

QUANTUM CRYPTOGRAPHY, OR
UNFORGEABLE SUBWAY TOKENS

Charles H. Bennett,¹ Gilles Brassard,²
Seth Breidbart³ and Stephen Wiesner⁴

1. IBM Research, Yorktown Heights, NY 10598
2. Université de Montréal, Département d'I.R.O.,
C.P. 6128, Succ. "A", Montréal, Québec H3C 3J7
3. P.O. Box 1526, Wall Street Station, New York,
NY 10268
4. MIT Research Laboratory of Electronics, MIT,
Cambridge, MA 02139

ABSTRACT

The use of quantum mechanical systems, such as polarized photons, to record information gives rise to novel cryptographic phenomena, not achievable with classical recording media: 1) A Verify Only Memory (VOM) that, with high probability, cannot be read or copied by someone ignorant of its contents; 2) the multiplexing of two messages in such a way that, with high probability, either message may be recovered at the cost of irreversibly destroying the other.

Quantum multiplexing can be combined with public-key cryptography to produce unforgeable subway tokens that resist counterfeiting even by an opponent with a supply of good tokens and complete knowledge of the turnstiles that test them.

* Supported in part by the National Science Foundation and Canada's NSERC Grant number A4107.

INTRODUCTION

One of the first places public-key cryptography¹⁻² was applied is at the Zero Power Plutonium Reactor in Idaho Falls, Idaho.³ Because of the presence of fissionable materials, such as uranium and plutonium, it is important that only authorized persons be allowed in the facility. This is controlled by personalized access cards containing information on their bearers hand. The novelty about this scheme is that it includes a digitalized signature based on a trap-door one-way function. Because the computer that reads these access cards is not secure, the people who work at the facility could obtain the validation instructions. This would not enable them to forge cards for unauthorized persons, however, because of the asymmetry of public-key cryptography. (Notice that if the computer is indeed insecure, enemies might modify its programming to introduce loopholes in the validation process.)

Security in the Idaho validation process depends on the fact that the access cards are personalized. Nothing prevents an enemy from copying cards that should fall into his hands, but of course such illegal copies would do him no good. We propose here unpersonalized access cards that cannot be reproduced. More precisely, it is infeasible for an enemy to come up with even a single counterfeit card that would allow him in the facility. This claim has to hold true if the would-be forger is allowed to perform any experiments whatsoever on any number of valid cards, and if he has complete knowledge of the validation algorithm. In short, anyone can verify if a given card is valid, yet only the mint can produce them.

Of course, there would be serious disadvantages to using unpersonalized access cards in high security areas: an enemy would be allowed in, should he steal a valid card from an authorized person. For other applications, however, it would be unsuitable for the access cards to be personalized. This is the case, for instance, whenever authorization is available to the public at large upon payment of admission. Would it not be convenient for a transit authority to issue subway tokens that anyone could check for validity, yet no one could counterfeit? The impossibility of fraud should not depend on the use of a special type of paper or other similar conventional ideas that offer no real protection against well-equipped forgers, nor should it involve on-line communication with the transit authority. We propose here a scheme based on a fundamental idea of quantum physics: the impossibility of simultaneously determining rectilinear and diagonal polarization of photons.

ESSENTIAL PROPERTIES OF POLARIZED LIGHT ⁴

Polarized light can be produced by sending ordinary light through a polarizing apparatus such as a Polaroid filter or Nicol prism. A beam of polarized light is characterized by its polarization axis, which is determined by the orientation of the polarizing apparatus in which the beam originates. Although polarization is a continuous variable, and can in principle be measured as accurately as desired by passing the beam through a second polarizer, the quantum mechanical uncertainty principle forbids measurements on any single photon from disclosing more than one bit about the beam's polarization. In particular, if a beam with polarization axis α is sent into a polarizer oriented at angle β , the individual photons behave dichotomously and probabilistically, being transmitted with probability $\cos^2(\alpha - \beta)$ and absorbed with the complementary probability $\sin^2(\alpha - \beta)$. Deterministic behaviour occurs only when the two axes are parallel (total transmission) or perpendicular (total absorption). If the two axes are not perpendicular, so that some photons are transmitted, one might hope to learn additional information about α by measuring the transmitted photons again with a polarizer oriented at some third angle; but this strategy is to no avail, because the transmitted photons in passing through the β polarizer, emerge with exactly β polarization, having lost all memory of their previous polarization α . Any other elementary two-state quantum system, such as a spin $\frac{1}{2}$ atom, behaves similarly dichotomously and probabilistically.

