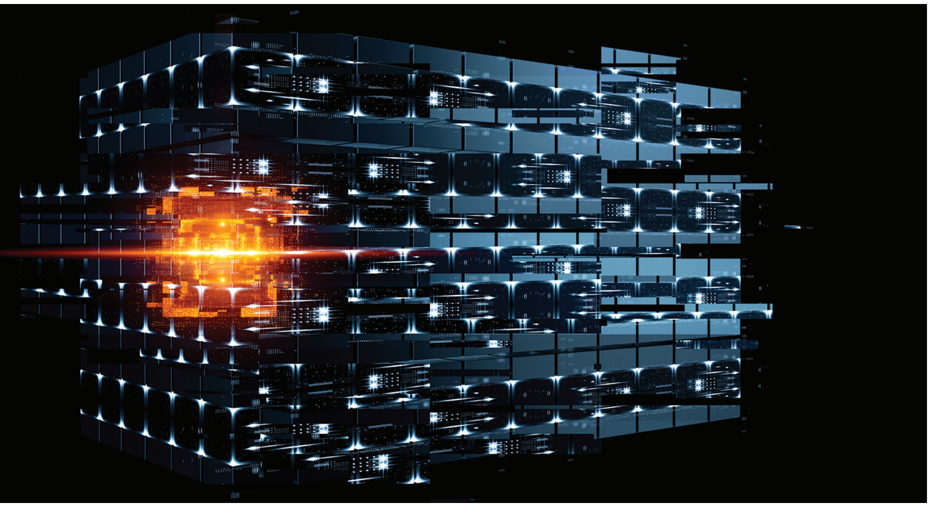
Against the Quantum Threat: Selective Compatibility

Disponible également en françaiss
www.isaca.org/currentissue

Identity theft is a serious issue in IT, and it facilitates countless other related frauds. A 2019 *ISACA® Journal* article titled "Chaos to the Rescue,"[1] discusses how to manage identity theft in IT. The article proposes five fundamental hypotheses about preventing fraud, the fifth of which is a consequence of the previous four:



JEAN JACQUES RAPHAEL | CISA, CISM, AZURE SECURITY ENGINEER, CEH, CNDA, ISO 27001 LI

Is a lead implementer of IT security at OctoSafes Inc. He is a gold ISACA® member and belongs to the ISACA Quebec City (Canada) Chapter. He can be reached at jean.j.raphael@octosafes.com.

JEAN CLAUDE CÉLESTIN | COMPTIA A+

Manages practical work at the University of Ottawa (Canada). He can be reached at jcele091@uottawa.ca.

ERIC ROMUALD DJIETHIEU | CDPSE

Is an IT security and telecommunication architect at Desjardins. He is also a cofounder of OctoSafes Inc. He can be reached at eric.romuald.djiethieu@octosafes.com.

1. Today, nobody needs a name or a number to be recognized by a computer.
2. Two objects cannot be entirely identical at a micrometer level.
3. To become safer, IT must obey new laws and new logic.
4. Information systems can protect people by protecting themselves.
5. "It is now possible, based on the previous hypotheses, to design information systems with limited compatibility (i.e., it can be impossible for two computers to communicate if there has not been some 'physical' interaction [remotely or not] between these two systems)."[2]

After publication, several objections were raised, in particular about the fifth hypothesis. Some readers felt as though the article was going back to the time of the terminal, when computers could only display results from the central server and only trained technicians could communicate with it via a console, incomprehensible codes and a green screen. But the question is: Will this backtrack always be possible or even necessary?

To answer this question, it is helpful to understand the evolution of cybernetics, the science of communications and regulation in living beings and machines[3] over the past 30 years. At one point, the original chips that equipped Commodore computers were relegated to the recycle bin. Of course, the original basic commands were still used, but to respond to the march of technological progress, personal computers (PCs) had to become compatible with each other. The IBM Compatible label enabled computers to talk to each other. It is thanks to this compatibility that the disk operating system (DOS) was developed and became the tool of choice for those who began to glimpse the formidable destiny of automatic information, or computing. This generalized compatibility has rendered great services to cybernetics, such as allowing computers to enter homes. Compatibility has rendered, and still renders in these times of teleworking, great services for information processing. Users know they can operate their computers for their daily needs without having to wonder if the programs will work, and they do not need to be programmers or technicians to obtain financial statements, statistical graphs, medical reports or strategic analyses. But what about security? As PCs have become more popular and useful, bad actors or individuals with malicious intent have made it their mission to discover ways to personally benefit. Thus, selective compatibility may be the only option to definitively remove the threat of attacks by establishing the need for privacy that information systems so desperately need.

