# Chapter 9
# Permutations, Cycles and Derangements

Permutations pervade much of mathematics including number theory. Besides innumerable peaceful uses, permutations were crucial in classical cryptography, such as the German *Geheimschreiber* (secret writer) and *Enigma* enciphering machines—and their demise. The *Geheimschreiber* was broken during World War II by the Swedish mathematician Arne Beurling—with the occasional help from the leading Swedish statistician Harald Cramér (see B. Beckman: *Codebreakers*).

Polish and British cryptanalysts were able to break the Enigma code by observing—among other factors—the cycle structure of the code. Cycles of permutations and their distributions are therefore considered in Section 9.4 of this chapter.[1]

## 9.1 Permutations

The number of arrangements ("permutations") of $n$ distinct objects equals the *factorial* of $n$:

$$n! := 1 \cdot 2 \cdot 3 \cdots n, \tag{9.1}$$

a formula easily proved by induction. Factorials grow very fast: while 5! equals just 120, 10! is already equal to 3 628 800. A good and relatively simple approximation is Stirling's famous formula:

$$n! \approx \sqrt{(2\pi n)} n^n \, \mathrm{e}^{-n}, \tag{9.2}$$

which yields 3 598 696 for $n = 10$.

A better approximation multiplies the Stirling result by $\mathrm{e}^{1/12n}$, yielding $10! \approx 3\,628\,810$ (for an error of less than 0.0003%!).

Factorials are also related to the "Euler" integral. Repeated partial integration shows that

[1] While the Germans, after a few years, became aware of the *Geheimschreiber's* vulnerability and curtailed its use, the fact that the Allies had broken *Enigma* was one of the best-kept secrets of the war. The *Enigma* decrypts therefore continued to provide the Allies with invaluable information during the entire war.

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_9, 

$$\int_0^\infty t^n \mathrm{e}^{-t}\, dt = n! \tag{9.3}$$

The related *gamma-function*

$$\Gamma(z) := \int_0^\infty t^{z-1} \mathrm{e}^{-t}\, \mathrm{d}t$$

is single-valued and analytic in the entire complex plane, except for the points $z = -n$ $(n = 0, 1, 2, \ldots)$ where it possesses simple poles with residues $(-1)^n/n!$. $\Gamma(z)$ obeys the recurrence formula

$$\Gamma(z+1) = \mathrm{z}\Gamma(z) \tag{9.4}$$

and the curious "reflection" formula

$$\Gamma(z)\Gamma(1-z) = -z\Gamma(-z)\Gamma(z) = \pi\mathrm{csc}(\pi z), \tag{9.5}$$

which for $z = 1/2$ yields

$$\Gamma(1/2) = \sqrt{\pi}.$$

## 9.2 Binomial Coefficients

As we learn in high school (?), the "binomial" $(1+x)^n$ can be expanded (multiplied out) as follows:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{9.6}$$

where the $\binom{n}{k}$ (read $n$ choose $k$) are the binomial coefficients—

$$\text{With 0! defined as 1, } \binom{n}{0} = \binom{n}{n} = 1, \tag{9.7}$$

$\binom{n}{1}$ equals $n$ and $\binom{n}{2}$ equals $n(n-1)/2 = 0, 1, 3, 6, 10, 15, \ldots$ the "triangular" numbers (see Sec. 7.4). The binomial coefficient $\binom{n}{2} = 1/2\ n(n-1)$ is (by definition) the number of *pairs* that can be selected from $n$ distinct objects. Thus, at a party of $n$ people, each guest clinking his glass with everyone else, produces a total of $1/2\ n(n-1)$ clinkings. (Of course, for n = 1, the number of possible clinkings is zero, just as there is no applause with just one hand clapping. For two people $(n = 2)$, there is just one clinking.)

Permutations when just two objects change places are called *transpositions*. Every permutation can be decomposed into a unique (modulo 2) number of transpositions. If this number is odd, the permutation is called *odd*. Otherwise it is called an *even* permutation. The identity permutation is even because the number of transpositions is 0 (an even number). For example for $n = 5$, there are a total of $n! = 120$

permutations of which 60 are odd and 60 are even, the latter forming the famous *symmetrical group* $S_5$ which was crucial in Galois' historic proof that the general quintic equation has no solution in radicals. This put to rest a problem that had baffled mathematicians for centuries.

