Cryptography
CS 555

Topic 36: Zero-Knowledge Proofs

Recap

- Commitment Schemes
- Coin Flipping
- Oblivious Transfer
- ~~Secure Multiparty Computation (Security Models)~~

Secure Multiparty Computation (Adversary Models)

- Semi-Honest (“honest, but curious”)
  - All parties follow protocol instructions, but…
  - dishonest parties may be curious to violate privacy of others when possible
- Fully Malicious Model
  - Adversarial Parties may deviate from the protocol arbitrarily
    - Quit unexpectedly
    - Send different messages
  - It is much harder to achieve security in the fully malicious model
- Convert Secure Semi-Honest Protocol into Secure Protocol in Fully Malicious Mode?
  - Tool: Zero-Knowledge Proofs
  - Prove: My behavior in the protocol is consistent with honest party

Computational Indistinguishability

- Consider two distributions X_ℓ and Y_ℓ (e.g., over strings of length ℓ).
- Let D be a distinguisher that attempts to guess whether a string s came from distribution X_ℓ or Y_ℓ.

The advantage of a distinguisher D is

$$Adv_{D,\ell} = \left|Pr_{s \leftarrow X_\ell}[D(s) = 1] - Pr_{s \leftarrow Y_\ell}[D(s) = 1]\right|$$

Definition: We say that an ensemble of distributions $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are <u>computationally indistinguishable</u> if for all PPT distinguishers D, there is a negligible function negl(n), such that we have

$$Adv_{D,n} \leq negl(n)$$

Computational Indistinguishability

Notation: $\{X_n\}_{n\in\mathbb{N}} \equiv_C \{Y_n\}_{n\in\mathbb{N}}$ means that the ensembles are computationally indistinguishable.

- Consider two d … ℓ).
- Let D be a disti … came from distribution X_ℓ …

The advantage of a distinguisher D is

$$Adv_{D,\ell} = \left|Pr_{s\leftarrow X_\ell}[D(s) = 1] - Pr_{s\leftarrow Y_\ell}[D(s) = 1]\right|$$

Definition: We say that an ensemble of distributions $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are <u>computationally indistinguishable</u> if for all PPT distinguishers D, there is a negligible function negl(n), such that we have

$$Adv_{D,n} \leq negl(n)$$

P vs NP

- **P** problems that can be solved in polynomial time

- **NP** --- problems whose solutions can be **verified** in polynomial time
  - Examples: SHORT-PATH, COMPOSITE, 3SAT, CIRCUIT-SAT, 3COLOR,
  - DDH
    - **Input:** $A = g^{x_1}, \mathrm{B} = g^{x_2}$ and Z
    - **Goal:** Decide if $\mathrm{Z} = g^{x_1 x_2}$ or $\mathrm{Z} \neq g^{x_1 x_2}$.
  - **NP-Complete** --- hardest problems in NP (e.g., all problems can be reduced to 3SAT)
- **Witness**
  - A short (polynomial size) string which allows a verify to check for membership
  - DDH Witness: x_1,x_2.

Decisional Diffie-Hellman Problem (DDH)

- Let $z_0 = g^{x_1 x_2}$ and let $z_1 = g^r$, where x_1,x_2 and r are random
- Attacker is given $A = g^{x_1}$, $B = g^{x_2}$ and z_b (for a random bit b)
- Attackers goal is to guess b
- **DDH Assumption**: For all PPT A there is a negligible function negl such that A succeeds with probability at most ½ + negl(n).

Suppose that Alice knows that $z_b = g^{x_1 x_2}$ and wants to convince Bob that this is true.

- **Method 1:** Send x_1 (or x_2) to Bob wo can verify that $A = g^{x_1}$ and that
$$z_b = B^{x_1} = g^{x_1 x_2}.$$

Decisional Diffie-Hellman Problem (DDH)

- Let $\mathrm{z}_0 = g^{x_1 x_2}$ and let $\mathrm{z}_1 = g^r$, where x_1,x_2 and r are random
- Attacker is given $A = g^{x_1}$, $\mathrm{B} = g^{x_2}$ and z_b (for a random bit b)
- Attackers goal is to guess b
- **DDH Assumption**: For all PPT A there is a negligible function negl such that A succeeds with probability at most ½ + negl(n).

