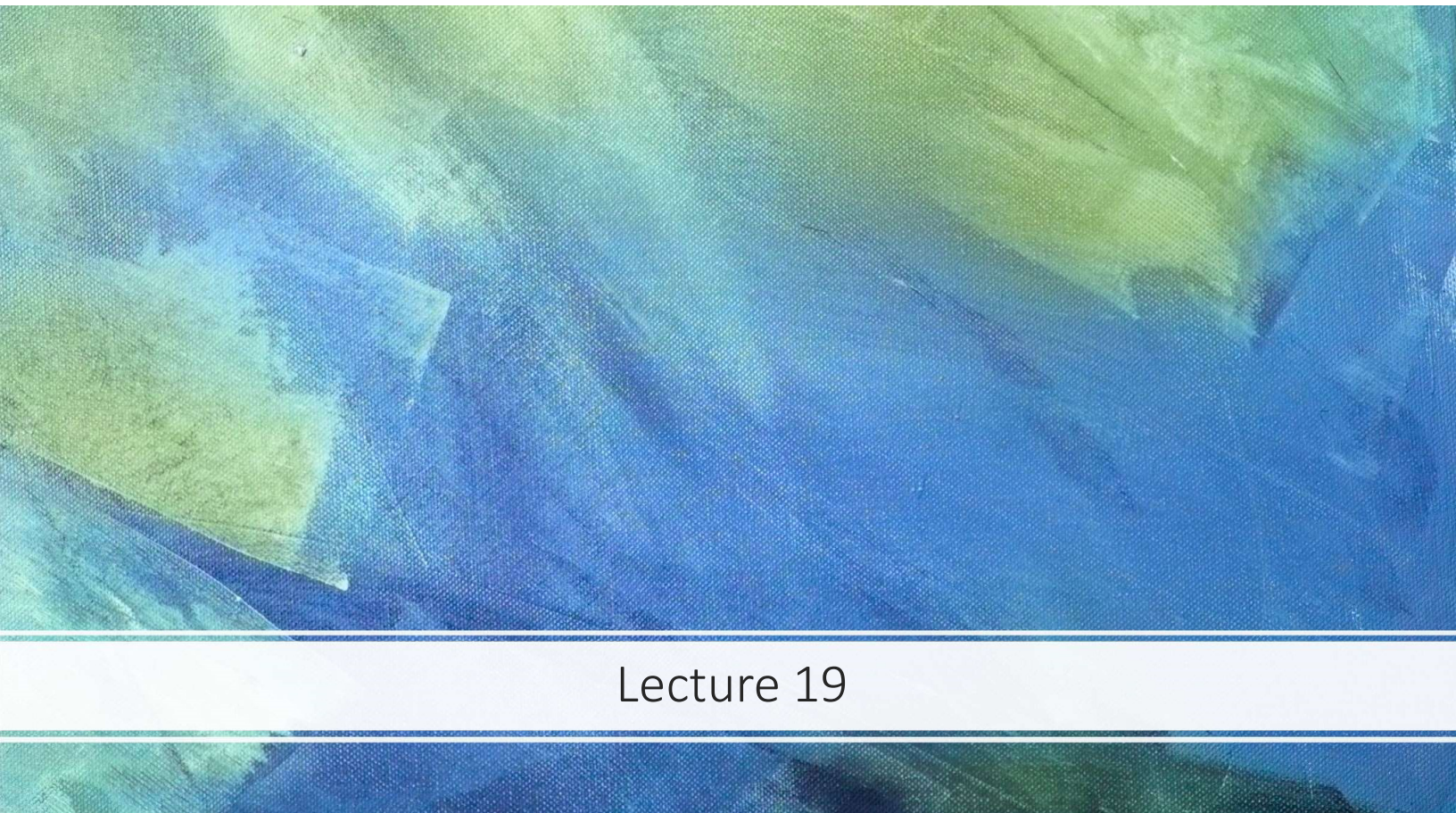
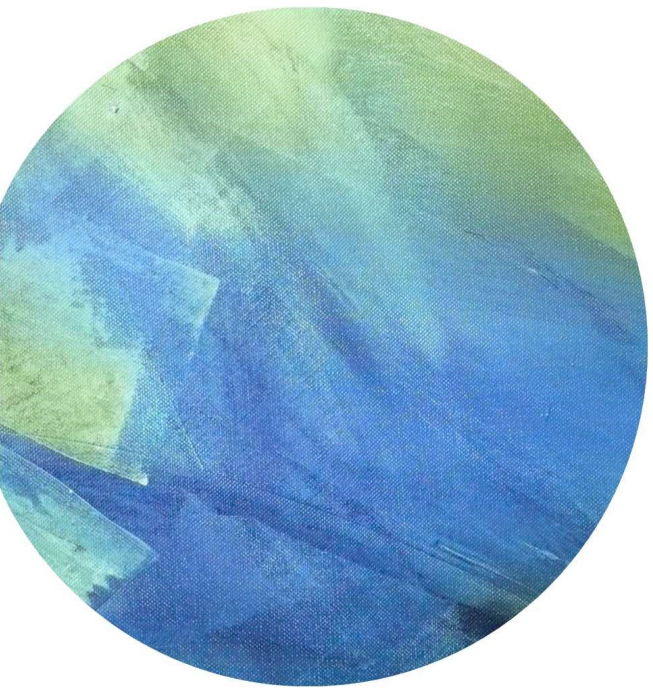

