So now we start Chapter 3 which is concerned with the actual Digital Signature itself meaning it is basically the heart of the paper. NEXT SLIDE.

So to start, 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. This all is relevant for the signing stage. NEXT SLIDE.

But first let's discuss key generation. Here in the middle 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. O_0 specifically is isomorphic to the endomorphism ring of E_0 which is an elliptic curve with no x^2 term. 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 norms 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

The secret isogeny will map from the special elliptic curve E_0 to some E_A`. We compute 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. E_A` is normalized into E_A and φ_{secret} is modified to map to this normalized version. 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 consisting of the connecting quaternion alpha, the basis $B_{A,T}$, and the basis point Q are returned along with the public key, E_A, and thus the key generation phase is complete. NEXT SLIDE