Theory and Practice of Cryptography

Theory of Cryptography

Recap of Week 2

Course materials on: http://saweis.net/crypto.shtml

Video on YouTube:
http://youtube.com/watch?v=KDvt_0cafPw

Today's Lecture

What does it mean for a cryptosystem to be secure?

How do we prove security?

What are zero knowledge proofs?

Does cryptography exist?

What does "secure" mean?

Would you trust a cryptosystem that leaked a single bit?

A Cryptographic Game

Alice:

1. Generates a public key and sends it to Bob.

3. Picks a random bit b

4. Sends Bob $c=E(m_b)$

Bob:

2. Sends Alice two messages: m_0 and m_1

5. Given c, tried to guess b

Semantic security

IND-CPA: Indistinguishability under chosen plaintext attack

RSA Example

Alice:

1. Sends Bob a RSA public key: (n, e) = (2701, 5)

3. Picks a random bit b=0

4. Sends Bob c=10^5 mod 2701 = 63

Bob:

2. Sends Alice m_0=10 and m_1=42

5. Bob can trivially tell that c=E(m_0) and outputs 0

RSA is not semantically secure

No deterministic cryptosystem is

ElGamal

Taher ElGamal, 1984:

- Cyclic group G and generator g
- Private key s
- Public key h = g^s
- E(h, m) = (g^r, mh^r) = (c, d)
- D(s, c, d) = d/(c^s) = mh^r/g^(rs) = m

Some nice properties:

- Semantic security (under DDH assumption)
- Ciphertexts can be re-randomized
- Homomorphic multiplication
- Supports precomputation
- Conducive to ZK proofs

Proof by reduction

Computational DH: Given (g, g^a, g^b) output g^(ab)
Decisional DH: Given (g, g^a, g^b) distinguish g^(ab) and g^c

If Bob has a non-negligible advantage in winning the IND-CPA game, we can use him as an oracle for solving the DDH.

If DDH is hard, then ElGamal is semantically secure.

DDH is thought to be hard in several efficiently computable groups, but is not hard in Zp*.

Lunchtime Attack

Alice:

1. Gives Bob access to both encryption and decryption oracles, E and D.

4. Picks a random bit b
5. Sends Bob c=E(m_b)

Bob:

2. Talks to both oracles.
3. Sends Alice two messages: m_0 and m_1

6. Talks to just the E oracle.
7. Guesses a bit b'

Adaptive Chosen Ciphertext Attack

Alice:

1. Gives Bob access to both encryption and decryption oracles, E and D.

4. Picks a random bit b
5. Sends Bob c=E(m_b)

Bob:

2. Talks to both oracles.
3. Sends Alice two messages: m_0 and m_1

6. Talks to both oracles, but can't ask D to decrypt c.
7. Guesses a bit b'

ElGamal IND-CCA2 Game

Alice:

1. Gives Bob public key (g, h) and decryption oracle D.

4. Picks a random bit b

5. Sends (c,d)=(g^r, m_bh^r)

Bob:

