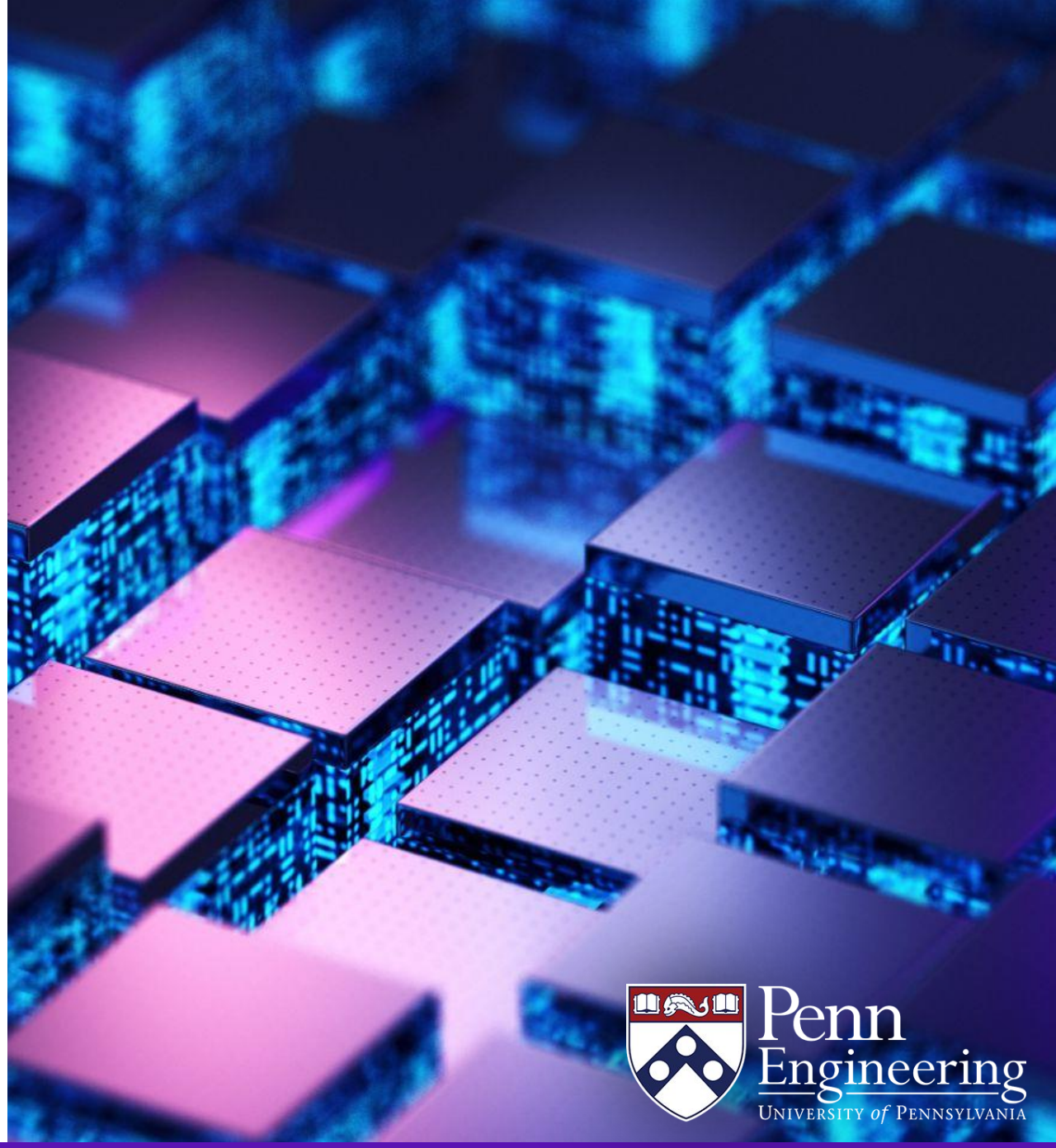
EAS 5830: BLOCKCHAINS

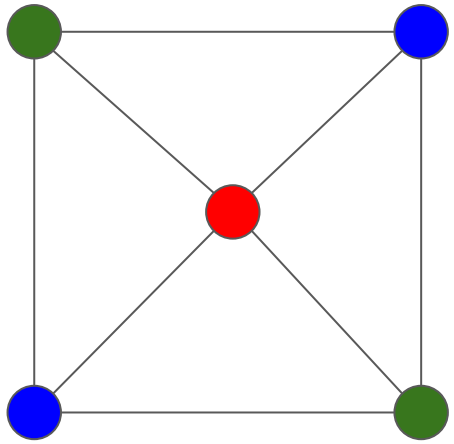
Zero-Knowledge Proof for Graph 3-coloring

