

Fault-tolerant backup storage system for confidential data in distributed servers

Olzhas Tasmagambetov, Yerzhan Seitkulov, Ruslan Ospanov, Banu Yergaliyeva

Department of Information Security, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan

Article Info

Article history:

Received May 08, 2023

Revised Jun 05, 2023

Accepted Jun 06, 2023

Keywords:

Backup storage

Cryptographic algorithms

Elliptic curve cryptography

Information security

System fault tolerance

ABSTRACT

This article addresses the critical issue of securing backup storage for confidential data, a key concern in safeguarding the operations of critical information systems dealing with extensive amounts of sensitive information. The study proposes a novel cryptographic fault-tolerant backup storage system for confidential data, leveraging cryptographic algorithms and protocols. These protocols enable message encryption, ensuring decryption is only possible after a specified time period. The proposed system combines various distributed key generation protocols, proactive secret sharing protocols, asymmetric encryption algorithms, and digital signature algorithms. By employing such cryptographic protocols, it becomes feasible to develop and implement a robust, fault-tolerant service for backing up confidential data.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Yerzhan Seitkulov

Department of Information Security, L. N. Gumilyov Eurasian National University

Astana, Kazakhstan

Email: yerzhan.seitkulov@gmail.com

1. INTRODUCTION

This study focuses on addressing the security concerns associated with backing up confidential data. It is an essential issue in maintaining the security of critical information systems that handle substantial volumes of sensitive information. Specifically, the practical methods and protocols developed in this work aim to facilitate the creation of a model for a fault-tolerant information storage service operating within specified time constraints. Requirements for methods of ensuring the availability and fault tolerance of information resources, hardware for processing and storing data are established for providing information security during maintenance of informatization objects [1]-[4]. At the same time, for this, the owners ensure the availability of a backup server room, data servers, data storage systems and data transmission channels. Depending on the class of data criticality and computing resources, deployment of a mirror-loaded hot “clone” of servers in a backup server room, an unloaded cold backup and storage of spare sets of server equipment and data storage systems, as well as copies of the information resources themselves, should be provided. In addition, redundancy of the life support systems of servers and the server room (guaranteed power supply (UPS, diesel generator sets)) and grounding, air conditioning and ventilation systems, gas fire extinguishing and access control independent of the fire safety systems of the building, as well as raised floors (to counteract flooding) is provided. Also, for critical data of a fault tolerance class with a utilization rate of at least 98.7 percent approaches to decomposition, their isolation, compatibility are used. In approaches to decomposition, computing resources are distributed between virtual machines. In approaches to their isolation, the crash of one of them does not affect the others. In approaches to compatibility, the software can run on standardized operating platforms. The above is associated with the requirements to exclude a single point of failure at the logical and physical levels of server hardware, software, separation of computing resources at the hardware and software levels.

Fault tolerance in accordance with uniform requirements is also implemented by organizational measures by developing procedures for recovering from failures and failures of servers and software, ensuring the safety of virtual machine images, and storing spare parts in close proximity to server rooms. To achieve reliability indicators of placement inside server rooms in critical informatization objects, methods of equipment location are used to reduce the risks of threats. At the same time, one of the aspects of the fault-tolerant use of information resources is the backup storage of a complete copy of archived data.

The daily operational activities of an employee using personal computers and information systems in state bodies are associated with the creation of various kinds of information necessary for decision-making and the provision of public services. The specified data and documents in electronic digital form may be with different levels of relevance to the solution of various kinds of tasks, but may be necessary in the future for the employee. Therefore, in the information and analytical activities of a civil servant, various kinds of “drafts”, “document templates”, saved responses to requests, extracts from legal acts that are not subject to accounting or do not meet the selection criteria for inclusion in the centralized information resources of the unit or archives. It should be noted that some part of the electronic information stored on computers contains personal data of citizens or other confidential information. In this regard, it can be assumed that such documents in each subdivision of the state body are stored on computer equipment, the circulation of which cannot be controlled, are of interest to intruders, and the loss of which can cause certain damage and paralyze the activities of the state body. In this light, the most secure model is the storage and processing of confidential data using a decentralized architecture in which concentration, processing and storage, as well as guaranteed destruction, are carried out according to certain protocols [5]-[7].

