

Reducing the Randomness Requirements for Quantum Money

David K. Wittenberg¹

*Technical Report CS-95-177
Computer Science Department
Brandeis University
dkw@cs.brandeis.edu*

January 23, 1995

¹The author gratefully acknowledges the support of the W. M. Keck Foundation.

1 Abstract

The original description of Quantum Money used two truly random bits for each photon stored. We show that the amount of randomness required is considerably less than that. By using game theory to analyze a quantum cryptographic protocol, we show that the protocol's security is remarkably insensitive to bias in one of the "random" bits. First we show that there is no loss in security if that bit produces a "1" between one quarter and three quarters of the time. Secondly, we show that it is possible to maintain some security even if that bit is absolutely predictable. This allows us to make uncopiable tokens using only 2 quantum states instead of the 4 which have previously been used, though one must still be able to detect all 4 states.

Keywords: Quantum cryptography, Game theory, Key distribution, Digital money.

2 Introduction

Wiesner [8] suggested using quantum cryptography to make unforgeable money (or subway tokens). This idea was expanded by Bennett *et al.* [3]. The history of quantum cryptography is described by Bennett *et al.* [2] in which they describe the first quantum cryptographic devices to be built. Brassard's bibliography [5] provides a good starting point, and his cryptography book [4] has a chapter on quantum cryptography, which provides an excellent introduction including both a description of the necessary physics and several quantum cryptography protocols.

Quantum Money is a procedure for making *tokens* using quantum cryptographic techniques such that any attempt to copy a token can be detected with extremely high probability. Unlike conventional cryptography, in quantum cryptography both the copy and the original would show the effects of copying.

Quantum cryptography is based on a fundamental tenet of quantum theory which states that one can not know the polarization of a photon in two conjugate bases simultaneously. Wiesner took advantage of this tenet by making tokens consisting of a vector of many photons, each with polarization known in one basis. The tokens can later be checked by measuring the polarization of the photons to see that none have changed from the polariza-

tion which was stored. Since the copier doesn't know which basis to measure in, she has a 25% chance of being caught for each photon she copies. The mint can, by making a token from many photons with polarizations chosen independently, make the probability of catching a copier exponentially close to 1.

Wiesner flips two unbiased coins, the first to determine which basis to use, and the second to determine which polarization to use in that basis. We investigate the results of bias in those coins and obtain the following results: Provided that the first coin (which determines the basis) is unbiased, if the second coin (which determines the polarization in that basis) yields heads between one quarter and three quarters of the time, the probability of detecting that a particular photon has been copied remains at one quarter.

Even if the second coin is completely predictable, as long as the first coin is unbiased, the probability of detecting that a photon has been copied is one eighth. This means that one need only be able to produce two different photon polarizations instead of the four which Wiesner required. Thus, by using twice as many photons, each specified by one bit, we show a different way to use a given amount of randomness to get almost the same security level. Reducing the number of different polarizations necessary (which equipment must produce) substantially reduces the cost of building associated equipment [9].

If the mint knows that it has a biased random number generator and uses a coin fairing scheme [6], this shows that it need fair only some of the coins well, and that the mint can accept a large bias in the others. By demonstrating a limit on the amount of fairing which is beneficial, this permits the mint to use fewer tosses of its biased random coins.

This analysis also applies to the probability of detecting Eve's use of the intercept/resend strategy in Bennett *et al.*'s quantum key-exchange protocol [2].

3 Notation

We follow the notation in Brassard's book [4], which differs somewhat from that in [2]. Formally, the internal state of a photon is a vector of unit length in a 2-D Hilbert space. That means that the photon is completely described as a linear combination of two complex basis vectors.

We define a *basis* to be a pair of quantum states which are routinely distinguishable by some apparatus. An example of a basis is (vertically polarized, horizontally polarized) applied to a photon. Define two bases to be *conjugate* if each vector of one basis has equal-length projections on all vectors of the other basis. That is, if a photon is prepared in one basis, it will behave completely randomly if measured in any conjugate basis.

The *rectilinear basis* for the Hilbert Space consists of a horizontal vector $r_1 = (1, 0)$, and vertical vector $r_2 = (0, 1)$. If $\gamma = \frac{\sqrt{2}}{2}$, the *diagonal basis* consists of $d_1 = (\gamma, \gamma)$ and $d_2 = (\gamma, -\gamma)$. There is a third conjugate basis, called the *circular basis*, composed of $c_1 = (\gamma, \gamma i)$ and $c_2 = (\gamma i, \gamma)$ which we ignore.

