11
quantum cryptography

In the preceding chapter we confronted the private key dilemma: once the private key was in the receiver's hands, the code is quite secret, but how to communicate the key itself? The progress made by using Euler's theorem could be erased by the power of quantum computers to factor very large numbers. But quantum thinking, itself, offers a solution. As stated by Nielsen and Chuang, "what quantum mechanics takes away with one hand, it gives back with the other: a procedure known as quantum cryptography ... exploits the principles of quantum mechanics to provide provably secure distribution of private information."[1]

Quantum physics allows a return to Fermat encryption, as it offers a secure communication scheme, so the secret code parameters, p and e, can be sent even though the code, itself, is not in place. Given the ability to send the code parameters, why not go ahead and send the secret message, itself? The answer resides in the probabilistic nature of quantum communication, and will, hopefully, become clear as the discussion proceeds.

The probabilistic nature of quantum communication is determined by three axioms; linear algebra foundations will prove to be quite useful.

11.1 quantum axioms

Quantum physics can be stated in an axiomatic structure; that is, all the results can be shown to follow logically from a limited number of axioms. There are only four

[1] Page 582, Quantum Computation and Quantum Information, Nielsen and Chuang.

axioms necessary, as in Nielsen and Chuang, but three will be enough for us in this chapter. The fourth deals with combining quantum units, and our cryptography excursion only requires us to work with one unit at a time; combination will be important, however, in the next chapter on synergy and production. The axioms take us to some strange places, and, for that reason, some physicists argue the structure is somehow incomplete. Nevertheless, the axioms are *very* predictive for physical phenomena and applications such as cryptography.

11.1.1 superposition

A quantum unit can be thought of as an electron or a photon or any other subatomic particle. The first axiom states that a quantum unit can be represented by a two element vector.

Definition 11.1 *a qubit is a two element vector with unit length.*

"Qubit" is short for quantum bit, and is distinguished from a classical bit (one or zero) in that it requires two numbers to describe.

Example 11.1 *Some examples of qubits are*

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Notice the example qubits all possess the unit length property, that is, vector multiplication of the transpose times the vector yields one.

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= 1 \\ \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}^T \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} &= \frac{1+1}{2} = 1 \end{aligned}$$

Actually, the length of a vector is defined as the square root of the transpose times the vector. Taking the square root doesn't matter when the answer is one, but sometimes it will, and we will have to be more careful.

Definition 11.2 *A complex number is written in the form $a + bi$ where a and b are real numbers and $i = \sqrt{-1}$ and is called an imaginary number.*

Qubits can be described using complex numbers.[2] For example, valid qubits are

$$\begin{bmatrix} i \\ 0 \end{bmatrix} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ -i \end{bmatrix}$$

[2] We won't really need complex qubits to accomplish quantum cryptography, but we will use them later when Euler's formula is in view. Besides they are just too beautiful to ignore.

For the calculation of the length of a vector with imaginary elements to make sense, a modification of vector multiplication is required.

Definition 11.3 *When transposing a vector (or matrix) with complex elements, change the sign on the imaginary part; this is called the complex conjugate of the vector.*

Use the complex conjugate to compute the length (actually the squared length) of the "imaginary" qubits.

$$\begin{aligned} \begin{bmatrix} i \\ 0 \end{bmatrix}^H &= \begin{bmatrix} -i & 0 \end{bmatrix} \\ \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ -i \end{bmatrix}^H &= \frac{1}{\sqrt{2}}\begin{bmatrix} -i & i \end{bmatrix} \end{aligned}$$

The superscript H means take the conjugate transpose; H stands for "Hermitian." when the vector (or matrix) has no complex elements, H means just the regular transpose. Now the computations of the length make sense.

$$\begin{aligned} \begin{bmatrix} i \\ 0 \end{bmatrix}^H \begin{bmatrix} i \\ 0 \end{bmatrix} &= \begin{bmatrix} -i & 0 \end{bmatrix}\begin{bmatrix} i \\ 0 \end{bmatrix} = -i^2 = 1 \\ \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ -i \end{bmatrix}^H \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ -i \end{bmatrix} &= \frac{1}{\sqrt{2}}\begin{bmatrix} -i & i \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} i \\ -i \end{bmatrix} = \frac{-i^2 - i^2}{2} = 1 \end{aligned}$$

The first axiom is called "superposition" because, as hard as it is to visualize, the qubit actually can be described by both numbers simultaneously. The numbers can describe the position, the charge, the angle or some other property of a subatomic unit. The simultaneous position, for example, is only resolved when the qubit is observed or "measured." Measurement is the third axiom; the next axiom describes how the quantum state is transformed to another state.