“Chaos to the Rescue,” describes the digital four-dimension (4D) card,[4] which is the substrate for selective compatibility. It is a PC that is connected to an authentication server (AS). Only democratic governments can collect the data (e.g., biometrics) that are exchanged and stored between these two systems due to their highly sensitive nature. Data about a person’s birth, death, names, DNA and physical characteristics are collected from the card. This information is associated with the encryption methods currently used to make the transactions carried out by the card inviolable. It is both an identity card and a passport and contains medical, academic and other asset records of the owner. The biometric data recorded on both the card and the AS are confirmed at each use by the real owner's retina and palm print scans to prevent identity theft.

The quest for a minimum of privacy was considered when conceiving the 4D card. Without a minimum of privacy (i.e., if certain characteristics such as genetic or biometric data were not unique to the card or to the data and kept only in ultra-secure servers by government authorities) it would be easy for anyone to commit a crime by stealing the physical card.[5]

From its creation, the 4D card has carried out thousands of exchanges that are indecipherable by human intelligence, but also unbreakable by a quantum compiler. The unique parameters include a baby’s name, social security number (SSN), biometrics and genetic data; the card’s unique schematic circuit layout and the digitalization of the card’s surface by a microlaser; and the location (i.e., global positioning system [GPS] data), date and hour calculated to the millisecond. The initial interaction joins the requirements of another hypothesis in “Chaos to the Rescue,” which stipulates that the machine can protect itself. According to this hypothesis, the two machines will be able to determine the encryption and communication protocols only at the start of each transaction. The protocols will be unique and random during each connection. It will be impossible for a middleman to find certain patterns by analyzing a very large number of data exchanged during these connections.[6]

Selective compatibility may be the only option to definitively remove the threat by establishing the need for privacy that information systems so desperately need.

The Emergence of Quantum Computing

For the past few decades, cyberneticians have seen the danger of the quantum threat coming and have tried in vain to thwart it. Despite attempts to meet the need for privacy using complex passwords and multifactor authentication (MFA), trojans still gain the upper hand through circumvention methods such as phishing. Meanwhile the quantum threat is getting closer.

The quantum computer is:

> *[A] machine that relies on the laws of quantum mechanics to store and manipulate information. Unlike a classical computer which manipulates bits of information (0’s or 1’s), a quantum computer manipulates what are called quantum bits—or qubits. These can be in state 0 or 1 but also in a superposition of these states.*[7]

But how does this impact current security information systems?

Because the quantum compiler can exponentially increase the computing power of the quantum computer, it is feared that the factorization of certain prime numbers hitherto impossible for classical computers will become commonplace for the quantum computer. The role that this factorization plays in the RSA algorithm illustrates the potential danger that the quantum compiler would have, for example, on banking systems and even the coding of ballistic missiles. With the quantum compiler, everything becomes theoretically decipherable.

The hope on the part of security practitioners is that these threats remain theoretical. This may be

For the past few decades, cyberneticians have seen the danger of the quantum threat coming and have tried in vain to thwart it.

possible if the principles of selective compatibility are put into practice to help thwart quantum decryption.

The stakes are so high that the US National Institute of Standards and Technology (NIST) has been researching the problem since 2016.[8]

Selective Compatibility

Selective compatibility is achieved through a set of technical tools, processes and protocols that allow a conditional connection between several information systems (e.g., the 4D card, the AS and the third-party information system). Unlike the connection modes currently used, communication involves new parameters such as:

- The unique physical characteristics of the card
- The unique biometric and genetic characteristics of the user
- A third-party information system with which the user has certain specific relationships (e.g., a bank, university, medical clinic)

As an extreme example, take the case of the President of the United States. Upon investiture, the president's 4D card establishes contact with all the strategic institutions of the country: the Pentagon, the US Congress and the US National Aeronautics and Space Administration (NASA). The president's level of accreditation is the highest; other officials have access corresponding to their rank or role. This information system is so segmented that it is impossible for a hacker to access such sensitive information.

