COS 433: Cryptography

Announcements:

- Problem Set 5 due 12/2
- Final problem set released Monday 11/30, due Thursday 12/10 11:59pm
  - No collaboration allowed
  - You may use anything available on our course website (including the lecture slides and textbooks)
  - No other sources may be consulted
  - No late submissions
- Check-in 3: Friday 12/11 and Monday 12/14

Proof Systems

Claim: $x \in L$



$P(x, w)$





$V(x)$

Output: $b \in \{0,1\}$

Definition: a proof system for a language $L \subset \{0,1\}^*$ consists of a pair of interactive algorithms (P, V) run on an input $x \in \{0,1\}^n$

- V will always be a $\mathbf{poly}(n)$-time algorithm
- P can be inefficient, or $\mathbf{poly}(n)$-time given a witness w

It must satisfy the following properties:

1. **Completeness**: if $x \in L$ and the two parties run (P, V), then V outputs 1 (accept)
2. **Soundness**: if $x \notin L$, then for any strategy P^*, V accepts with probability $\mathbf{negl}(n)$.

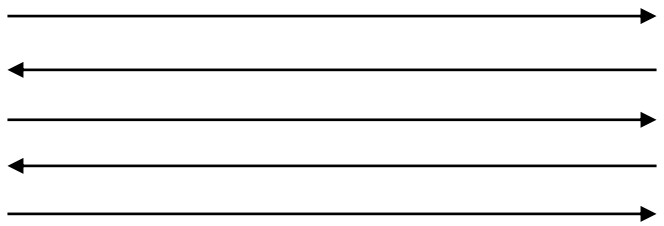
Zero-Knowledge Proofs

[Goldwasser-Micali-Rackoff '85]

Claim: $x \in L$



$P(x, w)$





$V(x)$

Output: $b \in \{0,1\}$

Definition: a proof system (P, V) for a language L is malicious verifier zero knowledge if for all polynomial-time V^*, there exists a polynomial-time simulator

$$\mathrm{Sim}^*(x) \to \tau$$

such that for all $x \in L$ and all valid w,

$$\mathrm{Sim}^*(x) \approx_c \mathrm{view}_{V^*}(x, w)$$

Simulation paradigm: everything V^* learned, V^* could have generated on their own!



Zero-Knowledge Proofs for NP





Theorem [Goldreich-Micali-Wigderson]:

Assuming OWFs, every language $L \in \mathbf{NP}$ has a ZK proof system!

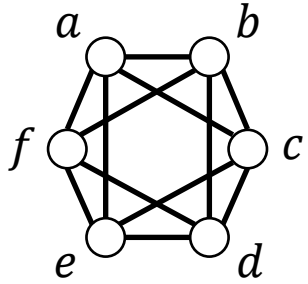
- Honest prover efficient given $\mathbf{NP}$-witness.
- ZK is computational

All languages with (non-interactive) proofs have ZK proofs!

Can be extended to all languages with interactive proofs ($\mathbf{IP}$)

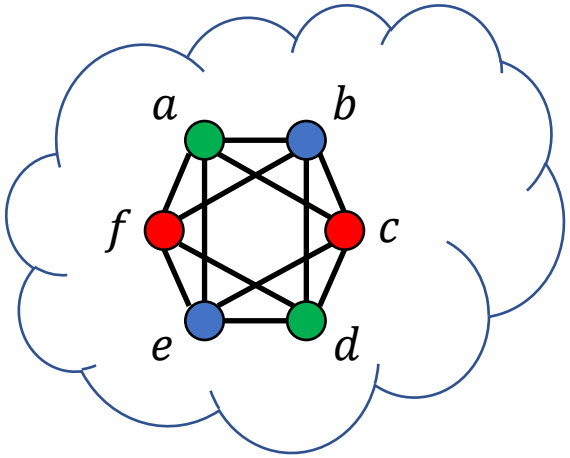
Zero Knowledge Proofs for NP

Claim: This graph has a 3-coloring.



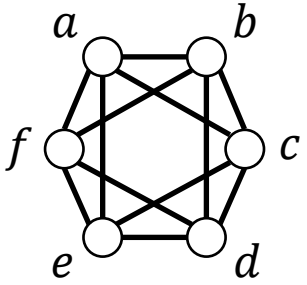
P V

Zero Knowledge Proofs for NP



Claim: This graph has a 3-coloring.

