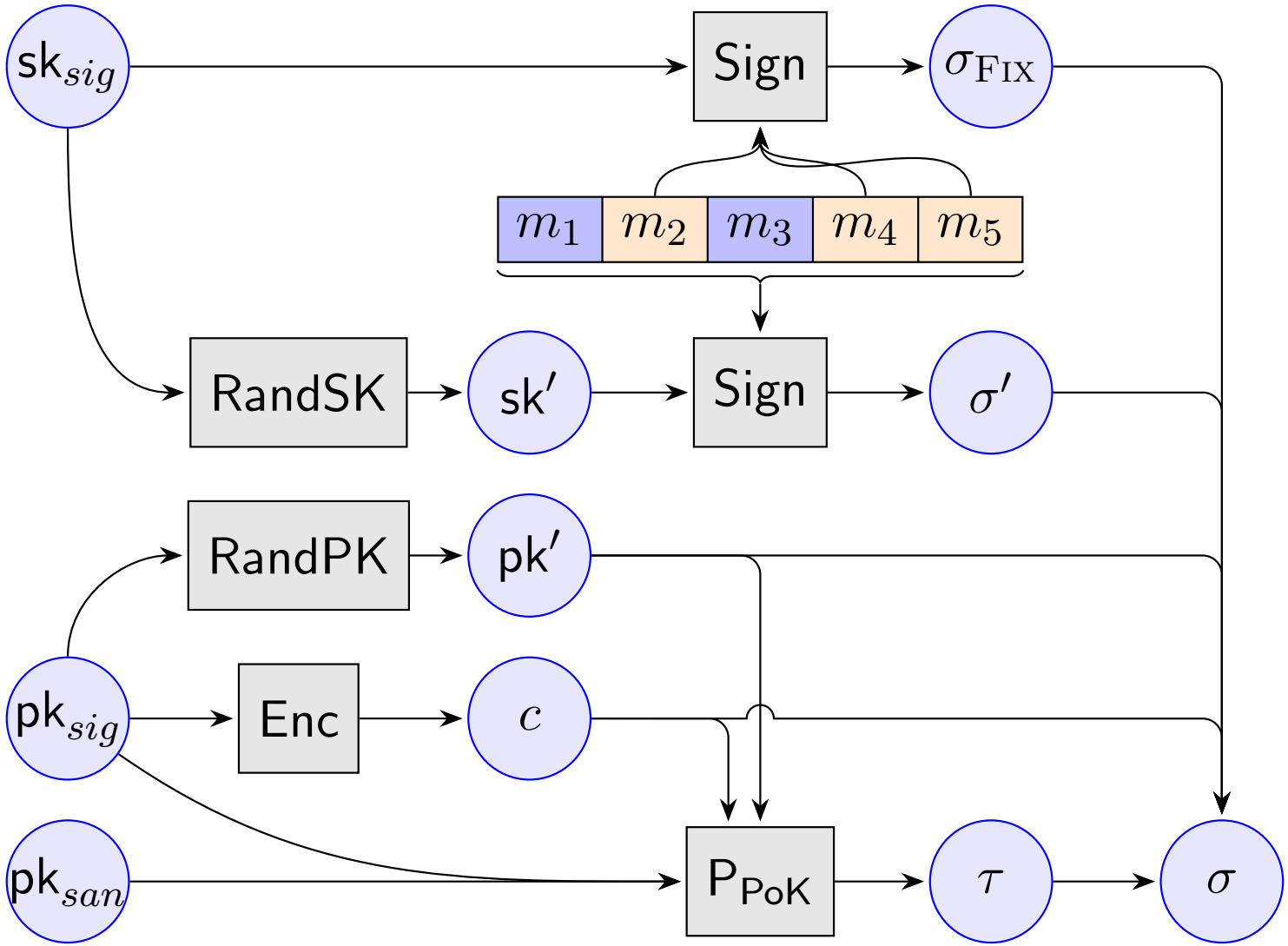
Our Construction



Our Construction

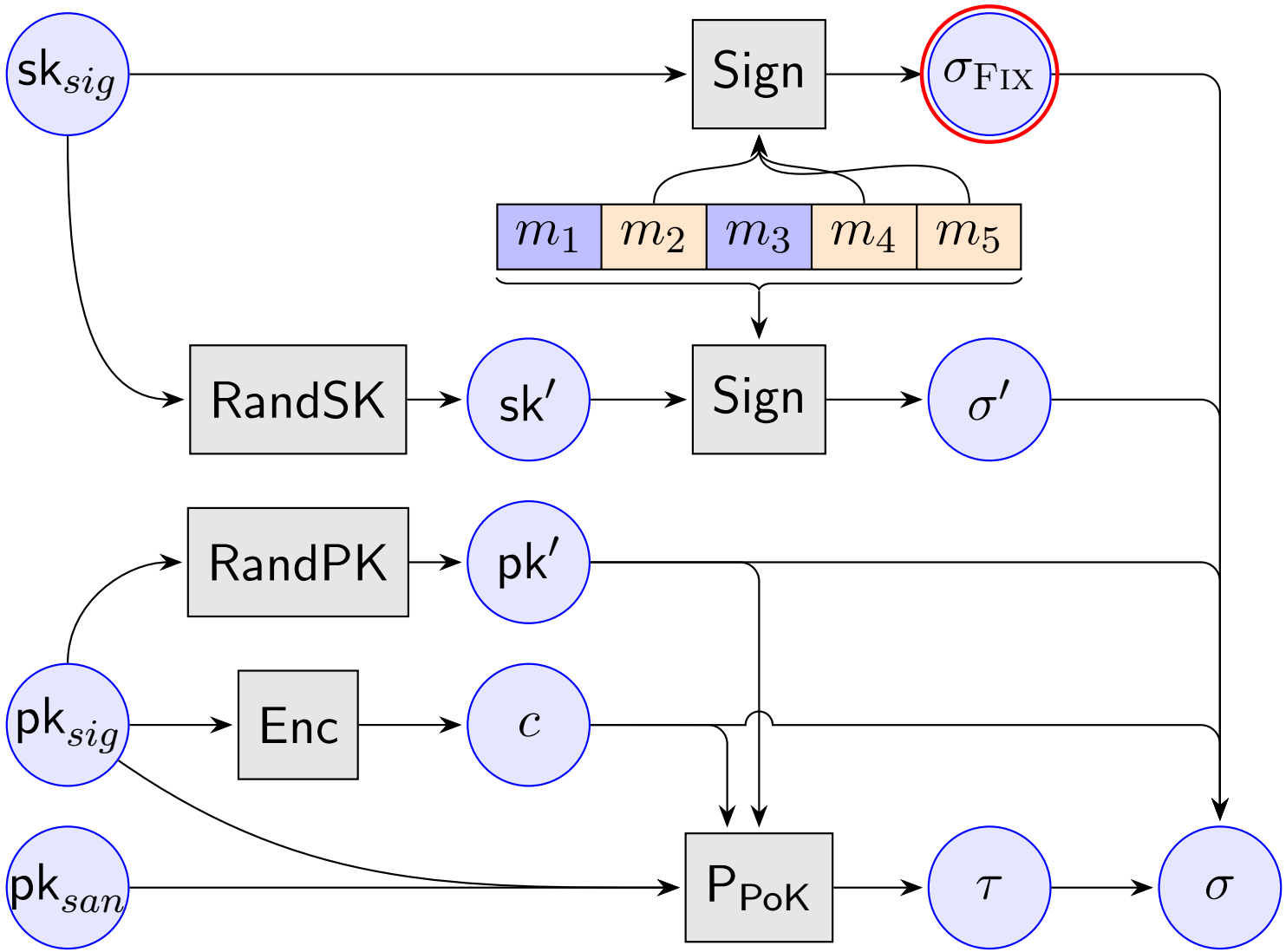


Our Construction



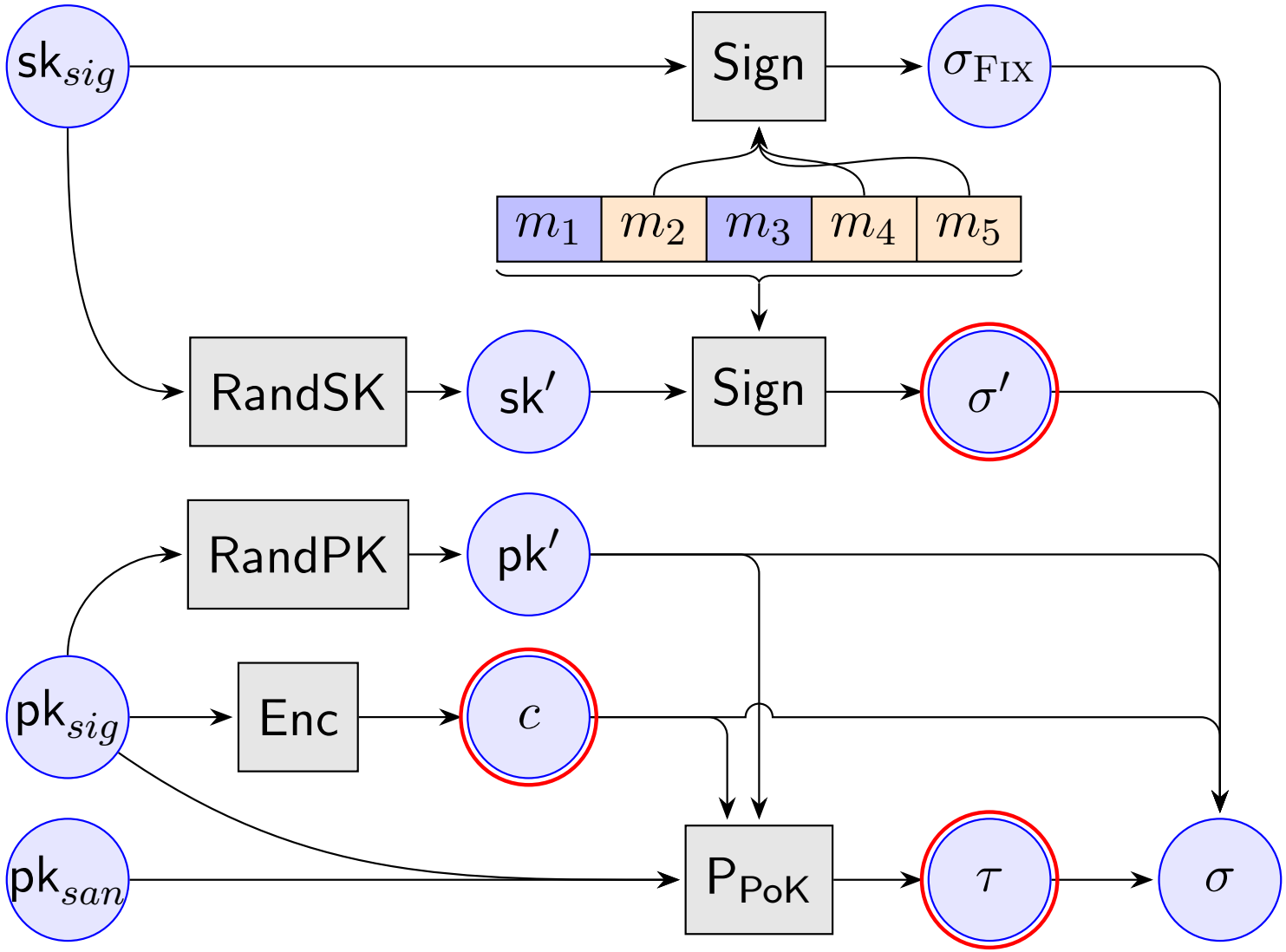
Our Construction

Immutability



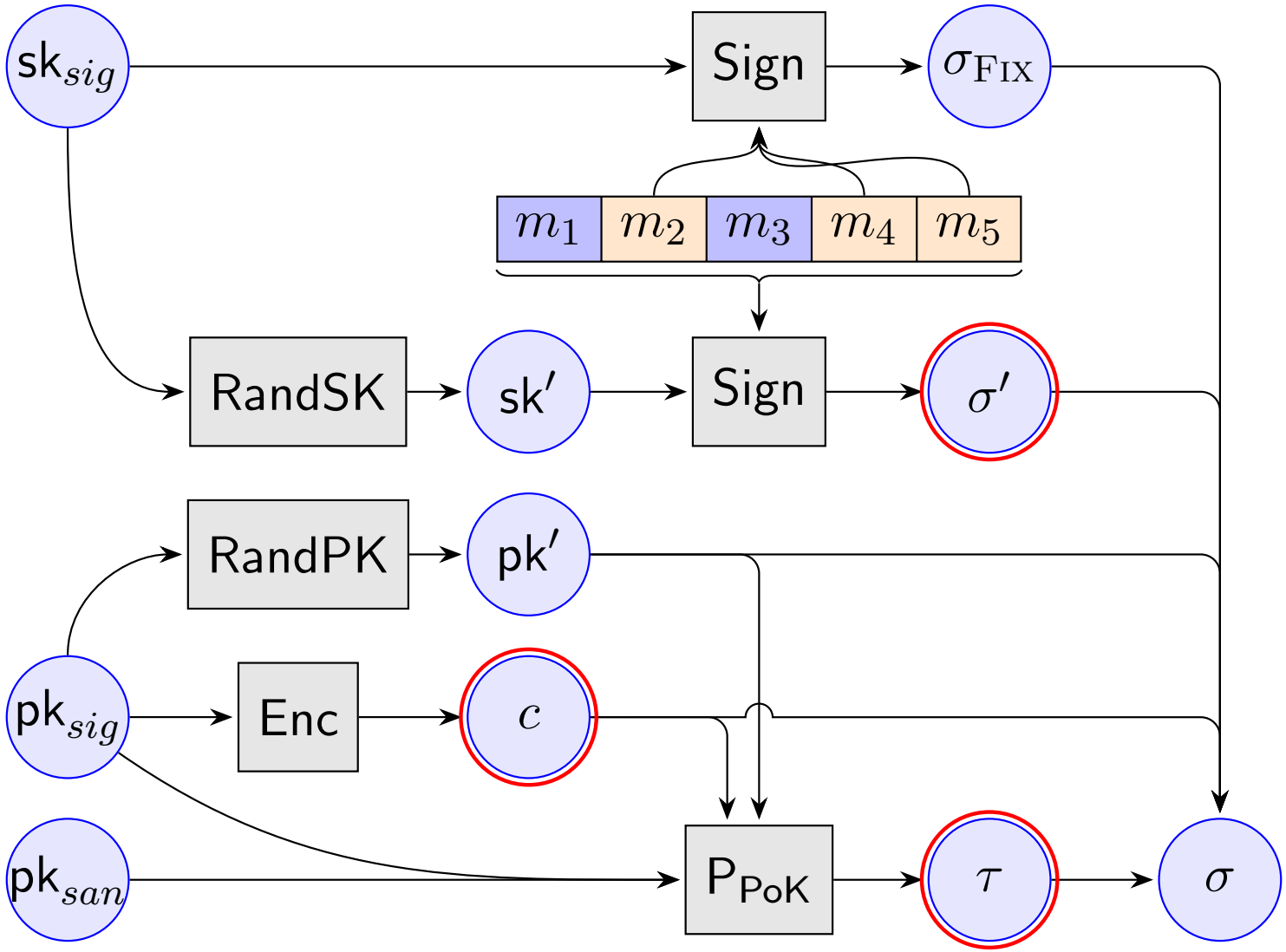
Our Construction

Sanitizer-Accountability



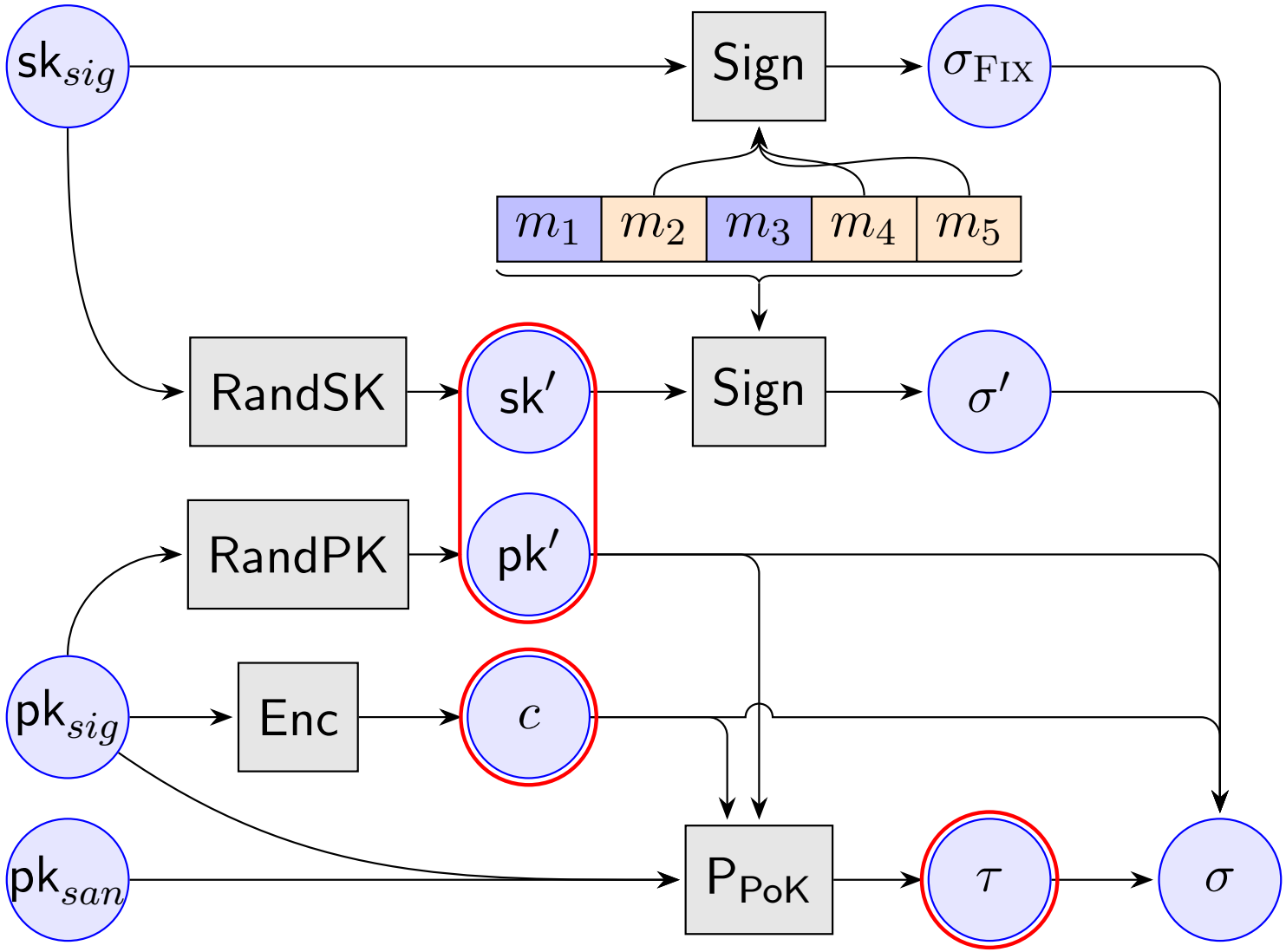
