slides available for download at:
www.math.cm.is.nagoya-u.ac.jp/~buscemi/crypto.pdf

Introduction to Cryptography

from ancient ciphers to quantum cryptography

ブシェーミ・F（計算機数理科学専攻）buscemi@is.nagoya-u.ac.jp

What is a “cipher”?

From the online Oxford Dictionary.

cipher

Pronunciation: /ˈsʌɪfə/

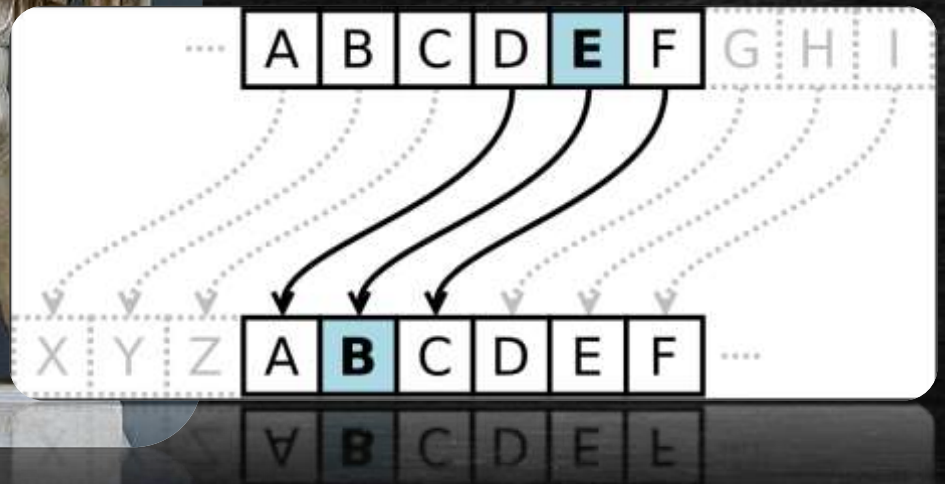
(also cypher)

NOUN A secret or disguised way of writing; a code.

Scytale (スキュタレー)

- from Greek σκυτάλη "rod"
- the Spartans, in particular, are said to have used this cipher
- it is a **permutation cipher**
- first mentioned in 7th century BC
- **very easy to crack** (probably used for message authentication, not encryption)

Caesar’s cipher

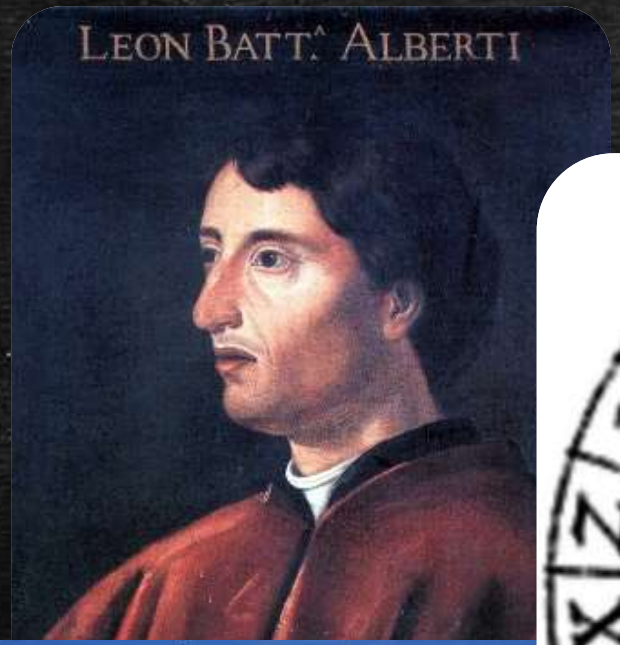


- it works by **substitution** (shift)
- in the example, each letter is replaced by the letter three places to the left
- Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW
- Example (plain): THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
- Example (cipher): QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
- very easy to crack… how?

Frequency analysis

Iraqi mathematician Al Kindi (c.801-873 AD)