Other innovations of modern technology that can facilitate and strengthen the implementation of selective compatibility include:

- The increasing integration of chaotic processes into daily lives
- The multiplication of the number of interconnections and the phenomenal increase in the speed of information circulation thanks to 5G communication
- Progress made in artificial intelligence
- The emergence of new types of coding replacing the (0, 1) symbols of binary language with other symbols such as those found in DNA
- The increasingly applicable advances toward the creation of the first quantum compiler

The New Direction of Cybernetics

The evolution of technology in recent years is dependent on three fundamental concepts:

1. **Boolean logic**—Based on binary calculation, Boolean algebra is the basis for the creation of computer science.[9]
2. **The Turing machine**—It is a fairly simple conceptual machine imagined by the computer scientist Alan Turing to explain how computers should work.[10]
3. **The Von Neumann's compilation theory**—Through this theory, John von Neumann, a Hungarian-American mathematician, physicist, computer scientist and engineer, introduced the notion of automatism, thanks to which the computer has become more than a calculator.[11]

Today's conventional computers are faster and can store more data in hard drives of smaller volumes than ever before, but they always obey these three concepts. This is what condemns any attempt to remedy the complex problems of failing to secure information systems. The fact that these three original concepts aimed above all to achieve optimal functioning of the computer and that security problems had not yet arisen or been considered makes it more difficult to integrate security mechanisms after the fact.

Hackers always manage to bypass controls and find loopholes. Therefore, information systems will never be flawless if they are based only on these three fundamental concepts. This is where the notion of selective compatibility comes into play. When a security breach is found, selective compatibility is used to contain that breach and prevent it from spreading.

The Pauli Exclusion Principle and Selective Compatibility

To implement the selective compatibility principle, it is helpful to first understand a classical interpretation to the quantum theory known as the Pauli exclusion principle.[12] This interpretation remains classic due to the fact that the principle of interposition, which requires that a qubit (qbit) can have both the values

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/*onlineforums

0 and 1,[13] is not taken into account. For example, according to this principle, if an electron is in an orbit of the conduction band for an interval of time, this represents the bit 1. The time interval during which the electron leaves this orbit or energy level represents the bit 0.

To better understand the behavior of electronic current within the silicon atom, there is the concept of covalent bonds.[14]

Each atom of an element of the periodic table consists of a positive nucleus made up of a certain number of protons and neutrons with one or more layers of electrons (e -) revolving around the nucleus in well-defined orbits. Metals are good conductors of electric currents because when a metal wire is subjected to a voltage, the electrons in the valence layer instantly pass to an upper layer, the conduction layer.

As shown in **figures 1** and **2**, with regard to the semiconductor element silicon (Si), passage to the conduction layer is more or less facilitated by doping elements such as phosphorus (with five electrons [e-] of valence) or aluminum (with three e- of valence).

Based on Pauli's exclusion principle, there is a completely new and more accurate interpretation of the classical interpretation of the conduction band. According to Pauli, two fermionic particles never meet in the same quantum state, so it must be considered that there is not only one conduction band, but that the electronic current is the result of several conduction bands.[15, 16]

Classical theorists did not believe it was necessary to consider subdivisions of the conduction band as subbands, each containing an electron at a specific energy level (or quantum state). According to Pauli, each electron is at an energy level distinct from other levels. Each energy level is determined by four quantum numbers denoted by the letters n, l, m, s (n, l, m and s are unique for each electron).[17] So, because at no time can two electrons orbiting around the atomic nucleus possess the same letters (n, l, m, s), it is quite possible to conceive of another behavior of the electronic current. By maintaining this interpretation in the context of physics, a significant problem in cybernetics is solved: preventing the quantum compiler from breaking the encryption keys currently used in securing sensitive information saved in current information systems. Because some data must remain confidential regardless of the compiler used, this classical adaptation of a quantum theory remains the only way to protect encrypted information from the quantum threat.

Classical Interpretation Based on the Pauli Exclusion Principle

A classical electronics deduction, based on the four valence electrons of the SI, is that it has, theoretically, 16 possible states (2^4) ranging from 0000 (four holes) to 1111 (four electrons).