11.1.2 transformation

Matrix algebra and, in particular, matrix multiplication, describes the transformation of a quantum state.

Definition 11.4 *Transformation of a qubit occurs by multiplication by a* 2×2 *matrix; the operation maintains the unit length property of the qubit.*

Example 11.2 *Three important matrix transformations are known as the Pauli matrices (for Wolfgang Pauli).*

$$\begin{aligned} X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}$$

Example 11.3 *Another important transformation is the Hadamard matrix (for Jacques Hadamard).*[3]

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Each example matrix is multiplied by the $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ qubit to check that unit length is preserved. Other qubits work the same way, and are worth checking, as well.

$$\begin{aligned} X\begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ Y\begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 \\ i \end{bmatrix} \\ Z\begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ H\begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned}$$

The X transformation is known as a "bit flip," as it flips the position of the bit. In the laboratory an X flips the polarity or some other property of a sub-atomic particle. Similarly H is known as a "beam splitter," and in the lab a beam of photons, for example, can be split into two parts. Z represents a "phase flip," as it changes the sign on part of the qubit, more easily seen in the following transformation.

$$Z\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

11.1.3 measurement

Measurement of a qubit is accomplished by projection (regression) of the qubit vector into orthonormal vectors called a basis. For encryption purposes we require

[3] We've used the symbol H for at least four things so far: the parity check matrix, Hermitian (on the previous page), entropy, and Hadamard transformation. However, the usage is standard, and usually (we hope always) the meaning is clear from the context.

only 2 bases; we will use the standard basis, $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, as well as the Hadamard basis, $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$.

The result of measuring a qubit is one or the other of the orthonormal vectors. That is, measurement changes the qubit being measured. This surprising axiom is very important for quantum processes, in general, and quantum cryptography, in particular.

The big question, then: which of the orthonormal vectors does the measured qubit turn into? The answer is in terms of probabilities, and that is another mysterious property of quantum physics. We are used to computing R^2 and interpreting it, when vector b is projected into vector a, as the component of b that resides in a. But now the vector b we are projecting is a quantum unit, and can not be physically decomposed any further. Quantum units are the basic elements of the universe. So we can't speak of a component of b, therefore we interpret R^2 as a probability that a particular measurement occurs. The probability interpretation is allowed, since, as we have seen, R^2 is a number between zero and one.

Definition 11.5 *Measurement of a qubit by orthonormal vectors changes the qubit into one of the orthonormal vectors. The probability of a particular vector being the result is the vector product of the resulting projection with itself (squared length of the projection).*

Example 11.4 *Measure the qubit* $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ *by the standard basis. That is, use the orthonormal vectors of the standard basis.*

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \textit{ and } \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

The result of the measurement will be one of the orthonormal vectors. To compute the probabilities, project the measured qubit into the two vectors. First, project $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$*, call it b, into the first eigenvector* $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$*, called* a*. The orthogonality conditions when vector b is projected into* a *is*

$$\begin{aligned} a^T\,(b - a\beta) &= 0 \\ \beta &= \frac{a^T b}{a^T a} \end{aligned}$$

Solving for the regression coefficient β*:*

$$\beta = \frac{a^T b}{a^T a} = \frac{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}}{\begin{bmatrix} 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}} = \frac{1}{\sqrt{2}}$$

Notice the denominator is always one, as the orthonormal vector is unit length by definition. This saves us some work: only the vector product of the qubit and the basis vector needs to be calculated.

The resulting projection, then, is

$$a\beta = \frac{a^T b}{a^T a} a = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

The probability the result of the measurement is $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is the squared length of the projection which is R^2, since the denominator is the hypotenuse of the right triangle, and, in this quantum case, has unit length.

$$R^2 = (a\beta)^T (a\beta) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \frac{1}{\sqrt{2}} = \frac{1}{2}$$

More generally,

$$(a\beta)^T (a\beta) = \beta^T a^T a \beta = \beta^2$$

since a has unit length. So, for the quantum case, where the vectors have unit length, the computations associated with projecting vector b into a are quite simple.

$$\begin{aligned} \beta &= a^T b \\ R^2 &= \beta^2 \end{aligned}$$

Similar computations show the measurement resulting in the other basis vector is also one-half, as it must be for the probabilities to sum to one.

