

Temas de Álgebra

exame - parte prática


8 de fevereiro de 2023

Sejam q primo e E uma curva elíptica sobre \mathbb{Z}_q com $N = \#E$. Apresenta-se, de seguida, uma variante do sistema de assinatura digital Nyberg-Rueppel. Suponha que Alice pretende assinar a mensagem $M \in E$ e enviá-la, juntamente com a assinatura, a Bob. Alice escolhe $A \in E$ e $a \in \mathbb{Z}_N$. Determina $B = aA$. Torna públicos A e B e mantém privado a . Escolhe ainda uma função $f : E \rightarrow \mathbb{Z}_N$, que torna pública. Vai assinar a mensagem da seguinte forma:

- Escolhe k aleatório tal que $(k, N) = 1$.
- Calcula $R = M - kA$.
- Calcula $s = k^{-1}(1 - f(R)a) \pmod{N}$.
- A mensagem assinada é (M, R, s) .

Bob verifica a assinatura fazendo:

- Calcula $V_1 = sR - f(R)B$ e $V_2 = sM - A$.
- Declara válida a assinatura se $V_1 = V_2$.

1. Mostre que de facto é uma assinatura digital (ou seja, mostre que de facto $V_1 = V_2$).
2.  Implemente o protocolo no sagemath.

Fim