Other special permutations with unique properties are those generated by primitive roots, the number-theoretic logarithm (index), and the Zech logarithm (see Chaps. 14 and 27).

If the $n$ objects consist of $m$ groups containing $k_1, k_2, \ldots, k_m$ elements, respectively, the binomial coefficients can be generalized to the *multinomials*. The multinomial coefficients are defined by

$$\frac{n!}{k_1!, k_2! \ldots k_m!}, \quad \text{where} \quad \sum_{r=1}^{m} k_r = n \tag{9.8}$$

The differences between consecutive triangular numbers equal 1, 2, 3, 4, 5, …, i.e. a set covering *all* positive integers. Thus, as the young Gauss discovered, they are sufficiently dense so that every positive integer can be represented by the sum of just 3 triangular numbers Δ. Or, as Gauss wrote in 1796 in his still new notebook:

$$\text{Eureka! n} = \Delta + \Delta + \Delta.$$

Note that already $n = 5$ requires 3 triangular numbers $(5 = 3 + 1 + 1)$.

By contrast, the *square* numbers, 0, 1, 4. 9, 16, 25 … have differences equal to 1, 3, 5, 7, 9 …, i.e. they cover only the odd numbers. They are therefore less dense and up to 4 squares are required to represent all positive integers. For example, $7 = 4 + 1 + 1 + 1$ cannot be represented by just 3 squares. The same is true for $n = 15, 23, 31, \ldots 28, \ldots$ (see Sect. 7.9 for more on the sum of 3 squares).

## 9.3 The Binomial and Related Distributions

If $p$ is the probability that one of $n$ possible events occurs, the probability of $k$ events occurring in $n$ independent trials is proportional to the binomial coefficient "$n$choose$k$". With k ranging from 0 to $n$, the (discrete) probability *distribution* is the so-called binomial distribution

$$p(k) = c\binom{n}{k}, 0 \le k \le n \tag{9.9}$$

where the constant $c$ must be chosen so that

$$\sum_{k=0}^{n} p(k) = c \cdot 2^n \tag{9.10}$$

equals 1, i.e. $c$ must equal $1/2^n$.

The mean value of $k$ equals $np$ and its variance is $np(1-p)$, which for fixed $n$ achieves its maximum for $p = 1/2$.

For large $n$, the binomial distribution looks like samples from a Gaussian (normal) distribution. And in fact, for large $n$, the binomial distribution can be approximated by a normal distribution with mean $np$ and variance $np(1-p)$.

For n $\to \infty$, but $np$ fixed: $np = m$, the binomial distribution turns into the important Poisson distribution

$$p_m(k) = \frac{m^k}{k!}\mathrm{e}^{-m}, \quad k = 0, 1, 2 \ldots \tag{9.11}$$

with mean *and* variance equal to $m$.

The Poisson distribution gives the number of "clicks" per second of a Geiger-counter near a radioactive source with an average click rate equal to $m$ clicks per second. The Poisson distribution also describes the occurrence of other "rare" events, i.e. events for which $p$ is so small that, even as n $\to \infty$, $np$ stays finite.

## 9.4 Permutation Cycles

One important subject in the study of permutations is their *cycle structure*. It was by the analysis of cycles, and particularly an invariance property of the cycle structure that the Polish mathematician Marian Rejewski, before the outbreak of World War II, was able to crack the *Enigma* enigma (see C. Christensen, *Mathematics Magazine*, Vol. **80**, No. 4 (October 2007), pp. 247–273).

For $n = 2$, the two possible permutations are the "identity" permutation (1, 2) and the transposition (2, 1). Note that the notation (2, 1) means that the first object is now in the second position and the second object appears in the first position.

Here (1, 2) has two cycles of period length 1 each:

$$1 \to 1 \text{ and } 2 \to 2.$$

Whereas the transposition (2, 1) has only *one* cycle of period length 2:

$$1 \to 2 \to 1.$$

Thus, the total number of cycles equals 3, two of which have period length 1 and one ($1 \to 2 \to 1$) has length 2.

Now let us study the cycle structure for the case of $n = 3$.

For the 6 permutations of 3 objects, cycle-analysis yields for the identity permutation (1, 2, 3): $1 \to 1$, $2 \to 2$, $3 \to 3$, i.e. 3 cycles of length 1.