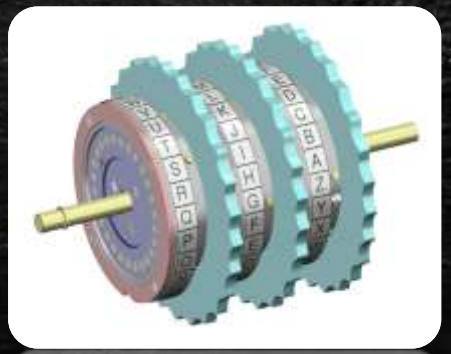
Alberti cipher



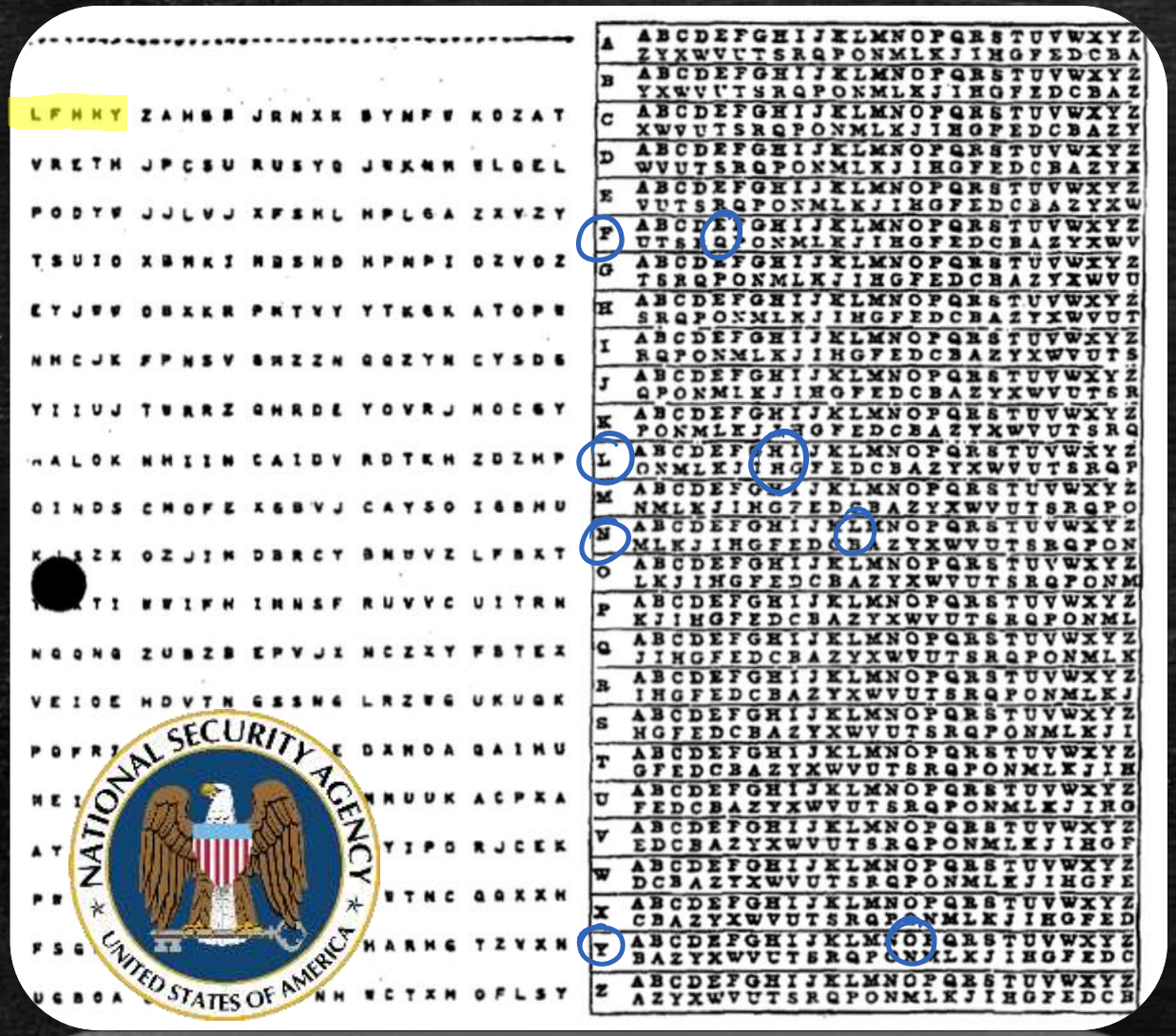
- Leon Battista Alberti (1404-1472): *De Cifris* (About Ciphers)
- it uses two disks: the outer one is fixed, the inner one is movable
- Example: outer disk ABCDEFGILMNOPQRSTVXZ1234
- Example: inner disk gklnprtuz&xysomqihfdbace
- it can **avoid frequency analysis attack**

Rotor machines

- the German **ENIGMA machine** was a kind of rotor machine
- state-of-the-art cryptography from 1920s to 1970s
- new substitution rule at each keypress
- idea similar to Alberti's disk

