RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: IDY-W02

Zero-knowledge proofs (ZKP): Privacy Preserving Authentication

Karla Clarke
Manager
KPMG

Rajan Behal
Managing Director
KPMG

RSAConference2019

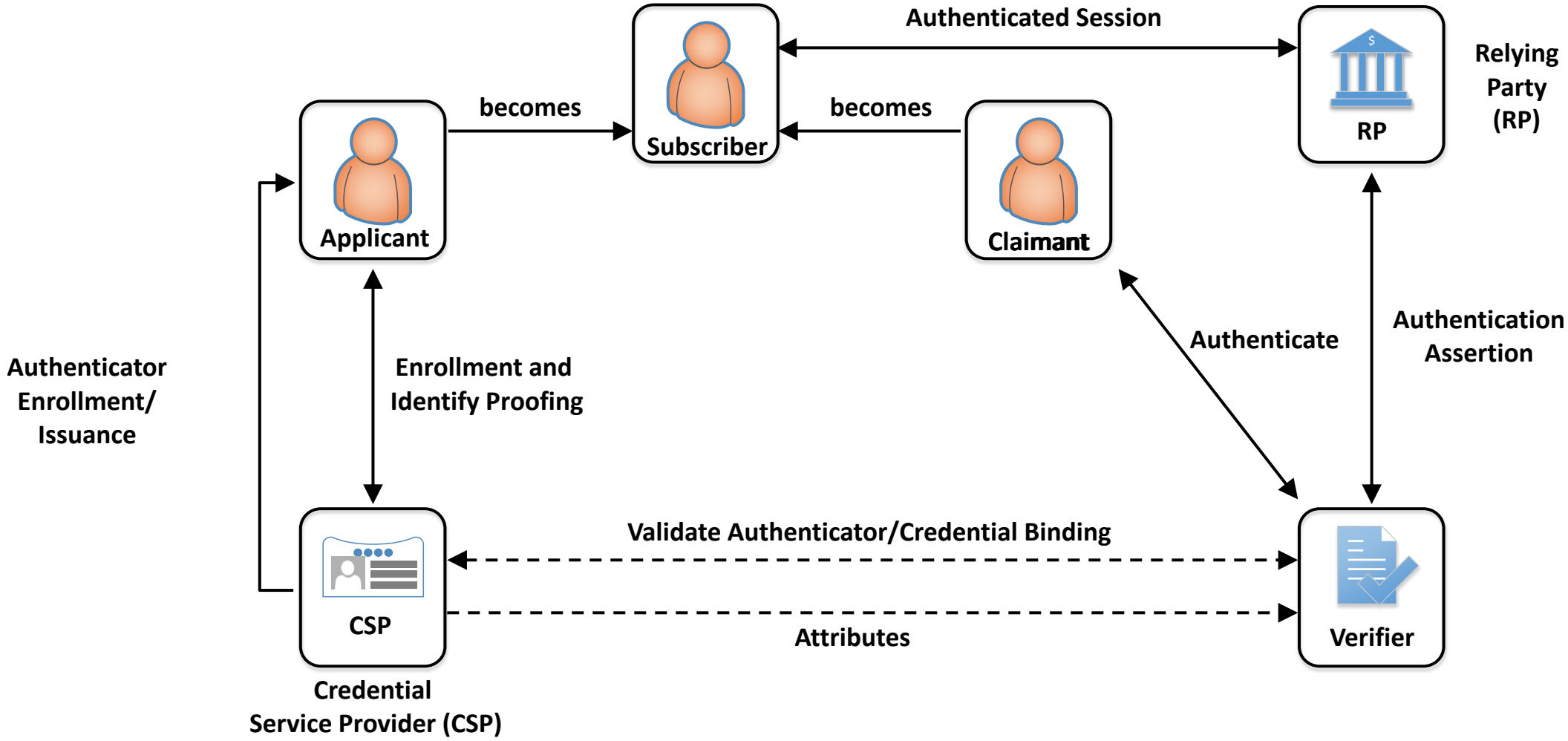
Privacy Preserving Digital Identity

Balancing Personal Privacy with Institutional Integrity

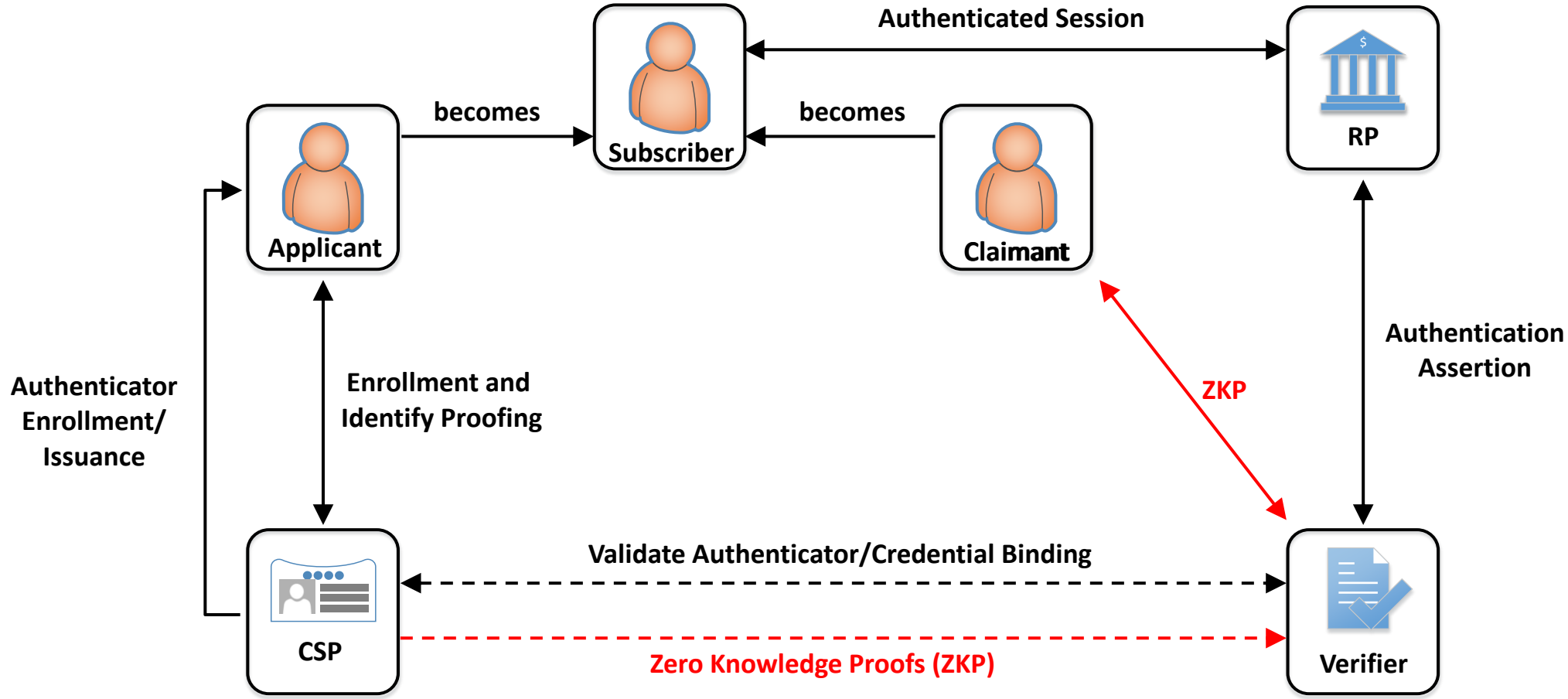
Risks

- Loss of privacy
- Data breaches
- Identity theft
- Surveillance

Digital Identity Model



Privacy Preserving Digital Identity Model



RSAConference2019

Zero-Knowledge Proofs

Definition

What is Zero-Knowledge Proof?

- Zero-knowledge proofs are an elegant technique to limit the amount of information transferred from a prover ‘A’ to a verifier ‘B’ in a cryptographic protocol.
  - The idea is to replace "knowledge" by "knowledge about knowledge"

- The name "zero-knowledge proofs" is slightly misleading, since the prover A reveals one bit of knowledge to the verifier B (is input I a member of language L?).
  - *L = interactive proof for the language L*

Zero-Knowledge Proof Properties

ZKP enables:

Completeness

- If statement is true, verifier will be convinced by prover.