P

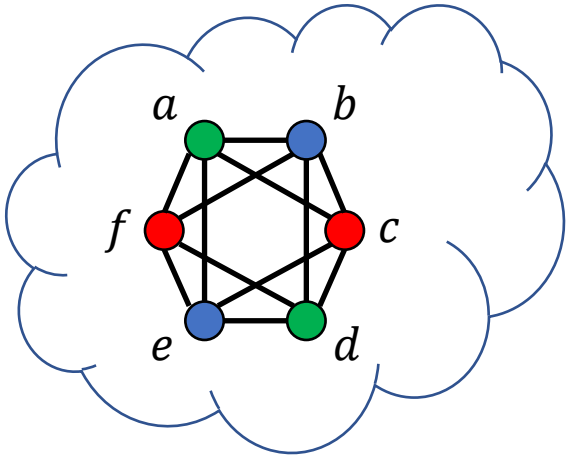


V

Intuition:

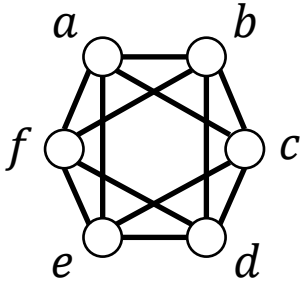
- P will send a message defining $|E(G)|$ different claims
- V will test one of these claims at random

Zero Knowledge Proofs for NP



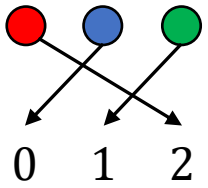
Claim: This graph has a 3-coloring.

P



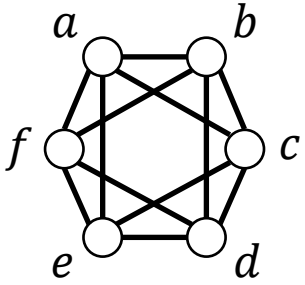
V

1) Randomize colors:



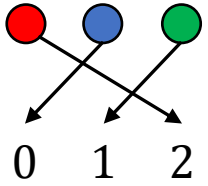
Zero Knowledge Proofs for NP

Claim: This graph has a 3-coloring.



P V

1) Randomize colors:

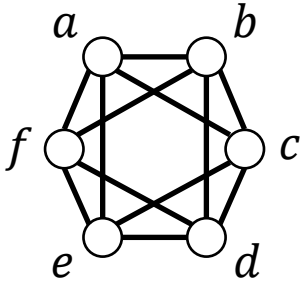


2) Commit:

a	b	c	d	e	f
1	0	2	1	0	2

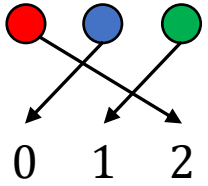
Zero Knowledge Proofs for NP

Claim: This graph has a 3-coloring.

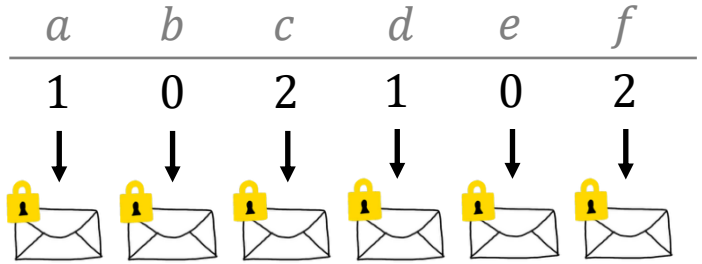


P V

1) Randomize colors:

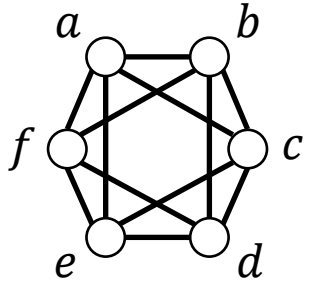


2) Commit:



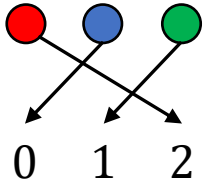
Zero Knowledge Proofs for NP

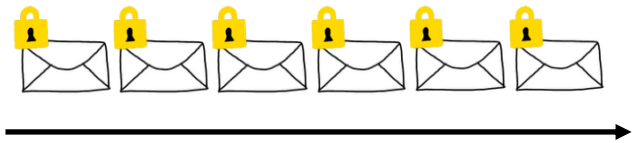
Claim: This graph has a 3-coloring.