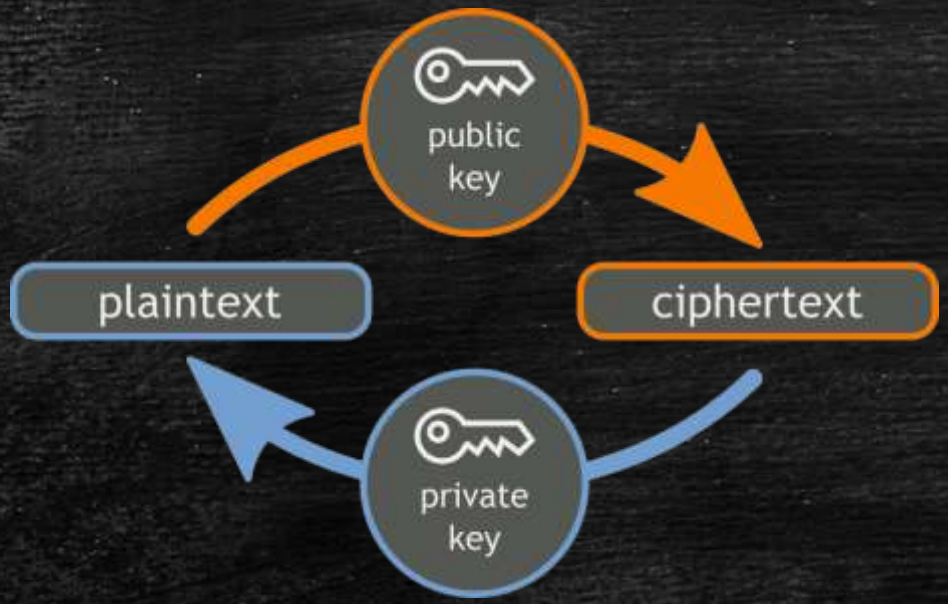


The one-time pad



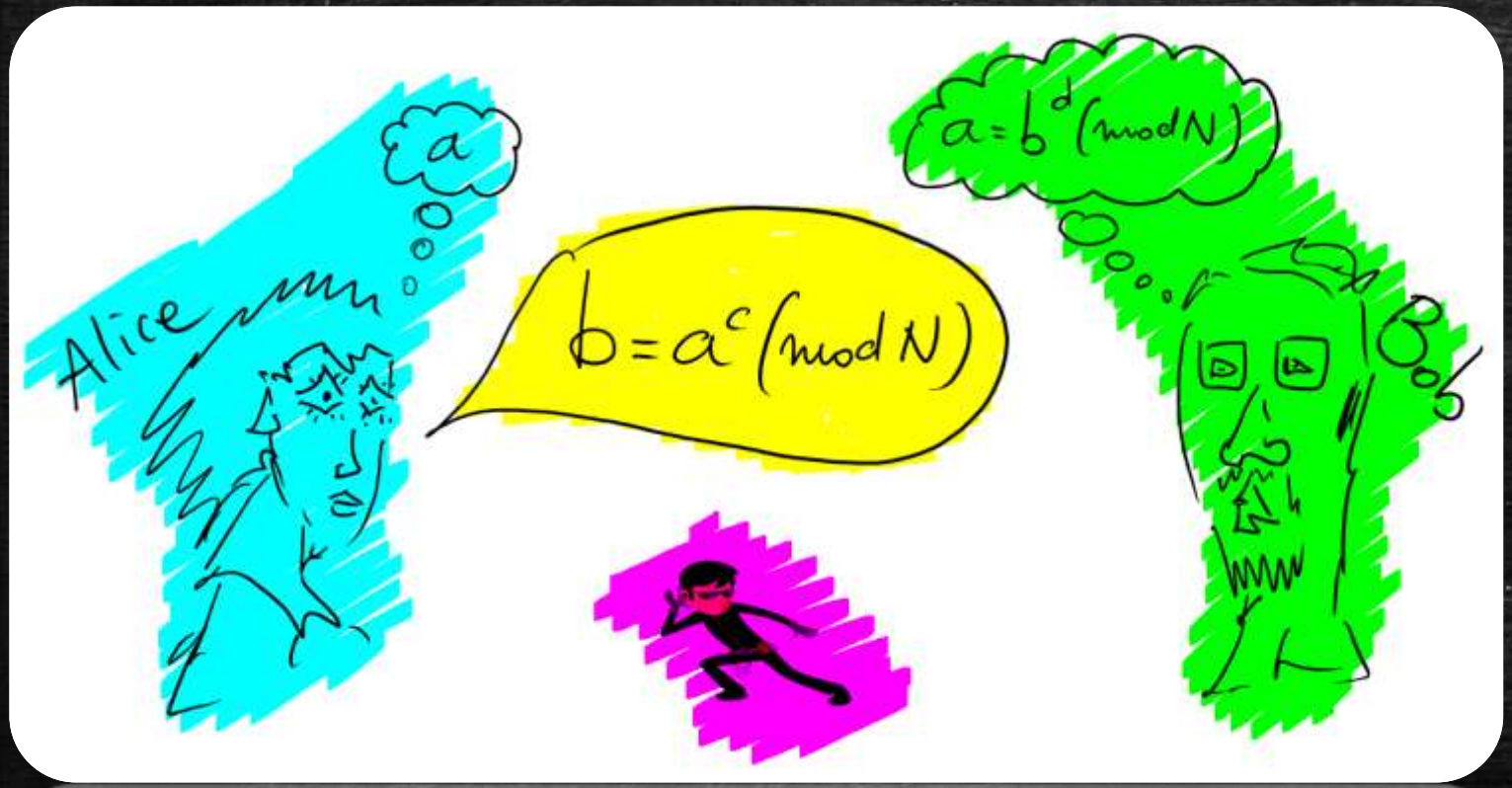
- one-time pad used by US National Security Agency in the 1950s
- **Unconditionally secure** (un-breakable)
- Plain text: HELLO
- Key: LFNNY
- Encryption: right side
- Cipher text: HQBBN
- Decryption: needs same sheet
- **Problem: distribution of the key!**

The 1970s revolution



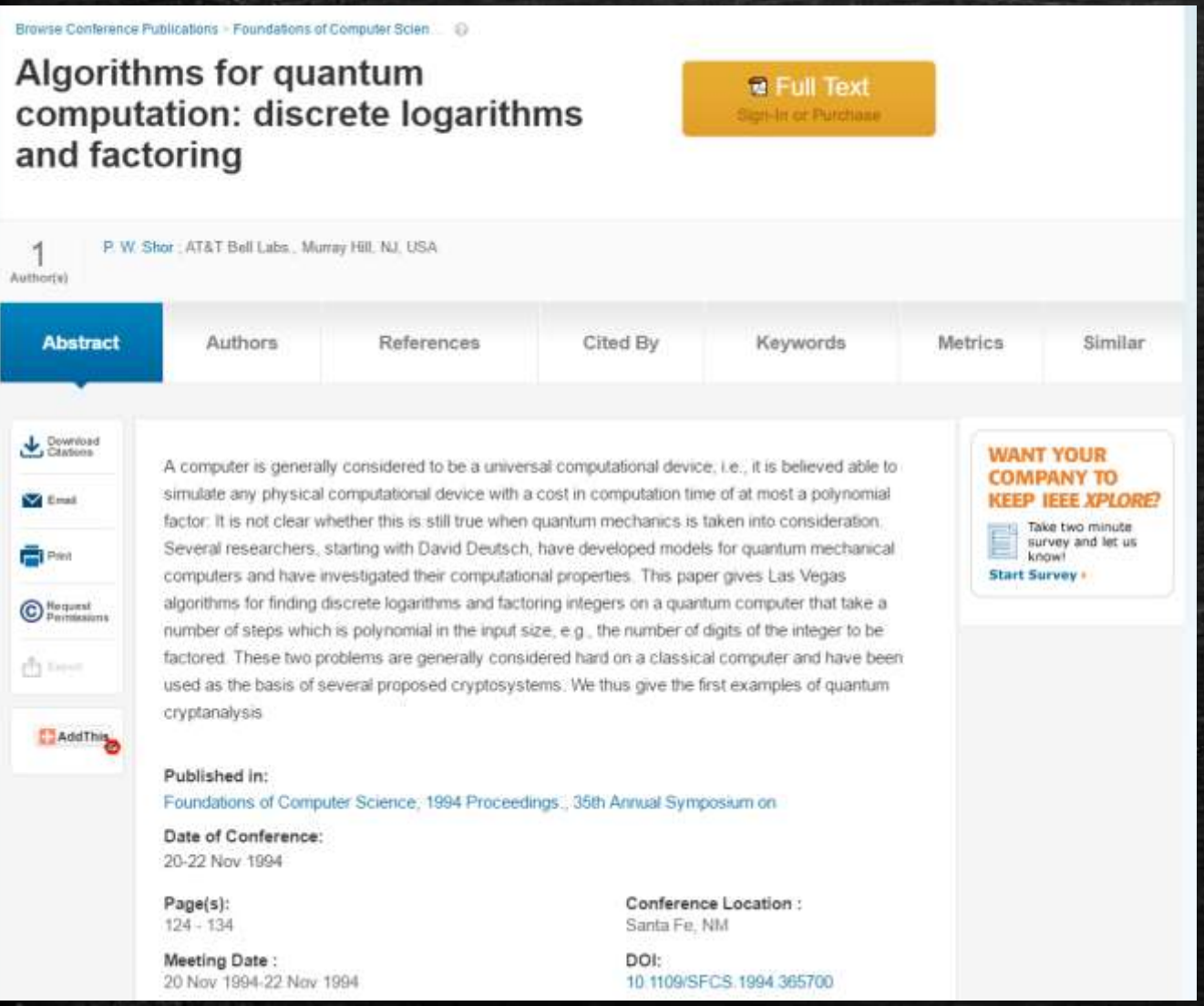
- idea of **asymmetric cryptography** (before, sender and receiver were "equal")
- the public key (known to anyone) is used to encrypt
- the private key (known only to the agency) is used to decrypt
- **RSA public-key cryptography** (Rivest, Shamir, Adleman, 1977; Cocks, 1973)