VERIFY ONLY MEMORY

In order to get the reader used to quantum physics ideas, this section describes a very simple irreproducible subway token scheme that is not quite satisfactory because the validation process must be kept secret. Counterfeiting remains infeasible, however, given any number of valid subway tokens, even under unlimited computing power. Nonetheless, the scheme would be compromised should an enemy steal a validation turnstile.

The heart of these quantum subway tokens is an array of 20 pairs of mirrors, each pair containing a single trapped polarized photon with definite polarization direction chosen from among the four directions 0° (\leftrightarrow), 45° (\nearrow), 90° (\updownarrow), and 135° (\nwarrow). The mirrors should be reflective enough to store the polarization information for a reasonable length of time. Such a sequence of trapped photons (or other two-state quantum systems) is called a VOM (verify-only memory)

because it can be verified, but not accurately read or copied by someone ignorant of its contents. Each individual photon is called a vit.

To verify the sequence in the VOM, it suffices to measure each vit with a polarizer set to make the photon behave deterministically, for example reading the 0° and 90° photons with a 0° polarizer and the 45° and 135° photons with a 45° polarizer. The fact that all photons were absorbed or transmitted as expected would confirm the validity of the VOM, in the sense that a VOM differing in too many positions would have but a small probability of behaving in the same way.

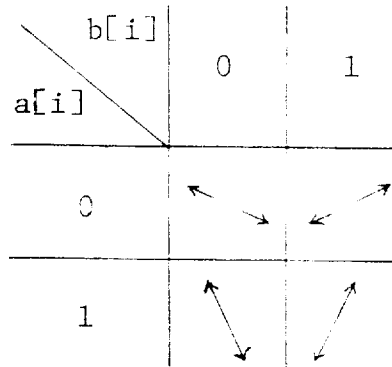
A counterfeiter ignorant of the VOM's contents, on the other hand, could not avoid measuring at least some of the photons neither parallel nor perpendicular to their prepared polarizations, thereby causing the photons to behave probabilistically and losing their stored information.

Suppose the counterfeiter goes ahead anyway, making some measurement and preparing a new VOM whose photons agree with the result of the measurement. Then, for each photon, the counterfeiter has a 50% chance of making the wrong measurement and in this case there is a 50% chance that the incorrectly forged photon will give the wrong answer when subjected to subsequent attempted verification. Thus the entire counterfeit VOM has only $(3/4)^{20}$, or about 0.3% chance of passing inspection.

Besides its VOM, a subway token needs to contain an ordinary machine-readable data string to enable the turnstile to know which quantum measurements to make. This data could be a unique serial number enabling the turnstile to look up the expected VOM contents in a master list stored in each turnstile. More elegantly, the VOM contents could correspond to a computationally secure authentication tag,⁵ which is computed from the data string together with some secret information known only of the turnstiles and the transit authority. Notice that this solution no longer offers security against unlimited computing power.

In this scheme, as in the others to be proposed later, the tokens must be distinct. A counterfeiter with access to a large number (20 would suffice) of tokens, known beforehand to be identical, could break the scheme by making both sets of measurements, and thereby learn the true VOM contents with only a small probability of error. Once this were known, the counterfeiter could make arbitrarily many copies of the given token.

Table 1. The polarization direction of photons in a quantum memory.

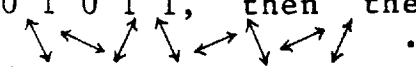


QUANTUM MULTIPLEXING

In order to obtain subway tokens that cannot be forged even if the validation mechanism is known, more sophistication is required. The major novel idea in this paper is that of Quantum Multiplexing. A quantum memory is a device capable of holding two pieces of information in such a way that either one can be read easily, but it should be computationally and/or physically infeasible to recover both. In particular, such a memory cannot be duplicated.