4 Model

4.1 Abstract Model

We consider a writer Alice (sometimes referred to as the *mint*) who prepares *tokens*, each consisting of many (perhaps 100) photons. An adversary, Eve, tries to copy a token without detectably changing the original token. Our model allows either the writer Alice or the eavesdropper Eve to set the polarization of a photon in either direction in either of two conjugate bases (rectilinear or diagonal). A 0 bit is encoded as a vertical polarization in the rectilinear basis, and as a 45° polarization in the diagonal basis; a 1 bit is encoded as a horizontal polarization in the rectilinear basis, and as a 135° polarization in the diagonal basis. Let P_r be the probability of Alice choosing the rectilinear basis, and P_0 be the probability of Alice choosing to send a 0. Without loss of generality, assume that P_r and P_0 are both at least .5. For convenience we will define $P_d = (1 - P_r)$ and $P_1 = (1 - P_0)$.

At this time we are ignoring the possibility of making a measurement or creating a photon at some angle between the two basis sets, such as a Breidbart basis [3].

4.2 Assumptions

- No photons change state except as a result of measurements.

- The random number generator Alice uses provides uncorrelated random bits with some bias known to Eve.
- All attempts to detect a photon succeed.
- We ignore noise. See [2] for a discussion of dealing with noise.

5 Eve's Strategies

5.1 Descriptions of Strategies

We model forgery detection as a two-person zero-sum game with a payoff function defined as the probability that Eve is caught. We start by considering all the strategies Eve could use, in the style of a game-theoretic analysis [7]. The fundamental theorem from game theory is that the optimum strategy for each player in a two-person zero-sum game is to randomly choose from several *moves* (note that a move is a deterministic description of what Eve should do, and it may depend on what she has already observed) with the probability of choosing each move determined by a linear programming calculation on the matrix whose entries are values of the payoff function, and whose indices are moves.

A *move* is a deterministic algorithm which describes a player's actions. There are several ways to calculate the payoff for each of Eve's moves, corresponding to different descriptions of the moves. We use one which has the advantage that all of the calculations are fairly simple, and physical reality presents no obstacle as all the entries in this table are possible. We describe Eve's move by a string of 5 bits $\alpha, \beta, \gamma, \delta, \epsilon$ which we interpret as follows: For α, β , and δ , 0 means the rectilinear basis, 1 the diagonal basis. For γ and ϵ , if the measurement is made in the rectilinear basis, 0 means a horizontal polarization, and 1 means a vertical polarization; on the diagonal basis, 0 means 45° polarization and 1 means a 135° polarization.

A *move* by Eve is described by the following algorithm: Read in the α basis. If you see a 0, write γ in the β basis, otherwise, write ϵ in the δ basis.

Note that the 5-bit description is complete, and minimum. Since there are 5 binary choices, there are 32 such moves. We first list the 32 moves and their payoff matrices with the mint's four moves in table 1.

The rows of the table are labeled by the decimal representation of the bit string $\alpha, \beta, \gamma, \delta, \epsilon$; where α denotes the basis which the forger measures in, β and δ give the basis and value the forger writes if she reads a zero, δ and ϵ give the basis and value she writes if she reads a one. Note that the second through sixth columns represent the bits $\alpha, \beta, \gamma, \delta, \epsilon$ respectively. The next four columns give the probability of detection for this move against the mint's four possible choices. The last column gives the expected probability of detection for the forger's move as a function of the bias in the mint's coins. If the move is dominated by another, the last column instead gives the dominating row number.

Of the 32 moves, 22 are dominated by other moves, leaving ten moves to consider. We can split those into two groups of five each, one group corresponding to measuring in the rectangular basis, and the other to measuring in the diagonal basis. Under the assumption that Alice chooses a rectilinear basis at least as often as she chooses a diagonal basis and she chooses to write 0s at least as often as she writes 1s, there are only two moves which are not dominated by other moves. One of those is the obvious one of measuring in the more likely (rectilinear) basis and copying the measurement. The other intuitively corresponds to saying that if seeing a 1 is very unlikely, when Eve sees a 1 she guesses that she measured in the wrong basis, and so sends a 0 in the other basis. Clearly this move works only when 1's are much less likely than 0's.