Suppose that Alice knows that $z_b = g^{x_1 x_2}$ and wants to convince Bob that this is true.

Suppose that Alice also doesn't want Bob to learn any information about x_1 or x_2. Is this possible?

Zero-Knowledge Proof

Two parties: Prover P (PPT) and Verifier V (PPT)

(P is given witness for claim e.g.,)

- **Completeness:** If claim is true honest prover can always convince honest verifier to accept.
- **Soundness:** If claim is false then Verifier should reject with probability at least ½. (Even if the prover tries to cheat)
- **Zero-Knowledge:** Verifier doesn't learn anything about prover's input from the protocol (other than that the claim is true).
- Formalizing this last statement is tricky
- **Zero-Knowledge:** should hold even if the attacker is dishonest!

Zero-Knowledge Proof

Trans(1^n,V’,P,x,w,r_p,r_v) transcript produced when V’ and P interact

- V’ is given input x (the problem instance e.g., $A = g^{x_1}$, $\mathrm{B} = g^{x_2}$ and z_b)
- P is given input x and w (a witness for the claim e.g., x_1 or x_2)
- V’ and P use randomness r_p and r_v respectively
- Security parameter is n e.g., for encryption schemes, commitment schemes etc…

$\boldsymbol{X_n} =$ **Trans(1^n,V’,P,x,w)** is a distribution over transcripts (over the randomness r_p,r_v)

(Blackbox Zero-Knowledge): There is a PPT simulator S such that for every V’ (possibly cheating) S, with oracle access to V’, can simulate X_n without a witness w. Formally,

$$\{X_n\}_{n\in\mathbb{N}} \equiv_C \left\{S^{V'(.)}(x, 1^n)\right\}_{n\in\mathbb{N}}$$

Zero-Knowledge Proof

Trans(1^n,V',P,x,w,r_p,r_v) transcript produced when V' and P interact

- V' is given input x (the problem instance e.g., $A = g^x$
- P … r the claim e.g.,
- V' … espectively
- Se … yption schemes,

X_n … n over transcript

Simulator S is not given witness w

Oracle V'(x,trans) will output the next message V' would output given current transcript trans

(Blackbox Zero-Knowledge): There is a PPT simulator S such that for every V' (possibly cheating) S, with oracle access to V', can simulate X_n without a witness w. Formally,

$$\{X_n\}_{n\in\mathbb{N}} \equiv_C \{S^{V'(.)}(x, 1^n)\}_{n\in\mathbb{N}}$$

Zero-Knowledge Proof for DDH

$$\boldsymbol{A' = g^{y}, B' = B^{y}}$$

$$\boldsymbol{challenge\ c} \in \{\mathbf{0}, \mathbf{1}\}$$

Response $\boldsymbol{r} = \begin{cases} \boldsymbol{y} & \boldsymbol{if\ c = 0} \\ \boldsymbol{y} + x_1 & if\ c = 1 \end{cases}$

$$\boldsymbol{Decision\ d} = \begin{cases} \mathbf{1} & \boldsymbol{if\ c = 0\ and\ A' = g^{r}\ \ and\ B' = B^{r}} \\ \mathbf{1} & \boldsymbol{if\ c = 1\ and\ AA' = g^{r}}\ \ and\ B' = B^{r}/Z \\ 0 & otherwise \end{cases}$$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Alice (prover);
$\mathbf{x_1}$ **(or** $\mathbf{x_2}$**)**
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Zero-Knowledge Proof for DDH

$$\boldsymbol{A' = g^y, B' = B^y}$$

$\boldsymbol{challenge\ c \in \{0,1\}}$

Response $\boldsymbol{r} = \begin{cases} \boldsymbol{y} & \boldsymbol{if\ c = 0} \\ \boldsymbol{y} + x_1 & if\ c = 1 \end{cases}$