2. Sends Alice two messages: m_0 and m_1

6. Asks D to decrypt (c, 2d) to get 2m_b

7. Correctly outputs b

ElGamal is not CCA2 secure

But Cramer-Shoup is under DDH

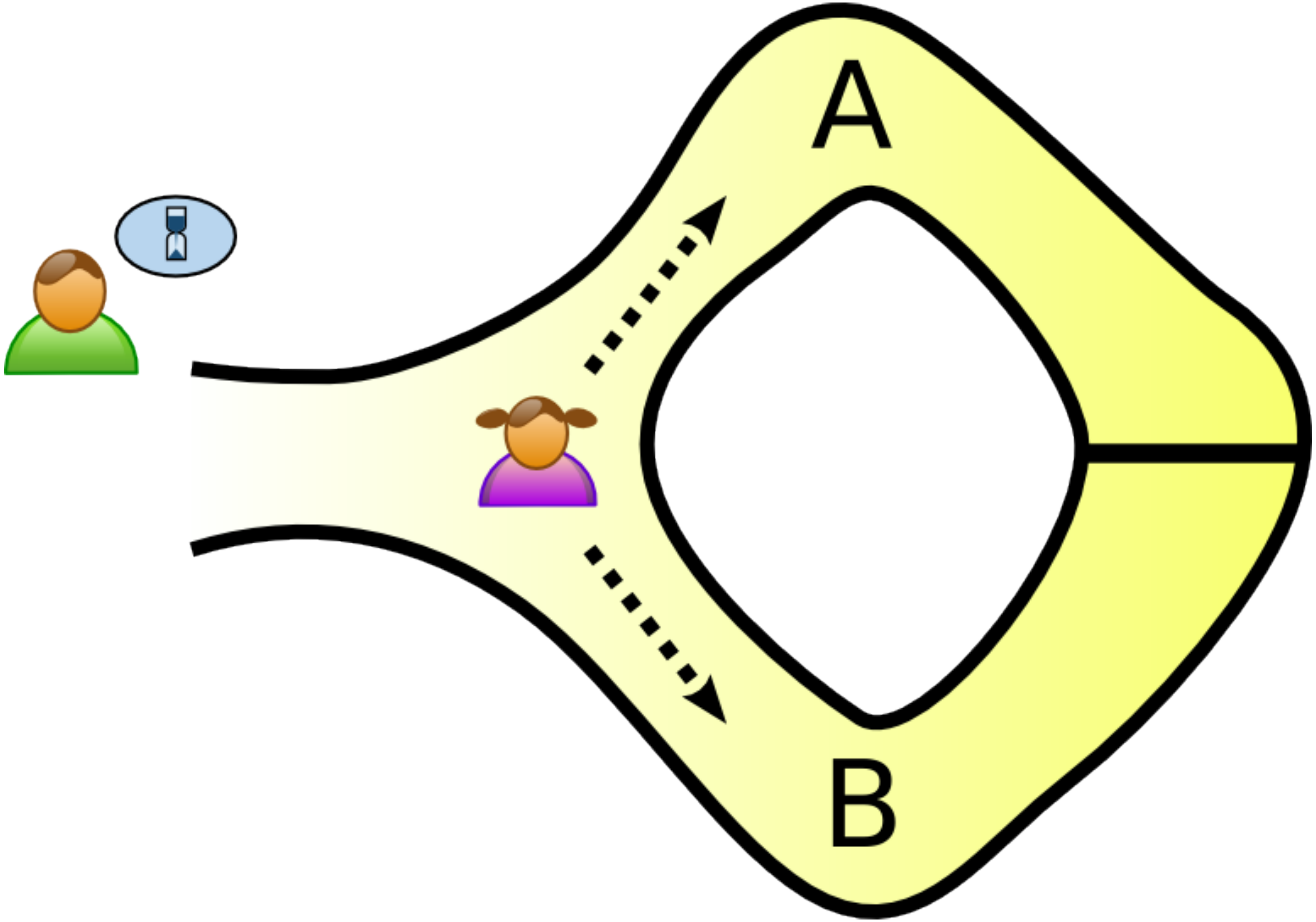
Recap

- RSA: Not semantically secure
- ElGamal: Semantically secure, not CCA2 secure
- Cramer-Shoup: CCA2 secure under DDH assumption
- RSA-OAEP: CCA2 secure in "random oracle model"
- Can convert any IND-CPA scheme into a IND-CCA2 scheme with the use of *zero knowledge proofs*