P V

1) Randomize colors:





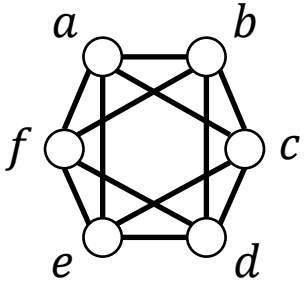
2) Commit:

a	b	c	d	e	f
1	0	2	1	0	2



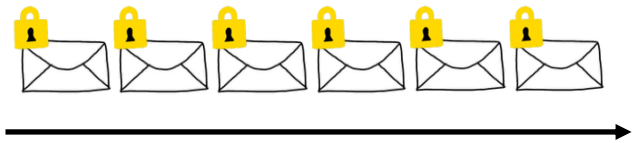
Zero Knowledge Proofs for NP

P



V

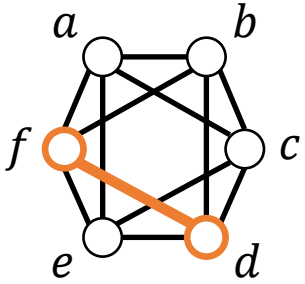
1) Randomize colors:



2) Commit:

Zero Knowledge Proofs for NP

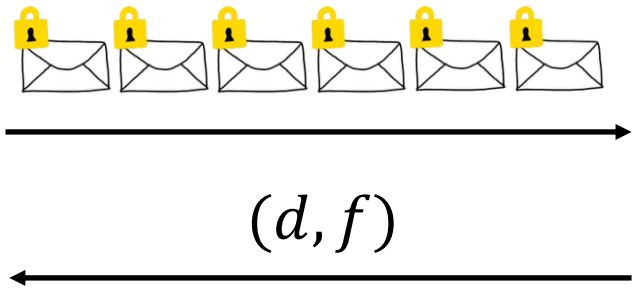
P



V

1) Randomize colors:

2) Commit:

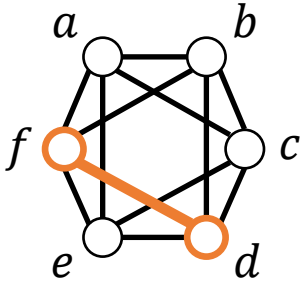


(d, f)

1) Sample a **challenge** edge.

Zero Knowledge Proofs for NP

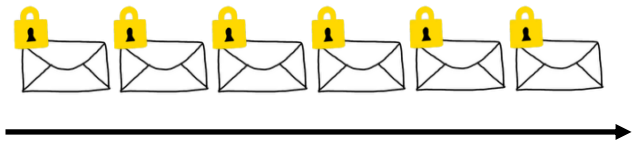
P



V

1) Randomize colors:

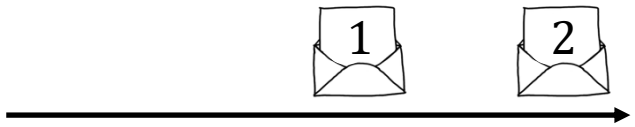
2) Commit:



(d, f)

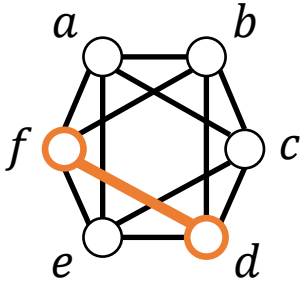
1) Sample a **challenge** edge.

3) Reveal edge colors



Zero Knowledge Proofs for NP

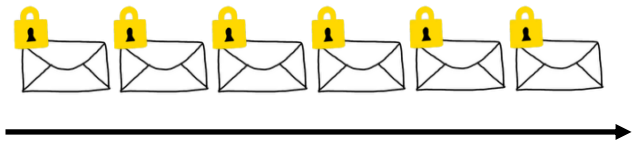
P



V

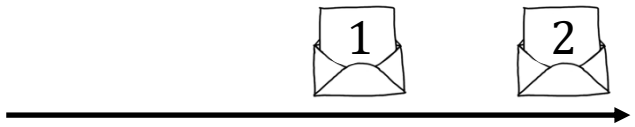
1) Randomize colors:

2) Commit:



(d, f)

1) Sample a **challenge** edge.



3) Reveal edge colors

2) Accept if colors are different.