In this paper, we consider a model of functioning of a fault-tolerant backup storage system of protected information during a specific period using encryption techniques within a secure cryptographic framework named as elliptic curve time-lapse cryptography (ECTLC). The procedure relies on time-lapse cryptography (TLC) [8], [9], which establishes a cryptographic protocol for encrypting client data in a manner that ensures decryption cannot occur before a specific designated time, regardless of whether the sender desires it. TLC incorporates the Pedersen’s distributed key generation (DKG) protocol, the Feldman’s threshold verifiable secret sharing (VSS) protocol, and the ElGamal encryption. The agreed-upon parameters of the ElGamal encryption algorithm, including a prime number p that generates a prime order element g , are utilized by TLC. These parameters can be found, for example, in request for comments (RFC) 3526 and RFC 5114. ECTLC employs analogous algorithms found in elliptic curve cryptography. More precisely, it employs a DKG protocol that is dependent on the discrete logarithm problem on elliptic curves, the Pedersen’s threshold VSS protocol, and the ElGamal encryption that is specifically tailored for elliptic curves (ECs). In this paper we propose new cryptographic fault-tolerant backup storage system of confidential data based on above mentioned cryptographic algorithms and protocols. It is different from Yergaliyeva *et al.* [10] where Shamir’s secret sharing technology and Diffie-Hellman protocol on an elliptic curve were used. Furthermore, there exists the potential to incorporate novel and enhanced algorithms into the protocol, which can offer increased efficiency and expanded functionality. Specifically, to guarantee data encryption over an extended duration, the proactive secret sharing protocol, as outlined in Sun *et al.* [11], can be employed.

2. METHOD

Now we consider the model of functioning of a fault-tolerant backup storage system of protected information during a specific period. The parties included in the suggested model consist of:

- a) The portal (Pr) responsible for receiving applications from clients to store confidential information.
- b) The client (Cl) is a party who utilizes the portal as a user.
- c) The service (Sr) – it consists of n distributed servers that are geographically separated from one another, error-free and secretly performing calculations provided by the protocol, securely storing all their secret data, having a secure method of backing up data for disaster recovery. The assumption is made that the servers do not engage in collusion, meaning they do not share or transfer confidential data among themselves. All servers can privately and secretly exchange information with each other, forming a network. A threshold value t is assumed such that at most $t - 1$ servers can break the protocol and at least t servers are reliable. The condition $n \geq 2t - 1$ ($t \leq (n + 1)/2$) must be satisfied, for example, if $n = 3$, then $t \leq 2$.

The model provides using the agreed parameters of the used elliptic curve: elliptic curve modulus-prime number p , EC equation, coefficients a and b of this equation from field F_p , EC point G of prime order p . These settings can be found, for example, at the website of the SafeCurves project [12]. SafeCurves is a project that aims to provide elliptic-curve cryptography (ECC) security, not just elliptic curve discrete logarithm problem (ECDLP) security. It provides criteria for choosing curves that keep simple implementations safe. Efficiency is an important factor in curve selection and most standards prioritize efficiency. However,

SafeCurves does not prioritize efficiency unless it interacts with security concerns. The SafeCurves website provides security ratings for various specific curves, some of which have been proposed for deployment or are currently in use. In the model under consideration, the M-511 elliptic curve can be used with the following parameters [12].

– The elliptic curve modulus, the prime number

$$q = 2^{511} - 1 =$$

67039039649712985497870124991029230637396829102961966888617807218608

82015036773488400937149083451713845015929093243025426876941405973284973216824503041861.

– The elliptic curve equation

$$y^2 = x^3 + 530438x^2 + x \text{ mod } q$$

– The equation coefficients a and b from the finite field

$$F_q: a = 530438, b = 1$$

– The base point of prime order N on the elliptic curve

$$G = (xG, yG) = (5,$$

17360859007097926424827522860389970695051812781717659187866778424758212450543074

5177116625808811349787373477), $N = 2^{508}$

1072475475963574762404453151406812184207075662743483302896554080882767

50620 = 83798799562141231872337656238786538296746036378702458610772259023261025

1879607410804876779383055508762141059258497448934987052508775626162460930737942299.

The M-511 curve satisfies requirements to basic parameters, ECDLP safety requirements and ECC safety requirements in addition to ECDLP safety. Curve M-511 has a sufficient security level of $2^{252.3}$, and therefore provides resistance to various attacks [12]. Overview of the model (protocol):

- Step 1: the client performs a typical login procedure on the portal.
- Step 2: the client submits a data encryption request (for a specific message, m) to Pr .
- Step 3: Pr forwards the Cl 's request to Sr , including the Cl 's unique ID, the moment of time T_{ID} when the request was dispatched, and the designated moment of time $T_{ID} + \delta_{ID}$ by which the Cl 's data should remain encrypted and inaccessible for decryption. These steps are illustrated in Figure 1.