Our Construction

Signer-Accountability



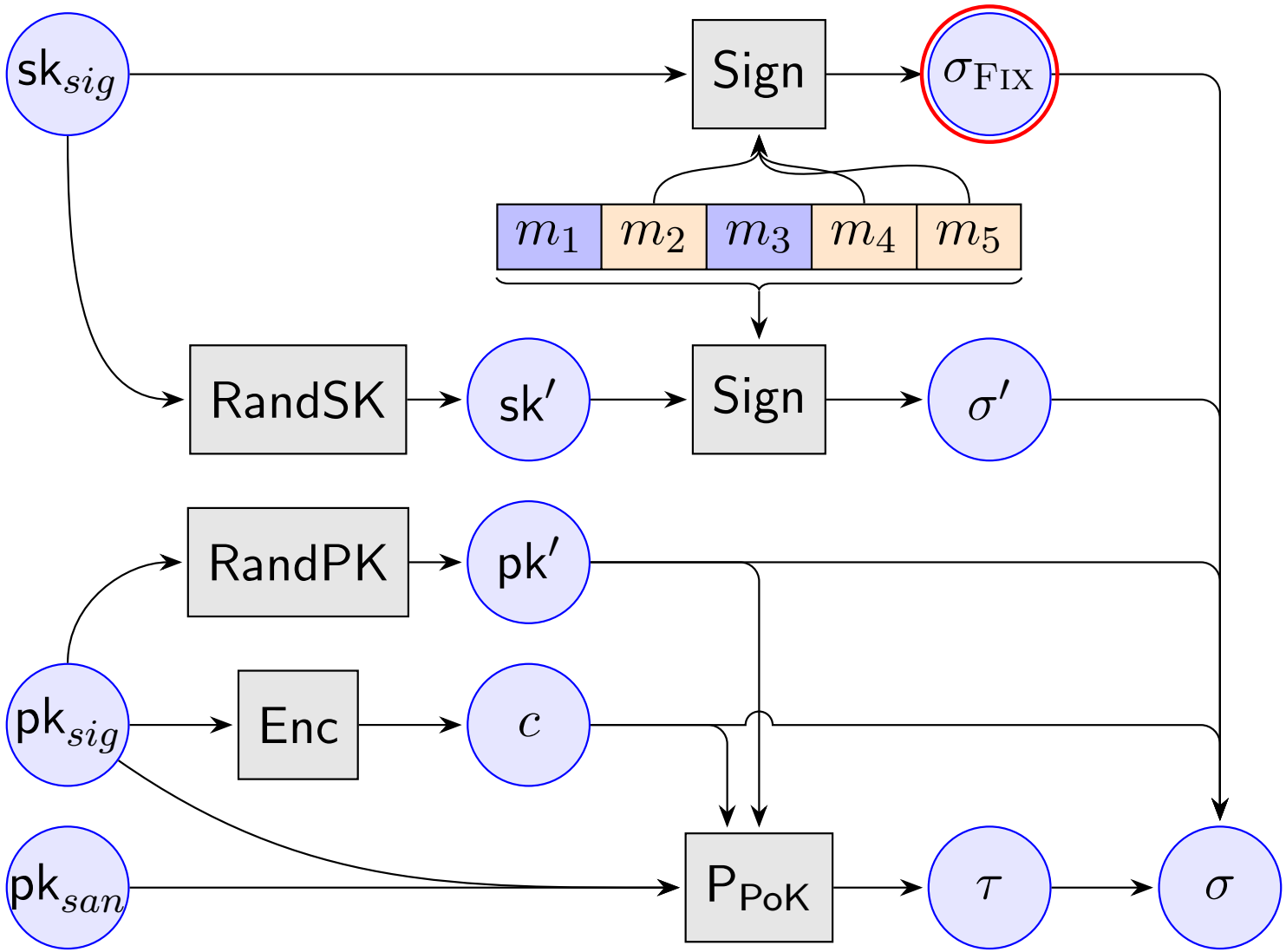
Our Construction

Transparency



Our Construction

Unlinkability



Comparison

Computation

	This Paper[1]	BFLS10 using	
		Groth07	FY04
KGen$_{sig}$	7E	1E	1E
KGen$_{san}$	1E	1E	4E
Sign	15E	194E+2P	2831E
Sanit	14E	186E+1P	2814E
Verify	17E	207E + 62P	2011E
Proof	23E	14E+1P	18E