Tool: Commitment Schemes

Commitment Schemes

Intuition: a (2-message) commitment scheme consists of an efficient algorithm

$$\mathrm{Com}(\mathrm{ck}, m; r)$$

satisfying the following two properties:

1. Computational Hiding: $\mathrm{Com}(\mathrm{ck}, m)$ does not reveal m (commitment key is public)

2. Statistical Binding: commitment c is only consistent with a single m (known ck)

    - Terminology: opening a commitment (for us) means revealing the randomness

Commitment Schemes

Definition: a (2-message) commitment scheme consists of an efficient algorithm

$$\mathrm{Com}(\mathrm{ck}, m; r)$$

satisfying the following two properties:

1. Computational Hiding: for all $\mathrm{ck} \in \{0,1\}^{\lambda}$ and all pairs of messages $m_0 \neq m_1$:

$$\mathrm{Com}(\mathrm{ck}, m_0) \approx_c \mathrm{Com}(\mathrm{ck}, m_1)$$

2. Statistical Binding: with probability $1 - \mathrm{negl}(\lambda)$ over the choice of $\mathrm{ck} \leftarrow \{0,1\}^{\ell(\lambda)}$, there do not exist $m_0 \neq m_1$ and r_0, r_1 such that $\mathrm{Com}(\mathrm{ck}, m_0; r_0) = \mathrm{Com}(\mathrm{ck}, m_1; r_1)$

Commitment Schemes

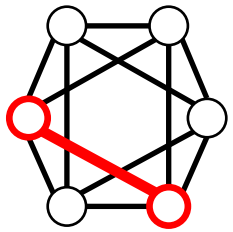
Theorem: if PRGs exist, then commitment schemes exist!

Construction (analysis on board):

$$\mathrm{Com}\left(\mathrm{ck} \in \{0,1\}^{3\lambda}, m; r \in \{0,1\}^{\lambda}\right) = G(r) \oplus m \cdot \mathrm{ck}$$

Zero Knowledge Proofs for NP

P V



Sample $\pi \leftarrow S_3$
Define $c_i = \pi \circ \chi(i)$
Sample r_i for every i

ck ← Sample ck

$\alpha = \mathrm{Com}(\mathrm{ck}, c_i; r_i)_{i=1}^n$ →

e ← $e = (v, w) \leftarrow E(G)$

$\gamma = (c_v, r_v, c_w, r_w)$ →

Check:
- $\alpha_v = \mathrm{Com}(c_v; r_v)$
- $\alpha_w = \mathrm{Com}(c_w; r_w)$
- $c_v \neq c_w$

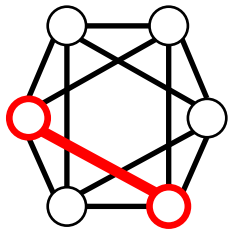
Completeness: π preserves proper colorings

Soundness: if G is **not** 3-colorable:

- (for almost all ck) Every string α implicitly defines a fixed coloring χ^* of G (by **binding** of Com)
- There exists an edge $e^* = (v, w)$ such that $\chi^*(v) = \chi^*(w)$
- If $e = e^*$ (inverse poly chance), P^* is stuck! (Repeat protocol to improve soundness error)

Zero Knowledge Proofs for NP

P V



Sample $\pi \leftarrow S_3$
Define $c_i = \pi \circ \chi(i)$
Sample r_i for every i

ck ← Sample ck

$\alpha = \mathrm{Com}(\mathrm{ck}, c_i; r_i)_{i=1}^{n}$ →

e ← $e = (v, w) \leftarrow E(G)$

$\gamma = (c_v, r_v, c_w, r_w)$ →

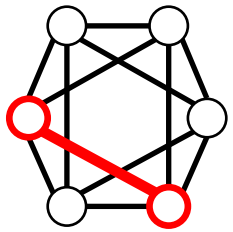
Check:
- $\alpha_v = \mathrm{Com}(c_v; r_v)$
- $\alpha_w = \mathrm{Com}(c_w; r_w)$
- $c_v \neq c_w$

ZK Intuition: Verifier sees

- Two random unequal colors
- Commitments to those two colors
- Unintelligible commitments to $n - 2$ other colors

Zero Knowledge Proofs for NP

Sim | **V**



Sample $e \leftarrow E(G)$
Sample $c_v \neq c_w$
Set $c_i = 0$ for other i
Sample r_i for every i

