補足

オラクルが公開するポイント R が 1 回限りである必要性について

オラクルが公開する R は 1 回限りでなければいけません。まず、オラクルはランダムなシークレット k を用いて R を計算します。

$$R = kG$$

オラクルが同じシークレット k と R を用いて、署名を 2 回提出するとします (s_1, s_2)。この時

$$s_1 = k - h(m_1, R)v$$

$$s_2 = k - h(m_2, R)v$$

となりますが、2 つの式の両辺の差をとることにより、

$$s_1 - s_2 = (k - h(m_1, R)v) - (k - h(m_2, R)v) = -(h(m_1, R) - h(m_2, R))v$$

これは、オラクルの秘密鍵 v が

$$v = -(s_1 - s_2)/(h(m_1, R) - h(m_2, R))$$

で計算できてしまうことを意味します。