However, by integrating the requirements of the Pauli Exclusion Principle into the classical model, there are eight electrons (1) or eight holes (0) (i.e., 256 [2^8]) in initial states for the same atom. Therefore, according to Pauli's interpretation, the conduction band is considered to be made up of eight electrons, each of which is in a well-defined energy state (i.e., binary values varying from 00000000 to 11111111).

FIGURE 1

N-Type Semiconductor

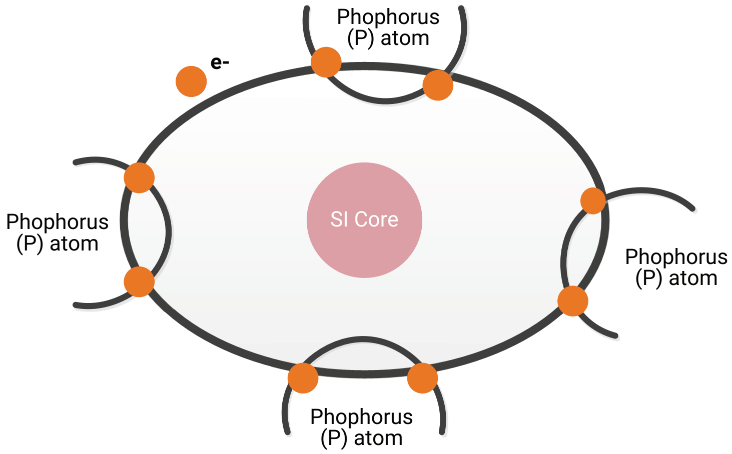
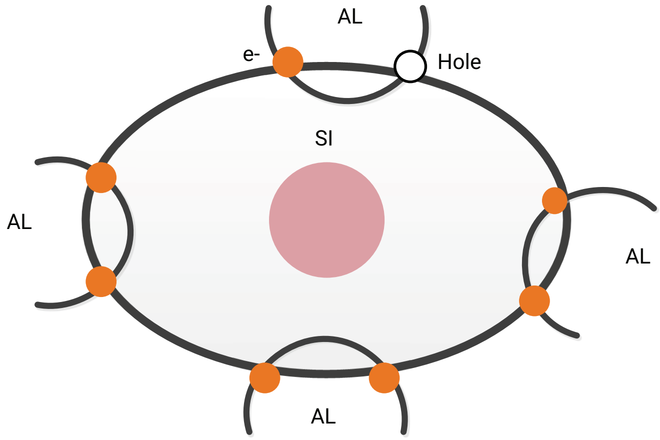


FIGURE 2

P-Type Semiconductor



Note: To respect the methodology, the covalent bonds are presented with the element Si; however, the latest generation of semiconductor elements could provide more satisfactory results.

Considering the immense services that the 16 initial states currently render in terms of encryption and hashing, there clearly are many more resources that could be drawn upon with 256 initial states in securing current data.

The Colored Bit Algorithm

A colored bit model can be used to explain how new electronic circuits built to simulate Pauli's energy level theory will work. Each color represents an electron at a specific energy level.

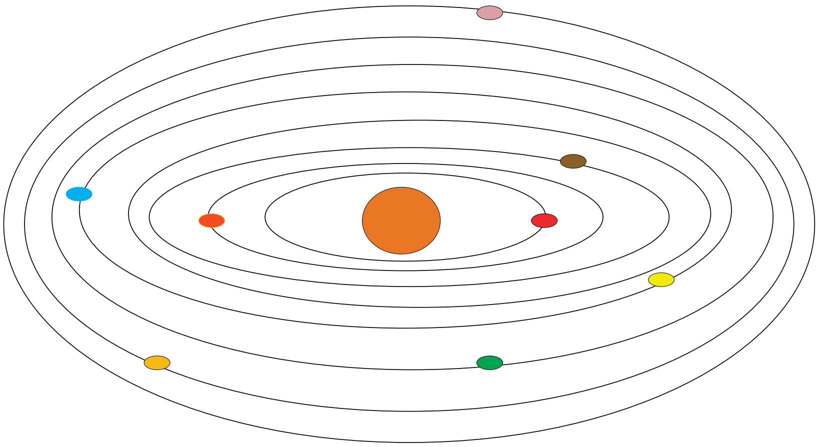
Figure 3 illustrates the covalent bonds for N-type semiconductors according to Pauli's energy level theory. A theoretical representation of the applications of this new interpretation of the electronic model is presented. This approach is not new. For example, theorists had to conceive of the transistor effect[18] before this component, which revolutionized all of modern science, was successfully produced in the laboratory. However, it should be noted that these concepts can only be referred to in this discussion because of lack of access to an electronic laboratory to test the circuit.

