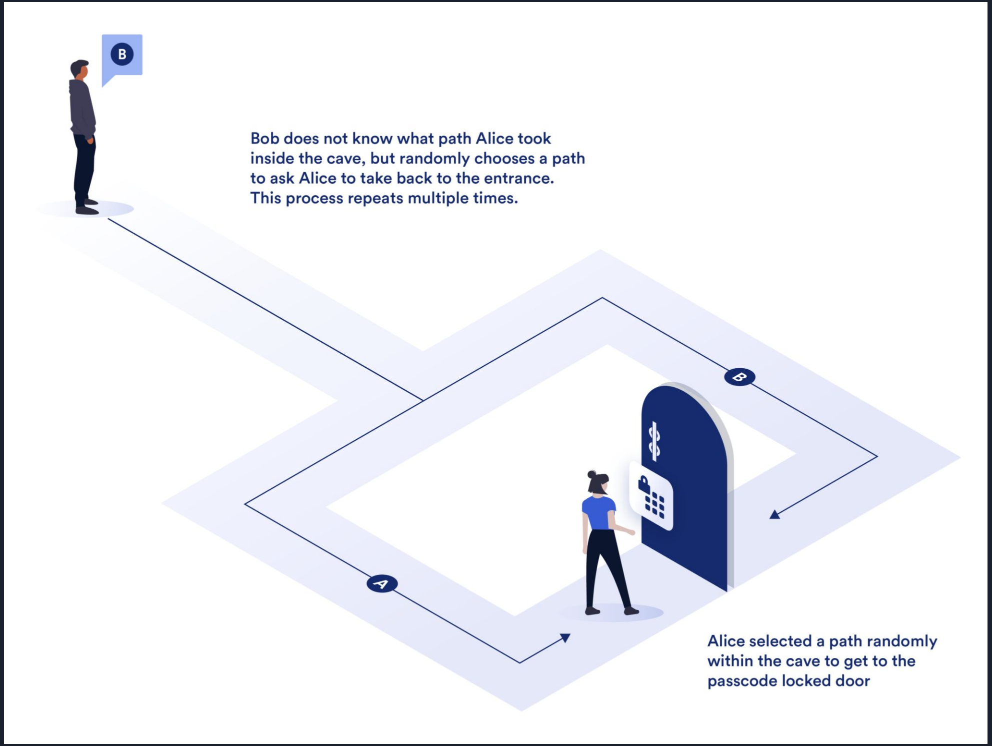
Chapter 3 - Signature

Section 3.1 - Σ-protocols and the Fiat-Shamir Heuristic

Interactive Proof of Knowledge

Zero-knowledge

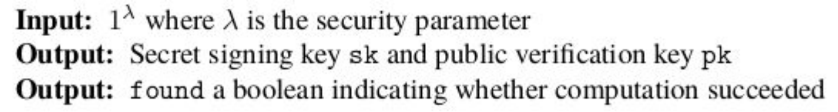


Bob does not know what path Alice took inside the cave, but randomly chooses a path to ask Alice to take back to the entrance. This process repeats multiple times.

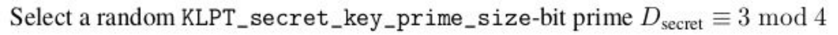
Alice selected a path randomly within the cave to get to the passcode locked door

Section 3.3 - Key Generation

SQIsign.KeyGen Algorithm



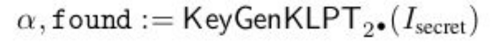
Input: 1^λ where λ is the security parameter
Output: Secret signing key $\texttt{sk}$ and public verification key $\texttt{pk}$
Output: $\texttt{found}$ a boolean indicating whether computation succeeded



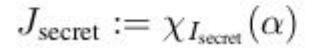
Select a random $\texttt{KLPT\_secret\_key\_prime\_size}$-bit prime $D_{\text{secret}} \equiv 3 \bmod 4$

Then a secret ideal is computed: $I_{\text{secret}} = \mathcal{O}_0\,(\gamma(a + i)) + \mathcal{O}_0(D_{\text{secret}})$

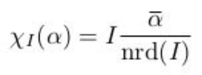
Connecting quaternion is found and used to find a connecting ideal



$\alpha, \texttt{found} := \mathsf{KeyGenKLPT}_{2^\bullet}(I_{\text{secret}})$



$J_{\text{secret}} := \chi_{I_{\text{secret}}}(\alpha)$



$\chi_I(\alpha) = I\dfrac{\bar{\alpha}}{\operatorname{nrd}(I)}$

Section 3.3 - Key Generation

$$\varphi_{\text{secret}}, \_, \texttt{found} := \mathsf{IdealToIsogenyEichler}_{2^\bullet}(J_{\text{secret}}, \mathcal{O}_0, B_{0,T})$$

$$E_0 : y^2 = x^3 + x$$

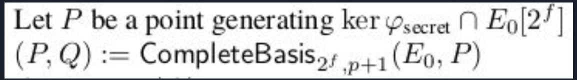
$B_{0,\,T}$ is a basis for $E_0[T]$, the T-torsion subgroup of E_0.

$$E_A, \varphi_{\text{secret}} := \mathsf{Normalized}(\varphi_{\text{secret}})$$

$$B_{A,T} := \varphi_{\text{secret}}(B_{0,T})$$

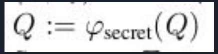
φ_{secret} maps $B_{0,\,T}$ to the basis for T-Torsion subgroup of E_A.

Section 3.3 - Key Generation



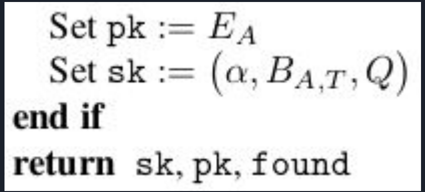
Let P be a point generating $\ker \varphi_{\text{secret}} \cap E_0[2^f]$
$(P, Q) := \mathsf{CompleteBasis}_{2^f, p+1}(E_0, P)$

P and Q are basis points.



$Q := \varphi_{\text{secret}}(Q)$

The secret isogeny is applied to Q.



```
    Set pk := $E_A$
    Set sk := $(\alpha, B_{A,T}, Q)$
end if
return sk, pk, found
```

The signing key (the knowledge) is the connecting quaternion, basis of T-torsion subgroup of E_A, and mapped basis point Q