For the permutation (1, 3, 2) we have 2 cycles: $1 \to 1$ and $2 \to 3 \to 2$, one of which has length 1 and the other cycle has length 2.

For (2, 1, 3), we find again 2 cycles, $2 \to 1 \to 2$ and $3 \to 3$, with lengths 1 and 2, respectively.

For (2, 3, 1), a "cyclic" permutation, we have just 1 cycle, $1 \to 2 \to 3 \to 1$, with length 3.

For (3, 1, 2), the other cyclic permutation, we find again just 1 cycle, $1 \to 3 \to 2 \to 1$, with length 3.

And, finally, for the permutation (3, 2, 1), we find 2 cycles, $1 \to 3 \to 1$ and $2 \to 2$, with lengths 1 and 2, respectively.

Thus, for $n = 3$, we have found a total number of 11 cycles, namely 2 permutations with 1 cycle, 3 permutations with 2 cycles and 1 permutation with 3 cycles. In general, the number of cycles is given by the Stirling numbers of the first kind ${S_n}^{(m)}$, with the generating function

$$x(x-1)\cdots(x-n+1) = \sum_{m=0}^{n} {S_n}^{(m)} x^m \tag{9.12}$$

and the recurrence relation

$${S_{n+1}}^{(m)} = {S_n}^{(m-1)} - n{S_n}^{(m)}.$$

In fact, the number of permutations of $n$ symbols which have exactly $m$ cycles equals

$$\#_n(m) = (-1)^{(n-m)}{S_n}^{(m)}, \tag{9.13}$$

which for $n = 3$ and for $m = 1, 2, 3$ yields the values 2, 3, 1, respectively.

The *total* number of cycles is given by the simple formula

$$\sum_{m=1}^{n} m\#_n(m) = \#_{n+1}(2), \tag{9.14}$$

which, for $n = 3$, yields 11 (as we already found by enumerating all 6 permutations for $n = 3$).

For more on the Stirling numbers, see Graham, Knuth and Patashnik: *Concrete Mathematics*, a veritable treasure trove of discrete (discreet?) mathematics.

Now let us look at the total number of different cycle *lengths*. By summing up the above results for $n = 3$, we find that there are a total of six cycles of period length 1, three cycles of length 2 and two cycles of length 3. Bell Labs mathematician S.P. Lloyd has shown that, in general, for the $n!$ permutations of $n$ distinct objects there are $n!$ cycles of length 1, $n!/2$ cycles of length 2 and, generally, $n!/k$ cycles of length $k$, $1 \le k \le n$.

Thus, the total number of cycles equals $n!(1 + 1/2 + \ +1/n)$. Here, the sum is the *harmonic number* $H_n$, which can be approximated by a definite integral from $x = 1/2$ to $x = n + 1/2$, over $1/x$, yielding

$$H_n \approx \ln(2(n + 1/2)). \tag{9.15}$$

However, considering that $1/x$ is concave (i.e. a "sagging" function), the factor 2 in the above formula overestimates $H_n$. Taking a cue from Euler, we replace the factor 2 by $e^{\gamma} \approx 1.781$, where $\gamma = 0.57721\ldots$ is Euler's constant. This yields the astonishingly accurate approximation

$$H_n \approx \ln(1.781(n + 1/2)), \tag{9.16}$$

giving (exact values in parentheses) $H_1 \approx 0.98$ (1.0), $H_2 \approx 1.49$ (1.5), $H_3 \approx 1.83$ (1.83…) and $H_{50} \approx 4.49915$ (4.49921) with an error of less than 0.007%. (Of course, $n!H_n$ must be an integer, so that multiplying the approximation for $H_n$ by $n!$ and rounding to the nearest integer gives an even better approximation for $H_n$).

In a computer simulation using the Random Permutation routine of Mathematica™, I found for $10^5$ random permutations of 50 objects, 100 098 cycles of length 1, 49 970 cycles of length 2 etc. down to 2 005 cycles of length 50 and a total number of cycles (450 836) in close agreement (0.2%) with the expected number of cycles of $10^5 \cdot H_{50} = 449\,921$. These agreements are remarkable, given that the investigated $10^5$ permutations are a very small fraction of the total of $50! \approx 3 \cdot 10^{64}$ permutations.