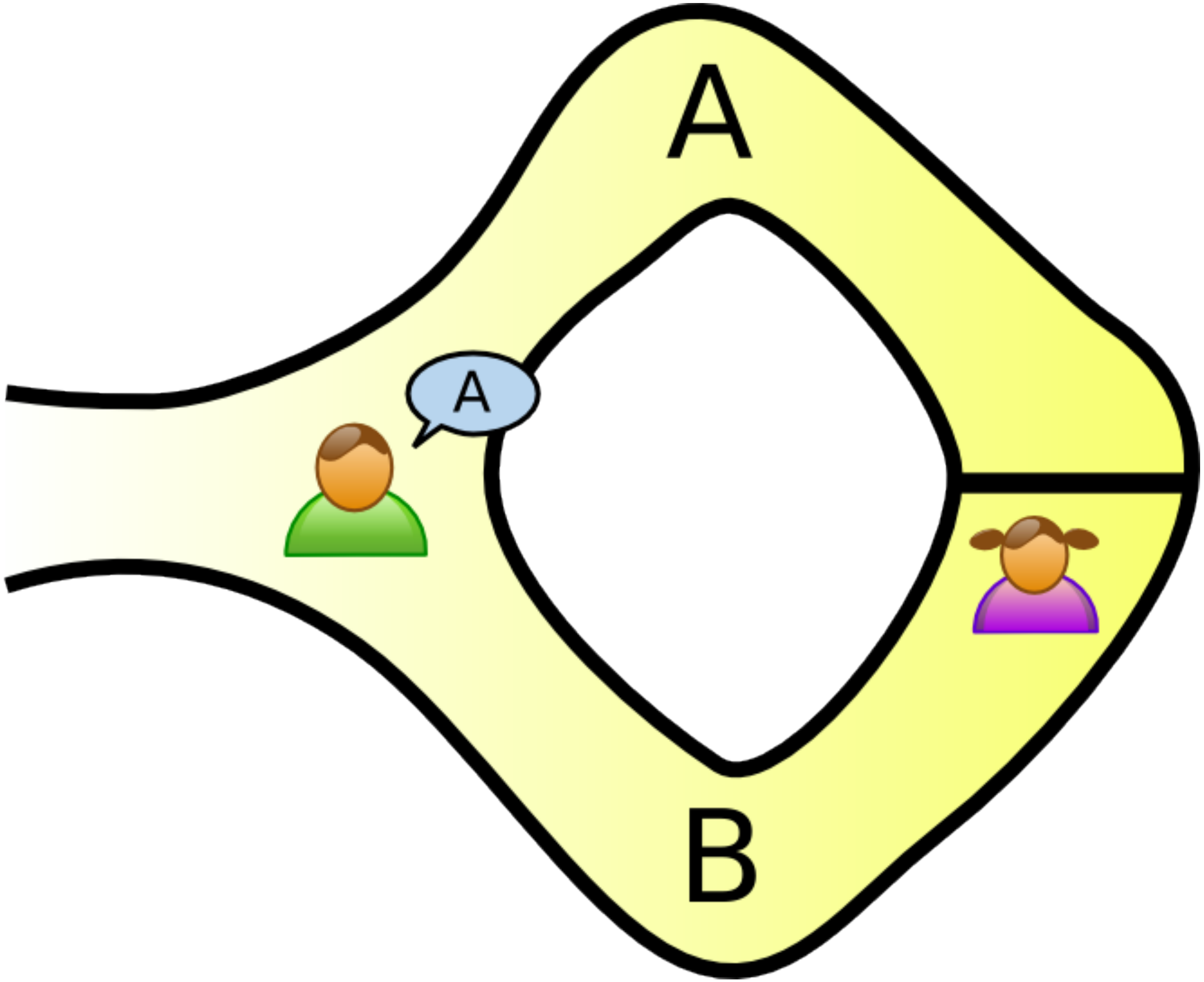
What's a zero knowledge proof?

Prove a statement without revealing anything but its veracity.