The proposed colored bit algorithm shown in **figure 4** should constitute the entry point to the realization of elementary logic circuits capable of simulating the completely classic operation of the Pauli exclusion principle.

The notion of a colored bit is a symbolic way to represent a mathematical reality. In fact, each color represents the energy level of the bit.

FIGURE 3

Representation of Conduction Bands According to the Pauli Exclusion Principle



Colored bits are not the same for each transaction. For instance, a red bit used in a channel for a bank transaction can become green for the next transaction addressed to the same bank on the same day. The bit may turn red again later, when the owner of the card communicates with a doctor or university, for example.

The need for privacy is necessary and already widely addressed by the use of passwords. However, passwords are failing because use of a password occurs a long time after the threat has taken hold and involves the same processes and logic as the threat. Whether to protect or to attack information systems, the same tools are used: the same Boolean machines with the same compilers that obey the same formal language rules.

Operation of a Seven-Line Display According to the Colored Bit Algorithm

After applying the colored bit algorithm, the next step is to create a matrix of diodes to materialize the notion of switching arising from the algorithm (**figure 5**). Creating this diode array is usually a laboratory exercise that allows beginner students to grasp how a basic switching circuit works. The traditional diode matrix is represented as it currently functions and then slightly modified to meet the requirements of the colored bit algorithm and of this interpretation of the Pauli Principle.

This matrix allows the switches to display numbers from 0 to 9 or certain letters such as A, C or E. It is made up of switches (SW), resistors (R), diodes (D) and light-emitting diodes (LEDs).

Variant 1 Adapted to the Principle of Energy Levels

Figures 6 and **7** show some modifications of the diode matrix presented. For the needs of the demonstration, the power switches were replaced by fixed capacitors (**figure 6**) and then by variable capacitors (**figure 7**).

Adding capacitors instead of switches makes it possible to pass a single frequency (e.g., 1) and to block all the other frequencies (0). This arrangement is not for practical use.

The circuit with variable capacitors shown in **figure 7** illustrates how a diode array should operate obeying the Pauli Exclusion Principle and the predictions of the colored bit algorithm. Depending on the time

FIGURE 4

Colored Bit Algorithm

```
//Declare
β: Boolean   // Value 0 (hole) ou 1 (electron)
t: float   // Time in microseconds
∑: states[7]   /* Sublayers array from 0 to 7 containing  β values
with 0 : Black; 1 :Brown; 2 :Red; 3 :Orange;  4 :Yellow; 5 :Green;
6 :Blue; 7 :Violet*/
/*Note that the colors have nothing to do with the electronic
coding used, for example, to determine the value of resistors.
Each color represents an accepted frequency, an energy level*/
C: channels[7]   /*Representing the bits from $\beta_3$ to $\beta_7$ addressed
to the recipient with Orange: Message encryption keys; Yellow:
Data concerning, for example, general management; Green: Data
concerning, for example, the human resources (HR) department;
Blue: Data concerning, for example, the finance department;
Violet: Data concerning, for example, the IT department*/
A: Authentification[3]   /* Array representing the bits from $\beta_0$ to
$\beta_2$ addressed to the Authentication server with Black: Physical
data of the 4D card; Brown: User biometric data; Red: global
positioning system (GPS) location data */
M : Message[4]   /* Representing the bits from $\beta_3$ to $\beta_7$ addressed
to the recipient with Orange: Message encryption keys; Yellow:
Data concerning, for example, general management; Green:
Data concerning, for example, the HR department; Blue: Data
concerning, for example, the finance department; Violet: Data
concerning, for example, the IT department*/
Begin   //Emission
Initialization
t=0.00
β becomes β
β becomes β
β becomes β
β becomes β
β becomes β
β becomes β
β becomes β
β becomes β
Display : states
∑= [β, β, β, β, β, β, β, β]
For  t from 0.00 to n.nn :
∑= [β, β, β, β, β, β, β, β]
Next
End  Next
// Transmission of signals through the Internet channels
β becomes β0
β becomes β1
β becomes β2
β becomes β3
β becomes β4
β becomes β5
β becomes β6
β becomes β7
Display : channels
c=[β0, β1, β2, β3, β4, β5, β6, β7]
End //Emission
Begin //Reception
Initialization
c=[β0, β1, β2, β3, β4, β5, β6, β7]
//Channels filtering and dispatching
Authentication // Bits for the authentication server
With:
β0 becomes β
β1 becomes β
β2 becomes β
Dispay: Authentication
A= [β, β, β]
End Authentication
Message // Bits for the office with encryption key
With :
β3 becomes β
β4 becomes β
β5 becomes β
β6 becomes β
β7 becomes β
Display: Message
M= [β, β, β, β, β]
End Reception
End
/* This program assumes that bit propagation occurs in parallel.
However, the circuits can be modified so that the propagation is
done in series resulting in the following pulse trains:*/
β becomes β5
β becomes β6
β becomes β7
β becomes β0
β becomes β1
β becomes β2
β becomes β3
β becomes β4
// In the channel containing, for example, the user's
biometric data. Or :
β becomes β6
β becomes β2
β becomes β3
β becomes β4
β becomes β7
β becomes β0
β becomes β1
β becomes β5
/* addressed to the IT department to increase the inviolability of
the information transmitted */
**
```

