Zero knowledge-proof

Ante Sosa

Faculty of Computer and Information Science
University of Ljubljana

December 12, 2018

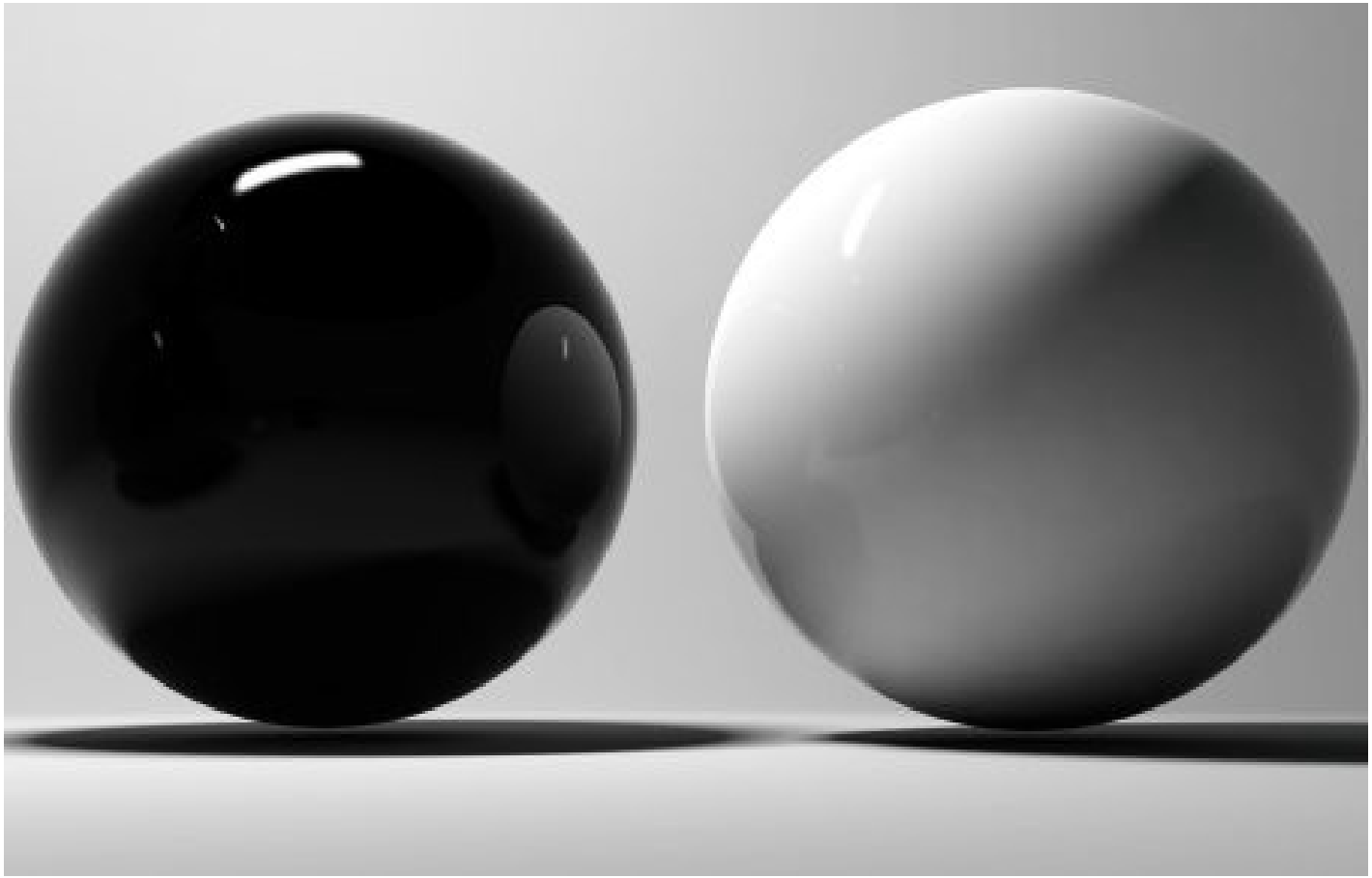
Agenda

1. Introduction
2. Two balls and the colour-blind verifier
3. Yao's millionaires problem
4. Discrete logarithm of a given value
5. Application on blockchain
6. Conclusion

