SPECIAL TECHNICAL KNOWLEDGE IN THE FIELD OF DIGITAL CURRENCY AND MINING NECESSARY FOR LAW ENFORCEMENT OFFICERS

Pavel Galushin[1], **PhD**
Siberian Law Institute of the Ministry of Internal Affairs of Russian Federation

ABSTRACT

Purpose: This paper discusses the question of what special technical knowledge in the field of digital currency and mining is necessary to solve and investigate crimes committed using information and communication technologies. The examples highlight the special role of fundamental training in mastering advanced technologies, as well as the advisability of including relevant topics in the educational process of law enforcement educational institutions.

Design/Methods/Approach: For new technologies, the degree of usefulness is almost impossible to assess: since the technology is new, there is no experience in its application. It turns out that the so-called Lindy effect is observed: the longer a technology exists, the more likely it is to continue to exist. The Lindy effect leads to a paradoxical conclusion: in order to be successful in information and communication technologies, one should not chase after "fashionable novelties", but study the fundamental patterns underlying a large class of such novelties at once.

Findings: Modern information technologies, including those related to cryptocurrency, are based on fundamental knowledge in the field of mathematics (number theory, graph theory, cryptography) and electrical engineering.

Originality/Value: Thus, modern trends in the development of information technologies and their penetration directly into the sphere of legal regulation of public relations at the level of laws require improving the training of lawyers and law enforcement officers.

With regard to technologies related to digital currency and blockchain, it is necessary to focus on a combination of fundamental training and the usefulness of the teaching materials for students.

Keywords: special knowledge, digital currency, cryptocurrency, mining, crime investigation, information technology.

About the author

Pavel Viktorovich Galushin, Candidate of Technical Sciences, Associate Professor of the Department of Applied Computer Science in Legal Disciplines and Special Equipment, Siberian Law Institute of the Ministry of Internal Affairs of Russia, Krasnoyarsk, Russian Federation.

1 galushin@gmail.com

PURPOSE

Crimes committed using information and communication technologies remain one of the most widespread and rapidly growing categories of crime. Among other trends, there is a rise in AI-driven cyberattacks (deepfake scams, automated phishing) the incidence of which has increased by 300% since 2021 (Giboney et al., 2023). Only 17% of cybercriminals face legal consequences due to jurisdictional issues (Ashurov, 2024). Thus, the detection rate of crimes committed using information and communication technologies remains low. It can be stated that their public danger continues to increase.

One of the most modern information and communication technologies used to commit crimes is cryptocurrency. The use of cryptocurrencies in organizing criminal activity significantly increases the degree of conspiracy of criminals, for example, in the field of illegal drug trafficking. However, in recent years, the use of cryptocurrencies and the underlying blockchain technology has gone beyond the limits of exclusively criminal activity in this area.

Modern society is characterized by the intensive development of information technologies and the growth of their influence on people's lives. At the initial stage, information technologies were only a means of automating familiar activities, so they did not require special legislative regulation. However, over time, the development of science and technology has led to the creation of prerequisites for the formation of such social relations that run counter to conventional ideas, and attempts to regulate them legally without taking into account the specifics of their functioning encounter serious problems.

One of these information technologies is the so-called cryptocurrency – a phenomenon at the intersection of economics and computer technology, which has recently attracted significant public attention. Cryptocurrency is an information system for exchanging property in electronic form and, at the same time, a unit of measurement of the amount of this property. This article discusses the principles of functioning of cryptocurrencies and the influence of these principles on the possibility of applying the concept of property rights to cryptocurrency.

Today, cryptocurrency is not only used to commit crimes as a means of increasing secrecy, but has itself become an object of criminal attacks. Cryptocurrency mining, in turn, is often committed in violation of the law: theft of electricity, distribution of malware, non-payment of taxes from the sale of cryptocurrency.

Thus, cryptography, blockchain technology and cryptocurrencies are becoming objects of consideration of civil, tax, administrative, criminal and even constitutional law.

An effective fight against offenses in all of these areas is impossible without at least a superficial understanding of the principles of operation of the relevant information and communication technologies. For example, determining the most appropriate legal mechanism for ensuring the safety of cryptocurrency during a criminal investigation is based on an understanding of what makes it possible to manage an account in cryptocurrency. This thesis is confirmed by the penetration of references to specific technologies into the texts of laws. For example, Federal Law "On the Basic Guarantees of Electoral Rights and the Right to Participate in a Referendum of Citizens of the Russian Federation" includes the term "chain of blocks" (i.e. blockchain technology) and encryption and decryption keys (i.e. asymmetric cryptography).