interval and the pulse having passed through the capacitors, the display will be of a definite color. After the bits are outputted with a specific color (i.e., frequency) from the computer that initiated the communication, they will be monochrome 0 or 1 across the Internet. However, when entering the servers concerned with the information, filters will sort and restore each bit to its original true frequency (i.e., color).[19]

An Example Scenario

To clearly understand how this new kind of information multiplexing works, consider an example of three employees working in a bank: one in the finance department, the second in human resources (HR) and the third in IT.

FIGURE 5

Traditional Diode Array

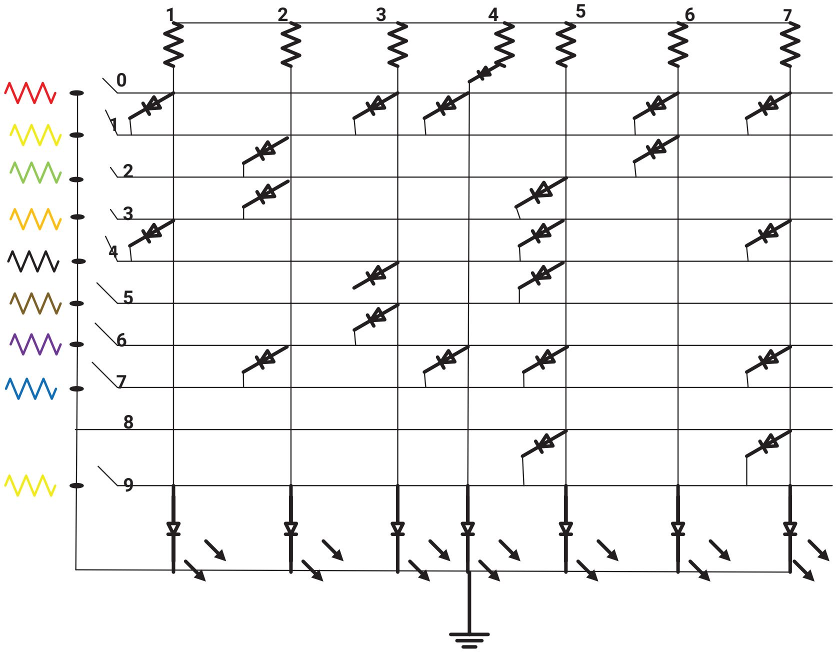
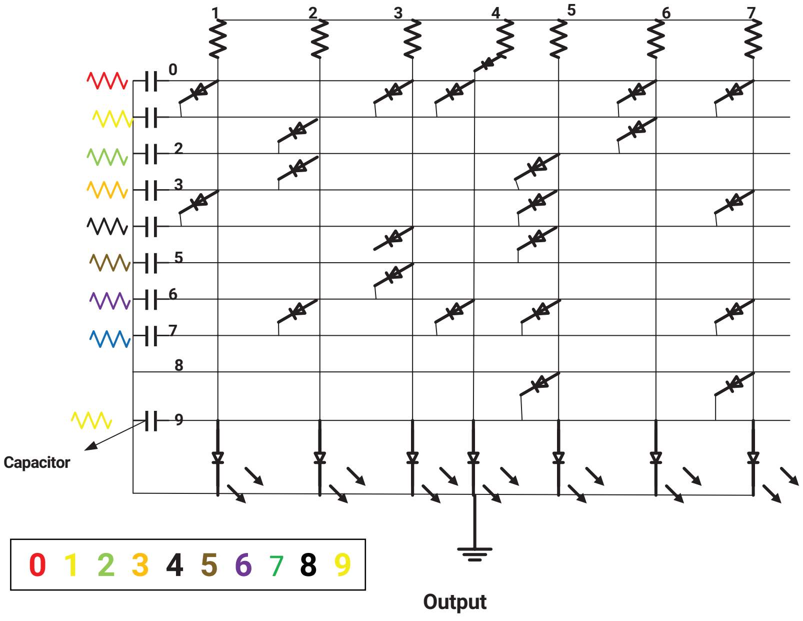


