Quantum Cryptography (spring 2022) Dominique Unruh

Exercise Sheet 08

Out: 2022-05-11 Due: 2022-05-18

1 Missing claims from QKD proof (ctd.)

(a)

Knowlets:	RawKey ProblemID: CountTError
Time:	
Difficulty:	

In the practice we showed (or will show) that in our QKD protocol, after the Bell test and after measuring the n-bit raw key, we have

$$H_\infty(K_A|E)_{\rho_{raw}} \geq -\log(N2^{-n})$$

where $N := |\{xy \in \{0,1\}^{2n} : |xy| \leq t\}|$. (Note: $|xy|$ does not refer to the Hamming weight of xy here, but to the number of non-00 bitpairs.)

Show that $N \leq (3n+1)^t$.

Hint: Think of how you can compactly describe the bitstring xy with $|xy|$ by only telling where the non-00 pairs are, and then calculate how many such descriptions there are.

(b)

Knowlets:	RawKey, RawKeyKeyDiff ProblemID: RawKeyDiff
Time:	
Difficulty:	

In the lecture, we claimed that if $\rho \in S^{\text{test}}_{\text{Ideal}}$, and we measure A's and B's system in the computational basis, then with probability 1, we have $|K_A \oplus K_B| \leq t$.

Show that this is true.

Hint: If you have trouble, start small. First show it for a state $|\widetilde{xy}\rangle$ with $|xy| \leq t$. Then show it for a pure state $|\Psi\rangle$ that is a superposition of such $|\widetilde{xy}\rangle$ (like the ones that occur in the definition of $S^{\text{test}}_{\text{Ideal}}$. And then got for $\rho \in S^{\text{test}}_{\text{Ideal}}$.

2 Discrete Fourier Transform

In this problem, note that the indexes in the definition of the DFT start with 0. I.e., the top-left component of $D_N = N^{-1/2}\,(\!(e^{2i\pi kl/N})\!)_{kl}$ is $N^{-1/2}\,e^{2i\pi 00/N} = N^{1/2}$.

(a)

Knowlets:	DFT ProblemID: DFTUni
Time:	
Difficulty:	

Show that the $N \times N$-DFT D_N is unitary.

Hint: Show first that for $\tilde{\omega} \in \mathbb{C}$ with $\tilde{\omega}^N = 1$ and $\tilde{\omega} \neq 1$, we have $\sum_{k=0}^{N-1} \tilde{\omega}^k = 0$. (What is $\tilde{\omega} \cdot \left(\sum_{k=0}^{N-1} \tilde{\omega}^k\right)$?)

(b)

Knowlets:	DFT ProblemID: DFTFreq
Time:	
Difficulty:	

(Bonus) Let $N > 0$ be an integer. Let $r \in \{1, \ldots, N\}$ with $r \mid N$. Let $x_0 \in \{0, \ldots, r-1\}$. Let $|\Psi\rangle := t^{-1/2} \sum_{k=0}^{t-1} |x_0 + kr\rangle$ where t is a normalization factor and $t := N/r$.

(If $r = \operatorname{ord} a \mid N$ for some group element a, then $|\Psi\rangle$ is the post-measurement state we have in Shor's order-finding algorithm directly before applying the DFT D_N.)

Let D_N be the $N \times N$-DFT. Let $|\Psi'\rangle := D_N |\Psi\rangle$. Consider a measurement on $|\Psi'\rangle$ in the computational basis and let γ denote the outcome. Show that $\Pr[\frac{N}{r} \text{ divides } \gamma] = 1$. (In other words, if $N \nmid \gamma r$ then $|\langle \gamma | \Psi' \rangle|^2 = 0$.)

(That is, at least in the case where $\operatorname{ord} a \mid N$, the order finding algorithm returns a multiple of $N/\operatorname{ord} a$.)

Hint: Show first that for some $\tilde{\omega} \in \mathbb{C}$ and $t \in \mathbb{N}$ with $\tilde{\omega}^t = 1$ and $\tilde{\omega} \neq 1$, we have $\sum_{k=0}^{t-1} \tilde{\omega}^k = 0$.

Note: This was sketched in the lecture. You only get points if your proof goes beyond the sketch in the lecture in detail/rigor.