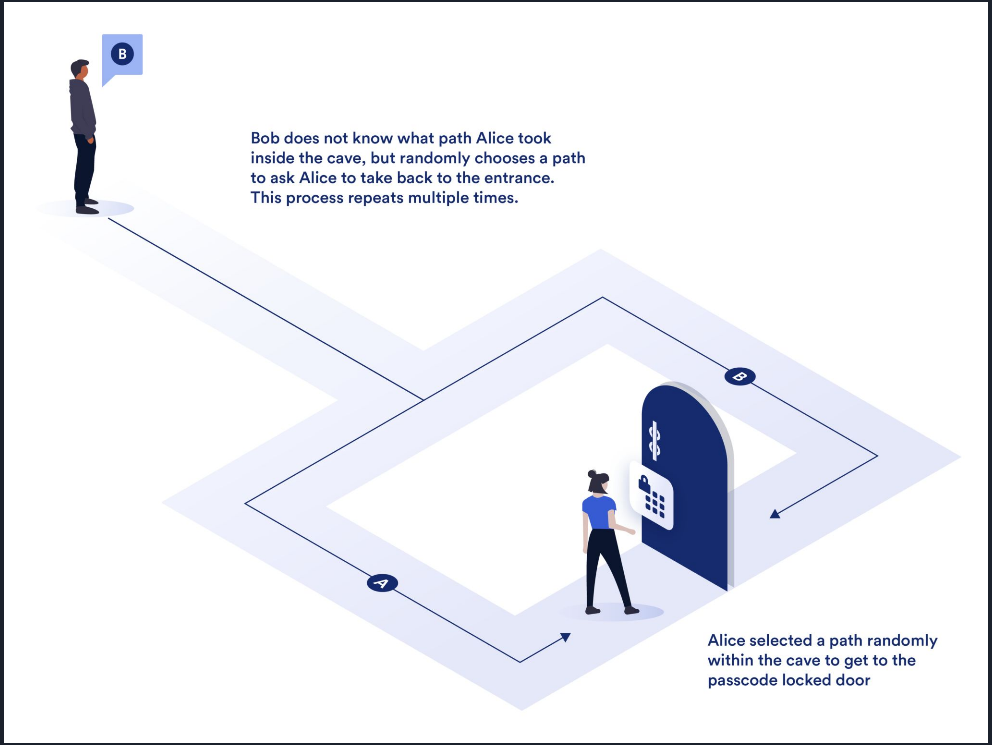
Chapter 3 - Signature

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

Interactive Proof of Knowledge

Zero-knowledge



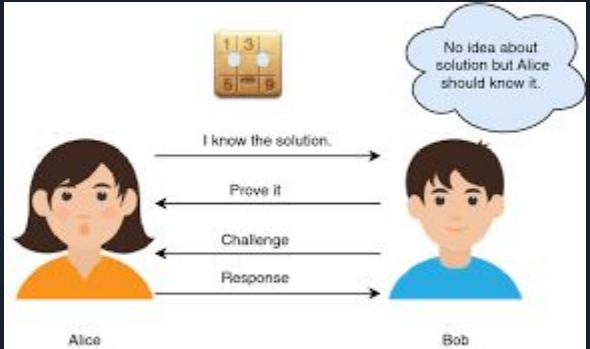
Endomorphism Ring

An endomorphism given an elliptic curve is an isogeny, $\varphi : E \rightarrow E$

$(f+g)(P) = f(P) + g(P)$

$(f \circ g)(P) = f(g(P))$

Three interactive phases



Public key: E_A

Private key (knowledge): $End(E_A)$

1) Commitment: Prover randomly generates $(E_1, End(E_1))$. Sends E_1 to verifier.
2) Challenge: Verifier randomly generates $\varphi_{chall} : E_1 \to E_2$ and sends φ_{chall} to prover.
3) Response: Prover uses $End(E_1)$ and φ_{chall} to compute $End(E_2)$. Then uses this and its knowledge to compute $\varphi_{resp} : E_A \to E_2$. Sends this to Verifier

Verifier who has the public key and E_2 can easily check if φ_{resp} is a correct isogeny

Fiat-Shamir Transform

Interactive to non-interactive proof of knowledge

Single signing and single verifying stage without explicit communication

Key difference is prover computes its own challenge using an unpredictable hash function that changes drastically for different commitments or different messages

Section 3.3 - Key Generation

SQIsign.KeyGen Algorithm

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

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

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

Connecting quaternion is found and used to find a connecting ideal

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

$$J_{\text{secret}} := \chi_{I_{\text{secret}}}(\alpha) \qquad \chi_I(\alpha) = I\frac{\overline{\alpha}}{\operatorname{nrd}(I)}$$

Section 3.3 - Key Generation

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

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

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

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

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

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

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