FIGURE 6

Seven-Branch Displays With Fixed Pulse Trains



These three employees work from home and use their 4D card to perform their daily tasks and other activities that may or may not require strict authentication. For example, the first employee uses his connection to work and consult his university file; the second employee uses his 4D card to do his job, but at the same time to chat with his friends without any need to authenticate; and the third employee sends several reports relating to the IT, HR and finance departments.

Using this new switching mode, the following scenarios become possible depending on the day, time and destination:

- For the first employee, the authentication server uses the data from the 4D card to decide that for each destination, a number of frequencies (i.e., colors) will be used. For example, in addition to the frequencies relating to the physical characteristics of the card and the biometric data of the user, the colors green, red and blue will be used for bank data, and orange, yellow and red will be used for university communications.
- For the second employee, the chat function is performed according to the traditional connection modes and only the data concerning the bank are processed by colored bits.
- For the third employee, colored bits are sometimes distinct and sometimes similar during the same time interval, allowing the employee to communicate with the three different departments.

How is this possible? Each of these protocols is programmed during the various points of physical contact that the authentication server has with the various 4D cards. These points of contact allow the authentication server and the 4D card to determine which filter will be used from end to end for each communication. During this time, the man in the middle will only see a certain number of monochrome bits (0 or 1), whether the system is equipped with a classic or a quantum compiler. All the data leaving the bank will pass through the Internet as a sequence of indistinguishable bits that are completely chaotic for any system not concerned with the actual communication. In addition, as noted in “Chaos to the Rescue,” the colored bits are found at layer 1, or the physical layer of the Open Systems Interconnection (OSI) model in charge of electronic current and bandwidth. The other traditional methods of encryption and hashing are associated with the colored bits to make any fraudulent decryption process impossible.

These colored bits provide a new kind of virtual security perimeter. While participating in encryption and factorization, the colored bits must first be considered as a *sauf-conduit*. Intruders cannot enter an information system without it because they cannot show the accurate authorization. So, the result could be that the man in the middle wastes time trying to decipher a set of useless bits that are merely a physical deformation in the internal structure of the card.

Conclusion

With the proliferation of applications on the dark web, counterfeiters on the Internet have many opportunities for wrongdoing. It is not a wild assumption that the methods of authentication that are reliable today will become subject to manipulations in the future. It is likely that attacks will take place when cybercriminals are equipped with quantum compilers and are able to breach the protections of the most critical information systems. In the future, the veracity and authenticity of information may become a true challenge. It is in the pursuit of authenticity that selective compatibility lies.

This research presents all the aspects that need to be implemented to achieve the security of information systems while ensuring that critical citizen data do not end up in the hands of those who could use it maliciously. It offers a new approach to addressing the quantum threat by using an intermediate solution based on the colored bit algorithm with new fundamental electronic circuits representing a materialization of the algorithm.