## 9.5 Derangements

A (complete) *derangement* is a permutation that leaves no object in its original place. A well-known derangement problem is that of $n$ envelopes and $n$ letters: What is the probability that not a single letter will end up in its proper envelope if the assignment of letters to envelopes is random? (For large $n$, the probability tends to $1/e \approx 0.37$ or 37%.) For two objects, there is exactly one derangement, the transposition (2, 1). For 3 objects, there are two complete derangements, the two cyclic permutations (2, 3, 1) and (3, 1, 2).

No matter what $n$ is there is always exactly one permutation, with no derangements, namely the identity permutation where *all* objects are in their original place. There are never any permutations with just a single derangement because if one object is "deranged", there must be another one that is also "out of place". From these facts (plus a few other "insights") I once guessed the proper formula for the number $D(n)$ of complete derangements of $n$ symbols:

$$D(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \tag{9.17}$$

where the sum converges to 1/e for $n \to \infty$.

This is not to be confused with the birthday problem: how many people must be present at a party so that the probability that at least two persons have the same birthday exceeds 1/2? (Answer: 23).

## 9.6 Ascents and Descents

One aspect of permutations that has taken on considerable significance in recent times is the question of the longest rising (or falling) subsequence. Thus, in the permutation (1, 3, 5, 2, 4) of the first five positive integers, the longest rising sub-

sequence is 1, 3, 5 while the longest *falling* subsequence is 5, 2. According to a theorem by the celebrated Paul Erdös and Gyorgy Szekeres, (proved by the pigeonhole principle) any list of $k^2+1$ distinct numbers contains an increasing (or decreasing) subsequence of length $k+1$.

Thus, for $k=2$, any list of $k^2+1=5$ distinct numbers contains a subsequence of length 3.

Here is a list of three random permutations of 5 numbers 1, 2, 3, 4, 5:

$$(3,4,5,1,2); \quad (2,5,3,1,4); \quad (2,3,4,1,5).$$

The longest monotone subsequence of the first permutation is an increasing subsequence, namely (3, 4, 5). The longest subsequence of the second permutation is a decreasing one: (5, 3, 1). Both have length 3.

The third permutation has a longest increasing subsequence of length 4, (2, 3, 4, 5), i.e. greater than the guaranteed minimum of 3. Note that non-monotonic members (like the 1 in the third permutation) can intervene. The members of such subsequences don't have to be contiguous. They are therefore sometimes called *scattered* subsequences.

It is interesting to observe that the distribution of increasing (or decreasing) subsequences of random permutations is related to the distribution of the eigenvalues of certain chaotic dynamical systems. Such distributions are therefore of great contemporary concern.

## 9.7 Quantum Decrypting

The days of the RSA[2] public-key encryption scheme may be numbered. The reader will recall that the difficulty of breaking RSA encrypted messages hinges on the difficulty of factoring large numbers. While the ever-advancing speeds of number-theoretic factoring[3] can be easily held at bay by using ever larger key numbers, going from, say, 300 digits to 400 digits, a new paradigm is arising on the cryptographic horizon that will thoroughly undo RSA: *quantum factoring*. In 1994 Peter Shor[4] then working at Bell Laboratories in Murray Hill, New Jersey, proposed a quantum algorithm for very fast factoring large composite numbers. Shor's algorithm is based on finding the order ("period length") of certain number-theoretic sequences.

As is well known (no, this is not translated from Russian), to compute the *de*crypting exponent $t$ from the (public) *en*crypting exponent $s$, the following

[2] The RSA algorithm was named after Donald Rivest, Adi Shamir and Leonhard Adleman who published it in 1977. It was actually invented by Clifford Cocks three years earlier in a project classified TOP SECRET by British Intelligence.

[3] In May 2007 the largest number factored was $2^{1039}$-1—which has over 300 decimal digits—with the help of some 500 computers running "in parallel" for 6 months (see *Discover Magazine* (January 2008), pp. 17–30).

[4] P. Shor: *Proc. 35th Annual Symposium of the Foundations of Computer Science*, p. 124. See also *SIAM Journal on Computing* **26** (1997), p. 1484, for a full version of Shor's paper.