Professor Brett Hemenway Falk

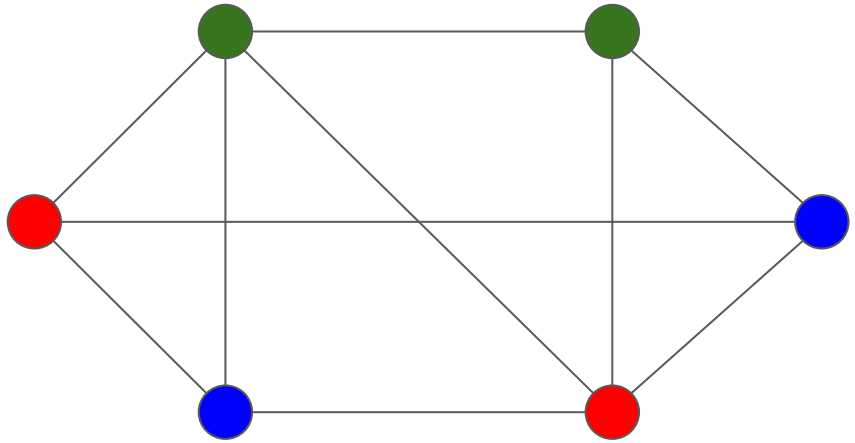


Graph 3-Coloring

- Given a graph, can you label every vertex with one of three colors such that no two adjacent vertices have the same color?



3-colorable



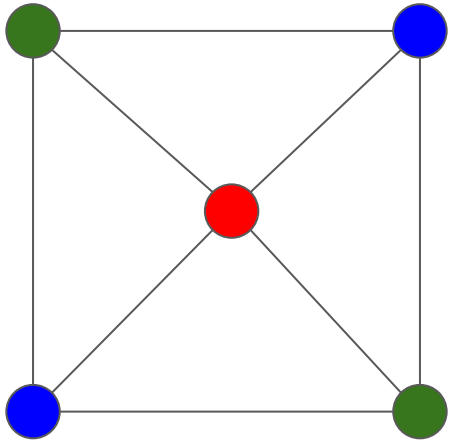
Not 3-colorable

3-Coloring is NP Complete

- Reducible to 3-SAT
- A ZK-Proof for 3-coloring can be used to create ZK-proofs for *any* NP statement

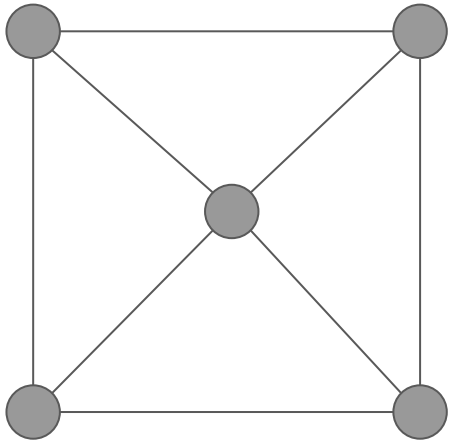
Proof of 3-Coloring: Setup

Prover



Knows a 3-coloring of the graph

Verifier



Knows the graph

Zero-Knowledge

- Prover and verifier engage in an interactive protocol
- At the end of the protocol the verifier is convinced the graph is 3-colorable
- The protocol does not help the verifier *find* the 3-coloring

Proof Protocol

- The prover commits to the color of each vertex
- The prover sends these commitments to the verifier
- The verifier chooses an edge, e, uniformly at random and sends e to the prover
- The prover decommits the colors assigned to the two endpoints of e
- The verifier checks that two node colors are different
- The prover permutes the colors and repeats the protocol

Completeness

- (An honest verifier will accept true statements)

- The prover commits to a 3-coloring the verifier will never reject

Soundness

- (A dishonest prover cannot convince a verifier of false statements)
- If the graph is not 3-colorable then for any coloring, there is at least one edge connecting two vertices of the same color
- The verifier chooses this edge with probability $1/n$
- After k repetitions, probability of cheating is $((n\text{-}1)/n)^k$

Zero-Knowledge

- At each repetition, the verifier sees the coloring of the endpoints of a single edge

- A simulator (who creates the queries) can create a transcript of the interaction *without* knowing a 3-coloring

Online Demo

http://web.mit.edu/~ezyang/Public/graph/svg.html