**Uniform sampling**: Là một thuật toán hoặc quá trình để lấy ngẫu nhiên các giá trị từ một phạm vi nhất định sao cho mỗi giá trị có cùng xác suất xuất hiện. Khi thực hiện uniform sampling, mỗi phần tử trong phạm vi được chọn có khả năng xuất hiện với xác suất như nhau.

**Discrete Gaussian distribution:** Phân phối Gaussian rời rạc là một phân phối xác suất được sử dụng trong hệ mật mã dựa trên lưới. Nó có tính chất đặc biệt là không đồng nhất và được sử dụng để tạo ra ngẫu nhiên từ khoảng giá trị nhất định.

**Polynomial multiplication:** Nhân đa thức là một phép toán trong đa thức, nơi các đa thức được nhân với nhau để tạo ra một đa thức mới. Trong ngữ cảnh của hệ mật mã dựa trên lưới, việc nhân đa thức được sử dụng trong các phép toán liên quan đến xử lý và tính toán trên các đa thức.

**Rounding:** Là một phép làm tròn số trong toán học. Trong ngữ cảnh của hệ mật mã dựa trên lưới, phép làm tròn thường được sử dụng để áp dụng một giá trị số thực (ví dụ: số thực trong phạm vi 0 đến 1) vào một giá trị số nguyên gần nhất trong phạm vi cho trước.

**XOF (Extendable-Output Function):** Là một hàm băm đặc biệt cho phép đầu ra có thể mở rộng đến độ dài tùy ý. Trong giao thức Dilithium, các hàm XOF (SHAKE-128 và SHAKE-256) được sử dụng để mở rộng đầu vào thành các chuỗi ngẫu nhiên có độ dài mong muốn.

**Public key và signature:** Trong mật mã, public key (khóa công khai) được sử dụng để mã hóa thông tin và signature (chữ ký) được sử dụng để xác thực tính toàn vẹn và nguồn gốc của thông tin. Đối với giao thức Dilithium, đặc điểm quan trọng là kích thước của public key và signature được tối ưu hóa để làm cho chúng nhỏ nhất có thể.

**Ring và modulo:** Trong hệ mật mã dựa trên lưới, các phép toán thường được thực hiện trên các vòng (ring) và với phép chia lấy dư (modulo) của một số nguyên. Trong Dilithium, các phép toán được thực hiện trên vòng Zq[X]/(Xn + 1) với q = 223 − 2^13 + 1 và n = 256.