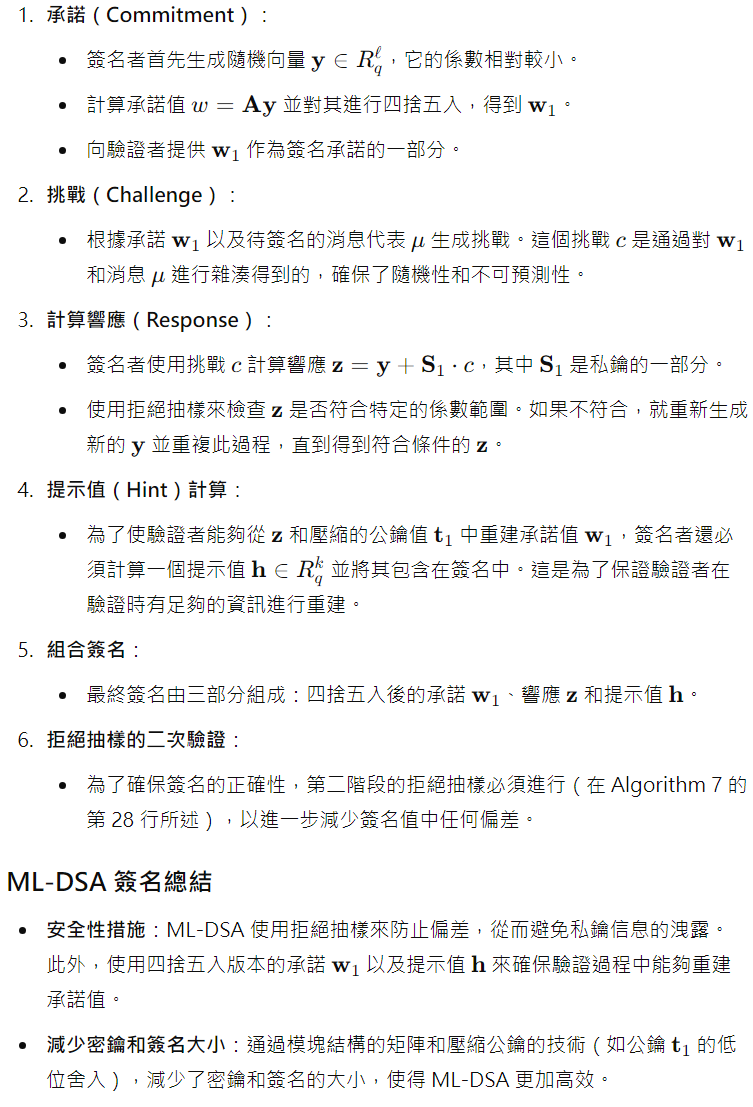
Fiat-Shamir With Aborts方法是什麼?



ML-DSA 簽名方案的步驟是什麼?



ML-DSA硬體加速辦法有哪些?

1. 使用DFT的變形NTT，並從memory-based與pipelined中選擇pipeliend，將NTT與INTT中會用到的bit-reverse用查表法替換
2. 根據Data flow graph去做硬體資源分配，將平行度提升到最高
3. 獨立的SHAKE-128和SHAKE-256 Hash模組