How does RSA work?



- choose primes p and q
- choose c such that c and (p-1)(q-1) do not have common factors
- compute d such that cd=1 modulo (p-1)(q-1)
- give c and N=pq to Alice
- encryption: $a \rightarrow b = a^c (mod\ N)$
- decryption: $b \rightarrow b^d (mod\ N) = a$
- **idea: factoring large integers is hard!**
- example: try to factor 43419877
- 43419877 = 5483 times 7919

Shor's algorithm (1994)



Browse Conference Publications > Foundations of Computer Scien...

Algorithms for quantum computation: discrete logarithms and factoring

Full Text
Sign-In or Purchase

1 Author(s)

P. W. Shor ; AT&T Bell Labs., Murray Hill, NJ, USA

Abstract | Authors | References | Cited By | Keywords | Metrics | Similar

Download Citations
Email
Print
Request Permissions
Export
AddThis

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. We thus give the first examples of quantum cryptanalysis.

Published in:
Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on

Date of Conference:
20-22 Nov 1994

Page(s):
124 - 134

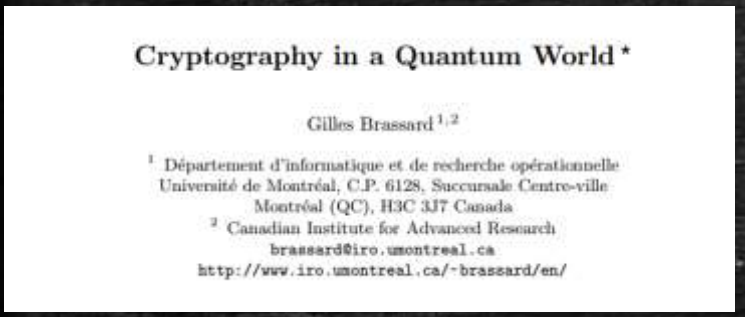
Conference Location :
Santa Fe, NM

Meeting Date :
20 Nov 1994-22 Nov 1994

DOI:
10.1109/SFCS.1994.365700

- Factoring large integers is hard on a computer
- Physics (quantum theory) can solve the problem efficiently (polynomial time)
- **RSA is not secure if quantum theory is correct!**
- Technological problems, but proof of principle works (and there are some experiments)

(Classical) Cryptography Today



Cryptography in a Quantum World*

Gilles Brassard[1,2]

[1] Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succursale Centre-ville
Montréal (QC), H3C 3J7 Canada
[2] Canadian Institute for Advanced Research
brassard@iro.umontreal.ca
http://www.iro.umontreal.ca/~brassard/en/

https://arxiv.org/pdf/1510.04256.pdf

It turns out that the American National Security Agency (NSA) is taking this threat *very* seriously indeed. This last August (2015), they issued a directive called "Cryptography Today" in which they announced that they "will initiate a transition to quantum resistant algorithms in the not too distant future" [39]. Most significantly, they wrote: "For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition". Said plainly, even though elliptic-curve cryptography is believed to be more secure than first-generation public key solutions against classical cryptanalysis, it is no longer considered to offer sufficient long-term security under the looming threat of a quantum computer to be worth implementing at this point. It's nice to see that *someone* is paying attention. For once, I'm glad that the NSA is listening! :-)

39. National Security Agency: Cryptography Today (Aug 2015), `https://www.nsa.gov/ia/programs/suiteb_cryptography/`, accessed on 8 October 2015

Does physics allow secure ciphers?