In addition, in civil law, in connection with the introduction of the concept of "digital rights", the construction "in accordance with the rules of the information system" appeared. Before our eyes, the concept of "proof" in mathematics and jurisprudence is merging.

Thus, in some areas fundamental to the functioning of the state, information and communication technologies are no longer a "black box" for jurisprudence, the details of which can be left to technical specialists.

One of the barriers that complicate the understanding of modern information and communication technologies by specialists in other subject areas (including jurisprudence) is their very dynamic development and the constant emergence of new technologies. It is simply impossible for one person to keep up with them all. Today, there are no specialists in information and communication technologies at all; this sphere is fragmented into areas that are increasingly isolated from each other. All this leads to the need for each person to choose which specific information and communication technologies to master.

This paper discusses the question of what special technical knowledge in the field of digital currency and mining is necessary to solve and investigate crimes committed using information and communication technologies from conceptual and theoretical perspectives.

DESIGN/METHODS/APPROACH

One of the considerations that allow choosing which information technologies to master is studying those information technologies whose benefits for professional activity are immediately obvious. However, for new technologies, the degree of usefulness is almost impossible to assess: since the technology is new, there is no experience in its application. But with this approach, a person acts reactively: he passively reacts to what is happening. With this approach, law enforcement agencies will be in a catch-up position in mastering information and communication technologies compared to criminals. In order to be prepared for the emergence of new information and communication technologies that can be used to commit crimes, a proactive approach is required.

It turns out that the so-called Lindy effect is observed: the longer a technology exists, the more likely it is to continue to exist. Thus, this effect statistically predicts that the longer a period something has survived to exist or be used in the present, the longer its remaining life expectancy. Longevity implies a resistance to change, obsolescence, or competition, and greater odds of continued existence into the future. In other words, the probability of disappearance of a certain technology decreases with time. That is, the logic of the life cycle of living beings, in which mortality increases with age, does not apply to them. (Taleb, 2021: 318)

The Lindy effect leads to a paradoxical conclusion: in order to be successful in information and communication technologies, one should not chase after "fashionable novelties", but study the fundamental patterns underlying a large class of such novelties at once.

This statement should not imply it is pointless to study new technologies at all. The point is in the choice of focus: what should a specialist focus on studying? New technologies can and even should be studied. After all, even technologies that are today believed to have been tested by time were once new. But at the same time, one must always keep in mind that something new can lose popularity as quickly as it attracted attention when it appeared. In reality, it is worth concentrating on technologies and knowledge that have existed for a long time.

Let us consider the key technologies that underlie the functioning of cryptocurrencies and are used to detect and solve cryptocurrency-related crimes, and try to trace the effect of the Lindy effect on them.

FINDINGS

The first cryptocurrency was Bitcoin; the name comes from the English words *bit* (the smallest unit of information in computing) and *coin*. An article describing this system was published in 2008 by a person or group of people under the pseudonym Satoshi Nakamoto (Nakamoto, 2008).

Bitcoin was created as a decentralized alternative to traditional electronic payment systems with centralized accounting, based, in essence, on the trust of participants in the organizer of the system (the state or a legal entity).

The exchange of property in electronic form requires maintaining a database that stores information on the status of accounts and transactions, as well as an authorization system – checking the right to dispose of accounts (implement transactions). In traditional electronic payment systems, this database and authorization system are managed by a trusted person – the organizer of this electronic payment system, who ensures the correct functioning.

If you refuse to have a trusted person, then a set of questions arises, without answers to which the functioning of such a system is impossible:

- How to check the right to dispose of property on the account?
- Where should the database of accounts and transactions be stored?
- How to ensure that transactions cannot be canceled after their completion?

Confirmation of the right to manage an account is carried out using asymmetric cryptography, namely, electronic signature technology. Creating an account in a cryptocurrency consists of randomly choosing a password and constructing an account number based on this password. The account number is open information and plays the role of the electronic signature verification key, and the password must be kept secret, since it is used to affix an electronic signature.

