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. O_0 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 O_0, 'a' is a random positive scalar less than D_{secret}, i is the quaternion element such that $i^2 = -1$. D_{secret} acts as the norm of I_{secret} meaning it is the gcd of the elements of

I_{secret}. Then alpha which connects I_{secret} to an equivalent ideal with a power of 2 norm called J_{secret} is computed. NEXT SLIDE

Here you can see the computation of the secret isogeny from the secret ideal J_{secret}, the maximal order O_0, and $B_{0, T,}$ which is a basis for $E_0[T]$. $E_0[T]$ is the T-torsion subgroup of E_0 meaning the set of all points on E_0 such that scalar multiplication with T yields infinity, the identity element. In SQI_{SIGN} 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, E_A, is generated and φ_{secret} is modified to map to this normalized curve. Then $B_{A, T}$ (a basis for E_A's T-torsion subgroup) is found by applying this secret isogeny to $B_{0, T}$. NEXT SLIDE

Here P is one of the basis points for the intersection of the kernel of the secret isogeny and the 2^f-Torsion subgroup of E_0. The other basis point, Q, is found using the CompleteBasis algorithm. The generating point Q is mapped from where it is on E_0 to a point on E_A. After a few more steps, the signing key and public key are returned and the key generation phase is complete. NEXT SLIDE