Diophantine equation must be solved:

$$s \cdot t \equiv 1 \bmod \phi(m)$$

where $\phi$ is Euler's $\phi$-function (also called totient-function) and $m$ is the (public) encrypting modulus. Now, if $m$ is the product of two primes, $p$ and $q$, then $\phi(m) = (p-1)(q-1)$. Thus, to obtain the value of $\phi$, the (secret) factors of $m$, i.e. the individual primes, must be known—not just their product!

How does Shor get these factors? Take a look at Euler's generalization of Fermat's "Little Theorem":

$$a^{\phi(m)} \equiv 1 \bmod m$$

for coprime $a$ and $m$. It follows that the sequence $a^k \bmod m$, $k = 1, 2, 3 \ldots$ has a period length that divides $\phi(m)$. For example, for $m = 10$, and $a = 3$, we get the sequence

$$3, 9, 7, 1, 3, 9 \ldots,$$

which has a period length of 4. (Remember: $9 \cdot 3 = 27 \equiv 7 \bmod 10$.) And 4 does indeed divide $\phi(10) = \phi(2 \cdot 5) = (2-1)(5-1) = 4$.

The same period length is obtained for $a = 7$: to wit 7, 9, 3, 1, 7, 9 …. But for $a = 9$ we get 9, 1, 9, 1 …, i.e. a period length of 2, but still a divisor of $\phi(10) = 4$.

The period lengths of $3^k$ and $7^k$ are therefore as long as possible. Such numbers $a$ are called primitive roots. 3 and 7 are thus two (the only) primitive roots of 10. (Only integers 1, 2, 4, $p^k$ and $2 \cdot p^k$, where $p$ is an odd prime, have primitive roots. The number of primitive roots equals $\phi(\phi(m))$, or 2 for $m = 10$.)

Now, if the primes $p$ and $q$ are different (and larger than 2), then $m = p \cdot q$ has no primitive roots and the period length $L$ can never attain the value $\phi(m) = (p-1)(q-1)$. But, $L$ is of course still a divisor of $(p-1)(q-1)$. In fact, in a large number of all (legal) choices of $a$, $L$ equals $(p-1)(q-r)/2$, so that the calculation of $p$ and $q$ from $L$ and $m = p \cdot q$ is easily accomplished.

One interesting relation between the period lengths of $a^k$ modulo $p$, $q$, and $pq$, respectively, is

$L_{pq} = \text{LCM}\ (L_p, L_q)$ where the $L$ are period lengths and LCM stands for "least common multiple".

For example, for $p = 5$ and $q = 7$ and $a = 3$ we get $L_5 = 4$, $L_7 = 6$ and $L_{35} = 12$, which is indeed the least common multiple of 4 and 6 and which also a divisor of $\phi(35) = 4 \cdot 6 = 24$. Here is a somewhat larger (randomly generated) example: $p = 229$, $q = 349$, $a = 7$, for which $L_p = 228$. $L_q = 348$ and $L_{pq} = 6612$—which divides $(p-1)(q-1) = 79344$ and is divisible by both 228 and 348, as it should as the least common multiple.

This is not surprising, because—as every physicist knows (but a mathematician still has to prove)—the period length $L_{ab}$ of two added oscillations (periodic sequences) with period lengths $L_a$ and $L_b$, respectively, is simply LCM ($L_a$, $L_b$). In physics and musicology this is known as a beat note and its frequency equals the largest common divisor of the two "beating" tones or, what is the same, the beat period is the least common multiple of the two (or more) beating periods. But there is

a big difference between telling the fundamental frequency (or period) of a musical note and determining the period length of a number-theoretic sequence $a^k$. For example, for $a = 97$ and the above ($p = 229$, and $q = 349$), the sequence $a^k$ mod ($pq$) starts as 97, 9409, 33542, 56734, … and continues in a seemingly random fashion showing no periodicity. Only after $6612 = 228 \cdot 348/12$ steps does it start over again: …, 11535, 1, 97, 94909, …. Such long periods are difficult to discern on a graphical printout. However, if converted to an audible tone, then even for fundamental period lengths as long as one or several seconds, the periodicity can be heard. (Typically, depending on the sampling rate, it sounds like the idling engine of a motorboat.)

