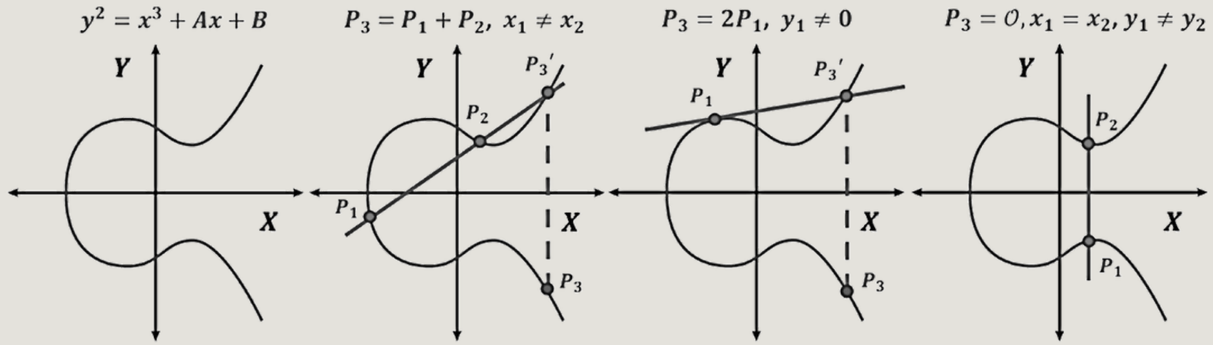
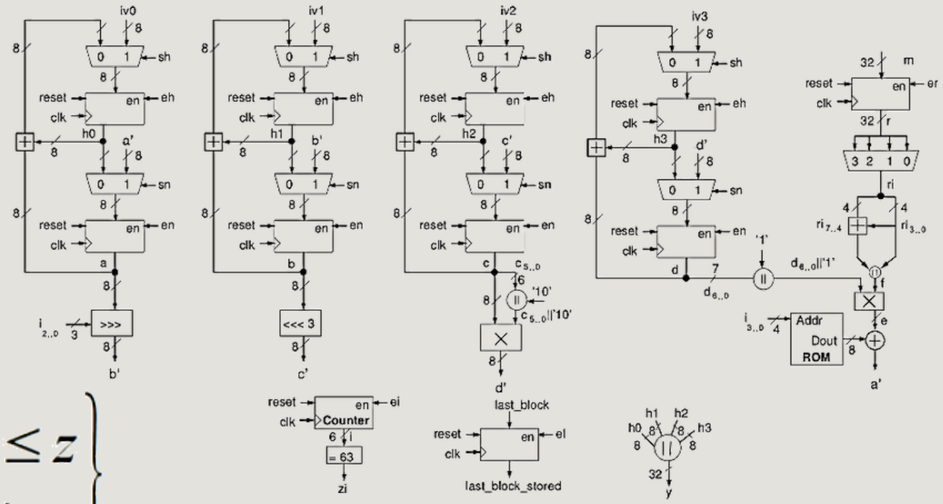
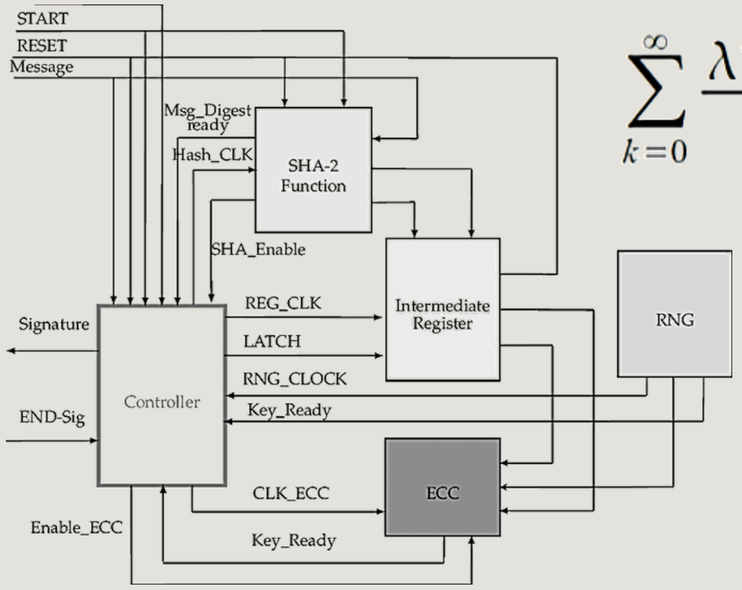
Disclaimer 2 : O que não veremos







$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

$$\sum_{i=0}^{32} 210{,}000 \frac{50}{2^i}$$

Algorithm 6 Split-ECDSA (SECDSA) signature generation
Input: message M, SCE-key $u \in \mathbb{F}_q^*$, PIN-key $\sigma \in \mathbb{F}_q^*$
Output signature (r, s).

1: Compute $\mathcal{H}(M)$ and convert this to an integer e.
2: Compute $e' = \sigma^{-1} \cdot e \bmod q$
3: Select random $k \in \{1, ..., q-1\}$
4: Compute $kG = (x, y)$ and convert x to integer $\bar{x}$
5: Compute $r = \bar{x} \bmod q$. If $r = 0$ go to Line 1
6: If $r \bmod q = 0$ then go to Line 1
7: Compute $s_0 = k^{-1}(e' + u \cdot r) \bmod q$. If $s_0 = 0$ go to Line 1
8: Compute $s = \sigma \cdot s_0 \bmod q$
9: Return (r, s)