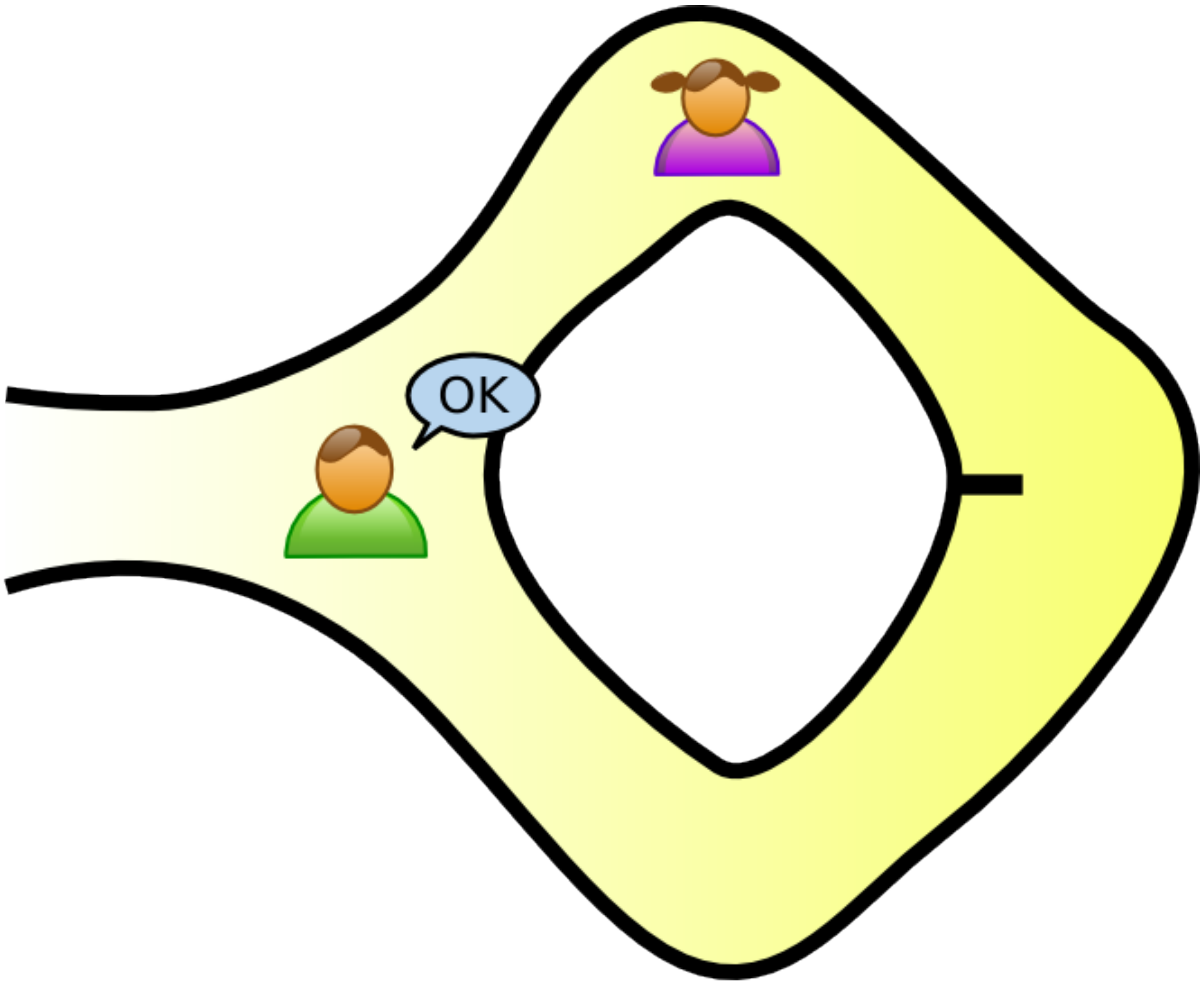
Ali Baba's Cave: Commitment



Ali Baba's Cave: Challenge

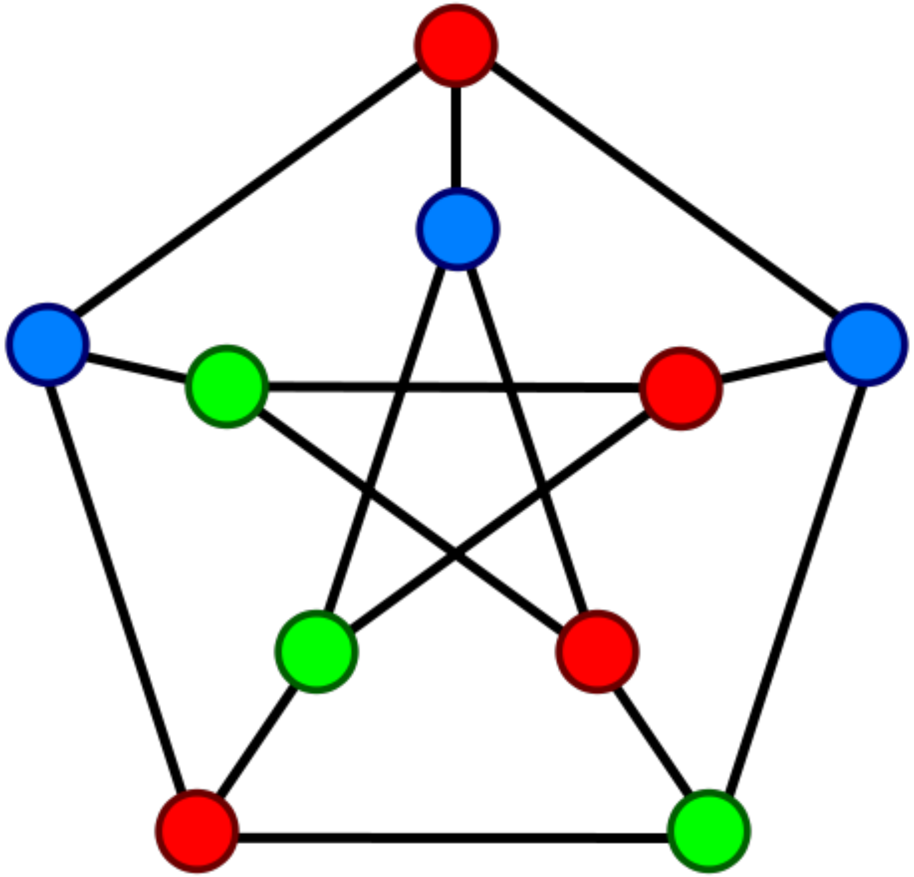


