Approach. composite-order pairing group

Let \( N = pq \) be a product of two large primes. \( N \) is public; \( p,q \) are secret.

Let \( G \) be a cyclic group of order \( N \). Then \( g_p := g^p \) generates a subgroup of order \( p \) and \( g_q := g^q \) generates a subgroup of order \( q \).

Boneh-Goh-Nissim:

**KeyGen: Sample** \( N = pq \) and pairing group \((G, GT, e)\) of order \( N \).

Sample \( x \leftarrow Z_N \). Let \( h = g_x^\ell \).

Output \( pk = (g,h) \) and \( sk = q \).

**Encrypt** \((pk, m)\): Sample \( r \leftarrow Z_N \) and set \( ct = h^r \cdot g^m \) (no need for \( g^\ell \)).

**Decrypt** \((sk, ct)\): Parse \( sk = q \) and \( ct = u \). Compute \( u^q \) and find \( m \) such that \( g_p^m = u^q \).

**Correctness:** \( (h^r \cdot g^m)^q = h^r \cdot g^m \cdot g_q^m = g_p^m \)

**Additive homomorphism:** \( (h_1^r \cdot g_1^m)(h_2^r \cdot g_2^m) = h_1^r \cdot h_2^r \cdot g_1^m \cdot g_2^m \)

**Multiplicative homomorphism:** \( e(h_1^r \cdot g_1^m, h_2^r \cdot g_2^m) = e(h_1^r, h_2^r) \cdot e(g_1^m, g_2^m) \)

encrypts \( m_1, m_2 \)
Security: relies on subgroup decision assumption

Hard to distinguish random element of subgroup from random element of full group:

\[(g, g^s, g^r) \approx (g, g^s, g^r)\] where \(r, s \in \mathbb{Z}_N\)

Non-interactive zero-knowledge (NIZK)

Zero-knowledge proofs: prove a statement \(X\) without revealing anymore about \(x\) other than fact that it is true

Syntax of NIZK proof system:

- **Setup** \(\rightarrow\) Outputs the common reference string \((crs)\)

- **Prove** \((crs, x, w) \rightarrow \pi\): Generates a proof that \(x \in L\)

- **Verify** \((crs, x, \pi) \rightarrow 0/1\): Checks whether proof is valid or not
Requirements:

- Completeness: If \( R(x, w) = 1 \), then
  \[
  \text{crs} \leftarrow \text{Setup} \\
  \pi \leftarrow \text{Prove} (\text{crs}, x, w) \\
  \Rightarrow \text{Verify} (\text{crs}, x, \pi) = 1
  \]

- Soundness: For all adversaries \( A \):
  \[
  \Pr [ x \notin L \text{ and } \text{Verify} (\text{crs}, x, \pi) = 1 : (x, \pi) \leftarrow A(\text{crs}) ] = \text{negl.}
  \]
  If \( A \) must be efficient, then we obtain argument systems.

- Zero-knowledge: There exists an efficient simulator \( S = (S_0, S_1) \) where for all efficient adversaries \( A \), \( |W_0 - W_1| = \text{negl.} \) where \( W_0 \) and \( W_1 \) are defined as follows:
  
  Real distribution: \( W_0 = \Pr [ A_{O_0}(\text{crs}, \cdot, \cdot) (\text{crs}) = 1 : \text{crs} \leftarrow \text{Setup} ] \)
  
  Simulated distribution: \( W_1 = \Pr [ A_{O_1}(\text{st}, \cdot, \cdot) (\text{crs}) = 1 : (\text{crs}, \text{st}) \leftarrow S_0 ] \)
  
  and \( O_0 (\text{crs}, x, w) \) outputs \( \text{Prove} (\text{crs}, x, w) \) if \( R(x, w) = 1 \)
  \[
  O_1 (\text{st}, x, w) \text{ outputs } S_1 (\text{st}, x, w) \text{ if } R(x, w) = 1
  \]

Take an NP relation \( R \). Let \( C \) be the circuit that computes \( R \).

If \( x \in L \), then there exists some \( w \) such that \( C(x, w) = 1 \).

Groth-Ostrovsky-Sahai (GOS) construction:

1. "Commit" to all of the wire values in the circuit
2. Prove that each output wire is the NAND of the input wires.
3. Open the output wire to a 1 (and the input wires associated with the statement)