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

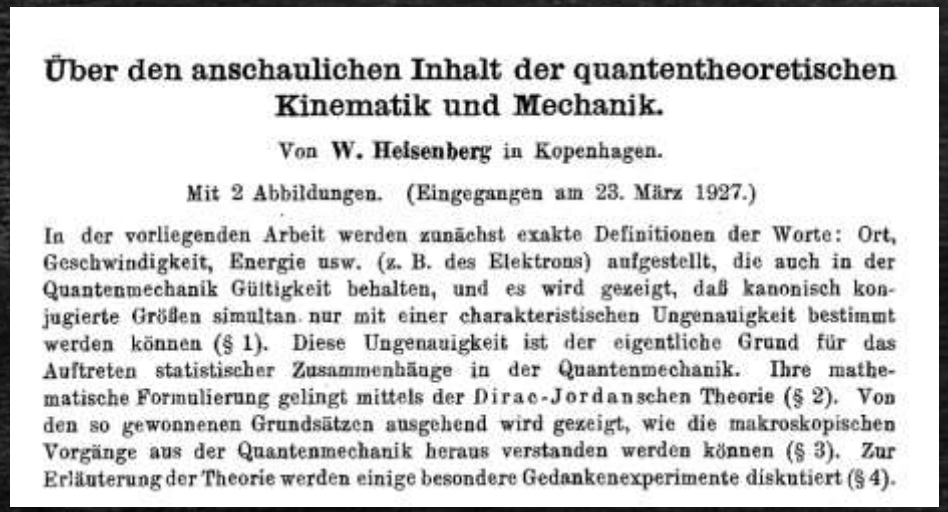
In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

- any piece of information (plain text, encrypted text, key, etc) is **carried by some physical system**
- Eavesdropper wants to get the information without being noticed (i.e., without disturbing the system)

Heisenberg's Uncertainty Principle

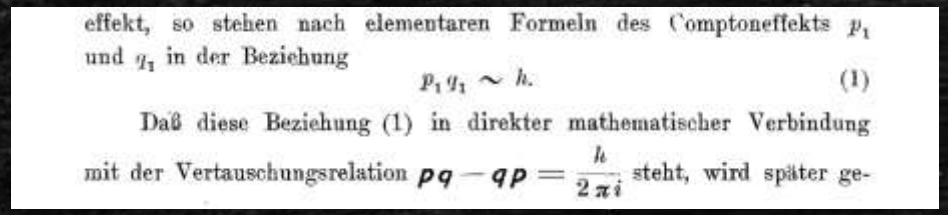


Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik.

Von **W. Heisenberg** in Kopenhagen.

Mit 2 Abbildungen. (Eingegangen am 23. März 1927.)

In der vorliegenden Arbeit werden zunächst exakte Definitionen der Worte: Ort, Geschwindigkeit, Energie usw. (z. B. des Elektrons) aufgestellt, die auch in der Quantenmechanik Gültigkeit behalten, und es wird gezeigt, daß kanonisch konjugierte Größen simultan nur mit einer charakteristischen Ungenauigkeit bestimmt werden können (§ 1). Diese Ungenauigkeit ist der eigentliche Grund für das Auftreten statistischer Zusammenhänge in der Quantenmechanik. Ihre mathematische Formulierung gelingt mittels der Dirac-Jordanschen Theorie (§ 2). Von den so gewonnenen Grundsätzen ausgehend wird gezeigt, wie die makroskopischen Vorgänge aus der Quantenmechanik heraus verstanden werden können (§ 3). Zur Erläuterung der Theorie werden einige besondere Gedankenexperimente diskutiert (§ 4).



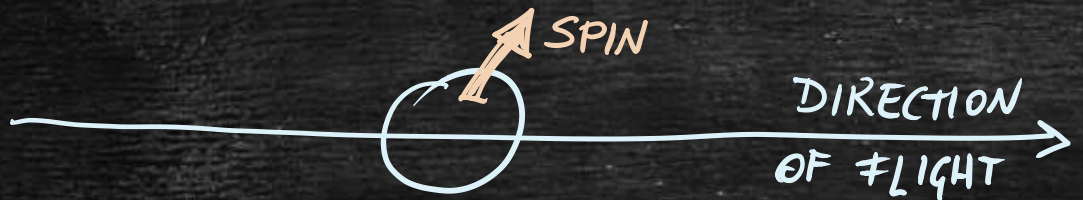
effekt, so stehen nach elementaren Formeln des Comptoneffekts p_1 und q_1 in der Beziehung

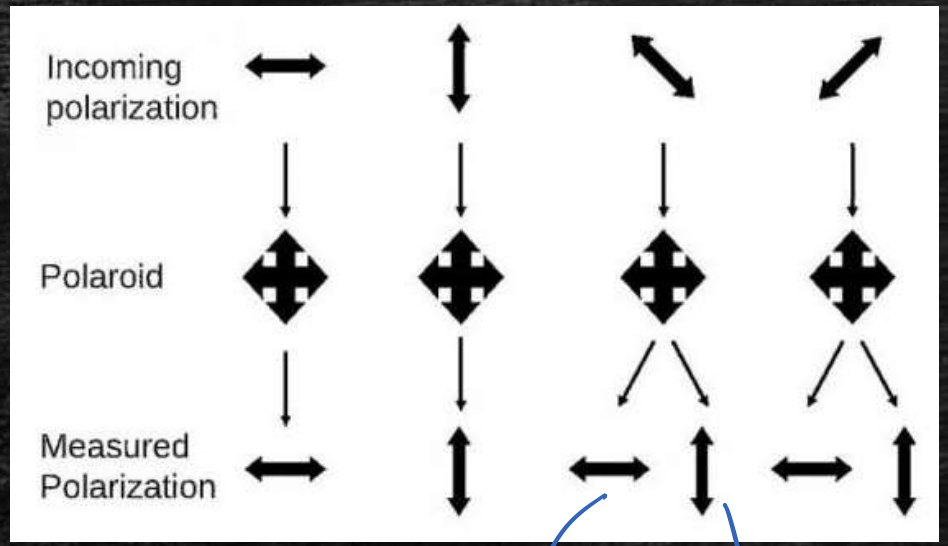
$$p_1 q_1 \sim h. \qquad (1)$$

Daß diese Beziehung (1) in direkter mathematischer Verbindung mit der Vertauschungsrelation $pq - qp = \frac{h}{2\pi i}$ steht, wird später ge-