Ali Baba's Cave: Response



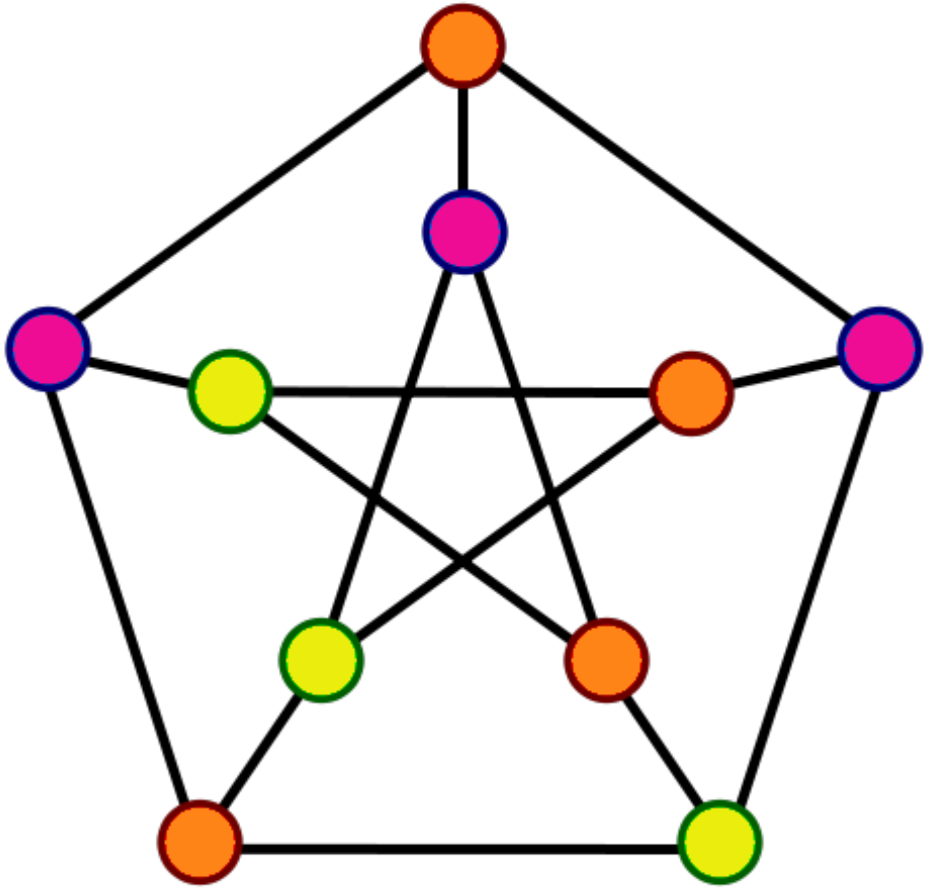
ZK Proof of Graph 3-Colorability

Alice knows a 3-coloring of a graph. Wants to prove it to Bob.