## 9.8 Decrypting without Factoring

While the need of factoring the encryption modulus $m$ into its prime factors was considered an article of faith for breaking RSA, some number theorists have come up with a method of decrypting RSA that does *not* require factoring. In fact, with a sprinkling of (elementary) group theory and Euler's Theorem, it can be shown that the Diophantine equation

$$s \cdot t \equiv 1 \bmod \phi(m)$$

can be solved for $t$ *without* factoring $m$. Surprisingly, $\phi(m)$ in the above equation can be replaced by the *order* of the (publicly transmitted) encrypted message modulo $m$, the (public) encryption modulus. For the still necessary period finding one could use the Shor algorithm. So, while RSA has not yet been cracked, it is good to know that factoring is not a *sine qua non*. Also, *the order* is usually smaller than $\phi(m)$.

As an example, let us take $p = 617$ and $q = 2273$, i.e. $p \cdot q = 1402441$. For an encrypting exponent $s = 101$ and message $n = \mathbf{31415}$, the encrypted message is $31415^{101}$ mod 1402441 which equals 81679. Now the decrypting exponent $t$, as usually obtained, is given by

$$s \cdot t \equiv 1 \bmod \phi(m),$$

which requires factoring of $m$ (a 7-digit number in the example).

In the alternative method, $\phi(m)$ in the above equation is replaced by the order of the cryptogram, 81697, modulo $m$. This yields for the decrypting exponent $t = 1122413$ and it is easy to confirm the correctness of this result by calculating, modulo $m$, $81697^t$ which equals, wonder of wonders, the original message: **31415**—and we still don't know (or care) what $p$ and $q$ are.

But where is the connection with quantum mechanics (QM) and its calculating speed? Well, QM is good at Fourier transforming or spectral analysis. And Shor finds the period lengths of $a^k$ by Fourier analysis on a "quantum computer". I put quantum computer between quotation marks because Shor's algorithm isn't really a full-blown quantum computer—it's just a super fast period-length finder relying on quantum mechanics.

Of course, as a final step, the Shor algorithm calls for a measurement leading, in a quantum system, to a "collapse" of the wave function. However, the system collapses with high probability to the desired state, namely the spectral peak whose frequency is to be determined.

## 9.9 Quantum Cryptography

In an early realization of quantum cryptography, Anton Zeilinger and co-workers[5] transmitted an image (of a prehistoric statuette of a woman—the "Venus von Willendorf"), making use of *entangled photon states* originally called "verschränkte Zustände" by Erwin Schrödinger.

Entangled states are at the core of the Einstein, Podolsky, Rosen (EPR) paradox. Einstein, for one, never believed in the *spukhafte Fernwirkungen* (spooky actions at a distance) that are implied by EPR. But he was wrong and the seeming paradoxon invented by him, Podolsky and Rosen is now an experimentally verified foundation of quantum physics.

The use of entangled states allows *single* photons to be used in the quantum encryption scheme—a breathtaking achievement, especially in view of the fact that in the original interpretation of quantum mechanics, its laws were considered to be applicable only to large ensembles (Of course, because of photon loss during transmission and detection, the "single-photon" schemes usually employ several photons).

In the quantum cryptography scheme, invented by Charles Bennet and Gilles Brossard[6]; (see Sect. 9.11), the encrypted data is transmitted via an open (public) channel. But the data is made unintelligible by a secret key, a *one-time-pad*. And it is the one-time pad key, a sequence of random bits, that is transmitted via a secure, unbreakable, quantum channel.

## 9.10 One-Time Pads

One-time pads are considered the only really secure method of encryption because the key bits are used only a single time and then never used again so that no statistical information can be exploited. (The clever use of statistical dependencies is of course the root of most decrypting schemes.—C.E. Shannon derived a mathematical requirement for a key to be secure involving its entropy and the entropy of the message to be encrypted.)

In the world's navies, secret keys are often printed with water-soluble ink on blotting paper. But sometimes the ship doesn't sink and the key is recovered—as in

[5] T. Jennewein *et al*: Quantum Cryptography with Entangled Photon Phys Rev. Lett. **84**, 4729–4732 (15 May 2000) See also Bouwmeester, Ekert, Zeilinger (Eds): *The Physics of Quantum Information* (Springer, 2000).