- in quantum theory in general, no information can be obtained without disturbing the system
- disturbance can be detected
- hence **eavesdropping too can be detected**
- this is the idea at the heart of quantum cryptography

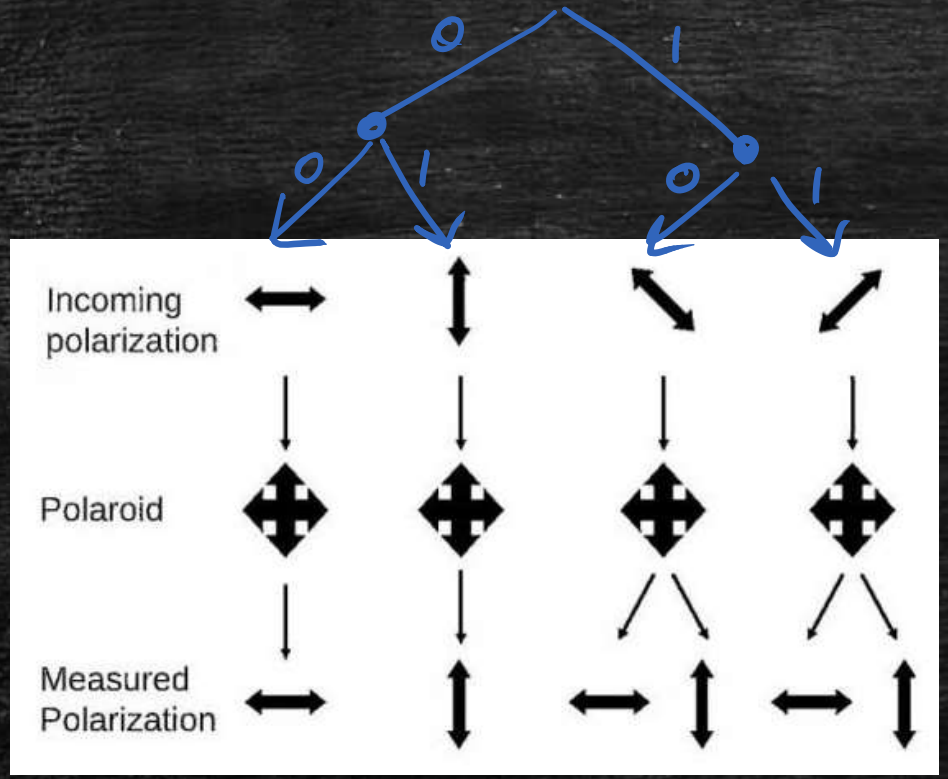
Quantum Cryptography: the idea





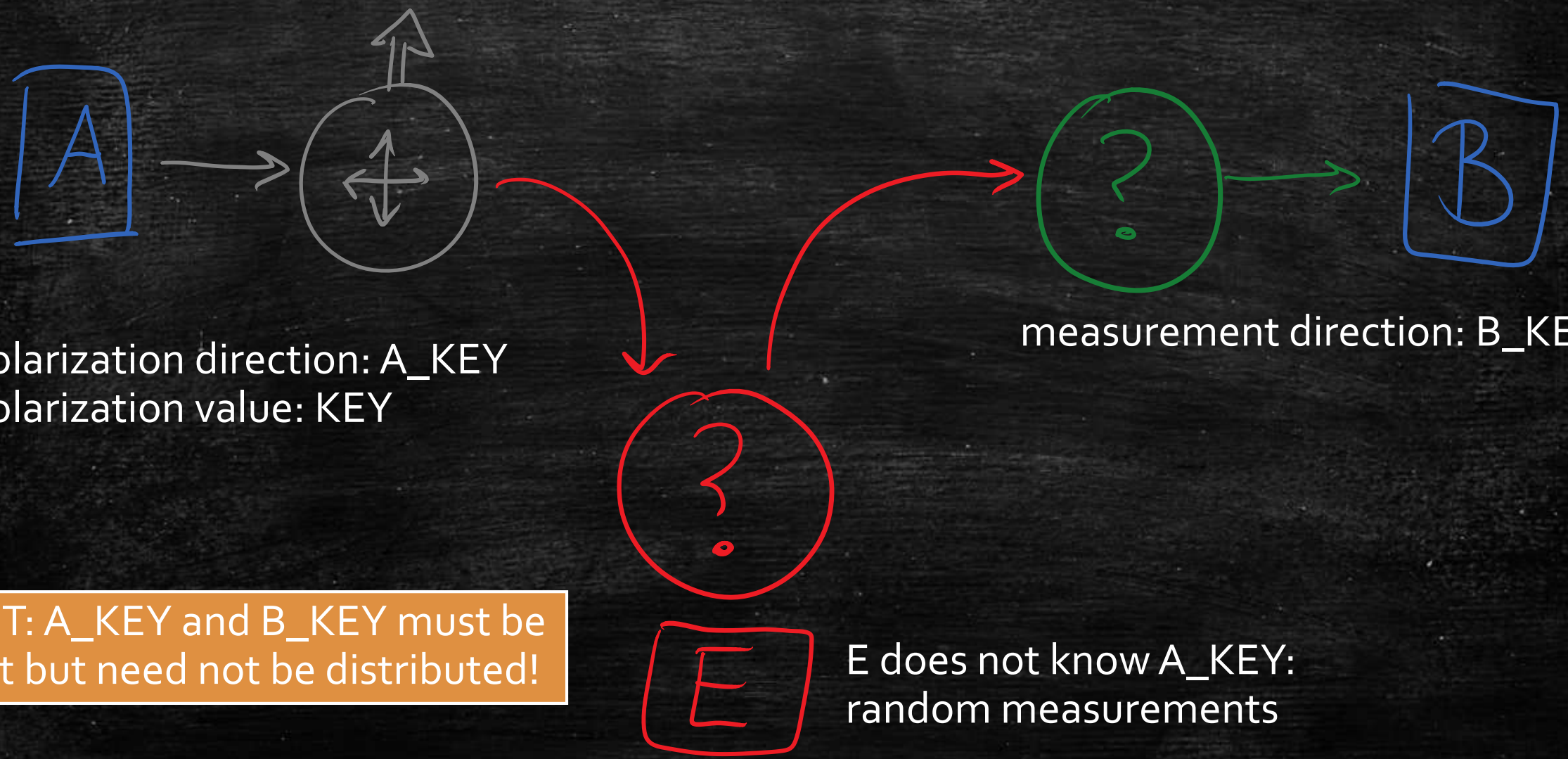
- Light is made of particles called photons
- Each photon has its own polarization, that can be ↑ or ↓ in some direction
- We cannot just measure "polarization"; we can only measure "polarization in some direction"
- If we measure polarization in the "correct" direction, we learn the "true" value
- If we measure polarization in the "wrong" direction, the result we obtain is completely random