Lecture 19



Outline

NIZKs from pairings

Recall: Pairings

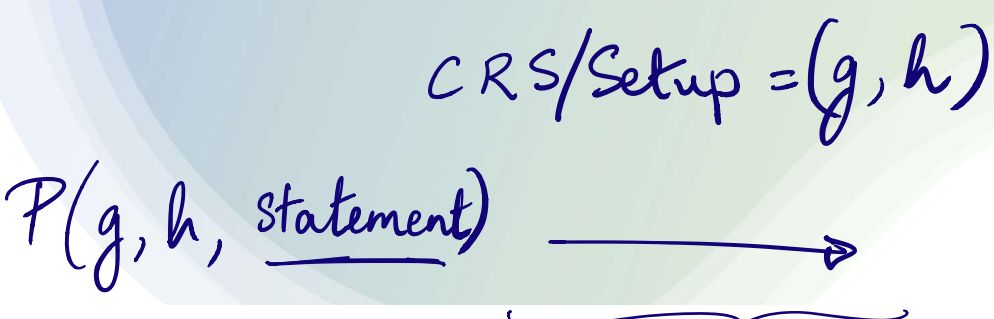
Pairing-based cryptography

- A pairing is an efficiently computable function e: $G_0 \times G_1 \rightarrow G_T$ such that:
  1. $g_T = e(g_0, g_1)$ is a generator of G_T
  2. For all $(u, u') \in G_0$ and $(v, v') \in G_1$,

     $e(u.u', v) = e(u,v).e(u',v)$ and $e(u, v.v') = e(u,v).e(u,v')$

- Consequences: $e(g_0^a, g_1^b) = e(g_0,g_1)^{ab} = e(g_0^b, g_1^a)$

Zero-Knowledge from Pairings



Another Assumption

- Subgroup Hiding Assumption
- Let G, G_T be cyclic groups of *composite* order N = pq
  Let (g, g_T) denote generators of (G, G_T), and define e: G x G → G_T
- Define $G_{(q)}$ to be the unique order-q subgroup of G (fact: such a subgroup exists!)
- Pick a generator g of G
- Set h_0 ← random generator of G, h_1 ← random generator of $G_{(q)}$
- Send (g, h_b) to Adv. Adv wins if it guesses b.

$G_{(q)} = \{1, g^p, g^{2p}, \ldots, g^{\alpha p}\}$

Commitments

- Commitments
- Public parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$)
- Commit (m;r) = $g^m h^r$
- This commitment is perfectly binding:
  - For all $m_1 \neq m_2$ in Z_p, Supp(Commit(m_1;r)) ∩ Supp(Commit(m_2;r)) = {}
- This commitment is computationally hiding:
  - By subgroup hiding, h ← Gen($G_{(q)}$) is indistinguishable from h ← Gen(G)
  - Perfectly hiding when h ← Gen(G)

$\{g^{m_1} h^r\}_r \cap \{g^{m_2} h^r\}_r$

$(0 \ldots p-1)$

$g^{\alpha p}$

g^{α} for $\alpha \leftarrow [N-1] / \{p, 2p, \ldots q, 2q \ldots\}$

$h \leftarrow Gen(G) \approx h = g^{\alpha}$ for random α.

$C = g^m h^r = g^{m + \alpha r}$ for random α.