Since Alice's strategy is completely determined by the bias of her coins, this is not a standard game theory problem, so we do not need the full power of game theory for this analysis. However using the first step of a game-theoretic analysis (removing moves which are dominated by other moves), We find that Eve's optimal behavior is not a random selection from several moves, but is always one particular move. This is called a *pure strategy*. Which pure strategy she should choose is a function of P_r and P_0 .

5.2 Payoffs

The obvious move is to measure in the more likely basis, and copy that measurement. Under our assumption that $P_r \geq .5$, this corresponds to move 1. If Eve measures in the correct basis, she will not be detectable. The probability of choosing the correct basis to measure in is P_r . So there is a $1 - P_r = P_d$ probability of measuring in a basis orthogonal to the one which

		Mint basis =				r				d				Detection probability or dominating row :
		r		d		r		d		r		d		
		0		1		0		1		0		1		
	α	β	γ	δ	ϵ									
0	r	r	0	r	0	0	1	.5	.5	1				
1	r	r	0	r	1	0	0	.5	.5	$.5p_d$				
2	r	r	0	d	0	0	.5	.25	.75	$.5p_r p_1 + .25p_d p_0 + .75p_d p_1 = .5p_1 + .25p_d$				
3	r	r	0	d	1	0	.5	.75	.25	$.5p_r p_1 + .75p_d p_0 + .25p_d p_1 = .5(p_r p_1 + p_d p_0) + .25p_d$				
4	r	r	1	r	0	1	1	.5	.5	1				
5	r	r	1	r	1	1	0	.5	.5	1				
6	r	r	1	d	0	1	.5	.25	.75	27				
7	r	r	1	d	1	1	.5	.75	.25	27				
8	r	d	0	r	0	.5	1	.25	.75	27				
9	r	d	0	r	1	.5	0	.25	.75	$.5p_r p_0 + .25p_d p_0 + .75p_d p_1 = p_r p_0 - .5p_0 + .75p_d$				
10	r	d	0	d	0	.5	.5	0	1	27				
11	r	d	0	d	1	.5	.5	.5	.5	1				
11	r	d	1	r	0	.5	1	.75	.25	27				
13	r	d	1	r	1	.5	0	.75	.25	$.5p_r p_0 + .75p_d p_0 + .25p_d p_1 = .5p_0 + .25p_d$				
14	r	d	1	d	0	.5	.5	.5	.5	1				
15	r	d	1	d	1	.5	.5	1	0	27				
16	d	r	0	r	0	0	1	.5	.5	27				
17	d	r	0	r	1	.5	.5	.5	.5	27				
18	d	r	0	d	0	.25	.75	.5	1	1				
19	d	r	0	d	1	.25	.75	.5	0	$.25p_r p_0 + .75p_r p_1 + .5p_d p_0 = .75p_r + .5p_0$				
20	d	r	1	r	0	.5	.5	.5	.5	27				
21	d	r	1	r	1	0	1	.5	.5	27				
22	d	r	1	d	0	.75	.25	.5	1	1				
23	d	r	1	d	1	.75	.25	.5	0	$.75p_r p_0 + .25p_r p_1 + .5p_d p_0 = .25p_r + .5p_0$				
24	d	d	0	r	0	.25	.75	0	.5	$.25p_r p_0 + .75p_r p_1 + .5p_d p_1 = .25p_r + .5p_1$				
25	d	d	0	r	1	.75	.25	0	.5	$.75p_r p_0 + .25p_r p_1 + .5p_d p_1 = p_r p_0 - .25p_r + .5p_d$				
26	d	d	0	d	0	.5	.5	0	1	27				
27	d	d	0	d	1	.5	.5	0	0	$.5p_r$				
28	d	d	1	r	0	.25	.75	1	.5	1				
29	d	d	1	r	1	.75	.25	1	.5	1				
30	d	d	1	d	0	.5	.5	1	1	1				
31	d	d	1	d	1	.5	.5	1	0	27				

Table 1: Payoff matrix

was set. If she measures in the wrong basis, the probability of correctly setting the polarization in any basis orthogonal to the mint's measurement is by definition .5. Thus: $P(\text{detect}) = \frac{1}{2}P_d$.

Note that P_0 does not appear, because the direction not set intentionally by the adversary will be 0 with $P = .5$ so the probability that it matches if that basis is measured is .5, regardless of how the bit was set originally.

