CSE610: Quantum Key Distribution and Communication

The *task* is for two communicating parties, "Alice" and "Bob", to possess the same long random binary string ρ without any other party knowing ρ. Once they have ρ, they can communicate messages x up to the length N of ρ with perfect secrecy via the classical **one-time pad** protocol:

- Alice sends $x' = x \oplus \rho$ to Bob.
- Bob, on receiving a string y' from Alice computes $y = y' \oplus \rho$.
- Presuming he and Alice stay "on the same page" of ρ, and that no mishaps befell the transmitted
  bits, it follows that $y = x$, so Bob can read what Alice sent.
- An eavesdropper can read x', but because ρ stays unknown and is completely random, having x' confers no information about x.

A big *cost* of this is that ρ can be used only once: if you also intercept $z' = z \oplus \rho$ then $x' \oplus z' = x \oplus \rho \oplus z \oplus \rho = x \oplus z$, so you have the difference of two well-formed plaintexts, from which much information about them can be inferred. So the one-time pad requires economical production of large numbers of random bits on demand.

A point of this to bear in mind is that the need for ρ presumes that Alice and Bob do not already have a secure channel for communication. They have only insecure channels that may be presumed no different from public reveal. The idea can work for multiple parties, which is why it is called quantum key *distribution* (QKD), but they must be told how many bits have been used by a communication involving only some of them in order to stay synchronized.

A third point is that communicating a *random* ρ is tantamount to communicating a message x. Thus the
task does not need to be immediately about communicating willful messages. It is also possible that ρ does not need to be received exactly. Plaintext messages x can be pre-processed by error-correcting codes (ECCs) as z so that damage to a moderately small proportion of bits still allows decoding x. Whether *quantum* ECCs can help with this part is getting ahead of the story. We will begin by supposing that Alice and Bob want to agree on ρ exactly.

A fourth point is that any sub-sequence of a random ρ is still random. Even if three-fourths of ρ gets wiped out, including (say) the whole first half, the leftover will still serve. This is an advantage over cases with ECCs on structured messages.

Entangle or Not?

In a perfect world, Alice would have a simple quantum solution. She would entangle pairs $|00\rangle + |11\rangle$ and send the second qubit to Bob, which they would both measure in the standard basis. By the postulates of quantum mechanics, Alice's results ρ will be perfectly random, and by entanglement, Bob will get the same results.

The zeroth problem is that willful entanglement is still relatively expensive. The first problem is that an eavesdropper, "Eve", can intercept and measure the qubits sent to Bob before sending them on.

- Her measuring them is the same to Alice as if Bob did.
- Bob will get Eve's measurement results. He could equally have gotten them himself, so he cannot tell the difference either.
- This is true even if Bob measures in a different basis from Eve.

Entanglement is indeed the basis of the second QKD proposal, by Artur Ekert of Oxford. But let's see the first, by Charles Bennett and Gilles Brassard in 1979--1984 (the **BB84** protocol).

BB84

The **nub** is that if Alice sends a qubit as $|0\rangle$ but Bob measures it as $|1\rangle$, then something affected it *en route*. What could have happened was an intermediary measuring it in the $|+\rangle, |-\rangle$ basis and getting either of those two results, whereupon Bob would have a 50-50 chance of getting $|1\rangle$ from his measurement. Likewise, if Alice sends $|+\rangle$ but Bob measures $|-\rangle$, then their privacy has been broken--though maybe by Mother Nature; i.e., not necessarily willfully.

The second "Quantum Fact" is that if the intermediary "Eve" measures in the $|0\rangle, |1\rangle$ basis, learning Alice's bit, then Bob will get the same bit but have no way to tell it has been read. Eve's measurement "collapses" what was already a basis state to the same basis state. This goes hand-in-hand with their being no bar on copying an unknown qubit value when it is known in advance to belong to a given orthonormal basis.

This raises the idea of leaving both Bob and Eve guessing as to which basis to measure in. When (a) Bob guesses right, (b) Eve guesses wrong, and (c) Eve's measurement flips the bit, Eve can be caught--if (d), this is a qubit that Bob and Alice "sacrifice" by publicly communicating their basis choices. Each of (a,b,c,d) is a potential halving of the **rate** of the protocol, meaning the proportion of valid bits of the eventual shared ρ to the total number N of qubits sent (by Alice).

Alice and Bob separately need a cost-effective way to generate truly-random bits to begin with. Each can do private measurements of qubits in the $|+\rangle$ state to get their private random strings. Tis is not part of the *task*, which is for Alice and Bob to agree on the *same* random string ρ. There are actually some non-trivial issues with getting truly-random bits that could be a separate topic, but we will presume this poses no difficulty.

Before the protocol begins, Alice and Bob agree on some matters of procedure, most particularly:

- which bits they will "sacrifice" as a test set T on which to catch Eve. The rule for T does not need to be kept secret; it can be "every odd bit of the good indices" (numbering bits from 0).
- what proportion e of errors/eavesdrops (i.e., flipped bits in T) they will tolerate. Maybe $e = 0$.