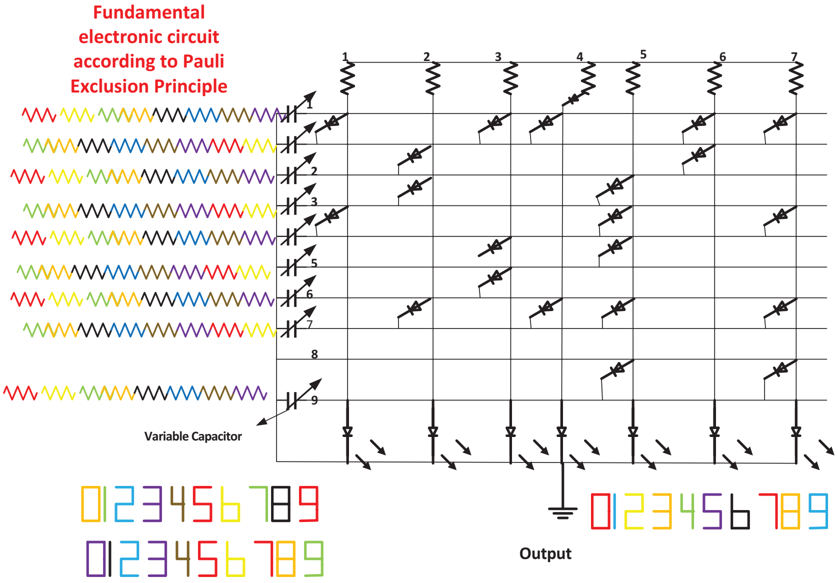
This research also aims to establish irrefutable accountability in information security. In the 21st century, accountability and authenticity must matter.

Endnotes

1 Raphael, J. J.; J. C. Célestin; E. R. Dijethieu; "Chaos to the Rescue," *ISACA® Journal*, vol. 4, 2019, *https://www.isaca.org/archives*
2 *Ibid.*
3 Dico en ligne Le Robert, "Cybernétique," *https://dictionnaire.lerobert.com/definition/cybernetique*
4 *Op cit* Raphael *et al.*
5 Nobody could steal information inside the card because of the chaotic encryption processes in place.
6 *Op cit* Raphael *et al.*
7 Collège de France "The Quantum Computing Ecosystem Is Emerging," 31 May 2021, *www.college-de-france.fr/site/frederic-magniez/Lecosysteme-de-linformatique-quantique-est-en-train-de-naitre.htm*
8 Calik, C.; M. Sonmez Turan; R. C. Peralta; "Boolean Functions With Multiplicative Complexity 3 and 4," *Cryptography and Communication*, vol. 12, 18 July 2020, *https://doi.org/10.1007/s12095-020-00445-z*

FIGURE 7

Seven-Branch Displays With Multifrequency Pulse Trains


Fundamental electronic circuit according to Pauli Exclusion Principle
1
2
3
4
5
6
7
1
2
3
5
6
7
8
9
Variable Capacitor
0123456789
0123456789
0123456789
Output

9 ScienceDirect, "Boolean Logic," *https://www.sciencedirect.com/topics/computer-science/boolean-logic*
10 Université de Toulon (La Valette-du-Var, France), *https://www.univ-tln.fr/*
11 Futura Sciences, "John Von Neumann," *https://www.futura-sciences.com/sciences/personnalites/matiere-john-von-neumann-256/*
12 Encyclopaedia Britannica, "Pauli Exclusion Principle," *https://www.britannica.com/science/Pauli-exclusion-principle*
13 Techno-Science, "Quantum Superposition Principle: Definition and Explanations," *https://www.techno-science.net/definition/8048.html*
14 Malvino, A. P.; D. J. Bates; *Electronic Principles*, McGraw Hill, USA, 2006
15 Georgia State University, Atlanta, Georgia, USA, "Pauli Exclusion Principle," *http://hyperphysics.phy-astr.gsu.edu/hbase/pauli.html*
16 Georgia State University, Atlanta, Georgia, USA, "Covalent Bonds," *http://hyperphysics.phy-astr.gsu.edu/hbase/Chemical/bond.html#c2*
17 Lobo, C.; "The Philosophical Meaning of the Pauli Exclusion Principle or the Position of the Problem of Individuation in Quantum Mechanics," Rue Descartes, 2020, *https://www.cairn.info/revue-rue-descartes-2020-2-page-166.htm*
18 Cité des Télécoms, "Invention of the Transistor and Integrated Circuit," *https://www.cite-telecoms.com/blog/histoire/200-ans-de-telecoms/les-temps-modernes/du-transistor-au-circuit-integre/*
19 *Op cit* Raphael *et al.*