My section will cover the first half of Chapter 3 which is the heart of the paper. NEXT SLIDE.

A sigma protocol is an interactive proof of knowledge where a prover needs to prove that it knows some piece of information. Zero knowledge means it needs to prove this without revealing the information itself. As an example, consider Alice and Bob where Alice knows the password to a locked door in a cave with 2 paths. She randomly chooses a path. Bob, who doesn’t know which path she took, randomly shouts out one of the paths. If Alice is able to reliably return to the entrance using the path Bob randomly shouted out when this experiment is repeated many times, it is extremely likely that she knows the password to open the door in the cave that allows her to appear at either side. Note that she never reveals the password. The Fiat-Shamir Heuristic transforms this interactive proof of knowledge into a non-interactive Digital signature scheme with the use of a hash function that is modeled as a random oracle. NEXT SLIDE.

Now let’s discuss key generation. Here you can see the formula that will be used to find a secret ideal. O0 is a maximal order meaning it is the largest possible proper subset of the quaternion algebra that also forms a ring with addition and multiplication. Gamma is a random element of O0, ‘a’ is a random positive scalar less than Dsecret, i is the quaternion element such that i2 = -1. Dsecret acts as the norm of Isecret meaning it is the gcd of the elements of Isecret. Then alpha which connects Isecret to an equivalent ideal with a power of 2 norm called Jsecret is computed. NEXT SLIDE

Here you can see the computation of the secret isogeny from the secret ideal Jsecret, the maximal order O0, and B0, T, which is a basis for E0[T]. E0[T] is the T-torsion subgroup of E0 meaning the set of all points on E0 such that scalar multiplication with T yields infinity, the identity element. In SQISIGN we assume T is smooth meaning it has only small prime factors. For this case, an algorithm like the Pohlig-Hellman algorithm guarantees an efficient solution for basis finding. The public key, EA, is generated and is modified to map to this normalized curve. Then BA, T (a basis for EA’s T-torsion subgroup) is found by applying this secret isogeny to B0, T. NEXT SLIDE

Here P is one of the basis points for the intersection of the kernel of the secret isogeny and the 2f-Torsion subgroup of E0. The other basis point, Q, is found using the CompleteBasis algorithm. The generating point Q is mapped from where it is on E0 to a point on EA. After a few more steps, the signing key and public key are returned and the key generation phase is complete. NEXT SLIDE