$\boldsymbol{Decision\ d} = \begin{cases} \mathbf{1} & \boldsymbol{if\ c = 0\ and\ A' = g^r\ \ and\ B' = B^r} \\ \mathbf{1} & \boldsymbol{if\ c = 1\ and\ AA' = g^r}\ \ and\ B' = B^r/Z \\ 0 & \quad otherwise \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Alice (prover);
$\mathbf{x_1}$ **(or** $\mathbf{x_2}$**)**
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Correctness: If Alice and Bob are honest then Bob will always accept

Zero-Knowledge Proof for DDH

$$A' = g^y, B' = B^y$$

$$challenge\ c \in \{0,1\}$$

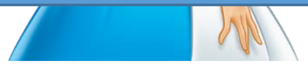
Response $r = \begin{cases} y & if\ c = 0 \\ y + x_1 & if\ c = 1 \end{cases}$

$$Decision\ d = \begin{cases} 1 & if\ c = 0\ and\ \boxed{A' = g^r\ \ and\ B' = B^r} \\ 1 & if\ c = 1\ and\ AA' = g^r\ \ and\ B' = B^r/Z \\ 0 & otherwise \end{cases}$$

(c=0)

$$g^r = g^y = A'$$

$$B^r = B^y = B'$$



Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Alice (prover);
$\mathbf{x_1}$ **(or** $\mathbf{x_2}$**)**
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Correctness: If Alice and Bob are honest then Bob will always accept

Zero-Knowledge Proof for DDH

(c=1)

$$\begin{aligned} g^r &= g^{y+x_1} \\ &= (g^y)g^{x_1} \\ &= AA' \end{aligned}$$

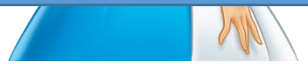
$$A' = g^y, B' = B^y$$

$$challenge\ c \in \{0,1\}$$

Response $r = \begin{cases} y & if\ c = 0 \\ y + x_1 & if\ c = 1 \end{cases}$

$$Decision\ d = \begin{cases} 1 & if\ c = 0\ and\ A' = g^r\ \ and\ B' = B^r \\ 1 & if\ c = 1\ and\ \boxed{AA' = g^r}\ and\ B' = B^r/Z \\ 0 & otherwise \end{cases}$$

Bob (verifier);
$A = g^{x_1}$,
B $= g^{x_2}$ and
$Z = g^{x_1 x_2}$



Alice (prover);
x_1 (or x_2)
$A = g^{x_1}$,
B $= g^{x_2}$ and
$Z = g^{x_1 x_2}$

Correctness: If Alice and Bob are honest then Bob will always accept

Zero-Knowledge Proof for DD

(c=1)

$$\boldsymbol{B^r/Z = g^{(y+x_1)x_2}/g^{x_1x_2}}$$
$$\boldsymbol{= g^{yx_2}}$$
$$\boldsymbol{= B'}$$

$$\boldsymbol{A' = g^y, B' = B^y}$$

$$\boldsymbol{challenge\ c \in \{0,1\}}$$

Response $r = \begin{cases} \boldsymbol{y} & \boldsymbol{if\ c = 0} \\ y + x_1 & if\ c = 1 \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1x_2}$

$$\boldsymbol{Decision\ d} = \begin{cases} \boldsymbol{1} & \boldsymbol{if\ c = 0\ and\ A' = g^r\ \ and\ B' = B^r} \\ \boldsymbol{1} & \boldsymbol{if\ c = 1\ and\ AA' = g^r}\ \ and\ \boxed{B' = B^r/Z} \\ 0 & \quad otherwise \end{cases}$$

Alice (prover);
x_1 (or x_2)
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1x_2}$

Correctness: If Alice and Bob are honest then Bob will always accept

Zero-Knowledge Proof for DDH

$$A' = g^y, B' = B^y$$

$$challenge\ c \in \{0,1\}$$

Response $r = \begin{cases} y & if\ c = 0 \\ y + x_1 & if\ c = 1 \end{cases}$

$$Decision\ d = \begin{cases} 1 & if\ c = 0\ and\ A' = g^r\ and\ B' = B^r \\ 1 & if\ c = 1\ and\ AA' = g^r\ and\ B' = B^r/Z \\ 0 & otherwise \end{cases}$$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