In order to multiplex messages A and B, we first expand them into A' and B', using an error correcting code that allows A and B to be recovered even if 14.7% of the bits are wrong. Let a[i] and b[i] denote the i-th bit of A' and B' respectively. For each i, the pair of bits (a[i], b[i]) is encoded by one single photon whose polarization angle is $(7-6b[i]-2a[i]+4a[i]b[i]) \times 22\frac{1}{2}$ degrees. In other words, the angle of the photon is given in Table 1.

If one tests each photon's vertical polarization, each bit of A' will be recovered with an error probability of $\sin^2 22\frac{1}{2}^\circ$, which is less than 14.7%. The message A can then be reconstructed, thanks to the error correcting code. Similarly, message B can be recovered if one tests the quantum memory's diagonal polarization.

For instance, if A and B are encoded into A' = 1 0 1 1 0 1 0 1 and B' = 0 0 1 0 1 0 1 1, then the photons will be polarized as follows: . A vertically polarized filter may read them as follows: 1 0 1 0 0 1 0 1, with one error on the fourth bit, which

will be of no consequence since the error correcting code will allow us to recover the original message A .

Of course, in order to have a reasonably small probability of failure with the error correcting code, it will be necessary to encode long enough messages. To be safe, we should also use an error correcting code capable of recovering messages with somewhat more than 14.7% of the bits wrong. Care must be taken, however, for too much redundancy might allow both messages to be recovered.

Any attempts to cheat by testing intermediate polarization angles would only succeed in losing both messages irreversibly, as long as each photon is measured independently of the others. In principle, however, there exist very complicated measurements that allow recovery of both messages by causing all the photons to interact simultaneously and coherently with the measuring apparatus. Although possible in principle, such measurements would be completely beyond the reach of present-day technology. We are currently investigating the hypothesis that this would indeed require a measuring apparatus of design computational complexity or physical bulk exponential in the length of the multiplexed messages. More details on this threat will appear in the final version of the paper.

UNFORGEABLE SUBWAY TOKENS

We are now ready to describe the unforgeable subway token scheme. Once and for all, the Transit Authority Administrator randomly selects two distinct large prime numbers congruent to 3 modulo 4, and computes their product. The latter, call it n , is revealed to the validating turnstiles. As we shall see, it will be sufficient to know n in order to validate tokens, yet knowledge of its factorization will be required to create them.

A unit is a triple $\langle x, y, a \rangle$ such that $0 < x < n/2$, $0 < y < n/2$, $0 < a < n$, a is relatively prime to n , the Jacobi symbol of x is plus one, and the Jacobi symbol of y is minus one. A unit is valid if $x^2 \equiv y^2 \equiv a \pmod{n}$. It is half valid if either x or y is a square root of a modulo n . Number theory tells us that valid units are plentiful as exactly one quarter of all numbers relatively prime to n have two distinct square roots modulo n that are below $n/2$, and these roots have complementary Jacobi symbols.⁶ Moreover, it was shown by Rabin⁷ that it is easy to come up with valid units as long as the prime factorization of n is known, whereas knowledge of a single valid

unit gives away the factorization of n . On the other hand, knowledge of n is sufficient to create half valid units. Under the assumption that it is infeasible for the enemy to discover the factors of n , it is therefore clear that none but the transit authority can compute valid units.

Whereas units are mathematical concepts, elements are their physical quantum implementation. An element consists of a classical memory, together with a quantum multiplexing memory. The classical memory records the field a of some unit. The quantum memory multiplexes the fields x and y of the same unit. An element is (half) valid if such is the case with its underlying unit. The validation process of an element goes as follows. A random decision of reading either x or y from the quantum memory is made, its Jacobi symbol is verified, and its square modulo n is computed and checked against a . The validation process succeeds if no errors are found. It should be obvious that the validation process always succeeds on valid elements, whereas it succeeds with a 50% probability on half valid elements.

We have already seen that an enemy cannot compute units (hence create elements) that are better than half valid, short of factoring n . The key observation is that, thanks to the unique features of quantum multiplexing, this remains true even given unlimited supplies of distinct valid elements. Indeed, the only information obtainable from a valid element is a pair of numbers such that one is the square of the other (modulo n). But, of course, such pairs can easily be computed without reading valid elements. In other words, elements can be validated with a 50% chance of being cheated, but they can neither be created nor reproduced.

