[Setup]

- $p = 2^{216}3^{137} - 1, E: y^2 = x^3 + 6x^2 + x \in F_{p^2}$
- $P_S, Q_S \in E[2^{216}]$, generator of $E[2^{216}], P_R, Q_R \in E[3^{137}]$, generator of $E[3^{137}]$

[Key generation]

- 개인키 $n_S \in \{1, \cdots, 2^{216} - 1\}$ 를 선택한 뒤 $S = P_S + n_S Q_S$ 연산한다
- 〈S〉를 커널로 하는 isogeny $\phi_S: E \to E_S: y^2 = x^3 + A'x^2 + x$를 연산한다.
- 공개키 : E_S, 개인키 : $n_S(\phi_S)$

[서명생성]

- INPUT : message, 개인키
- Output : (e, s)
- 256 개의 랜덤한 점 $R_0, \cdots, R_{255} \in E[3^{137}]$ 에서 선택한다.
- $\langle R_i \rangle$를 커널로 하는 isogeny $\phi_{\mathrm{R}_i}: E \to E_{\mathrm{R}_i}$ 를 연산한다.
- 각 i 에 대해 $\phi_{\mathrm{R}_i}(\mathrm{S})$와 $\phi_s(R_i)$ 를 연산한다.
- $\ker \beta_i = \langle \phi_s(R_i) \rangle$ 인 isogeny $\beta_i: E_S \to E_i$ 를 각 i 에 대해 연산한다.
- $r = \left(j(E_0)||\cdots||j(E_{255})\right)$ 로 하고, $e = H(r||m)$ 을 연산한다. 여기에서 j 는 j-invariant 를 의미하고, H 는 SHA-256 을 사용한다.
- $(b_0, \cdots, b_{255}) = e$ 로 하여, b_i를 0 또는 1 이라 한다.
- $s = (K_0, \cdots, K_{255})$를 다음과 같이 연산한다. $K_i = \begin{cases} \phi_{\mathrm{R}_i}(\mathrm{S}) & b_i = 0 \\ \phi_s(R_i) & b_i = 1 \end{cases}$
- 서명은 (e, s) 이다. $\left(E_{R_0}, \cdots, E_{R_{255}}\right)$를 검증자와 공유한다.

[서명검증]

- INPUT : (e', s'), message, 공개키
- Output : Valid, invalid
- 서명값 $e' = (b_0', \cdots, b_{255}')$ 와 $s = (K_0', \cdots, K_{255}')$ 를 이용해 다음과 같이 연산한다.
- 만약 $b_i' = 0$ 이면, $\ker \alpha_i = \langle K_i' \rangle$ 인 isogeny $\alpha_i: E_{\mathrm{R}_i} \to E_i$ 를 연산한다.
- 만약 $b_i' = 1$ 이면, $\ker \beta_i = \langle K_i' \rangle$ 인 isogeny $\beta_i: E_S \to E_i'$ 를 연산한다.
- $r = \left(j(E_0'), \cdots, j(E_{255}')\right)$ 로 한 뒤, $c = H(r||m)$ 을 연산한다. $c = e'$ 이면 valid, 그렇지 않으면 invalid 를 출력한다.