Alice (prover);
x_1 (or x_2)
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

Soundness: If $Z \neq g^{x_1 x_2}$ then (honest) Bob will reject w.p. ½ (even if Alice cheats)

Zero-Knowledge Proof f

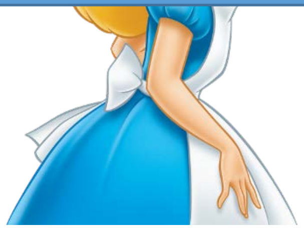
Case 1: for all y either

$A' \neq g^y$ or $B' \neq B^y$

$\rightarrow Pr[reject] \geq Pr[c=0] = \frac{1}{2}$

$A' = g^y$

$challenge\ c \in \{0, 1\}$



Response $r = \begin{cases} y & if\ c = 0 \\ y + x_1 & if\ c = 1 \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
$B = g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

$$Decision\ d = \begin{cases} 1 & if\ c = 0\ and\ \boxed{A' = g^r\ and\ B' = B^r} \\ 1 & if\ c = 1\ and\ AA' = g^r\ and\ B' = B^r/Z \\ 0 & otherwise \end{cases}$$

Alice (prover);
x_1 (or x_2)
$A = g^{x_1}$,
$B = g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

Soundness: If $Z \neq g^{x_1 x_2}$ cheats then (honest) Bob will reject w.p. ½ (even if Alice cheats)

Zero-Knowledge Proof for

Case 1: $A' = g^y$ and, $B' = B^y$

If Bob accepts (c=1) then

1) r =x_1+y since

$\rightarrow AA' = g^{y+x_1}$

2) $Z = {B^r}/{B'} =$

$g^{x_2(x_1+y)-yx_2} = g^{x_2(x_1)}$

$A' = g^y, B' =$

challenge $c \in \{0$

Response $r = \begin{cases} y & if\ c \\ y + x_1 & if \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
B $= g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

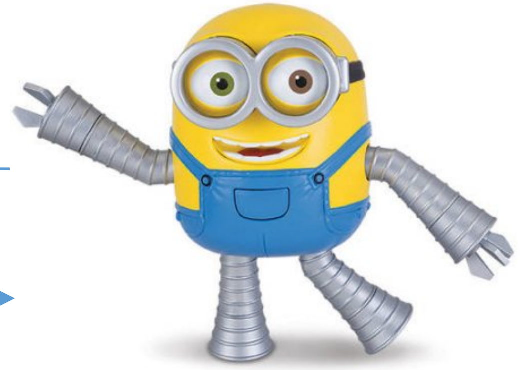
$$Decision\ d = \begin{cases} 1 & if\ c = 0\ and\ A' = g^r\ \ and\ B' = B^r \\ 1 & if\ c = 1\ and\ AA' = g^r\ \ and\ \boxed{B' = B^r/Z} \\ 0 & otherwise \end{cases}$$

x_1 (or x_2)
$A = g^{x_1}$,
B $= g^{x_2}$ and
$Z \neq g^{x_1 x_2}$

Soundness: If $Z \neq g^{x_1 x_2}$ cheats then (honest) Bob will reject w.p. ½ (even if Alice cheats)

Zero-Knowledge Proof for DDH

$$\begin{cases} A' = g^y, B' = B^y & \text{if b=0} \\ A' = g^y/A, B' = \frac{B^y}{Z} & \textit{otherwise} \end{cases}$$



$$\textit{challenge } c \in \{0, 1\}$$

Response $r = \begin{cases} y & \textit{if c=b} \\ \perp & \textit{otherwise} \end{cases}$

$$\textit{Decision } d = \begin{cases} 1 & \textit{if } c = 0 \textit{ and } A' = g^r \textit{ and } B' = B^r \\ 1 & \textit{if } c = 1 \textit{ and } AA' = g^r \textit{ and } B' = B^r/Z \\ 0 & \textit{otherwise} \end{cases}$$