Here is the BB84 protocol:

1. Alice generates random binary strings $r \in \{0,1\}^N$ and $s \in \{|, /\}^N$.
2. For $i = 0$ to $N-1$:
   (a) if $s_i = |$ then Alice sends a qubit $\mathbf{q}_i = |0\rangle$ if $r_i = 0$; $\mathbf{q}_i = |1\rangle$ if $r_i = 1$.
   (b) if $s_i = /$ then Alice sends $\mathbf{q}_i = |+\rangle$ if $r_i = 0$ and $\mathbf{q}_i = |-\rangle$ if $r_i = 1$.
3. Bob independently generates a random string $s' \in \{|, /\}^N$ (this can be before or after Alice sends the qubits---either way, Eve cannot know s or s' at step 2).
4. For $i = 0$ to $N-1$:
   (a) if $s'_i = |$ then Bob measures $\mathbf{q}_i$ in the $|0\rangle, |1\rangle$ basis, recording $r'_i = 0$ for the outcome $|0\rangle$ and $r'_i = 1$ for the outcome $|1\rangle$.
   (b) if $s'_i = /$ then Bob measures $\mathbf{q}_i$ in the $|+\rangle, |-\rangle$ basis, recording $r'_i = 0$ for the outcome $|+\rangle$ and $r'_i = 1$ for the outcome $|-\rangle$.
5. Alice and Bob publicly reveal their strings s and s'. The set I of **good indices** are those i for which $s[i] = s'[i]$, that is, when Bob guessed to measure in the same basis Alice used.
6. Alice and Bob also reveal r_i and r'_i for $i \in I \cap T$.
7. If there are at most e indices $i \in I \cap T$ such that $r_i \neq r'_i$, then they **accept** the results. Else, they re-run the whole protocol from the start to try again.

Here is an example of a possible run and outcome---assuming no errors caused by Eve:

s	|	|	/	/	/	|	|	/	|	/	/	|
r	0	1	1	0	1	0	1	1	0	0	1	1
$\mathbf{q}$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve?												
s'	/	|	|	/	|	|	|	/	/	/	/	|
T				*			*			*		*
r'		1		0		0	1	1		0	1	1
ρ		1				0		1			1	

Alice and Bob were somewhat lucky to get a shared ρ of length 4 rather than 3 from $N = 12$. Mind you, if one of the four *ed bits in r' had been flipped, they would figure that since they have only a 1-in-4 chance of catching Eve on any one bit, then plausibly all four test bits are known to Eve, and hence would ear all bits of ρ were untrustable as well.

If Alice and Bob accept with $e = 0$, then they can be confident that there are no errors on $I \setminus T$ either. The final output ρ then is the substrings formed by the bits r_i (same as r'_i) for $i \in I \setminus T$. If they allow $e > 0$, then they can use **randomness extraction** to arrive at a shorter string ρ that is still random and with high probability reduces Eve's knowledge of ρ from e bits to nearly zero bits. (A simpler way, if they don't mind the final ρ having expected length $\Theta(N/\log N)$ rather than length proportional to N, is to apply the decoding function of a k-**error correcting code** to the good sequence, where $k = 4e|I \setminus T|$. This would subtract out Eve's expected knowledge of about k bits of the good sequence, assuming the proportion of eavesdrops on $I \setminus T$ is similar to that on $I \cap T$. The factor of 4 is because

Eve gets caught only one-fourth the time on the indices in I, when she guesses the wrong basis and the bit happens to flip. Note that I is random and unknowable to Eve at the time she could act, because it depends on how s' relates to s, and its subsequences of even and odd indices were likewise unknowable.)

Presuming success is achieved with $e = 0$ on T and $|T| = |I|/2$, the expected length of ρ is $0.25N$. The factor on N is the **rate**. This is because half the indices expect to be good, and we are sacrificing half for the test set. With smaller choices of T, rates over 27% have been reported. If $e = 1/32$ is tolerated, then the rate is knocked down to $1/8$ at most when T is half of I.

B92

This is the simplification that does away with Alice's random s and has her send $|0\rangle$ when $r_i = 0$ and $|-\rangle$ when $r_i = 1$ (or she could use $|+\rangle$ for that instead, as long as Bob knows which one she is using). Bob still has to guess which basis to measure each transmitted qubit in, and of course, what he gets depends on his choice of basis, which is according to his s' random string.

- If $s'_i = |$ and he gets $|1\rangle$, he knows that Alice could not have sent $|0\rangle$ in a clean run, so he figures Alice sent $|-\rangle$ and records $r'_i = 1$.
- If $s'_i = |$ and he gets $|0\rangle$, then a clean send could have been $|0\rangle$ or $|-\rangle$, so Bob punts.
- If $s'_i = /$ and Bob gets $|+\rangle$, then Alice could not have cleanly sent $|-\rangle$, so Bob figures it was $|0\rangle$
  and records $r'_i = 0$.
- If $s'_i = /$ and Bob gets $|-\rangle$, then it could have been $|0\rangle$ from Alice as well, so Bob punts.

Thus Bob records Alice's bit only in the 25% chance that he guesses the "wrong" basis and yet the bit still goes as Alice intended. That caps the rate at 0.25 even before we bring Eve into the picture. One good thing is that Bob's revealing the set I of indices on which he recorded bits does not give useful information to Eve in retrospect.

Unfortunately, the indices on which Bob punts cannot be used to catch Eve either. Note that Eve can never be caught if she guesses Alice sent $|0\rangle$ and uses the standard basis, or when she guesses Alice sent $|-\rangle$ and so uses the $\mathbf{X}$ basis. She will get the same as what Alice sent and not be detectable at all. So when Alice sends $|0\rangle$, the only way Eve can be caught is when she uses the $\mathbf{X}$ basis, Bob uses the standard basis, and Bob gets $|1\rangle$, which he records as $|-\rangle$ giving 1. Bob and Alice again have to sacrifice some of their good indices to see Eve's activity.

E91