Quantum Key Distribution: easy BB84



- three random strings: the KEY=(1110101…), Alice's key A_KEY=(0100101…), and Bob's key B_KEY=(1011010…)
- Alice's encoding: A_KEY decides the polarization direction, KEY decides polarization ↑ or ↓
- Bob's measurement: B_KEY decides the measurement direction
- at the end, Alice announces A_KEY: all events in which A_KEY and B_KEY differ are discarded
- in the remaining events, Bob measurement outcomes should perfectly agree with KEY
- how to be sure? Alice and Bob sacrifice some more events to compare KEY with Bob's outcomes
- if too many errors are found, that means that there was an eavesdropper and the protocol is aborted
- the remaining shared KEY is then used for one-time pad

BB84: the typical scenario



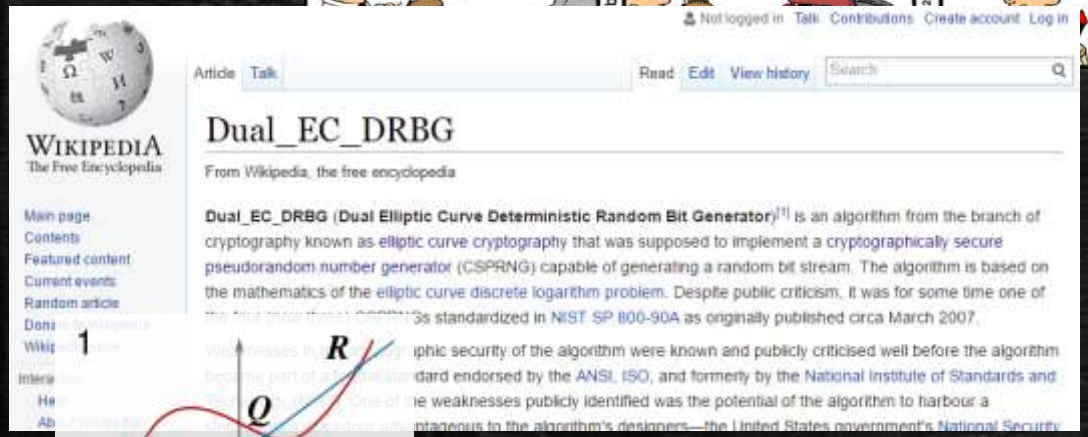
polarization direction: A_KEY
polarization value: KEY

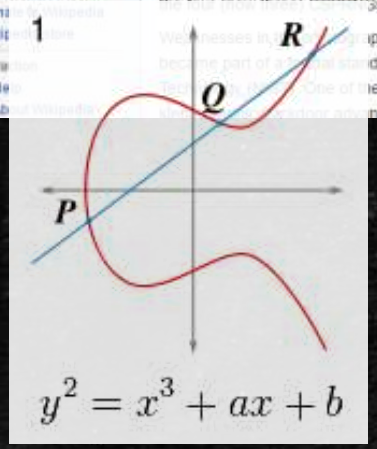
measurement direction: B_KEY

POINT: A_KEY and B_KEY must be secret but need not be distributed!