Bob (verifier);
$A = g^{x_1}$,
$B = g^{x_2}$ and
$Z = g^{x_1 x_2}$

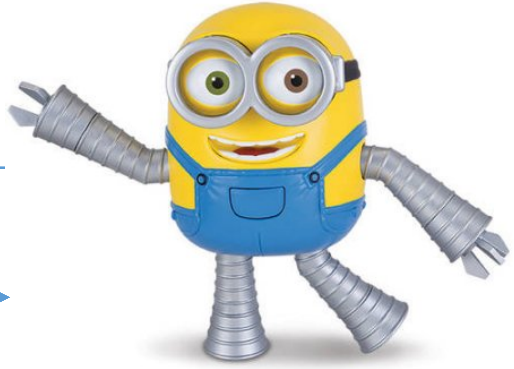
Simulator;
Cheat bit b,
Random y
$A = g^{x_1}$,
$B = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Zero-Knowledge: Simulator can produce identical transcripts (Repeat until $r \neq \perp$)

Zero-Knowledge Proof for DDH

$$\begin{cases} A' = g^y, B' = B^y & \text{if b=0} \\ A' = g^y/A, B' = \frac{B^r}{Z} & \textit{otherwise} \end{cases}$$

$\textit{challenge } c \in \{0,1\}$



Response $r = \begin{cases} y & \textit{if c=b} \\ \perp & \textit{otherwise} \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

$$\textit{Decision } d = \begin{cases} 1 & \textit{if } c = 0 \textit{ and } A' = g^r \textit{ and } B' = B^r \\ 1 & \textit{if } c = 1 \textit{ and } AA' = g^r \textit{ and } B' = B^r/Z \\ 0 & \textit{otherwise} \end{cases}$$

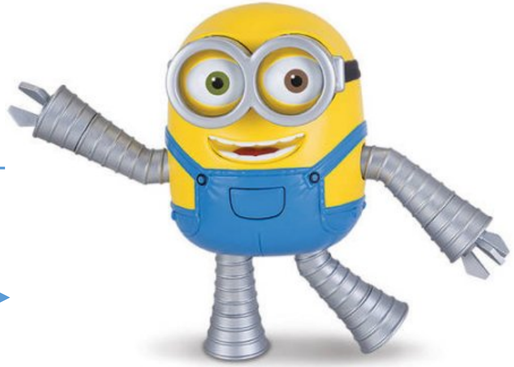
Simulator S;
Cheat bit b,
Random y
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Zero-Knowledge: If this is a valid tuple then $\{X_n\}_{n\in\mathbb{N}} \equiv \{S^{V'(.)}(x, 1^n)\}_{n\in\mathbb{N}}$

Zero-Knowledge Proof for DDH

$$\begin{cases} \boldsymbol{A' = g^y, B' = B^y} & \textbf{if b=0} \\ \boldsymbol{A' = g^y/A, B' = \frac{B^r}{Z}} & \boldsymbol{otherwise} \end{cases}$$

$$\boldsymbol{challenge\ c \in \{0,1\}}$$



Response $\boldsymbol{r} = \begin{cases} \boldsymbol{y} & \boldsymbol{if\ c{=}b} \\ \perp & otherwise \end{cases}$

Bob (verifier);
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

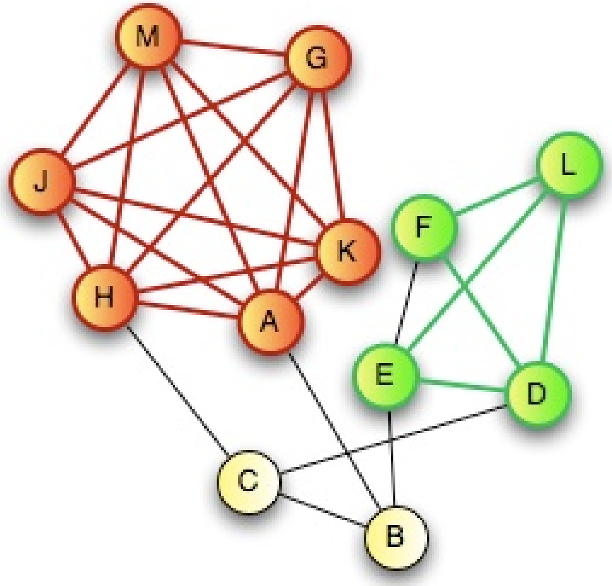
$$\boldsymbol{Decision\ d} = \begin{cases} \mathbf{1} & \boldsymbol{if\ c = 0\ and\ A' = g^r\ \ and\ B' = B^r} \\ \mathbf{1} & \boldsymbol{if\ c = 1\ and\ AA' = g^r}\ \ and\ B' = B^r/Z \\ 0 & otherwise \end{cases}$$