Soundness

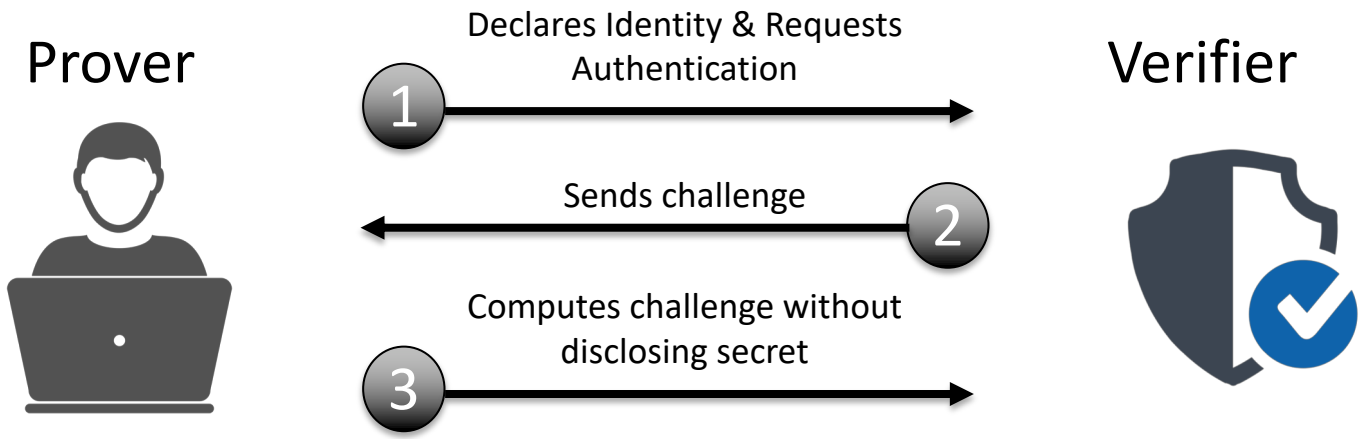
- If statement is false, a cheating prover cannot convince verifier it is true.

Zero-Knowledge

- Verifier learns nothing beyond the statement's validity.

ZKP Usage with Authentication

- Performing authentication without exchanging passwords
- Enterprises can protect proprietary information by sharing proofs about the data without sharing the actual data