To transfer funds from one account to another, the owner simply signs (using specialized software) the corresponding order with his electronic signature and sends it to all participants in the system. At the current level of development of science and technology, there is no method for counterfeiting an electronic signature in a reasonable time, while anyone can verify that the order was actually signed by the account owner.

In cryptocurrencies, the current state of accounts, as a rule, is not stored at all, but is determined by the history of transactions. At the same time, the transaction database must be stored by all interested participants in the system. This, in turn, requires solving the problem of database consistency among different participants and its special case – the impossibility of canceling a transaction after it has been completed.

To confirm the right to manage a cryptocurrency wallet, an electronic signature is used, which in turn is based on asymmetric cryptography, and hash functions are used to link blocks in the blockchain without significantly increasing their volume.

Both asymmetric cryptography and hash functions are used not only in digital currencies (Rogaway & Shrimpton, 2004). Hash functions are operations that convert data (transaction details in the context of cryptocurrency) into fixed-length number. The key property of a good hash functions is that even a tiny change in the input produces a totally different hash output. In cryptocurrency, each block of transactions includes a hash of the previous block.

This is the essence of blockchain technology. The goal of mining is to manipulate the order of transactions and add random data to form a block so that its hash starts with a certain number of zeros, which is determined by the combined computing power of all miners. For hash functions used in cryptography and cryptocurrencies, this problem, according to modern concepts, can only be solved

by brute force. In addition, if a malicious participant attempts to alter one transaction, they would have to modify all subsequent blocks. That process requires as much resources as initial mining, therefore it is not practical.

Asymmetric cryptography is very widely used today due to the fact that it allows you to organize a secure channel for transmitting information over an unprotected one, for example, over the Internet. Therefore, it is used for authorization and data transfer by online banks, social networks and, in general, any sites that provide for the exchange of confidential information with users. This is possible because asymmetric cryptography uses two keys: a public key for encryption and a private key for decryption. There is no effective algorithm for recovering the private key from the public key. Therefore, the public key can be published or transmitted over an insecure communication channel.

Asymmetric cryptography is based on the achievements of number theory, which were obtained in the 17th and 18th centuries: Fermat's little theorem and Euler's theorem (Stallings, 2017). In turn, the roots of number theory can be easily traced back to the Common Era, for example the concept of a prime number (Dunham, 2018). All the mentioned results in complexity do not go beyond the school mathematics curriculum. A specific type of asymmetric cryptography used in the Bitcoin cryptocurrency is based on the use of so-called elliptic curves. The corresponding cryptographic methods were proposed in 1985 (Koblitz & Miller, 1985), while the study of elliptic curves was actively conducted in the 19th century (Weierstrass, 1863/2015), some results used in elliptic cryptography belong to Newton (Silverman, 2009: 45–50), and the first known consideration of such curves is given in Diophantus's Arithmetic, written in the 3rd century AD (Goldfeld, 1985: 25).

Of course, the development of the first cryptocurrency (Bitcoin) is a brilliant achievement, and its creator or creators were geniuses in several fields at once. But in order to understand the principles of cryptocurrency functioning, there is no need to be such a genius: there are complete descriptions of Bitcoin functioning intended for schoolchildren.

Despite the very recent emergence of cryptocurrencies (2009 – the emergence of Bitcoin, mass popularity among the general population – 2017), their principles are based on fundamental results that appeared long before the 21st century and are widely presented in the literature. Thus, the role of fundamental knowledge for information and communication technologies is confirmed by the example of cryptocurrencies.

When investigating such crimes, knowledge of electrical engineering becomes relevant for law enforcement officers. For example, the amount of stolen electrical energy can be estimated by the amount of cryptocurrency obtained through mining. A quick search of legal scientific literature reveals several publications in which "kilowatt per hour" or "kW/h" is mistakenly indicated as the unit of measurement for the volume of consumed or produced electrical energy. In reality, a kilowatt is a unit of power, i.e. energy consumption per unit of time. Accordingly, the unit of measurement for electrical energy can be "kilowatt hour", similar to such a unit of measurement for working time as "person-year".