Judge	6E	1E+2P	2E

E=modular exponentiation,P= pairing evaluation

[1] Instantiated with Schnorr signatures, Cramer-Shoup Encryption, and Fiat-Shamir transformed Σ-protocols.

Comparison

Computation

	This Paper[1]	BFLS10 using	
		Groth07	FY04
KGen$_{sig}$	7E	1E	1E
KGen$_{san}$	1E	1E	4E
Sign	15E	194E+2P	2831E
Sanit	14E	186E+1P	2814E
Verify	17E	207E + 62P	2011E
Proof	23E	14E+1P	18E
Judge	6E	1E+2P	2E

E=modular exponentiation,P= pairing evaluation

[1] Instantiated with Schnorr signatures, Cramer-Shoup Encryption, and Fiat-Shamir transformed Σ-protocols.

Comparison

Storage

	This Paper[2]	BFLS10 using	
		Groth07	FY04
pk_{sig}	7	1	1
sk_{sig}	14	1	1
pk_{san}	1	1	5
sk_{san}	1	1	1
σ	14	69	1620
π	4	1	3

measured in group elements

[2] Instantiated with Schnorr signatures, Cramer-Shoup Encryption, and Fiat-Shamir transformed Σ-protocols.

Comparison

Storage

	This Paper[2]	BFLS10 using Groth07	BFLS10 using FY04
pk_{sig}	7	1	1
sk_{sig}	14	1	1
pk_{san}	1	1	5
sk_{san}	1	1	1
σ	14	69	1620
π	4	1	3

measured in group elements

[2] Instantiated with Schnorr signatures, Cramer-Shoup Encryption, and Fiat-Shamir transformed Σ-protocols.

Conclusion

We construct an **unlinkable sanitizable signature scheme** that can be instantiated at least **one order of magnitude more efficiently** than previously known schemes.

Thank You!

Nils Fleischhacker
fleischhacker@cs.uni-saarland.de

Full Version: ia.cr/2015/395