[6] See C.H Bennet and G. Brossard, in *Proc. IEEE Int. Conference on Computers*, Bangalore (1984).

the case of the German submarine *U 505* that was "sunk" off West Africa on June 4th, 1944, by the U.S. Navy and then dragged to Bermuda across the Atlantic below the water's surface (to hide the fact that the key was captured). Three weeks later the captured code books were at Bletchley Park, the British deciphering center (with Alan Turing in residence).[7]

An ingenious variant of the one-time pad was used by the famous Soviet spy Richard Sorge. Sorge (who, on KGB orders, joined the Nazi party as a camouflage) memorized which page of the German *Statistisches Jahrbuch* for 1937 (publicly available at German embassies around the world) he had to consult on any particular day to extract the key. He was able to tell Stalin that the Japanese would "go south" and not attack the Soviet Union, which allowed the Russians to transfer their crack Siberian divisions to Moscow in November 1941—with the well-known result: Hitler's first major defeat.[8]

## 9.11 The Bennet-Brossard Key Distribution Scheme (BB84)

The seed idea for the BB84 scheme was the (totally impractical) proposal for "quantum money" by Stephen Wiesner in which each dollar bill, in addition to its serial number, carries 20 different polarized photons known only to the issuing bank. Because of the rules of quantum mechanics, such a bill could never be copied because the secret polarizations where (randomly) choses from *two* possible "channels": either horizontal/vertical or $\pm 45^\circ$. Here a "1" might be encoded by a vertical or a $+45^\circ$ polarization. A "0" would be encoded by a horizontal or $-45^\circ$ polarization.

If the potential money faker measured, for example, a $\pm 45^\circ$ photon with a horizontal/vertical photon counter, he would get a random result—without knowing that it was random! The bank, on the other hand, knowing all 20 polarizations, would, of course, have no problem reading the secret code and verifying the validity by comparing it to the serial number of the bill. The only problem with this lovely, totally secure, scheme: how do you store 20 photons for any length of time in a paper bill?

While the idea of using two different polarization channels was impractical for the creation of quantum money, it was resurrected for a quantum-mechanical secret-key distribution scheme called BB84. Here Alice, who wants to send secret messages to Bob (in the presence of an eavesdropper Eve) first constructs a one-time key pad shared with Bob. For this purpose she generates a sequence of random 1s

[7] *U 505* is now at the Museum of Science and Industry in Chicago. Earlier submarines whose codebooks (and equipment) were captured include *U 110* (May 1941) and *U 559* (October 1942).

[8] Sorge was made a posthumous Hero of the Soviet Union under Khrushchev and a street in *East* Berlin was named after him. The German Democratic Republic also issued a postage stamp with a portrait of Sorge—but not until after Stalin's death, who loathed Sorge—a "thorn in his side"—for being privy to his greatest blunder: ignoring the massive warnings of the imminent Nazi attack in June 1941.

and 0s[9]. Alice also generates a sequence of polarization channels chosen randomly from horizontal/vertical and $\pm 45^\circ$.

Next she transmits to Bob the random bits, each one over one of the randomly chosen polarization channels. Bob detects the photons he receives with randomly chosen polarization channels, which of course agrees only 50% of the time with the channel used by Alice. In a subsequent public communication Alice tells Bob which channels she has used and Bob discards all results measured by his using the wrong channel. Alice can do this publicly because she only communicates the channels and not the actual bits she transmitted. So evil Eve is none the wiser.

Quantum mechanics also guarantees that any eavesdropping can be easily detected. As a consequence of Heisenberg's indeterminacy principle, Eve's observing the photon stream from Alice to Bob will necessarily change some of the photon polarization states. To know that this is happening, Alice and Bob only have to compare some, say 50, bits and, if they all agree, they can safely assume that their photon link was undisturbed. If they do this publicly, they cannot of course use the check bits for encrypting.

One of the remaining principal difficulties is the inability of the polarized photon channel to work over large distances in the atmosphere, (which is apt to change polarizations) thereby precluding—for the time being—worldwide key distribution via satellites. However, optical glass fibers are sufficiently stable and such systems have in fact been successfully implemented.

Another open—political—problem is whether states should allow the free use of quantum cryptography because it would allow criminals unfettered communication.

[9] based on some *physical* source of randomness, such as a radioactive decay. If she were to use an algorithmic (pseudo) random number generated instead, she would of course, according to John von Neumann, live in a state of sin—there is no way to generate truly random numbers on a computer.