RSAConference2019

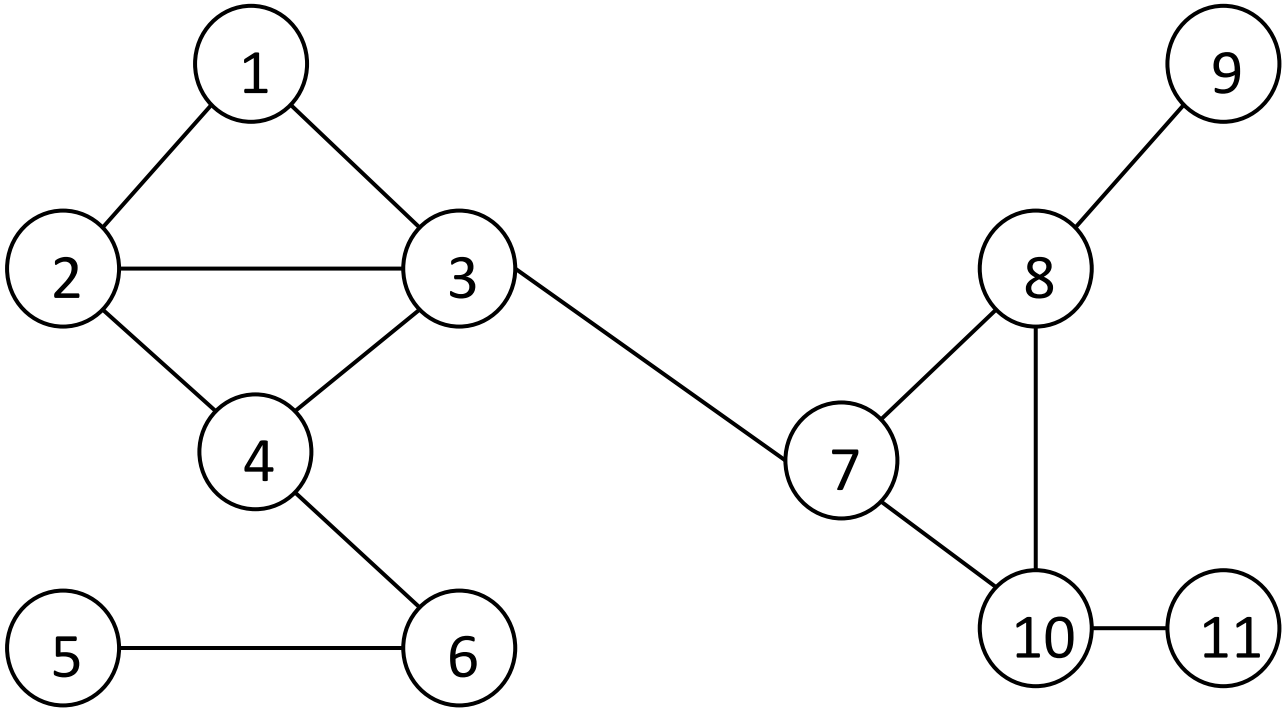
Zero-Knowledge Proof Illustration

Quick Activity!

Zero-Knowledge Proof Illustration

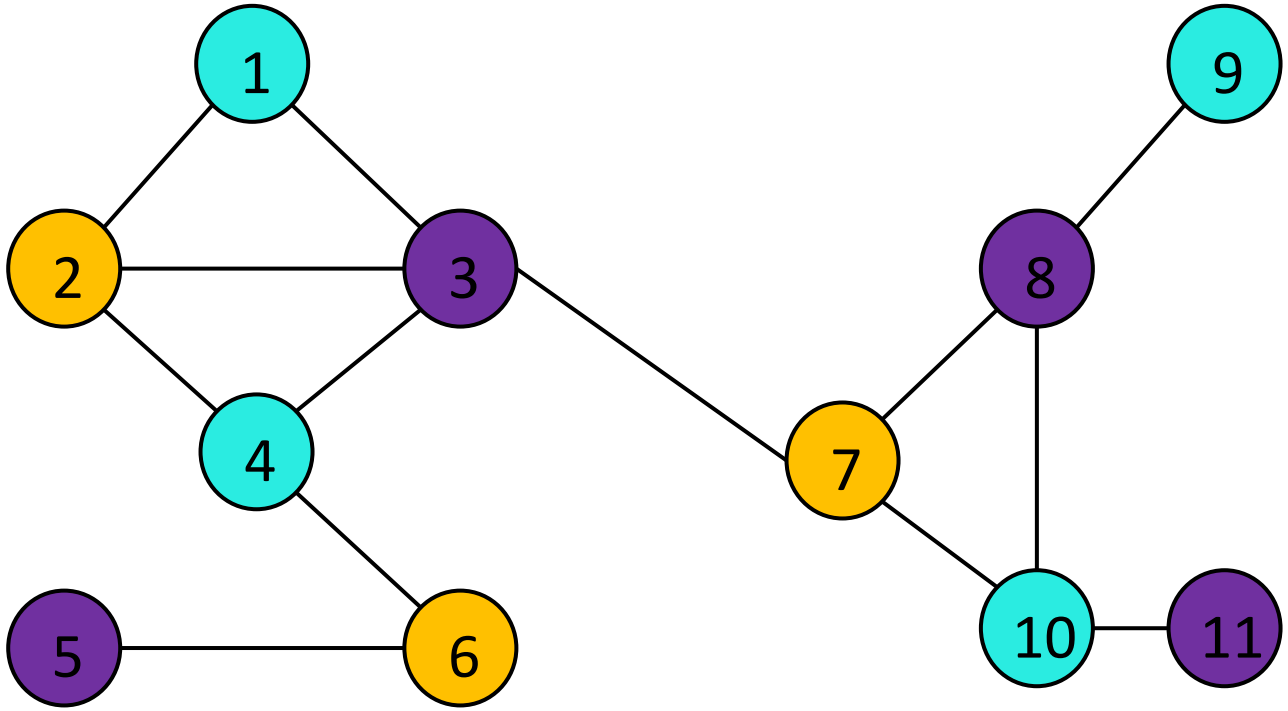
The Challenge:

Mathew Green



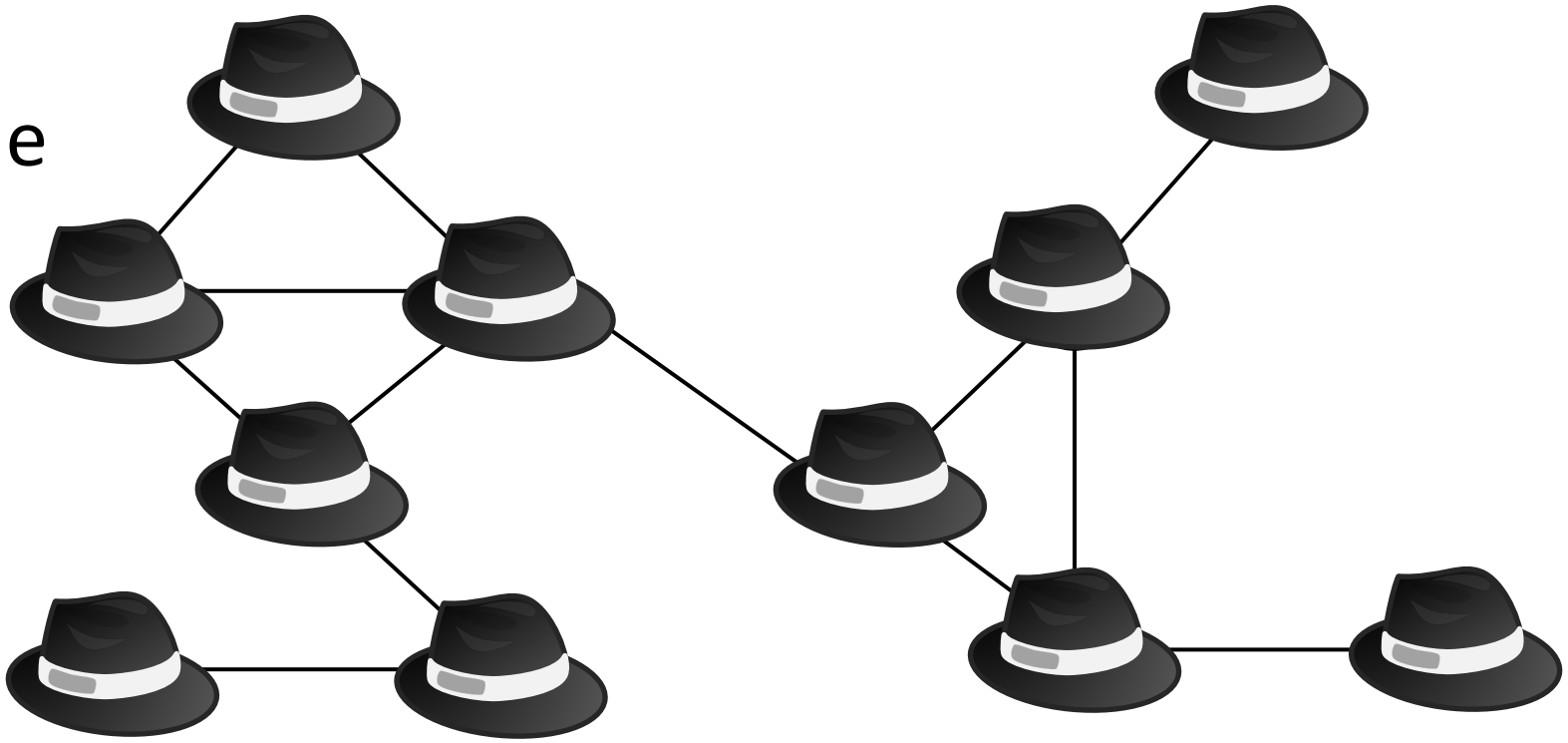
Zero-Knowledge Proof Illustration

The Solution:



Zero-Knowledge Proof Illustration

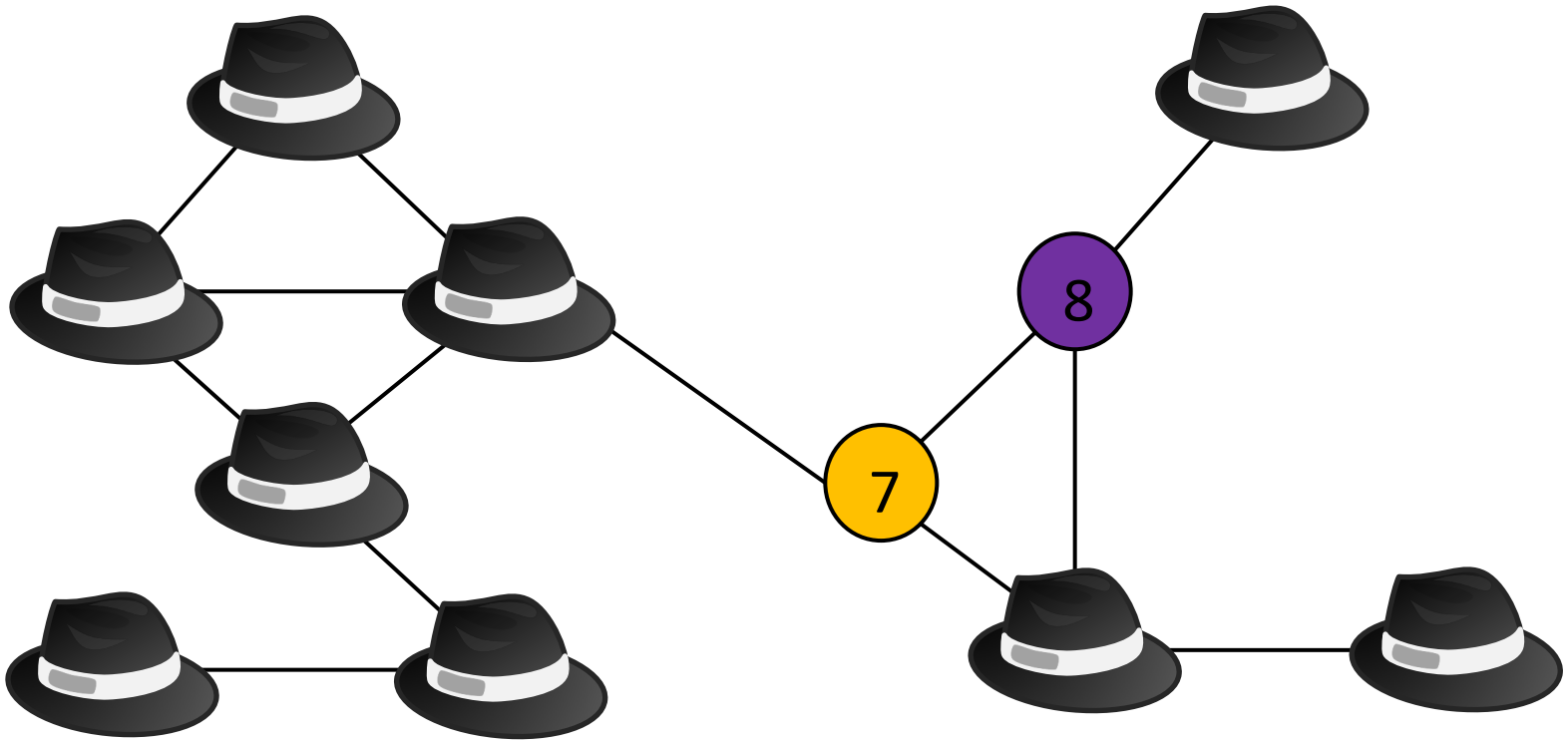
- The hats perfectly covered ‘protects’ the solution



