www.konferenciaonline.org.ua

Міжнародна наукова інтернет-конференція

Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення

Випуск 102

ISSN 2522-932X

Google Scholar

AKADEMIA NAUK STOSOWANYCH
WYŻSZA SZKOŁA ZARZĄDZANIA I ADMINISTRACJI W OPOLU

16-17 вересня 2025 р.

м. Тернопіль, Україна – м. Ополе, Польща
2025

УДК 001 (063)

Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 102)*:* матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 16-17 вересня 2025 р.) / редкол. : О. Патряк та ін. ГО “Наукова спільнота”, WSZIA w Opolu. Тернопіль : ФО-П Шпак В.Б. 2025. 136 с. – ISSN 2522-932X

Збірник доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 102) 16-17 вересня 2025 р. на сайті www.konferenciaonline.org.ua

Наша адреса: Оргкомітет МНІК "Конференція онлайн"
а/с 797, м. Тернопіль 46005
тел. моб. 068 366 0 525
e-mail: inetkonf@ukr.net

URL Інтернет-конференції: http://www.konferenciaonline.org.ua/
ISSN 2522-932X

Volodymyr Tokariev, *PhD,*
Associate Professor of the department
of Information systems Simon Kuznets
Kharkiv national university of economics
ORCID: 0000-0002-7143-6165

Cai Yinda, *master, department*
of Information systems, Simon Kuznets
Kharkiv national university of economics

RESEARCH OF MODERN DIGITAL SIGNATURE METHODS

Internet address of the article on web-site:
http://www.konferenciaonline.org.ua/ua/article/id-2307/

In a face-to-face conversation, we can determine a person's identity by knowing their face, voice, or other biometric characteristics. In the digital world, it is more difficult to verify your face. When a user connects to their banking provider on the Internet, they need to know that their information is protected, that they are using a true website, not a false website. Transport layer security protocol provides this by using digital signatures when identifying a person. Digital signature schemes are the main ones in DNSSEC. They protect programs from accepting false DNS data. This happens when the DNS data cache is poisoned. The science that uses digital signatures when identifying a person is called cryptography. Cryptography is used to maintain the confidentiality of data and information when they are transmitted through network channels.

Cryptography began with the classical Caesar cipher to modern cryptosystems based on modular arithmetic. Then quantum computing appeared. The advent of quantum computing created a threat to modern cryptosystems based on modular arithmetic.

Complex computing systems are the basis of modular arithmetic ciphers. These ciphers cannot be solved in a short time. To solve this problem, researchers have developed quantum algorithms that can withstand quantum computing attacks.

A quantum computer is a machine that uses quantum-physical phenomena to perform calculations that are fundamentally different from those of the basic computer. When the basic computer is in a fixed state, a quantum computer is in a superposition state. Basic computers perform logical operations using a specific physical state.

Their operations are based on one of the states. A single state, on or off, up or down, 1 or 0, is called a bit. The internal state of the underlying computer is hidden.

The only way to obtain information about the state of the underlying computer is to perform a measurement. A quantum bit is usually called a qubit. Unlike a classical bit, a qubit can be in a state as shown in fig.1.

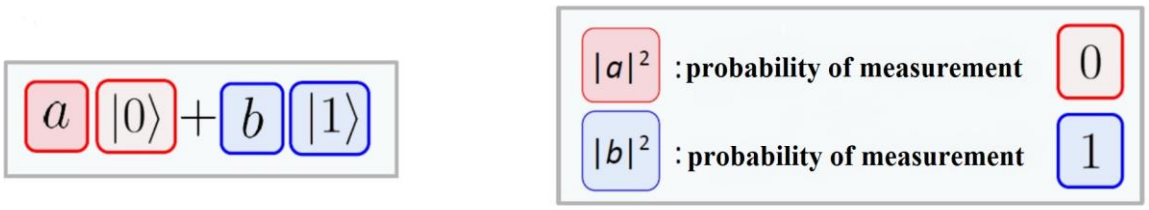

Fig.1. Quantum qubit

Note that a and b are complex numbers, the square of their modulus gives the probability of being in the state after measurement. The total probability of the qubit state must be equal to one: $|a|^2 + |b|^2$.