Introduction

- Definition.
- Properties:
  - Completeness
  - Soundness
  - Zero-knowledge
- Problems:
  - Two balls and the colour-blind verifier
  - Yao's millionaires problem
  - Discrete logarithm of a given value

Two balls and the colour-blind verifier



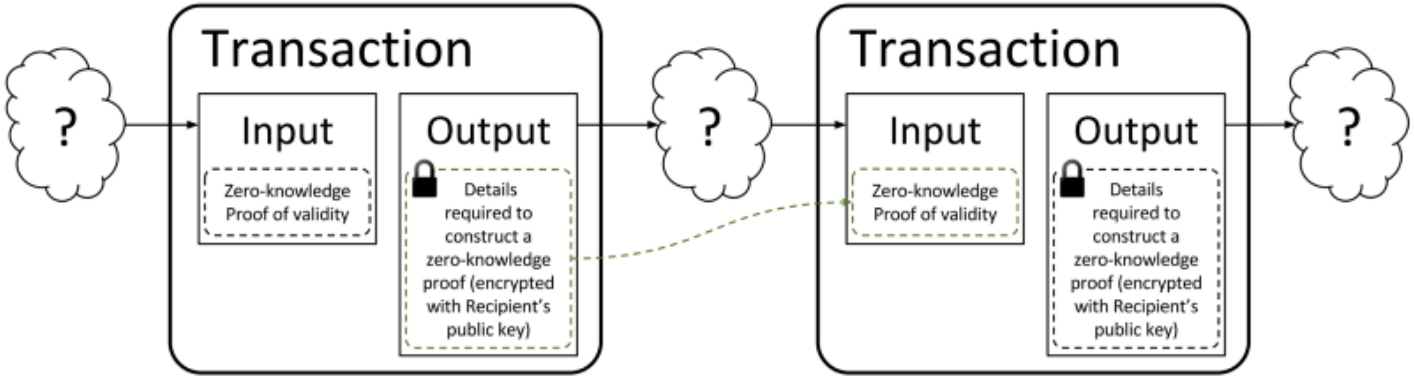
Yao's millionaires problem

- $s = s_n s_{n-1} \dots s_1 \ \in \{0,1\}^n$
- $S_s^0 = \{s_n s_{n-1} \dots s_{i+1} 1 | s_i = 0, 1 \leq i \leq n\}$.
- $S_s^0 = \{s_n s_{n-1} \dots s_i | s_i = 1, 1 \leq i \leq n\}$.
- If x is encoded in S_x^1 and y is encoded in S_y^0 than $x > y$ if and only if S_x^1 and S_y^0 has common element.

Discrete logarithm of a given value

- $\alpha^x \equiv \beta \pmod{N}$ Both prover and verifier know the values of α, β, but x is known only by prover.
- The protocol proceeds as follows:
  - The prover chooses by random $r \in \{1, \ldots, \phi(N)\}$, calculates $\gamma :\equiv \beta^r \pmod{N}$ and sends it to verifier.
  - The verifier chooses $b \in \{0, 1\}$.
  - Prover sends $y :\equiv r + bx \pmod{N}$ to verifier.
  - Verifier checks if $\alpha^y \equiv \alpha^r \beta^b \pmod{N}$ holds.

Application on blockchain



Conclusion

References

- Y. Lin and W. G. Tzeng, An Efficient Solution to The Millionaires's Problem Based on Homomorphic Encryption, 2005.
- D. Chaum, J. H. Evertse, J. van de Graaf, An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations. Advances in Cryptology - EuroCrypt '87: Proceedings. 304: 127-141, 1987.
- R. Gennaro, C. Gentry, B. Parno, M. Raykova, Quadratic Span Programs and Succinct NIZKs without PCPs, 2012.

Questions