Zero-Knowledge Proof Illustration

Proof of Solution:

- Remove any two hats
- See vertices are different colors



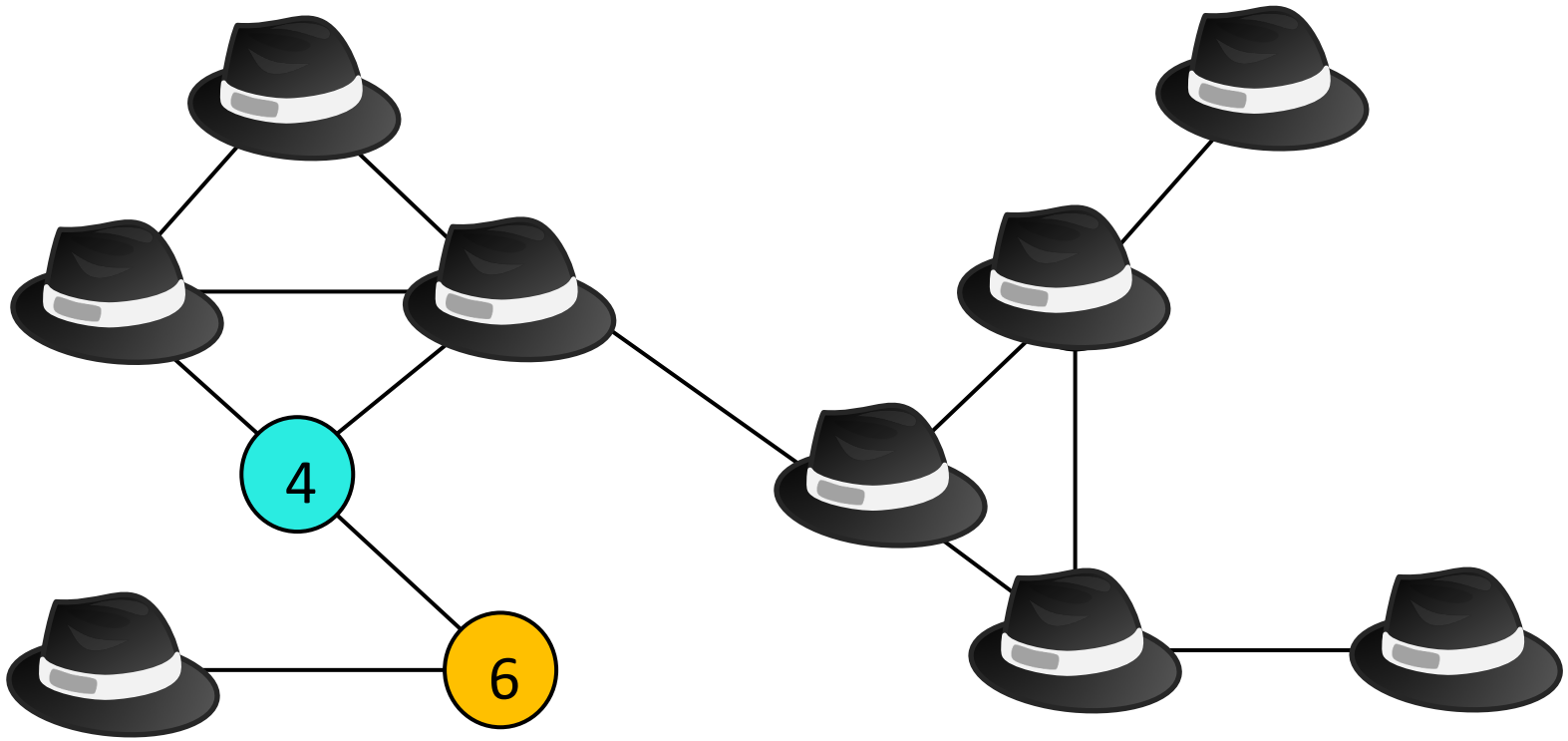
Zero-Knowledge Proof Illustration

Repeat this process:

- Clear previous solution
- Add randomness
- Solve again

Accept or reject:

- Complete for preset number of rounds
- Telecom accepts or rejects



RSAConference2019

Zero-Knowledge Proof Variants

Practical Application

Zero-Knowledge Proof Variants

ZKP	Interactive, multiple messages, need stable communication channel
NIZKP	Not interactive, one message
Graph Isomorphism	Interactive, compare graphs, efficient computation
zk-SNARK	Need one-time, trusted setup to generate key at launch
zk-STIK	Scalable Transparent Interactive Oracle of Proof (IOP) of Knowledge
zk-STARK	No setup, working on memory issues, I or NI, post-quantum secure
Designated Verifier	DVNIZK, not just any entity can be verifier, verifier must know secret
Bulletproof	No setup, 188 bytes, 10 ms in some cases, not post-quantum secure
Laticce-Based	Lattice-based cryptography, post-quantum secure, research

Zero-Knowledge Proof Practical Application

Where to apply ZPK:

- Authentication
- Messaging
- Secure Sensitive Information (PCI Data)
- Data Sharing
- File System Control
- Storage Protection

Zero-Knowledge Proof : Use Cases

- ING is a Netherlands based bank
- Experian
- UK citizens using the GOV.UK

Zero-Knowledge Proof : Technology Landscape

MIRACL

KRIPTAN

Microsoft UProve

Velix.ID

NUGGETS

SEDICCII

SOVRIN

STRATUMN

IBM

Val:ID

NuID

QEDit

PEER MOUNTAIN

CIVIC

RSAConference2019

Considerations

Potential Challenges

Zero-Knowledge Proof Considerations

- Transparent
- Universal
- Compliant with upcoming ZKP Standards
- Interactive, non-interactive
- Secure (threat model)
- Post-quantum secure

Zero-Knowledge Proof Challenges

- Low usability
- Expensive
- Requires high compute power

Zero-Knowledge Proof Application

- Assess use cases for privacy preserving authentication and authorization
- Evaluate and perform a POC with a ZKP Identity landscape solution
- Protect identities using ZKP

Questions

RSAConference2019

References

Stand on the Shoulders of Giants

References

- Anwar, H. (2018, November 30). What is ZKP? A Complete Guide to Zero Knowledge Proof. Retrieved from https://101blockchains.com/zero-knowledge-proof/#7
- Attribute-based Credentials for Trust (ABC4Trust) Project
- AU2EU Project, Authentication and Authorization for Entrusted Unions
- Bitansky, Nir; Weizman, Zvika Brakerski; Kalai, Yael. 3-Message Zero Knowledge Against Human Ignorance
- Camenisch, Jan and E. Van Herreweghen, Design and implementation of the IBM Idemix anonymous credential system , in Proceedings of the 9th ACM conference on Computer and communications security
- Camenisch, Jan; Dubovitskaya, Maria; Enderlein, Robert; et al. Concepts and languages for privacy-preserving attribute-based authentication
- Cutler, Becky. The Feasibility and Application of Using Zero-Knowledge Protocol for Authentication Systems
- Durcheva, Mariana. Zero Knowledge Proof Protocol Based on Graph Isomorphism Problem
- Feige, U., Fiat, A., & Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of cryptology*, *1*(2), 77-94.
- Fleischhacker, Nils; Goyal, Vuypil; Jain, Abhishek. On the Existence of Three Round Zero-Knowledge Proofs
- Geraud, Rémi. Zero-Knowledge: More Secure than Passwords
- Grassi, P. A., Richer, J. P., Squire, S. K., Fenton, J. L., Nadeau, E. M., Lefkovitz, N. B., . . . Theofanos, M. F. (2017). Digital identity guidelines: Federation and assertions. doi:10.6028/nist.sp.800-63c
- Green, Matthew. Zero Knowledge Proofs: An Illustrated Primer https://cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/ (November 2014).
- Limited, M. U. (n.d.). Miracl. Retrieved from https://www.miracl.com/experian-case-study