Approach. composite-order pairing group.

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

Let $\mathbb{G}$ be a cyclic group of order N. Then $g_p := g^q$ generates a subgroup of order p and $g_q := g^p$ generates a subgroup of order q.

Boneh-Goh-Nissim:

KeyGen: Sample $N = pq$ and pairing group $(\underbrace{\mathbb{G}, \mathbb{G}_T}_{\text{both have order } N}, e)$ of order N.

Sample $x \xleftarrow{R} \mathbb{Z}_N$. Let $h = g_q^x$.

Output $pk = (g, h)$ and $sk = q$

Encrypt(pk, m): Sample $r \xleftarrow{R} \mathbb{Z}_N$ and set $ct = h^r \cdot g^m$ (no need for g^r)

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

Correctness: $(h^r \cdot g^m)^q = h^{rq} \cdot g^{mq} = g_p^m$

Additive homomorphism: $(h^{r_1} \cdot g^{m_1})(h^{r_2} \cdot g^{m_2}) = \underbrace{h^{r_1 + r_2} g^{m_1 + m_2}}_{\text{encrypts } m_1 + m_2}$

Multiplicative homomorphism: $e(h^{r_1} \cdot g^{m_1}, h^{r_2} \cdot g^{m_2})$

$$= \underbrace{e(h^{r_1}, h^{r_2} g^{m_2})\, e(g^{m_1}, h^{r_2})\, e(g^{m_1}, g^{m_2})}_{\text{encrypts } m_1 m_2}$$

<u>Security</u>: relies on subgroup decision assumption

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

$$(g, g_q^s, g_q^r) \overset{c}{\approx} (g, g_q^s, g^r) \quad \text{where } r, s \overset{R}{\leftarrow} \mathbb{Z}_N$$

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 $\longrightarrow$ Outputs the common reference string (crs)
- Prove (crs, x, w) $\longrightarrow \pi$: Generates a proof that $x \in \mathcal{L}$
- Verify (crs, x, π) $\rightarrow$ 0/1 : Checks whether proof is valid or not

Requirements:

- Completeness: If $R(x, w) = 1$, then

$$\left.\begin{array}{l} crs \leftarrow \text{Setup} \\ \pi \leftarrow \text{Prove}(crs, x, w) \end{array}\right. \Rightarrow \text{Verify}(crs, x, \pi) = 1$$

- Soundness: For all adversaries A:

$$\Pr\left[x \notin \mathcal{L} \text{ and Verify}(crs, x, \pi) = 1 : \begin{array}{l} crs \leftarrow \text{Setup} \\ (x, \pi) \leftarrow A(crs) \end{array}\right] = \text{negl.}$$

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: $W_0 = \Pr\left[A^{O_0(crs, \cdot, \cdot)}(crs) = 1 : crs \leftarrow \text{Setup}\right]$

Simulated distribution: $W_1 = \Pr\left[A^{O_1(st, \cdot, \cdot)}(crs) = 1 : (crs, st) \leftarrow S_0\right]$

and $O_0(crs, x, w)$ outputs $\text{Prove}(crs, x, w)$ if $R(x, w) = 1$] and $\perp$ otherwise
$O_1(st, x, w)$ outputs $S_1(st, x, w)$ if $R(x, w) = 1$

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

if $x \in \mathcal{L}$, 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)