Naturally, some familiarity with electrical engineering and physics would help to avoid such annoying mistakes. In the case of scientific publications, their immediate harm is not great, but in the case of legally significant documents, the situation can be worse: from damage to the reputation of government agencies to invalidation of investigative protocols. Let us emphasize that here again we are talking about a fundamental fact that does not depend on new models of mining equipment. Investigation of crimes committed using cryptocurrency or encroaching on cryptocurrency accounts is extremely difficult due to the anonymity of wallets. However, the exchange of cryptocurrency for material assets (which is the ultimate goal of most crimes in this area) mainly takes place through exchange sites or

stock exchanges, since it is quite difficult to find a counterparty who would agree to accept cryptocurrency as payment.

This means that the issue of determining the identity of the owner of a cryptocurrency wallet comes down to tracking the chain of transactions leading to the wallet on the exchange or exchanger. Cryptocurrency accounting is decentralized and information about all cryptocurrency transactions is available in open sources, such as exchange websites. However, manual tracking of transaction chains in real conditions is time-consuming and error-prone. Blockchain analysis systems have been developed to automate such actions.

Such systems, as a rule, represent web services from the end user's point of view, functioning on the basis of multiprocessor servers. Designing such hardware and software complexes is a separate engineering task. To model the performance of such complexes, the apparatus of queuing theory is used, and for optimization, evolutionary methods of global optimization are used (Galushin, Serikova, Terskov & Yarkov, 2020).

One of the foundations of blockchain analysis systems is graph theory: a section of mathematics that studies the structure of connections between objects of arbitrary nature. In the case of blockchain analysis, the objects are cryptocurrency wallets, and the connections are transfers between wallets.

The origins of graph theory go back to antiquity: the philosopher and mathematician Porphyry of Tyre used the image of a tree as an illustration of the dichotomous division in his work "Introduction" to classify the philosophical concept of matter (Barnes, 2003), and a tree can be considered one of the varieties of graphs. The real scientific study of graphs began when Leonard Euler, in his article published by the St. Petersburg Academy of Sciences on the solution of the famous problem of the Königsberg bridges, dated 1736, was the first to apply the ideas of graph theory in proving certain statements (Hopkins & Wilson, 2004). In the 19th century, graph theory was used in electrical engineering and organic chemistry (Biggs, Lloyd & Wilson, 1986).

Today, this mathematical theory is very actively used in practice, since graphs can be used to describe computer and social networks. Such a direction as "social network analysis" can be largely characterized as applied graph theory. Social network analysis can be used in the disclosure and investigation of crimes, since it allows you to extract information stored on the Internet in an implicit form. From the above, it is clear that the basis of blockchain analysis, which appeared relatively recently and is necessary for the disclosure and investigation of crimes committed using cryptocurrencies, is graph theory, which appeared in the 18th century and was finally formed in the middle of the 20th century. At the same time, this scientific direction had law enforcement applications before the advent of cryptocurrencies. Specialists who have studied elements of graph theory for use in the analysis of social networks have received a certain advantage in the study of blockchain analysis.

We again see that fundamental facts established long before the advent of computers are useful in terms of studying the most modern information and communication technologies.

One of the common types of crimes related to cryptocurrency in recent years has been the theft of electricity for mining. The fact is that for mature cryptocurrencies, mining requires a large amount of computing resources, and therefore – electricity costs.

The question of qualifying such an act as an administrative offense or a crime depends on the amount of stolen electricity. Let's consider how electricity consumption can be related to income from mining.

As an example, let us consider Bitcoin, since this cryptocurrency is historically the first, has had and continues to have an impact on most other cryptocurrencies and still has the highest capitalization.

The costs of cryptocurrency mining can be considered from three aspects: the cost of computing resources, the cost of electricity and the cost of money. The cost of computing resources is measured in terahashes (billions of calculations of the hash function values of the cryptocurrency, hereinafter also – Th). The performance of mining equipment is called hashrate, accordingly, it is measured in terahashes per second (hereinafter also – Th/s).

Electricity costs are measured in kilowatt-hours (kWh) and depend on computing costs, performance, and power consumption of the equipment. Costs in monetary terms depend on electricity costs and the price of electricity, excluding capital costs in the form of purchasing equipment and premises for mining.

Ultimately, the profitability of mining and the damage from illegal mining are determined by a number of factors that have a significantly different nature: from fundamental physical laws to tariff regulation policies in a particular region.