Scientists in China report that their quantum computer has solved a complex mathematical problem in a millionth of a second. This is 20 billion years faster than the world's fastest supercomputer could handle the same task. But it's not that simple, since efficient algorithms need to be created to run on quantum computers. A number of physical problems related to loss of coherence and error correction need to be solved.

To protect against quantum computer attacks, developers of security services and services must constantly assess the risk associated with the choice of cryptographic algorithms and develop new algorithms for the quantum world.

Література:

1. Токарєв В., Ільїна І., Шевченко І., Гриценко І. Про один підхід до рішення асиметричної TSP – задачі при B2C доставках за допомогою платформи "Swarm-bot" – system у фізичному неорганізованому середовищі. Системи управління, навігації та зв'язку, 2023. – №4(74), сс. 110-113.

2. L. E. Gryzun, V. V. Tokariev. Mobile applications design for digital education: IT-students' engagement experience on conditions of online learning the course "Mobile technologies". Proceedings of the 2nd Workshop on Digital Transformation of Education, co-located with the 18th International Conference on ICT in Education, Research, and Industrial Applications: (ICTERI 2023). CEUR Workshop Proceedings, 2023. Ivano-Frankivsk. Ukraine, pp. 110-123..

3. Koshovyi M. D., Pylypenko O. T., Ilyina I. V., Tokarev V. V. Growing tree method for optimization of multifactorial experiments, Radio Electronics, Computer Science, Control, 2023. – № 3, pp. 55-61.

4. Koshevoy N., Ilina I., Tokariev V., Malkova A., Muratov V. Implementation Of The Gravity Search Method For Optimization By Cost Expenses Of Plans

For Multifactorial Experiments. Radioelectronic and Computer Systems, 2023. – Vol. 1(105), pp. 23-32.
5. Ільїна І. В., Токарєв В. В., Яковлєв А. В., Шевченко І. І. Використання системи підтримки прийняття рішень для організації гуманітарної логістики, Системи управління, навігації та зв'язку, 2024, №1(75), сс. 88-91.

***Volodymyr Tokariev**, PhD,*
Associate Professor of the department
of Information systems, Simon Kuznets
Kharkiv national university of economics
ORCID: 0000-0002-7143-6165

***Denys Shvarov**, master, department*
of Information systems, Simon Kuznets
Kharkiv national university of economics

RESEARCH OF CLOUD TESTING METHODOLOGY SOFTWARE

Internet address of the article on web-site:
http://www.konferenciaonline.org.ua/ua/article/id-2306/

The most important task of a modern vendor of an IT company engaged in the development and sale of software is to reduce non-production costs, including the maintenance and servicing of its own IT infrastructure. One of the most effective ways to solve this problem is to switch to the use of cloud services. Cloud computing is the latest computing standard that is widely used to support software design tasks, including testing. As practice shows, such an IT direction as cloud testing helps to meet the needs of software vendors for hardware and software resources through the use of a flexible and relatively inexpensive cloud platform for testing.

However, it is important to note that to implement the wide capabilities of cloud testing, it is necessary to use an effective testing methodology. Testing methodology is a conceptual framework applicable to organizational testing processes, test management processes and / or dynamic testing processes in order to simplify testing. The main objectives of cloud testing are:

- confirmation of the quality of cloud applications, including their functionality, business procedures, performance and scalability, taking into account a set of requirements imposed on applications;
- checking cloud compatibility in the cloud infrastructure.

The following groups of cloud testing types are distinguished:

1. Cloud computing architecture testing.

Cloud computing architecture, like any other application or software, consists of two main sections: Front-End and Back-End.

Front end is a client or any application that uses cloud services.

Back-end is a network of client machines with servers that have a computer program and a data storage system.