Sample ck

ck →

$\alpha = \mathrm{Com}(\mathrm{ck}, c_i; r_i)_{i=1}^{n}$ →

e ←

$\gamma = (c_v, r_v, c_w, r_w)$ →

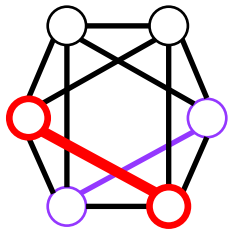
HVZK:

For 3-colorable G, this is like $\mathbf{view}_V(x, w)$, but $c_i = \pi \circ \chi(i)$ has been replaced by 0 (for $i \notin \{v, w\}$)

$\mathrm{Sim}(x) \approx_c \mathrm{view}_V(x, w)$ by the hiding property of Com

Zero Knowledge Proofs for NP

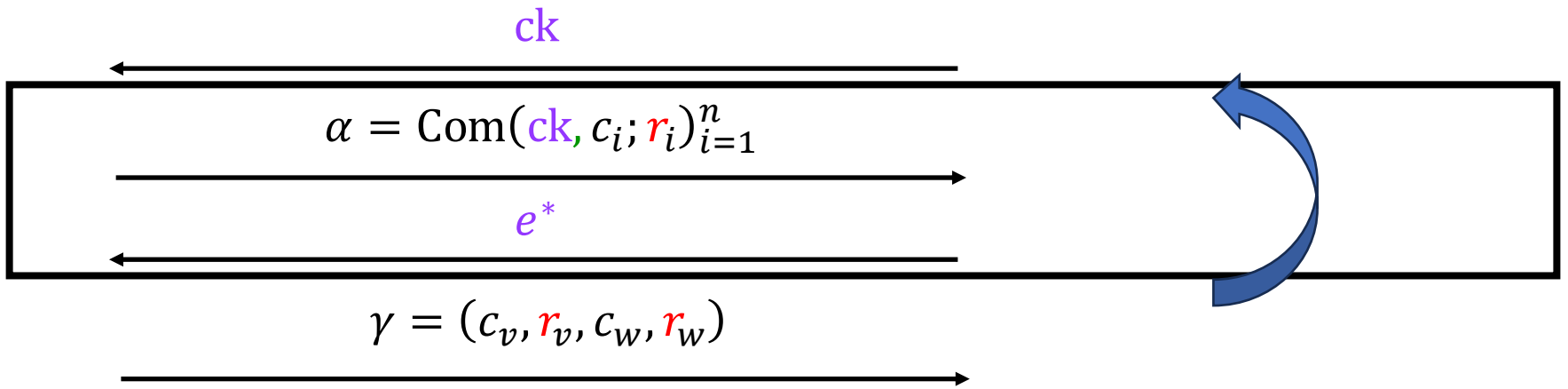
Sim^*



V^*

Sample $e \leftarrow E(G)$
Sample $c_v \neq c_w$
Set $c_i = 0$ for other i
Sample r_i for every i

If $e^* = e$:
Else, "**rewind**"



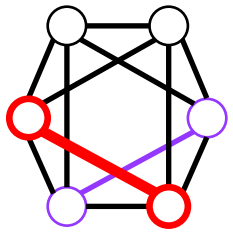
ZK: same idea as for QR

Claim 1: terminates in $|E(G)| \cdot \lambda$ attempts with all but negligible probability

Proof: by Com hiding, $\Pr[e^* = e] = \frac{1}{|E(G)|} + \mathrm{negl}(\lambda)$ (else V^* has learned info about c)

