Recall the DDH assumption: Let \( \text{Gen} \) be an algorithm s.t. \( \text{Gen}(1^k) \) outputs a group \( G \) of order \( q \) with generator \( g \).

\[
\begin{align*}
D_{\text{DDH}}(1^k) &= \{ (G, q, g) \leftarrow \text{Gen}(1^k); \ (\alpha, \beta) \leftarrow \mathbb{Z}_q^2 : G, q, (g, g^\alpha, g^\beta, g^{\alpha\beta}) \} \\
D_{\text{Random}}(1^k) &= \{ (G, q, g) \leftarrow \text{Gen}(1^k); \ (\alpha, \beta, \gamma) \leftarrow \mathbb{Z}_q^3 : G, q, (g, g^\alpha, g^\beta, g^\gamma) \}
\end{align*}
\]

Recall the El Gamal cryptosystem:

Key Gen \((1^k)\): Run \( \text{Gen}(1^k) \) to get \( G, q, g \). Pick \( x \leftarrow \mathbb{Z}_q \). Let \( A = g^x \).

Output \( sk = x \), \( pk = (A, (g, q, g)) \).

Encrypt \((m \in G, pk)\): Pick \( r \leftarrow \mathbb{Z}_q \). Output \( (R, P) = (g^r, A^r \cdot m) \).

Decrypt \(( (R, P), sk) \): Output \( m = \frac{P}{R^x} \).

Also recall the CCA2 security game:

\[
\text{Challenger} \\
\quad \rightarrow \quad pk \quad \rightarrow \quad A \\
\quad \leftarrow \quad C_1 \\
\quad \cdots \\
\quad m_1 \\
\quad \downarrow \\
\quad m_0, m_1 \\
\quad \downarrow \\
\quad C^* = \text{Enc}(m_0) \\
\quad \leftarrow \quad C_1 \neq C^* \\
\quad \cdots \\
\quad m_1 \\
\quad \leftarrow \quad b' \\
(C \text{ wins if } b' = b)
\]

Note that El Gamal is not CCA2-secure. Given \((R, P)\), we can form the related ciphertext \((Rg, PA)\), which is an encryption of the same message.
Cramer-Shoup Lite:

KeyGen (1^k): Run Gen(1^k) to get G, g, q.
Output \( \text{sk} = x, y \)
\( \text{pk} = A, B \quad (A = g^x, B = g^y) \)

Encrypt \((m \in G, \text{pk})\): Want Form \((R, P, T)\)
\(R = g^r, P = A^m, T = B^r\)

Cramer-Shoup Lite:

KeyGen (1^k): Output \( \text{sk} = x, y, \hat{g}, w \)
\( \text{pk} = A, B, \hat{g} \quad (A = g^x \hat{g}^y, B = g^x \hat{g}^w, \hat{g} \text{ another generator}) \)

Encrypt \((m, \text{pk})\): Output \((R, \hat{g}^r, P, T)\)
\(g^r, \hat{g}^r, A^m, B^m \)

Decrypt: Test if \( T = R^x \hat{g}^w \). If no, fail.
If yes, output \( m = R^x \hat{g}^y \).

This is CCA1-secure, but not CCA2-secure.

Thm: Cramer-Shoup Lite is CCA1-secure.

Intuition for reduction: We do not know sk but can still decrypt successfully.

Natural approach: On input a DDH tuple \((g, \hat{g}, R^x, \hat{R}^y)\),
- KeyGen: Compute sk, pk correctly (so we know sk).
- Respond to \(A\)'s queries: use Decrypt
- Prepare challenge ciphertext: \((R^x, \hat{R}^z, P^x, T^x)\)
  \( P^x = m (R^x)^y (\hat{R}^z)^y \)
  \( T^x = (R^x)^p (\hat{R}^z)^p \)

  - When \(A\) outputs \(b\), if \(b = b\), guess "DH". Else guess "random".

We want to show:

1. If input is DDH, ciphertext is correct encryption of \(m_b\), so \(A\) correctly guesses \(b\) with prob. \(\frac{1}{2} + \epsilon\), nonneg. \(\epsilon\).
2. If input is random, \(A\)'s view is independent of \(b\), so \(A\) correctly guesses \(b\) with prob. \(\frac{1}{2}\).
1. \((R^*, \hat{R}^*, \hat{R}^*, T^*)\)

\[
g^y = \hat{g}^{-m_b(R^*)^x \hat{g}^y} = m_b g^{r x + \alpha y}
= m_b g^{(x+\alpha y) r}
= m_b (g^x, \hat{g}^y)^r
= m_b A^r
\]

2. Let's show this for unbounded \(U\). \(U\) learns \(x\) from \(\hat{g} = g^x\), \(x + \alpha y\) from \(A\), and \(\hat{g}^x\) from \(B\).

**Claim:** \(U\) cannot find a ciphertext \((R, \hat{R}, P, T)\) where
\(T = R^r \hat{R}^*\) but \(T \neq B^r\).

From decryption queries, \(U\) learns \(x + \alpha y\) (which it already knows from \(A\)). Let
\(m_b = g^{m_b}\)
\(P^* = m_b (R^*)^x (\hat{R}^*)^y\).
\(U\) learns \(m_b + R x + \alpha y\), but \(m_b\) and \(m_b\) are equally likely.
The value \(R x + \alpha y\) is random given \(U\)'s view.

**Cramer-Shoup (Final Version):**

**Update** Lite version s.t.:

- **sk:** \(x, y, \hat{x}, \hat{y}, w, \hat{w}, w'\)
- **pk:** \(A, \hat{A}, B, \hat{B}, B', H\)

\((A = g^x \hat{g}^y, B = g^{\hat{x} w}, B' = g^{\hat{x'} w'})\)

**Enc** \((m, pk)\):

- Pick \(r\).
- \(R = g^r, \hat{R} = \hat{g}^r, P = m \cdot A^r, T = (B \cdot B')^r\)
- for \(\beta = H(R, \hat{R}, P)\)

\(H\) is a collision-resistant hash function (CRHF), i.e. it is hard to find \(x\) and \(x'\) s.t. \(x \neq x'\), \(H(x) = H(x')\). \(H\) has domain \(\mathbb{Z}_q\).

**Decrypt:** \(T^2 = R^{2 r} \hat{R}^{2 \alpha w} \hat{A}^{w} \hat{B}^{\alpha w} \). If yes, output \(m = \frac{\beta}{\hat{R}^r \hat{A}^r}\).

**Thm:** Cramer-Shoup is CCA2-Secure.

We don't give a proof, but the challenge ciphertext is \((R^*, \hat{R}^*, m_b(R^*)^x (\hat{R}^*)^y, (R^*)^{2 r} \hat{R}^{2 \alpha w} \hat{A}^{w} \hat{B}^{\alpha w})\).