R^2, as we said, is now a probability because of the quantum properties of the vectors. That is, it is certainly possible to write mathematically the initial vector as a weighted sum of the two basis vectors.

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

But this is not possible physically. The result of the measurement can not be the combination of two indivisible units. It must, instead, be one of the basis vectors or the other. So R^2 does not describe the proportion, but the probability.

Example 11.5 *Measure* $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *by the standard basis.*

The regression coefficient β when the qubit is projected into the first basis vector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is

$$\beta = a^T b = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1$$

The squared length of the projection is

$$R^2 = \beta^2 = 1$$

So the result of the measurement is the first basis vector with certainty. Whenever the qubit is identical to one of the basis vectors, measurement will *always* yield that basis vector.

Example 11.6 *Measure* $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *by the Hadamard basis.*

The Hadamard basis vectors are

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ and } \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Projecting the qubit into the first basis vector

$$\beta = a^T b = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}$$

Compute the squared length of the projection to find the probability.

$$R^2 = \beta^2 = \frac{1}{2}$$

Each basis vector has equal probability of being the result of the measurement.

11.2 Dirac notation

Dirac notation was developed by Paul Dirac. It is disconcerting, at least, to change the notation at this stage. Nonetheless, there are real advantages to doing so. The notation simplifies writing things down, especially when the problems get complicated. And sometimes the notation actually illuminates the process. But no matter how we feel about it, the notation is standard in the area, so, if we wish to read about what people are up to, we'll need to follow the notation: everyone uses it.

The standard qubit $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is written as $|0\rangle$, and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ as $|1\rangle$. A general qubit $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ can be written

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$$

To transpose a qubit, or complex conjugate transpose, simply reverse the brackets.

$$\begin{aligned}\begin{bmatrix}1\\0\end{bmatrix}^T &= \langle 0| \\ \begin{bmatrix}0\\1\end{bmatrix}^T &= \langle 1|\end{aligned}$$

It is a bit easier to write vector products.

$$\begin{aligned}\begin{bmatrix}1 & 0\end{bmatrix}^T\begin{bmatrix}0\\1\end{bmatrix} &= \langle 1|\,0\rangle = 0 \\ \begin{bmatrix}0 & 1\end{bmatrix}^T\begin{bmatrix}1\\0\end{bmatrix} &= \langle 0|\,1\rangle = 0\end{aligned}$$

Whenever the two qubits in a vector product are the same, the result is one.

$$\begin{aligned}\langle 1|\,1\rangle &= 1 \\ \langle 0|\,0\rangle &= 1\end{aligned}$$

The notation for the Pauli transformations are simplified a little bit.

$$\begin{aligned}X\,|0\rangle &= |1\rangle & X\,|1\rangle = |0\rangle \\ Y\,|0\rangle &= i\,|1\rangle & Y\,|1\rangle = -i\,|0\rangle \\ Z\,|0\rangle &= |0\rangle & Z\,|1\rangle = -\,|1\rangle\end{aligned}$$

The Hadamard transformation introduces two new symbols, $|+\rangle$ and $|-\rangle$.

$$\begin{aligned}H\,|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \\ H\,|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle\end{aligned}$$

Notice that $|+\rangle$ and $|-\rangle$ are the orthonormal vectors of the Hadamard basis.

Projections are accomplished in Dirac notation. Project $|0\rangle$ (which we denote as vector b) into $|0\rangle$ (denoted as a).

$$\begin{aligned}a\beta &= a^T ba \\ &= \langle 0\,|0\rangle\,|0\rangle = |0\rangle\end{aligned}$$

Project $|0\rangle$ into $|+\rangle$.

$$\begin{aligned}\langle + |0\rangle \, |+\rangle &= \frac{1}{\sqrt{2}} |+\rangle \text{ since} \\ \langle + |0\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\end{aligned}$$

The squared length of the projection of $|0\rangle$ into $|+\rangle$ is

$$\frac{1}{\sqrt{2}} \langle +| +\rangle \frac{1}{\sqrt{2}} = \frac{1}{2}$$

Therefore, when $|0\rangle$ is measured using the Hadamard basis, there is an equal probability (equal one-half) of either $|+\rangle$ or $|-\rangle$ being the result of the measurement. This and similar measurements are the basis of the quantum encryption solution to the private key problem.