Zero Knowledge Proofs for NP

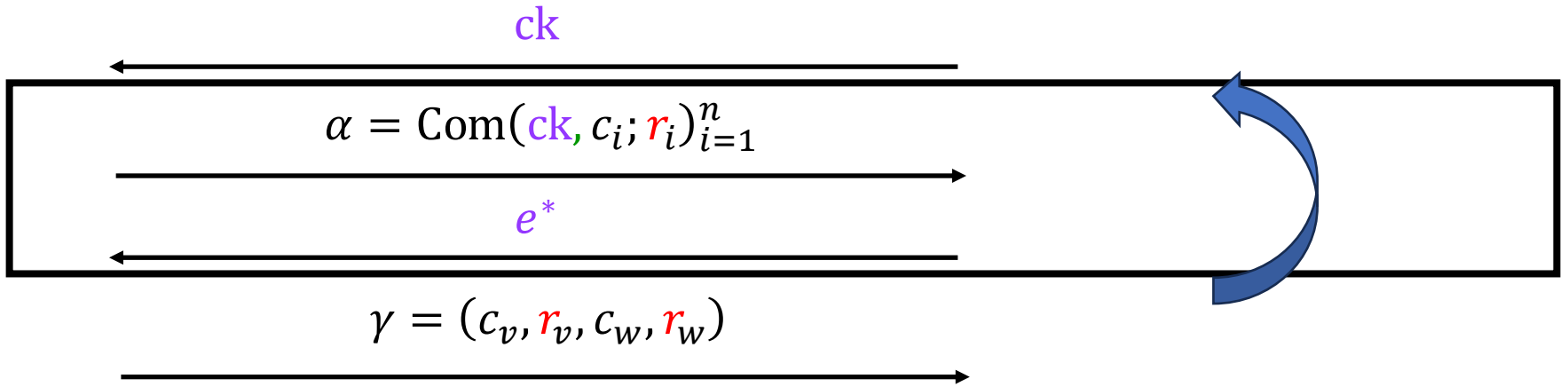
Sim^*



V^*

Sample $e \leftarrow E(G)$
Sample $c_v \neq c_w$
Set $c_i = 0$ for other i
Sample r_i for every i

If $e^* = e$:
Else, "**rewind**"



ZK: same idea as for QR

Claim 1: terminates in $|E(G)| \cdot \lambda$ attempts with all but negligible probability

Claim 2: output computationally indistinguishable from $\mathrm{view}_{V^*}(G, \chi)$ (by Com hiding)

Zero-Knowledge Proofs for NP

Theorem [Goldreich-Micali-Wigderson]:

Assuming OWFs, every language $L \in \mathbf{NP}$ has a ZK proof system!

Proof Systems as a Foundation

digital signatures

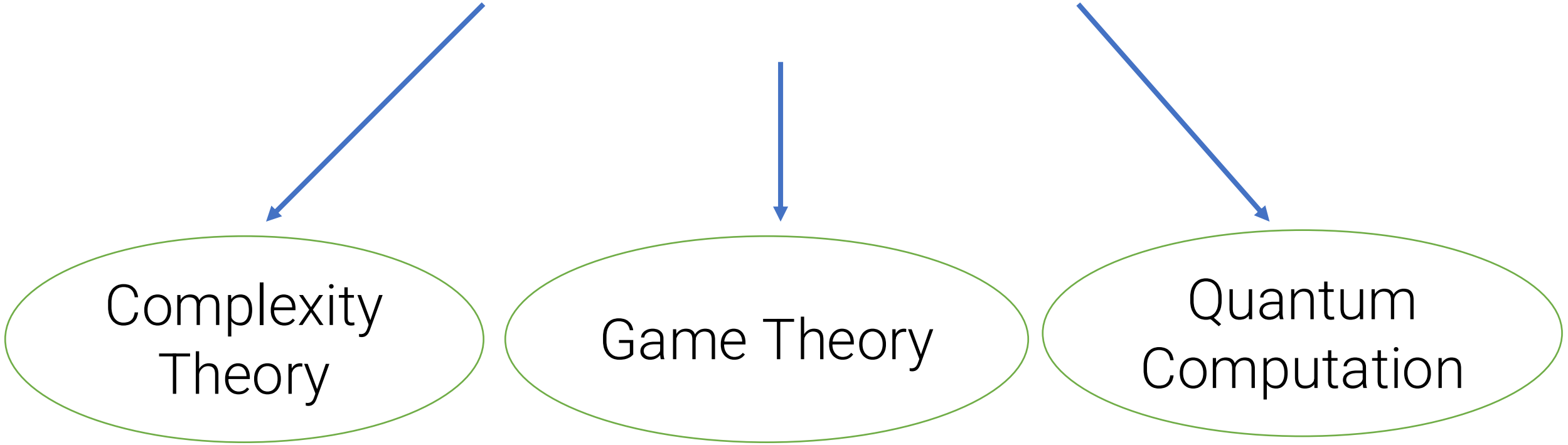
blockchains and cryptocurrencies

secure multiparty computation



Cryptographic Proofs

Proofs: A Lens into Computation



IP = PSPACE
[LFKN90, S90]
PCP Theorem
[BFLS91, ALMSS92]

Cryptographic Hardness of Finding Nash Equilibrium
[Papadimitriou94,Valiant08]

Classical Verification of Quantum Computation
[Mahadev18]

Next time: Homomorphic Encryption