How effective are the other (non-dominated) moves? The non-obvious moves copy the measurement if it is the more likely value, and if the measurement is the less likely value, they write the more likely value in the other basis. If we allow one value to be more likely in one basis, and the other value to be more likely in the other basis, there are clearly four such moves. Here, we consider only the case where P_0 is independent of the basis chosen. If we allowed P_0 to be a function of the basis Alice chooses, we have to consider more moves, but the general sense remains the same.

Because we know which values are more likely (recall that we assume that $P_r \geq .5$ and that $P_0 \geq .5$), we need only calculate the probability of Eve's getting caught in one of those four.

The probability that Eve will be detected with this move (number 2 in table 1) is:

$$0 + .5P_r(1 - P_0) + .25(1 - P_r)P_0 + .75(1 - P_0)(1 - P_r)$$

which reduces to

$$.75 - .25P_r - .5P_0$$

This is less than the probability of Eve being detected using a simple move when $P_r < 2P_0 - 1$. Since by assumption $P_r \geq .5$, this can only happen when $P_0 \geq .75$. So if the choice of basis is unbiased, and if $.25 \leq P_0 \leq .75$ the probability of detecting eavesdropping remains at .25.

Even if the choice of value is constant, the chance of detecting eavesdropping is $.75 - .25(.5) - .5 = .125$. This is half the chance of detecting eavesdropping using two unbiased coins.

This gives a quantum cryptography technique which requires the mint to produce only two states. While quantum cryptography systems with two states are known [1], this analysis shows that a standard quantum cryptographic system works with only two states.

Eve's optimum strategy turns out to be a *pure* strategy (*ie.*, a single move), which is a simple function of P_r and P_0 . Which strategy to use is

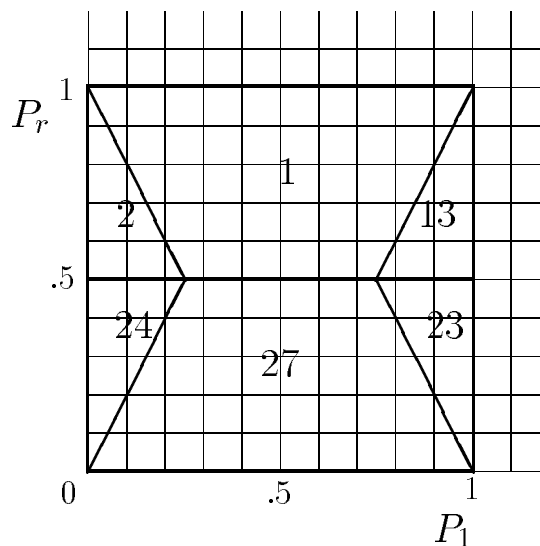


Figure 1: Dividing lines between Eve's optimal strategies. The numbers in each region give the strategy to be used there.

shown in figure 1. If we consider Eve's probability of detection as a function of P_r and P_1 , this is a projection of that three-dimensional graph onto the P_r, P_0 plane. The middle section of the horizontal line is at height .25, the top and bottom horizontal lines are at height 0, and the vertical line's height ranges from 0 at the top and bottom to .125 in the middle. All the surfaces are planar. The surface looks remarkably like a pup tent.

6 Acknowledgments

My thanks to Steve Wiesner for explaining quantum cryptography to me, for asking the question which led to this work, and for his comments on early versions. Marty Cohn was very helpful in clarifying the description of the several moves, and in making this paper more readable.

References

- [1] Charles H. Bennett. Quantum cryptography using any two nonorthogonal

- states. *Physical Review Letters*, 68(21):3121–3124, May 1992.
- [2] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.
 - [3] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – Proceedings of Crypto 82*, pages 267 – 275, New York, 1983. Plenum Press.
 - [4] Gilles Brassard. *Modern Cryptology: A Tutorial*. Number 325 in Lecture Notes in Computer Science. Springer Verlag, Berlin, 1988.
 - [5] Gilles Brassard. Cryptology column — quantum cryptology: A bibliography. *Sigact News*, 24(3):16–20, 1993.
 - [6] Josh D. (Benaloh) Cohen. Fairing of biased coins in bounded time. Technical Report YALEU/DCS/TR-372, Yale University Department of Computer Science, March 1985.
 - [7] John von Neumann and Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton University Press, Princeton, NJ, second edition, 1947.
 - [8] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78 – 88, 1983.
 - [9] Stephen Wiesner. Personal Communication, 1993.