Solutions to Daily Due Oct 26 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

Problem 2 was the QKD pairs activity on discord, with nothing to solve. Encoding from lecture: in the L basis, $|\uparrow\rangle = 0$ and $|\rightarrow\rangle = 1$; in the V basis, $|\nwarrow\rangle = 0$ and $|\nearrow\rangle = 1$. The key facts: measuring a photon in the basis it was prepared in returns its bit with certainty; measuring it in the other basis returns 0 or 1 with probability $\frac{1}{2}$ each, and leaves the photon in the state measured.

Problem 1: Alice and Bob on paper

(1) Alice's photons. Combine her basis and bit using the encoding:

Photon	1	2	3	4	5	6	7	8
Alice's basis	L	V	V	L	V	L	L	V
Alice's bit	1	0	1	1	0	0	1	0
Alice sent	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$
Bob's basis	L	L	V	V	V	L	V	V
Same basis?	yes	no	yes	no	yes	yes	no	yes
Bob's bit	1	1	1	0	0	0	1	0

(2) The key. They keep the photons where the bases agree: photons $1, 3, 5, 6, 8$. On those, Bob's measurement is guaranteed to equal Alice's bit, and indeed his bits there $(1, 1, 0, 0, 0)$ match hers. The shared secret key is

$$1\,1\,0\,0\,0.$$

Photons 2, 4, 7 are discarded. (On those, Bob's bits $1, 0, 1$ happen to agree with Alice's on photons 2 and 7, but that is luck, not information, so they are thrown out.)

(3) Photon 2. Alice sent $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)$ and Bob measured in the L basis. The outcome is $|\uparrow\rangle$ (bit 0) or $|\rightarrow\rangle$ (bit 1), each with probability $\frac{1}{2}$. Bob happened to get 1. Nothing went wrong; the quantum rules say the outcome is random. It tells Bob nothing about Alice's bit because the *other* possibility, Alice sending $|\nearrow\rangle$ (bit 1), gives exactly the same 50/50 distribution in the L basis. The outcome is independent of which V-basis photon she sent.

(4) What Eve learns. The public conversation consists of the two lists of bases. So Eve learns which positions were kept $(1, 3, 5, 6, 8)$ and which basis each kept bit was encoded in. She does *not* learn the bits themselves: the bases alone say nothing about whether Alice chose 0 or 1 at each position. (She also can't go back and measure the photons in the right bases now: they were already absorbed by Bob's detector.)

Problem 3: how long is the key?

(1) Alice and Bob each choose L or V independently with probability $\frac{1}{2}$, so they agree with probability $\frac{1}{2}$.

(2) Each of the 16 photons survives independently with probability $\frac{1}{2}$, so the key length is binomial with $n = 16$ and $p = \frac{1}{2}$. The expected length is $16 \cdot \frac{1}{2} = 8$. The probability of exactly 8 is

$$\binom{16}{8}\left(\tfrac{1}{2}\right)^{16} = \frac{12870}{65536} \approx 0.196,$$

so roughly one pair in five gets a key of exactly the expected length; the rest get a bit more or a bit less. (Your actual key length is whatever it was.)

(3) For an expected 128 kept bits, Alice should send about $2 \cdot 128 = 256$ photons. In practice she sends somewhat more (say 300), since the length fluctuates (its standard deviation is $\sqrt{256 \cdot \frac{1}{2} \cdot \frac{1}{2}} = 8$), and since some kept bits will be sacrificed to check for Eve (problem 5).

Problem 4: Eve intercepts one photon

Alice sends $|\nearrow\rangle$ (bit 1 in the V basis).

(1) Eve's measurement in the L basis. $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$, so Eve gets

$$|\uparrow\rangle \text{ with probability } \tfrac{1}{2}, \qquad |\rightarrow\rangle \text{ with probability } \tfrac{1}{2},$$

and sends Bob a fresh $|\uparrow\rangle$ or $|\rightarrow\rangle$ accordingly. Either way, the diagonal photon Alice sent is gone.

(2) Bob's measurement in the V basis. Whichever photon Eve forwarded, it is an L-basis state, and both L-basis states are 50/50 in the V basis:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle), \qquad |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle).$$

So in either case Bob gets $|\nearrow\rangle$ (bit 1, as Alice intended) with probability $\frac{1}{2}$, and $|\nwarrow\rangle$ (bit 0, an error) with probability $\frac{1}{2}$. Overall Pr(Bob measures 1) $= \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$. Without Eve it would have been 1.

(3) If Eve had guessed V. She measures $|\nearrow\rangle$ in its own basis, gets $|\nearrow\rangle$ with certainty, and forwards an identical $|\nearrow\rangle$. Bob then measures 1 with certainty. Eve has learned the bit and left no trace. Eve's problem is that she can't tell in advance which basis to use, so she is in this lucky case only half the time.

Problem 5: catching Eve

(1) The $\frac{1}{4}$. Consider a photon where Alice and Bob used the same basis. Eve guesses a basis at random.

- With probability $\frac{1}{2}$ she guesses right. Then she measures Alice's bit exactly and forwards the same photon; Bob measures it correctly. No disagreement.
- With probability $\frac{1}{2}$ she guesses wrong. Then (as in problem 4) she forwards a photon from the wrong basis, and Bob's measurement is a coin flip, disagreeing with Alice with probability $\frac{1}{2}$.

So

$$\Pr(\text{disagree}) = \tfrac{1}{2} \cdot 0 + \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4}.$$

(2) Eve undetected. Each compared bit agrees with probability $\frac{3}{4}$, independently, so all 20 agree with probability

$$\left(\tfrac{3}{4}\right)^{20} \approx 0.0032,$$

about one chance in 315. Comparing more bits drives this down exponentially; with 100 bits it is about 3×10^{-13}. Note that this also costs Alice and Bob those bits (they are now public), which is one reason to send more photons than the key length requires.

(3) Bases versus bits. The bases carry no information about the key: they only say *which* positions survive, and (per problem 1(4)) each kept bit is equally likely to be 0 or 1 as far as Eve can tell. The timing also matters: the bases are announced only *after* Bob has measured, so Eve can no longer use them to choose the right measurement basis; the photons are gone. The bits, on the other hand, *are* the key. Announcing them would hand Eve the secret, and whatever Alice and Bob encrypt with it.