11.3 quantum encryption

Recall the private key problem is the inability to communicate the code parameters, p and e, in a secure fashion. Quantum encryption offers a solution to the private key problem because of the way quantum measurement works: measurement changes the qubit. Even if bad guys intercept the key, they can't help but change it. If evidence of tampering shows up, the key is discarded, and the procedure starts again.

Here's how the sender of the key proceeds. For simplicity start with a lot of $|0\rangle$ qubits. Then process each one using one of four possible procedures. So as to not reveal anything about the chosen preparation on an individual qubit, the sender can generate a string of random numbers to decide which procedure to use on each qubit. There are four possible procedures.

	procedures:
1	unchanged = $|0\rangle$
2	$X \, |0\rangle = |1\rangle$
3	$H \, |0\rangle = |+\rangle$
4	$HX \, |0\rangle = |-\rangle$

The sender, then, has a string of qubits, each qubit is one of four possible states. The string is sent to the receiver. The receiver then measures each qubit in the string using either standard or Hadamard basis. The receiver might as well generate a string of random numbers to decide which measurement to use on which qubit, as he (and any bad guys) have no information about how the qubits were prepared.

Notice that if the receiver measures with the standard basis for sender transformation procedures 1 and 2, the receiver sees exactly the qubit that was sent. Recall the standard orthonormal vectors are $|0\rangle$ and $|1\rangle$, and that, when the measured qubit equals the basis vector, the basis vector is the result of the measurement with certainty.

However, still with sender procedures 1 and 2, if the receiver uses the Hadamard basis, then the qubit will be distorted. The result of the measurement will be $|+\rangle$ or $|-\rangle$, each with probability one-half, as demonstrated at the end of the previous section.

After the measurements are concluded the receiver announces publicly the measurement schedule employed That is, the receiver states which qubits were measured using standard and which using Hadamard. The receiver most assuredly does *not* announce the result of the measurement; the whole point is to keep that information from the bad guys.

The sender then compares the qubit preparation procedures with the announced measurement schedule.. If the measurement was standard, and the preparation either procedure 1 or 2, then the sender says (publicly) keep the qubit as part of the key. Likewise, Hadamard measurement will be matched with either procedure 3 or 4. The other qubits are discarded. In this fashion as many qubits as desired can be communicated, and the key, that is p and e, can be arbitrarily long. Notice the public communications are of no use to the bad guys. All that can be learned is what measurements are appropriate for what qubits, *not* the results of the measurements. It is too late, at this point, to actually conduct the measurements as the qubits have already been transmitted.

An important part of the procedure is what happens if a bad guy attempts to eavesdrop on the communication, that is, intercept the qubits while in transit. What happens, of course, is that with high probability the eavesdropper will alter the qubit. Even if the eavesdropper knows which *set* of measures to use, standard and Hadamard in this case, with probability one-half the wrong one is chosen. And repeated measurements increase the probability pretty quickly. If only ten qubits are measured, for example, the probability that none of them are altered is

$$\left(\frac{1}{2}\right)^{10} = .000977$$

The alteration free probability can be made as small as desired by sending more qubits. Using the communicated code parameters, p and e, to send a test message is one way to check to see if the qubits arrived without tampering. As seen in the previous chapter, even a minute variation in one of the code parameters results in a significant distortion to the message.[4]

[4] There is another issue not covered here: qubits are fragile and could become altered naturally, without interference from eavesdropping. That complicates the problem somewhat, but there are possible remedies; there exist quantum self-correcting codes, for example.

To summarize the procedures -

		receiver	
sender procedures		measure	basis vectors
1	unchanged = $\|0\rangle$	std	$\|0\rangle$ and $\|1\rangle$
2	$X\|0\rangle = \|1\rangle$		
3	$H\|0\rangle = \|+\rangle$	Had	$\|+\rangle$ and $\|-\rangle$
4	$HX\|0\rangle = \|-\rangle$		

The string of qubits received and verified can serve as encryption parameters. The string can be read as a binary number, for example, and the next highest prime number chosen as p, or e. We have accomplished the objective of specifying a quantum private key communication procedure. Now the code parameters, p and e, can be used confidently in a regular Fermat encryption scheme.