In order to reduce the probability of being cheated, a subway token consists of a collection of twenty valid elements. In order to validate a token, the turnstile randomly chooses, independently for each element on the token, which half of this element's quantum memory should be read for validation. The best a forger could produce under such circumstances is a token composed of twenty half valid elements. The turnstile would therefore decide to read precisely the valid entries, hence accept the forged token, with a probability smaller than one millionth. This should discourage the most daring forgers. It is also possible for the forger, as we leave the reader find by himself, to convert a deterministically sure \$19 into a probabilistic value of \$10.

Finally, we would like to point out a free bonus gained from the utilization of this unforgeable subway token scheme. Should a would-be forger steal a turnstile in the hope of forging tokens, we have seen that he would not get any useful information from his felony. It is amusing to realize that his efforts would have been a complete waste since it will not even be possible for him to reuse the already validated tokens found inside the turnstile: the mere fact that these tokens have been validated by the stolen turnstile implies that their relevant information has been already destroyed!

CONVENTIONAL IMPLEMENTATIONS OF VOM AND MULTIPLEXING

The effects of quantum multiplexing can be achieved to a large extent through the use of more conventional devices, such as shielded, tamper proof, shift registers. Let x and y be two length n messages to be multiplexed in the quantum memory sense. Consider a $5n$ bit long shift register such that only the n middle bits can be read from the outside. The register is initialized with x as the n leftmost bits, y as the n rightmost bits, and zeros in the $3n$ middle bits. Bitwise left and right shifts can be requested from the outside. Clearly, it is easy to gain access to either x or y : shift the register $2n$ bits to the right (for x) or to the left (for y) and look through the middle bit window. Moreover, when the first bit of x appears in the window, the last bit of y has already been irreversibly lost through the right end of the shift register.

Although more practical, this implementation could perhaps be fooled. For one thing, how could one ever be 100% sure that the shift register is indeed tamper proof? Perhaps a new kind of ray could violate its contents without the register sensing it. Another potential loophole in this implementation is that some measurable phenomenon could leak out when bits "fall off" the shift register.

Rather curiously, it seems that a conventional implementation of the simpler VOM is somewhat more complicated than a mere shift register. We leave to the reader the problem of finding how to do it.

CONCLUSION

The more conventional VOM and multiplexing memories discussed above would allow practical implementation of unforgeable subway tokens. Their unforgeability would however be based on current technological limitations. Similarly, David Chaum has proposed a fairly different, more economical, solution to the technologically unforgeable subway token problem.⁸ On the other hand, the quantum subway tokens proposed in this paper offer protection against technological breakthroughs, but they could not be built with today's technology. The best available device known of the authors for holding quantum information is capable of preserving it for just over a second. However, the continuing advance of cryogenic and optical techniques promises considerably longer life time in the future.

REFERENCES

1. W. Diffie and M.E. Hellman, New Directions in Cryptography, IEEE Trans. Info. Th., IT-22:644 (1976).
2. R.L. Rivest, A. Shamir and L. Adleman, On Digital Signatures and Public-Key Cryptosystems, CACM, 21:120 (1978).
3. G.B. Kolata, New Codes Coming into Use, Science Magazine, 208:694 (1980).
4. P.A.M. Dirac, "The Principles of Quantum Mechanics, 4th edition," Oxford University Press (1958).
5. G. Brassard, Computationally Secure Authentication Tags Requiring Short Secret Shared Keys, in: "Advances in Cryptography: Proceedings of CRYPTO 82," R. Rivest, ed., Plenum Press, New York (1983).
6. M. Blum, Coin Flipping by telephone: A Protocol for Solving Impossible Problems, in: "Proceedings of 24th Comcon," IEEE, New York (1982).
7. M.O. Rabin, Digitalized Signatures and Public-Key Functions as Intractable as Factorization, MIT/LCS/TR-212 (1979).
8. D. Chaum, personal communication (1982).

Session V: Special Session on Cryptanalysis