Simulator;
Cheat bit b,
Random y
$A = g^{x_1}$,
$\mathrm{B} = g^{x_2}$ and
$Z = g^{x_1 x_2}$

Zero-Knowledge: If this is NOT a valid tuple then $\{X_n\}_{n\in\mathbb{N}} \equiv_C \left\{S^{V'(.)}(x, 1^n)\right\}_{n\in\mathbb{N}}$

(Otherwise, we can use distinguisher to break DDH)

Zero-Knowledge Proof for all NP

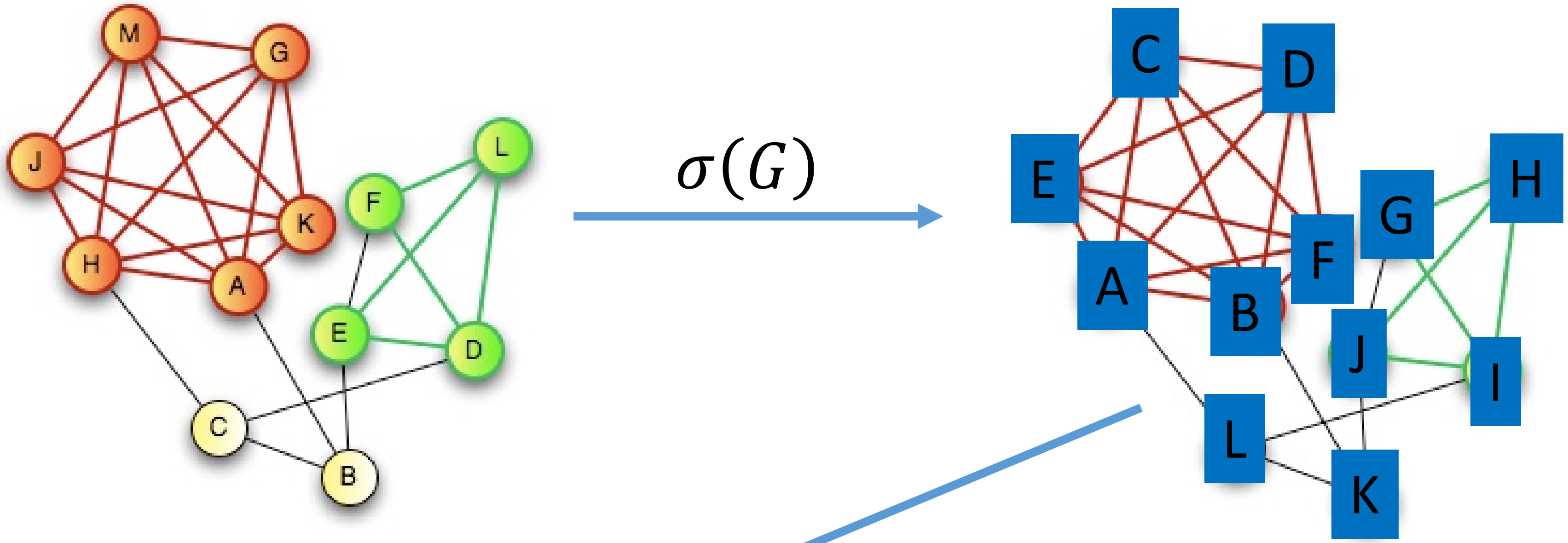


- CLIQUE
  - Input: Graph G=(V,E) and integer k>0
  - Question: Does G have a clique of size k?