All values are indicated with significant rounding, since the Bitcoin network hashrate and, as a consequence, all other values are subject to fluctuations. The order of the numbers is of interest. In addition, manufacturers are constantly releasing new models of mining equipment, which also affects the values of the indicators. The income of a Bitcoin cryptocurrency miner consists of two parts: the release of a new cryptocurrency and the commission of all transactions included in the block. At the moment, the commission is many times inferior to the release of a new cryptocurrency. Therefore, we will also ignore the presence of a commission.

We will proceed from the total hashrate of the Bitcoin network. The exact value of this value is unknown, but it can be estimated based on the complexity of the block and the number of blocks "mined" per unit of time. According to blockchain.com, this value is growing quite steadily and is currently estimated at approximately 680 million TH/s.

The Bitcoin network adjusts the mining difficulty so that a new block is formed on average every 10 minutes (Antonopoulos, 2017). Multiplying the average block formation time by the hashrate, we get the required number of calculations to form one block: 408 billion terahashes.

Today, the miner's reward for a block is 3.125 bitcoins. Dividing the required number of calculations to form one block by the miner's reward for a block, we get 130,560,000,000 terahashes per 1 bitcoin.

Let us determine the period in which such a number of calculations can be performed on modern equipment. Let us take for evaluation the ASIC Bitmain Antminer S21 Pro, released in July 2024. Its hashrate is 234 TH/s, so to "mine" 1 bitcoin it will need about 560 (or 155 thousand hours, about 6500 days). Considering that the power consumption of such a device is 3510 W, about 540 thousand kW-hours will be spent on "mining" 1 bitcoin. Calculations for other ASICs give comparable results.

The EU average electricity price for households, including taxes and levies is 0.29 euro per kWh or about 0.3 US dollars (Eurostat, 2023). That is, mining one bitcoin will cost about 160 thousand US dollars. The market price of one bitcoin is about 100 thousand dollars at the moment of writing of this article.

The calculations given can be used as a basis for the methodology for conducting an economic examination when considering cases related to violation of mining rules.

Furthermore, these considerations show that investigating crimes committed using cryptocurrency requires knowledge from various fields, including such different ones as law and electrical engineering.

ORIGINALITY/VALUE

Thus, in the context of active counteraction to the detection and investigation of crimes by criminal groups engaged in the illegal distribution of drugs via the Internet, law enforcement officers should constantly improve their professional level in the field of Internet technologies and telecommunications.

In higher education institutions of law enforcement agencies, it seems appropriate to teach the topics in such an order as to move from the general to the specific. For example, in the first year, within the framework of the discipline "Computer Science and Information Technology in Professional Activity", theoretical foundations are studied and practical skills are acquired as both necessary for solving and investigating crimes, and applicable in other aspects of professional activity, including studying other disciplines of specialization.

Then, within the framework of the course "Fundamentals of Cybersecurity", students will learn how the general principles of computer science and information technology can be applied to preserve state secrets, ensure anonymity and security when working on the Internet and solving other official tasks. In addition, here, when studying cryptography, the principles of functioning of cryptocurrencies can be studied. This occurs after or in parallel with the study of disciplines considering the humanitarian and legal aspects of these issues, for example, "Secrecy Regime". Finally, in the senior years, a special course is taught by several departments (crime investigation, forensics and criminal procedure), which synthesizes the knowledge, skills and abilities studied in various disciplines and practical training in territorial bodies for the purpose of solving and investigating cybercrimes in accordance with the current needs of law enforcement agencies and trends in the methods of committing crimes.

The described approach allows, on the one hand, to build the educational process in such a way that in the junior years, knowledge and skills are acquired that, due to their fundamental nature, will not become obsolete by the time of graduation (and for information technology, even 4 years of a bachelor's degree is a very long time), and in the senior years – knowledge and skills that are directly in demand in practical activities, but tend to quickly become obsolete (for example, specific methods of committing crimes and organizing criminal activity, certain software used by attackers, etc.). Due to the very dynamic development of information technologies and the constant adaptation of criminal activity, the professional development of an employee cannot end after graduation. Higher education must be supplemented by regular advanced training.

With regard to information and communication technologies related to digital currency and blockchain technologies, it is necessary to focus on a combination of fundamental training and the usefulness of the taught material for professional service activities.