E does not know A_KEY:
random measurements

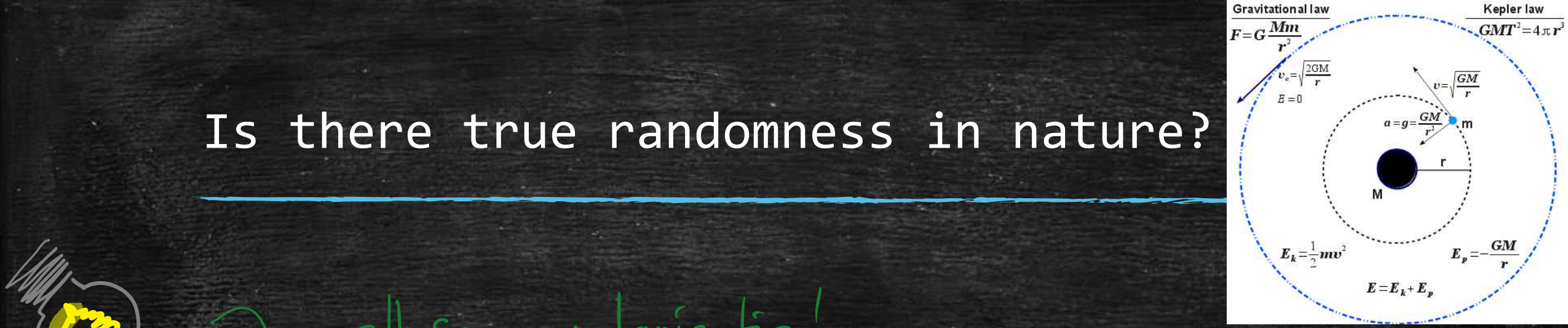
The role of randomness

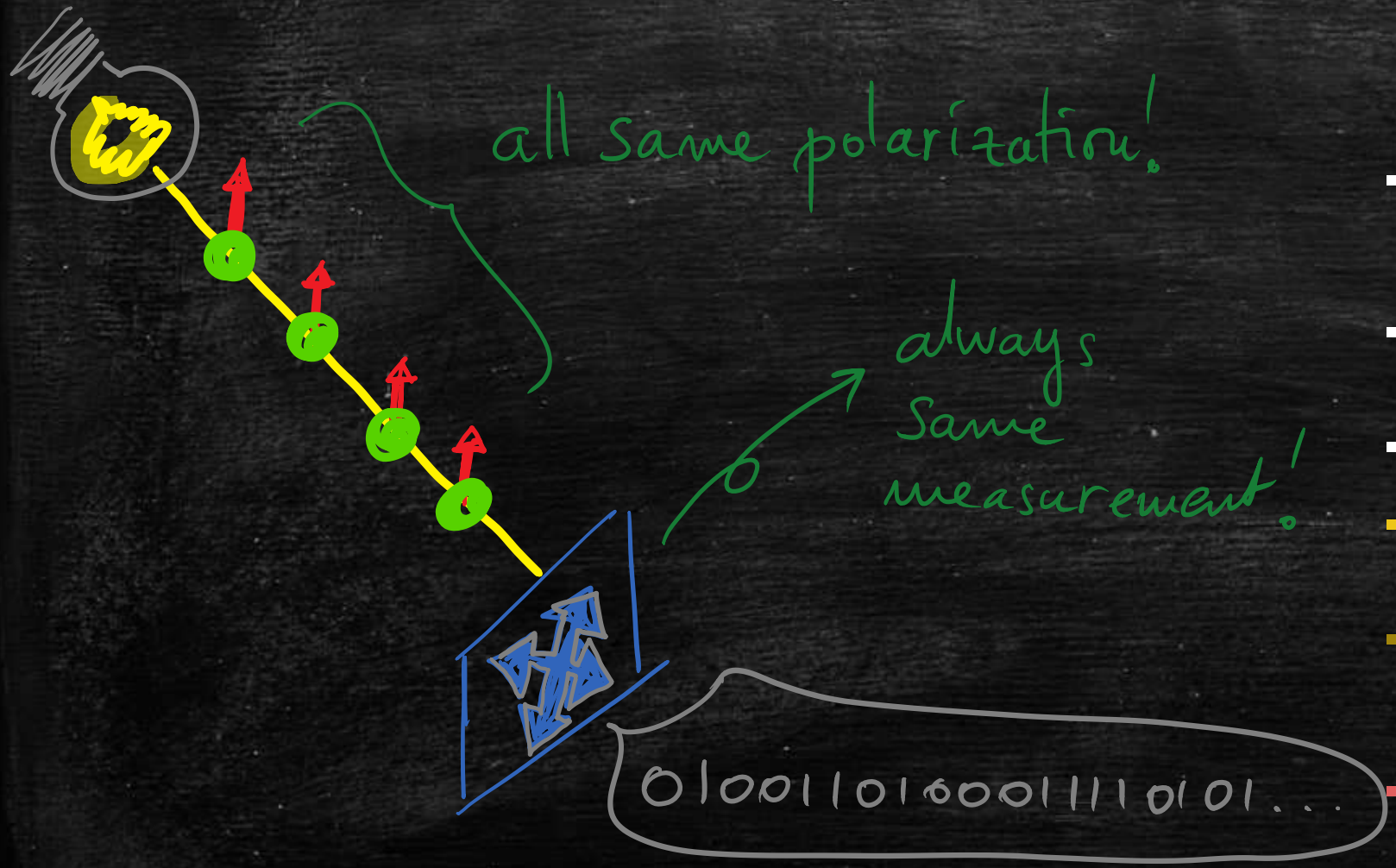




- Alice's and Bob's private keys must be unknown to the eavesdropper
- Can we guarantee that a random key is truly random?
- From Wikipedia: In September 2013, The New York Times reported that internal NSA memos leaked by Edward Snowden [...] concluded that the Dual_EC_DRBG standard did indeed contain a backdoor for the NSA.
- without true randomness there is no cryptography!

Is there true randomness in nature?





- produce a stream of photons, all polarized in the same direction, all same value
- measure polarization in the other direction
- obtain a stream of uniform random bits
- no randomness is needed in the process!
- randomness can be certified! (if quantum theory is true, the bits must be private and random)
- we can even buy both laser and measurement device directly from the eavesdropper…

Conclusions

- Ancient cryptography: art and technology, not science
- Modern cryptography: works because some problems are "hard" to solve on a computer
- Quantum computer: not yet completely understood, but it is sometimes exponentially faster than usual computers
- Can cryptography exist in a quantum world? Yes, but it has to be "quantum" cryptography!
- BB84 protocol: eavesdropper can be detected
- Role of randomness: quantum random number generator
- **The future of information security lies in between mathematics and physics!**

レポートについて

今日学んだ暗号化方法の中から
一つを選んで、それを簡単に説明せよ。

提出方法：e-mail to buscemi@is.nagoya-u.ac.jp
including **名前** and **学生番号**

締切：2016年6月10日（金）