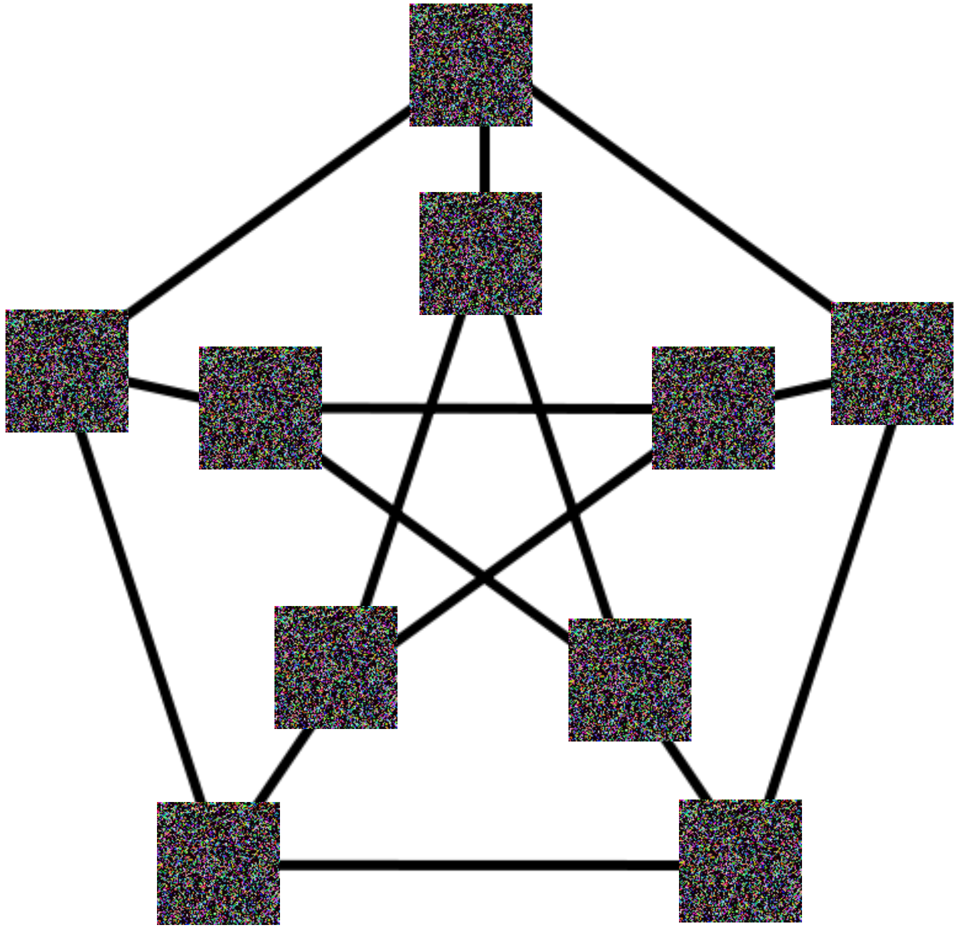
ZK Proof of Graph 3-Colorability

Each round, she randomly relabels her graph coloring:



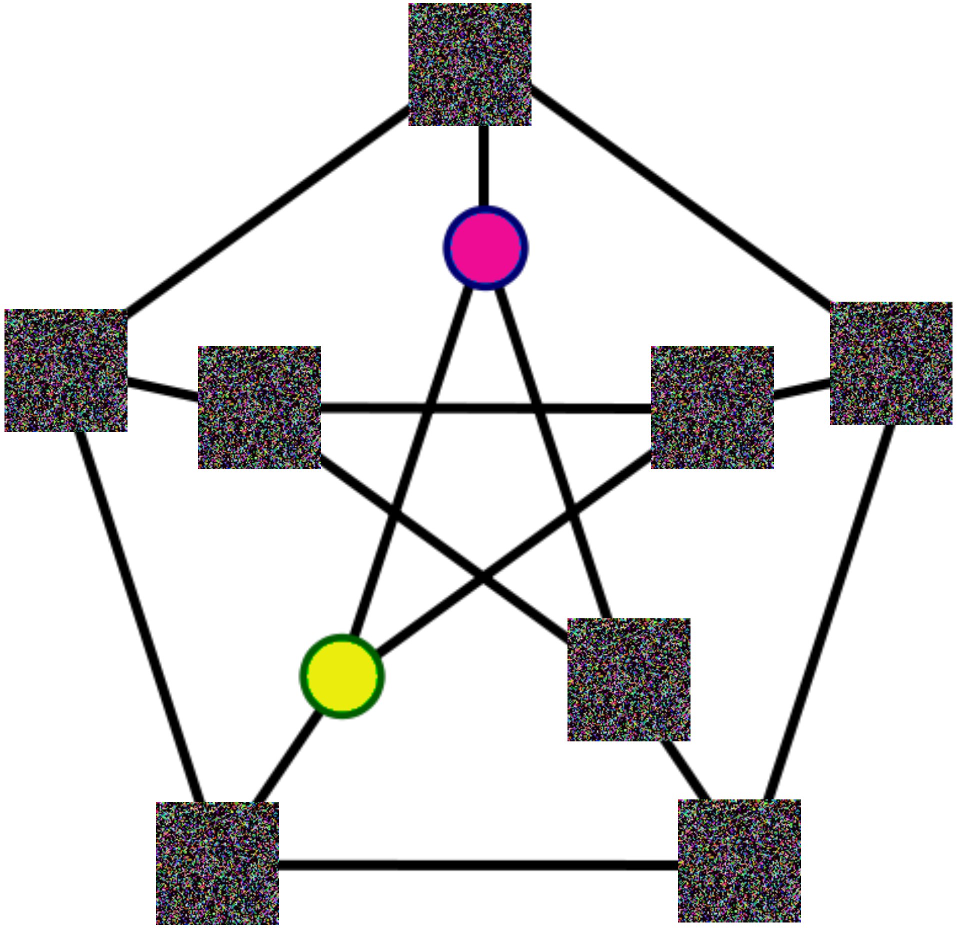
ZK Proof of Graph 3-Colorability

Alice sends Bob a commitment of each relabeled vertex:



ZK Proof of Graph 3-Colorability

Bob challenges Alice with an edge. She reveals the vertices:



Future of Zero Knowledge

Potential applications:

- Authentication
- Secure Multiparty Computation
- Voting Protocols

Much work to be done and many flavors in the literature: *Perfect, statistical, computational, honest-verifier, non-interactive, concurrent, resettable, public-coin, constant-round, witness indistinguishable, precise, etc.*

Crypto "Complexity Classes"

The following all imply each other:

- One way functions
- Pseudo-random generators
- Symmetric-key encryption
- Public key signature schemes
- Bit commitments

Trapdoor permutations imply...

- Public key encryption, which imply...
- Key agreement protocols, which imply...
- One-way functions

Does cryptography exist?

We don't know.

Cryptography implies P≠NP

But P≠NP should not imply crypto

"Hardness" in practical systems?

Hardness based on several different mathematical problems:

- Factoring is in (NP ∩ co-NP) and BQP
- Discrete logarithms
- Finding shortest vectors in a lattice
- Decoding random binary linear codes

Next Week: Ben Adida

Cryptographic voting protocols