Despite the very recent emergence of cryptocurrencies, their principles are based on fundamental results that appeared long before the 21st century and are widely presented in the literature. Thus, the role of fundamental knowledge for information technology is confirmed by the example of cryptocurrencies.

The development of the first cryptocurrency (Bitcoin) is a brilliant achievement, and its creator or creators are geniuses in several fields at once. Yet in order to understand the principles of cryptocurrency, there is no need to be as brilliant: there are complete descriptions of Bitcoin, intended for schoolchildren.

In addition, cryptocurrency and related technologies, due to their novelty and attractiveness, can become a good motivation for studying the field of cryptography in general. The next step is to overcome the prejudice about the boringness of mathematics. Indeed, few people can be interested in mechanical calculations, but they have a very indirect relation to the essence of mathematics and do not attract even mathematicians themselves. At the same time, the author's experience shows that the discussion

of, for example, "illegal prime number" arouses interest and lively discussion among students of legal specialties. On this basis, one can develop interest in number theory.

Modern trends in the development of information technologies and their penetration directly into the sphere of legal regulation of public relations at the level of laws require improving the training of lawyers and law enforcement officers.

With regard to technologies related to digital currency and blockchain, it is necessary to focus on a combination of fundamental training and the usefulness of the taught material for students.

The introduction of all concepts should be motivated, using examples from jurisprudence and the practice of combating crime. The facts and results presented by the teacher should be applicable both to subsequent topics and in the professional activities of students.

However, such an approach to teaching puts forward very high demands on the authority of the teacher, which should be based not only on discipline and coercion to submission due to subordination, but also on a high level of qualification of the teacher. Ideally, a modern teacher should combine deep knowledge of information technology and practical experience in law enforcement agencies.

REFERENCES

Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the open blockchain (2nd ed.). O'Reilly Media.

Ashurov, A. (2024). Jurisdictional Challenges in Cross-Border Cybercrime Investigations. *Central Asian Journal of Multidisciplinary Research and Management Studies*, 1 (8), 22-30. doi: 10.5281/zenodo.11234768.

Barnes, J. (2003). Porphyry: Introduction. Clarendon Press.

Biggs, N., Lloyd, E. K., & Wilson, R. J. (1986). Graph theory: 1736–1936. Clarendon Press.

Dunham, W. (2018). Prime numbers and their historical development. *Journal of Humanistic Mathematics*, 8(2), 4–25. https://doi.org/10.5642/jhummath.201802.04.

Eurostat. (2023). Electricity price statistics. European Commission. Downloaded April 20, 2025 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_price_statistics

Galushin, P. V., Serikova, O. Yu., Terskov, V. A. & Yarkov, K. V. (2020) A performance model of a multiprocessor computer appliance of a real-time control system. *IOP Conf. Ser.: Mater. Sci. Eng.* 734 012103 DOI 10.1088/1757-899X/734/1/012103.

Giboney, J. S., Anderson, B.B., Wright, G. A, Oh, S., Taylor, Q., Warren, M., Johnson, K. (2023). Barriers to a Cybersecurity Career: Analysis across Career Stage and Gender. *Computers & Security*, 103316.

Goldfeld, D. (1985). Gauss's class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, 13(1), 23–37. https://doi.org/10.1090/S0273-0979-1985-15352-2.

Goldman, A. (1964). The flip side of the Beatles. *The New Republic*, 150 (10), 13–15.

Hopkins, B., & Wilson, R. J. (2004). The truth about Königsberg. The College Mathematics Journal, 35(3), 198–207. https://doi.org/10.1080/07468342.2004.11922068.

Koblitz, N., Miller, V. (1985). Use of elliptic curves in cryptography. *Advances in Cryptology – CRYPTO '85 Proceedings*, 218, 417–426.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, Downloaded April 20, 2025 https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

Rogaway, P., & Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. Lecture Notes in Computer Science, 3108, 371–388. https://doi.org/10.1007/978-3-540-24660-2_29

Silverman, J. H. (2009). The arithmetic of elliptic curves (2nd ed.). Springer.

Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

Taleb, N. N. (2012). Antifragile: Things That Gain from Disorder. Random House.

Weierstrass, K. (1990). On the theory of elliptic functions (J. Smith, Trans.). In Selected Works of Karl Weierstrass (pp. 45–80). Dover Publications. (Original work published 1863).