Problem 1: Universal hash functions

(a) Let $S$ be the set of all binary $\ell \times m$-matrices. I.e., $S = \mathbb{F}_2^{\ell \times m}$. Let $X$ be the set of all $m$-bit vectors. I.e., $X = \mathbb{F}_2^m$. Let $Y = \mathbb{F}_2^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := sx$.

Show that $F$ is a universal hash function.

Note: You may use the fact that for any fixed $z \neq 0$, and uniformly distributed $s \in \mathbb{F}_2^{\ell \times m}$, $sz$ is uniformly distributed on $\mathbb{F}_2^\ell$. (Bonus points if you prove that fact, too.)

(b) (Bonus problem) Let $S := X := \mathbb{F}_2^m$ be a finite field (encoded in the standard way as an $\mathbb{F}_2$ vector space). Let $\text{trunc}_\ell(x)$ denote the first $\ell$ bits of $x$. Let $Y := \{0, 1\}^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := \text{trunc}_\ell(sx)$.

Show that $F$ is a universal hash function.

Note: You may use that $\text{trunc}_\ell(a - b) = \text{trunc}_\ell(a) - \text{trunc}_\ell(b)$. (This is immediate from the encoding of $\mathbb{F}_2^m$.)

Problem 2: Concrete parameters

Consider the QKD scheme described in Definition 45 in the lecture notes. Theorem 5 in the lecture notes shows that the protocol is $\varepsilon$-secure for a certain $\varepsilon$ that depends on the protocol parameters.

Suggest a choice of parameters such that $\varepsilon \leq 2^{-80}$ and $\ell = 256$. How many qubits are transmitted for that choice?

Note: The parameter choice should be possible! That is, you need to make sure that there is a universal hash function $F$ and an error correcting code with the right parameters.

Note: For any integers $a, b > 0$ with $b < 2^a - 1$, there exists a so-called Reed-Solomon code with code words of length $a(2^a - 1)$, correcting $\lfloor b/2 \rfloor$ errors, and with syndrome length $ab$.

Note: You do not need to find an optimal solution.