Example 11.7

sender	*qubit*	*receiver*	*msmt*	*public communication*	
procedure	*sent*	*procedure*	*result*	*rec to sender*	*sender to rec*
null	$\|0\rangle$	*std*	$\|0\rangle$	*std*	*yes*
X	$\|1\rangle$	*Had*	$\|+\rangle/\|-\rangle$	*Had*	*no*
H	$\|+\rangle$	*std*	$\|0\rangle/\|1\rangle$	*std*	*no*
HX	$\|-\rangle$	*Had*	$\|-\rangle$	*Had*	*yes*

The sender prepares, and sends, four qubits as in the table. The receiver (randomly) chooses the measurement procedures. (A random choice prevents any eavesdropper from using the same measurement schedule.) The measurement result for the first qubit yields the qubit as sent. For the second qubit the measurement result is probabilistic: the notation $|+\rangle/|-\rangle$ implies either $|+\rangle$ or $|-\rangle$ will result, each with probability one-half. The last two columns are public announcements. The receiver sends the measurement schedule; the sender can then tell which qubits were measured appropriately, and tells the receiver which measurements to keep. Notice the public communications are worthless to an eavesdropper, as it is not possible to infer the measurement of the qubit.

Example 11.8 *Inject an attempt by an eavesdropper to intercept the quantum communication.*

sender	qubit	e'dropper	e'dropper	receiver	msmt	public comm.	
proc.	sent	procedure	msmt result	proc.	result	r to s	s to r
null	$\|0\rangle$	std	$\|0\rangle$	std	$\|0\rangle$	Z	yes
X	$\|1\rangle$	std	$\|1\rangle$	Had	$\|+\rangle/\|-\rangle$	X	no
H	$\|+\rangle$	std	$\|0\rangle/\|1\rangle$	std	$\|0\rangle/\|1\rangle$	Z	no
HX	$\|-\rangle$	std	$\|0\rangle/\|1\rangle$	Had	$\|+\rangle/\|-\rangle$	X	yes

Notice particularly the fourth qubit: the eavesdropper's attempt to intercept garbles the qubit, so what reaches the receiver is different from what is originally sent.

Even though the sender directs the receiver to use the fourth qubit, it will not work as part of a Fermat encryption technique, as a test message will determine.

11.4 summary

The quantum solution to the private key problem relies on quantum measurement in which the qubit being measured ends up as one of the eigenvectors of the measurement matrix. So any attempt to eavesdrop changes the message in a discernible fashion. In this way the code parameters, p and e, can be communicated securely, and Fermat encryption is back in.

In general the measurement result is probabilistic. For encryption purposes we only had use for discrete probabilities equal to zero, one-half, and one. Euler's formula allows us to examine settings with continuous probability results, and that will be employed in the next chapter.

11.5 reference

Nielsen, Michael A. and Isaac L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

11.6 exercises

Exercise 11.1 *Measure $|0\rangle$ using Hadamard basis. Report the possible vector results and the associated probabilities.*

Measure $HX|0\rangle$ using standard basis.

Measure $HX|0\rangle$ using Hadamard basis.

Exercise 11.2 *Fill in the missing elements of the following quantum communication table.*

sender	qubit	receiver	msmt	public communication	
procedure	sent	procedure	result	rec to sender	sender to rec
null	$\|0\rangle$	Had	?	?	?
X	?	std	?	?	?
H	?	Had	?	?	?
HX	?	std	?	?	?

Exercise 11.3

sender	*qubit*	*e'dropper*	*e'dropper*	*receiver*	*msmt*	*public comm.*	
proc	*sent*	*proc*	*msmt result*	*proc*	*result*	*r to s*	*s to r*
null	$\|0\rangle$	*Had*	*?*	*std*	*?*	*?*	*?*
X	*?*	*Had*	*?*	*Had*	*?*	*?*	*?*
H	*?*	*std*	*?*	*std*	*?*	*?*	*?*
HX	*?*	*std*	*?*	*Had*	*?*	*?*	*?*

Exercise 11.4

sender	*qubit*	*receiver*	*msmt*	*public communication*	
procedure	*sent*	*procedure*	*result*	*rec to sender*	*sender to rec*
null	$\|0\rangle$	*std*	*?*	*?*	*?*
X	*?*	*Had*	*?*	*?*	*?*
H	*?*	*std*	*?*	*?*	*?*
HX	*?*	*Had*	*?*	*?*	*?*