Proof that a commitment is to 0 or 1

- Commitments
- Public parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$)
- Commit (m;r) = $g^m h^r$

- $c = \{g^0 h^r\}_r \cup \{g^1 h^r\}_r$ ⇔ $c \in G_{(q)}$ or $cg^{-1} \in G_{(q)}$

  ⇔ $e(c, cg^{-1})^q = \mathbf{1}_T$

$e(c, cg^{-1})^q$?

V shouldn't learn q!

If it did, would dist. Gen($G_{(q)}$) from Gen(G)
∴ break hiding of com

Proof that a commitment is to 0 or 1

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$

- Proof = (y_1, y_2, y_3) where
  - s ← Z_n* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

Verify (c, y_1, y_2, y_3) → check

- e (c, cg^{-1}) = e (y_1, y_2) and
- e (y_1, g) = e (h, y_3)

$e(y_1, g) = e(h, y_3)$

$e(y_1, g) = e(h, g^s)$

y_1 better be h^s for

$\Rightarrow$ y_1 is indeed h^s for some s

(and is not, say, g^{100}!)

Proof that a commitment is to 0 or 1: Soundness

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$

- Proof = (y_1, y_2, y_3) where
  - s ← Z_n^* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

Verify (c, y_1, y_2, y_3) → check

- e (c, cg^{-1}) = e (y_1, y_2) and
- e (y_1, g) = e (h, y_3)

$e(y_1, y_2) = e(h^s, u^{rt}) = e(h^r, u^{st}) = e(h^r, u)$ ($e(h,u)^{rst}$)

$= e(h^r, g^{2m-1} \cdot h^r)$

$m=0 \Rightarrow e(y_1, y_2) = e(h^r, g^{-1} \cdot h^r) = e(c, cg^{-1})$

$m=1 \Rightarrow e(y_1, y_2) = e(h^r, g \cdot h^r) = e(cg^{-1}, c) = e(c, g^{-1})$

If $m \notin \{0,1\}$, but P followed all proof steps correctly, i.e. $y_1 = h^s$, $y_2 = u^{rt}$ for $u = g^{2m-1} \cdot h^r$, $y_3 = g^s$.

Then want to show: V rejects the proof.

Proof that a commitment is to 0 or 1: Soundness

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$ $m \notin \{0,1\}$ say $m = 2$
- Proof = (y_1, y_2, y_3) where
  - s ← Z_n^* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

Verify (c, y_1, y_2, y_3) → check

- e (c, cg^{-1}) = e (y_1, y_2) and → FAIL!
- e (y_1, g) = e (h, y_3)

$e(y_1, y_2) = e(h^s, u^{rt}) = e(h^r, u^{st}) = e(h^r, u) = e(h^r, g^{2m-1} \cdot h^r)$

[Recall: $(h = g^{\alpha p})$ for some α.]

$= e(g^{\alpha pr}, g^{2m-1} g^{\alpha pr}) = e(g, g)^{(\alpha pr)(2m-1+\alpha pr)}$

$e(c, cg^{-1}) = e(g^m h^r, g^{m-1} h^r) = e(g, g)^{(m+\alpha pr)(m-1+\alpha pr)}$

Note: $(m+\alpha pr)(m-1+\alpha pr) = (\alpha pr)(2m-1+\alpha pr) \iff m \in \{0,1\}$ [No matter what value αpr takes]

Since $m < p$, one of these terms can be a multiple of p only when $m = 0$ or $m = 1$.

Proof that a commitment is to 0 or 1: Soundness

Statement : c is com(0) or com(1).

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$

- Proof = (y_1, y_2, y_3) where
  - s ← Z_n^* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