- CLIQUE is NP-Complete
  - Any problem in NP reduces to CLIQUE
  - A zero-knowledge proof for CLIQUE yields proof for all of NP via reduction

- Prover:
  - Knows k vertices $v_1,\ldots,v_k$ in G=(V,E) that form a clique

Zero-Knowledge Proof for all NP



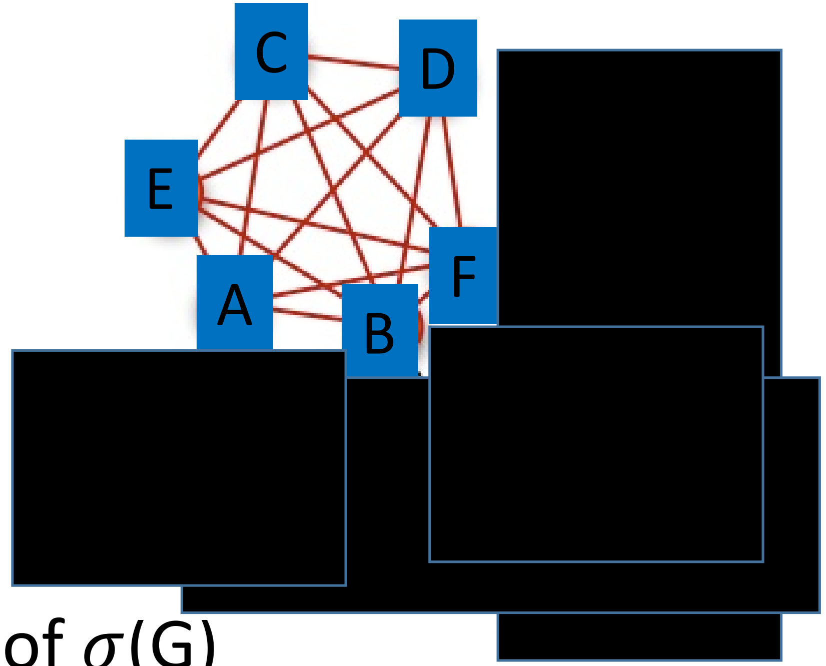
Adjacency matrix $A_{\sigma(G)}$

$$\begin{array}{c|ccc} & A & & L \\ \hline A & & & \\ & & \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 0 \end{pmatrix} & \\ L & & & \end{array}$$

Commitment to $A_{\sigma(G)}$

$$\begin{array}{cc} & \begin{array}{ccc} A & & L \end{array} \\ \begin{array}{c} A \\ \\ L \end{array} & \begin{pmatrix} Com(0, r_{A,A}) & \cdots & Com(1, r_{A,L}) \\ \vdots & \ddots & \vdots \\ Com(1, r_{L,A}) & \cdots & Com(0, r_{L,L}) \end{pmatrix} \end{array}$$

Zero-Knowledge Proof for all NP



- Prover:
  - Knows k vertices $v_1, \ldots, v_k$ in G=(V,E) that for a clique

1. Prover commits to a permutation σ over V
2. Prover commits to the adjacency matrix $A_{\sigma(G)}$ of σ(G)
3. Verifier sends challenge c (either 1 or 0)
4. If c=0 then prover reveals σ and adjacency matrix $A_{\sigma(G)}$
    1. Verifier confirms that adjacency matrix is correct for σ(G)
5. If c=1 then prover reveals the submatrix formed by first rows/columns of $A_{\sigma(G)}$ corresponding to $\sigma(v_1), \ldots, \sigma(v_k)$
    1. Verifier confirms that the submatrix forms a clique.

Zero-Knowledge Proof for all NP

- **Completeness**: Honest prover can always make honest verifier accept
- **Soundness**: If prover commits to adjacency matrix $A_{\sigma(G)}$ of σ(G) and can reveal a clique in submatrix of $A_{\sigma(G)}$ then G itself contains a k-clique. Proof invokes binding property of commitment scheme.
- **Zero-Knowledge:** Simulator cheats and either commits to wrong adjacency matrix or cannot reveal clique. Repeat until we produce a successful transcript. Indistinguishability of transcripts follows from hiding property of commitment scheme.

Next Class: Multiparty Computation

- Read Wikipedia entry on Garbled Circuits
- https://en.wikipedia.org/wiki/Garbled_circuit