Quantum Cryptography (spring 2023)	Dominique Unruh

Exercise Sheet 08

Out: 2023-04-03 Due: 2023-04-10

1 Universal hash functions

(a)

Knowlets:	UHF ProblemID: MatrixUHF
Time:	
Difficulty:	

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.)

Hint: $sx = sx'$ iff $s(x - x') = 0$.

(b)

Knowlets:	UHF ProblemID: FieldUHF
Time:	
Difficulty:	

Let $S := X := \mathbb{F}_{2^m}$ be a finite field (encoded in the standard way as an $\mathbb{F}_2$ vector space). Let $trunc_\ell(x)$ denote the first ℓ bits of x. Let $Y := \{0, 1\}^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := trunc_\ell(sx)$.

Show that F is a universal hash function.

Note: You may use that $trunc_\ell(a - b) = trunc_\ell(a) - trunc_\ell(b)$. (This is immediate from the encoding of $\mathbb{F}_{2^m}$.)