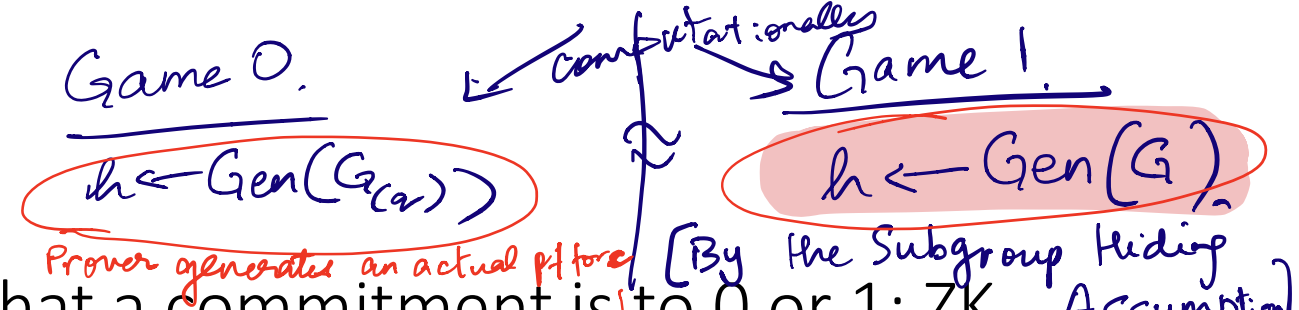
Verify (c, y_1, y_2, y_3) → check
- e (c, cg^{-1}) = e (y_1, y_2) and
- e (y_1, g) = e (h, y_3)

$e(y_1, y_2) = e(h^s, u^{rt}) = e(h^r, u^{st}) = e(h^r, u)$
$= e(h^r, g^{2m-1} \cdot h^r)$

Q1: What about provers that do NOT set $y_1 = h^s$ for some s?
2nd verification check WILL FAIL.

Q2: what about provers that do NOT set $y_2 = u^{rt}$? Say $y_2 = g^\beta$

$e(y_1, y_2) = e(h^s, g^\beta) = e(g, g)^{(\alpha ps)(\beta)} \overset{??}{=} e(g, g)^{(m+\alpha pr)(m-1+\alpha pr)} \leftarrow e(c, cg^{-1})$



Proof that a commitment is to 0 or 1: ZK

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$

- Proof = (y_1, y_2, y_3) where
  - s ← Z_n^* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

Verify (c, y_1, y_2, y_3) → check

- $e(c, cg^{-1}) = e(y_1, y_2)$ and
- $e(y_1, g) = e(h, y_3)$

$h \leftarrow Gen(G) \sim h = g^\alpha$ for $\alpha \leftarrow \{1, \ldots N-1\} / \{p, 2p \ldots q, 2q \ldots\}$

$g, h = g^\alpha, c = g^m h^r = g^{m+\alpha r}$: Perfectly hides m

Sim is given c & must generate a proof. Setup: $h = g^\alpha$.

$y_1 = c^r$ $y_2 = (cg^{-1})^{1/r}$ $\Leftrightarrow e(y_1, y_2) = e(c^r, (cg^{-1})^{1/r}) = e(c, cg^{-1})$

$e(y_1, g) = e(c, g)^r$. $e(h, y_3) = e(g^\alpha, g^{\frac{tr}{\alpha}}) = \ldots^{r/\alpha}$

(NOTE: FLIP c and cg^{-1} if c is NOT a generator but cg^{-1} is.)

Proof that a commitment is to 0 or 1: ZK

- Commitments
- Parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$). Commit (m;r) = c = $g^m h^r$

- Proof = (y_1, y_2, y_3) where
  - s ← Z_n^* , t = s^{-1} mod n , u = $g^{2m-1}h^r$
  - $y_1 = h^s$, $y_2 = u^{rt}$, $y_3 = g^s$

Verify (c, y_1, y_2, y_3) → check

- e (c, cg^{-1}) = e (y_1, y_2) and
- e (y_1, g) = e (h, y_3)

These Commitments are Homomorphic

- Commitments
- Public parameters: (g, h) where g ← Gen(G) and h ← Gen($G_{(q)}$)
- Commit (m;r) = $g^m h^r$

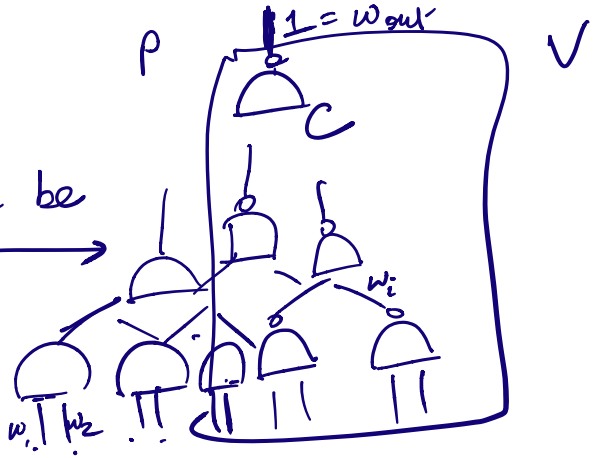
- These are homomorphic:

- Commit(m_1;r_1) . Commit(m_2;r_2) = g^{m1+m2} h^{r1+r2} = Commit(m_1+m_2;r_1+r_2)

Putting things together

FACT:

All statements can be converted →



Statement: Circuit *C* built from NAND gates.
Prove there exist assignments to wires $w = (w_1, w_2 \ldots w_{out})$ such that $C(w) = 1$

Proof: Commit to each bit w_i as $c_i = com(w_i; r_i)$. $= g^{w_i} h^{r_i}$

For the output wire w_{out} set $c = com(w_{out}; 0 \ldots 0) = g^1 \cdot h^{0 \ldots} = g$

Prove that all commitments c_i are to w_i in {0,1}

Putting things together

Statement: Circuit *C* built from NAND gates.

Prove there exist assignments to wires $w = (w_1, w_2 \ldots w_{out})$ such that $C(w) = 1$

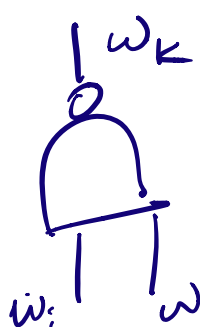
$\forall$ wires in the circuit

Proof: Commit to each bit w_i as $c_i = com(w_i; r_i)$.

For the output wire w_{out} set $c = com(w_{out}; 0 \ldots 0)$

Prove that all commitments c_i are to w_i in {0,1}

For every (NAND) gate in the circuit, with input wires w_i, w_j and output w_k, prove that c_k is a commitment to the NAND of w_i and w_j, where c_i is a com to w_i, and c_j is a com to w_j



$c_i c_j$
c_k

Putting things together

w_i	w_j	w_k
0	0	1
0	1	1
1	0	1
1	1	0

- For every NAND gate with input wires (i,j) and output wire k,
  $w_k = w_i$ NAND w_j $\Leftrightarrow$ $w_i + w_j + 2w_k - 2 \in \{0,1\}$

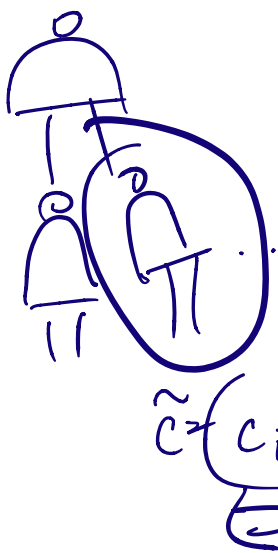
$c_i = com(w_i; r_i) = g^{w_i} h^{r_i}$ $\quad c_j = g^{w_j} h^{r_j}$ $\quad c_k = g^{w_k} h^{r_k}$

$$c_i \cdot c_j \cdot (c_k)^2 \cdot g^{-2} = \left(g^{(w_i + w_j + 2w_k - 2)} \cdot h^{r_i + r_j + 2r_k} \right) = \tilde{c}$$

HOMOMORPHIC PROOF COMMITMENT.

Why is this useful?

- Commit to each wire w_i in the circuit as $c_i = com(w_i; r_i)$
- For the output wire set $c_{out} = com\ (1; 00…0)$
- Prove that for every i, c_i is a commitment to 0 or 1



$\tilde{c} = com(w_i + w_j + 2w_k - 2)$

$\tilde{c} = (c_i c_j c_k^2 g^{-2})$ is a com to 0/1

w_k^2 w_i NAND w_j

Why is this useful?

- Commit to each wire w_i in the circuit as $c_i = com(w_i; r_i)$
- For the output wire set $c_{out} = com(1; 00…0)$
- Prove that for every i, c_i is a commitment to 0 or 1
- For all NAND gates with input wires (i,j) and output wire k, prove that $w_i + w_j + 2w_k - 2 \in \{0,1\}$
- Use homomorphism property:
  prover and verifier compute $c' = c_i\, c_j\, c_k^2\, g^{-2} = (g^{w_i + w_j + 2w_k - 2}).(h^{r_i + r_j + 2r_k})$
  prover proves that c' is a commitment to 0 or 1

V has $c_i = com(w_i)$ $c_j = com(w_j)$

How to compute $com(w_k)$? $\tilde{c} = c_i \cdot c_j$
$= com(w_i + w_j)$

$$w_i + w_j + 2w_k - 2 = 0.$$

$$2w_k = -w_i - w_j + 2.$$