Quantum Cryptography (spring 2021)	Dominique Unruh
Exercise Sheet 10	
Out: 2021-04-26	Due: 2021-05-04

1 Alice and Bob are being clever

Alice and Bob had a few clever ideas. In each case, explain why the idea is not a good one.

(a)

Knowlets:	QKDIntro ProblemID: Laser
Time:	
Difficulty:	

Alice noticed that with a sufficiently strong laser pointer, she can make a beam that is still easily seen on the moon. Since Bob is on a holiday on the moon, they decide to do a key exchange. For this, they take an off-the-shelf QKD protocol (one that only requires that Alice sends randomly polarised photons, and that Bob measures in a random polarisation direction – no quantum computers needed). And as the photon source, Alice uses her laser pointer. That is, she sends short light flashes of the laser pointer through her polarisation filter as specified by the QKD protocol.

(b)

Knowlets:	QKDIntro ProblemID: Repeater
Time:	
Difficulty:	

Alice and Bob want to use some QKD protocol over a long distance (300 km). Unfortunately, all QKD protocols and implementations they know of do not manage to do more than 250 km (because otherwise the error rate on the channel would become too high). Fortunately, in the middle between Alice and Bob lives Charlie, an untrusted yet helpful person. To get rid of the errors, they let Charlie work as an amplifier: Each qubit is sent to Charlie, and Charlie measures the qubit and resends it using a fresh photon.

(c)

Knowlets:	QKDIntro ProblemID: CompressedQKD
Time:	
Difficulty:	

In a usual QKD protocol Alice would first send the qubits. Then she would wait for Bob to receive these. Then Alice sends the bases in which she produced the check qubits (or some other classical information needed for the check/purification/privacy amplification; this depends on the protocol they use). Alice and Bob decide to be more efficient and do a "compressed QKD". Since it is only Alice that sends something, anyway, she sends all information simultaneously. I.e., she sends the qubits and the

classical information at the same time (over the quantum and the authenticated classical channel, respectively) and thus achieves at least doubled throughput.

2 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:	

(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 $trunc_\ell(x)$ 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 $\mathbb{F}_{2^m}$.)