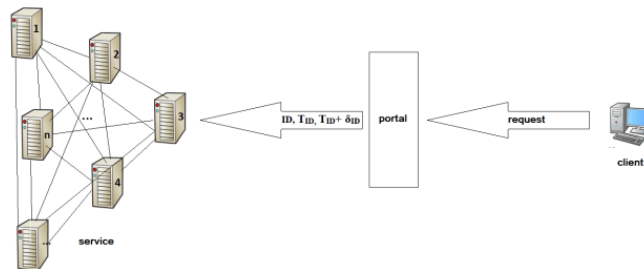


Figure 1. Steps 1-3

- Step 4: each service server P_i receives a request.
- Step 5: each server P_i chooses random values $a_{i0}, a_{i1}, \dots, a_{ik}, b_{i0}, b_{i1}, \dots, b_{ik}$, where $k = t - 1$, from the field F_p (i.e., $0 \leq a_{ir} < p, 0 \leq b_{ir} < p$). a_{i0} is a part of the private key.
- Step 6: then each server P_i calculates $s_{ij} = a_{i0} + a_{i1}j + a_{i2}j^2 + \dots + a_{ik}j^k \pmod{q}$ and $s'_{ij} = b_{i0} + b_{i1}j + b_{i2}j^2 + \dots + b_{ik}j^k \pmod{q}$, where $j \neq i$ is a number of the server $P_j, 1 \leq j \leq n$.
- Step 7: then each server P_i calculates $C_{ir} = a_{ir}G + b_{ir}G', 0 \leq r \leq k$ (here the operations of adding the points of an elliptic curve and multiplying a point by a number are applied).
- Step 8: then each server P_i sends s_{ij} and s'_{ij} to the servers P_j over private communication channels between P_i and P_j , and publicly publishes $C_{ir} (0 \leq r \leq k)$ with its digital signature $SIGN_i$.
- Step 9: each server P_i , having received s_{ji} and s'_{ji} from the servers $P_j, 1 \leq j \leq n, j \neq i$, checks for equality $s_{ji}G + s'_{ji}G' = \sum_{r=0}^k i^r C_{jr} (*)$.

If equality (*) does not hold for values s_{ji} and s'_{ji} received from the server P_j , then the server P_i complains against P_j . If the server P_i receives a complaint against himself, he publishes s_{ij} and s'_{ij} with his digital signature $SIGN_i$, satisfying the equality (*).

- Step 10: each server P_i marks as disqualified each server that received more than k complaints or responded to a complaint with values that do not satisfy the equality (*).
- Step 11: each server P_i creates a set Q of all non-disqualified servers. Each server P_i from the set Q calculates $A_{i0} = a_{i0}G$ and publishes A_{i0} with its digital signature $SIGN_i$.
- Step 12: each server P_i from the set Q receives A_{j0} and calculates the public key $PK_i = \sum_{j \in Q} A_{j0}$.
- Step 13: each server P_i forms the key structure (KS) $K_{ID} = (ID, T_{ID}, \delta_{ID}, PK_{ID} = PK_i)$ with its digital signature $SIGN_i$.
- Step 14: each server P_i sends the generated KS to Pr .
- Step 15: Pr transmits the received KS to Cl . These two steps are illustrated in Figure 2.

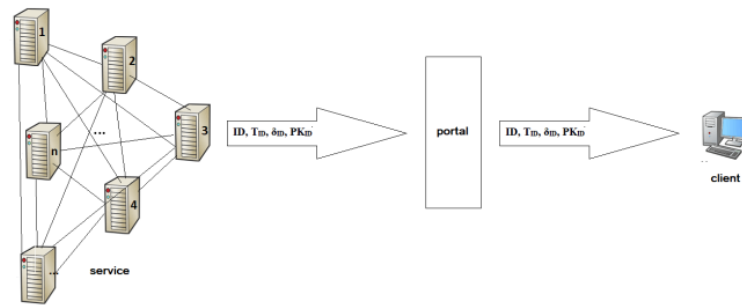


Figure 2. Steps 14-15

- Step 16: the client verifies $DSs\ SIGN_i(K_{ID})$ against the published $KSs\ K_{ID}$, ensuring that they match and meet the minimum requirements for t participants, and also verifies the identity associated with the key structures.
- Step 17: Cl generates a symmetric key s to encrypt the message m .
- Step 18: Cl encrypts the message m with the key s .
- Step 19: Cl encrypts the symmetric key s as follows. The key s is placed at the point of the elliptic curve: a point $M = (x, y)$ is chosen such that the part of the vector x is fixed and corresponds to the key s , and the vector y satisfies the elliptic curve equation for the selected x , i.e., y is the square root modulo p (Shanks' algorithm). A random number r , $0 < r < q$ is chosen. $C_1 = rG$: $rG = G + G + \dots + G$ is calculated (r times) (+ is addition operation on an EC). $C_2 = M + rPk$ is calculated, where Pk is the public key (elliptic curve point). A pair (C_1, C_2) is a ciphertext.
- Step 20: the client sends an encrypted message m and an encrypted symmetric key s to the portal. This step is illustrated in Figure 3.

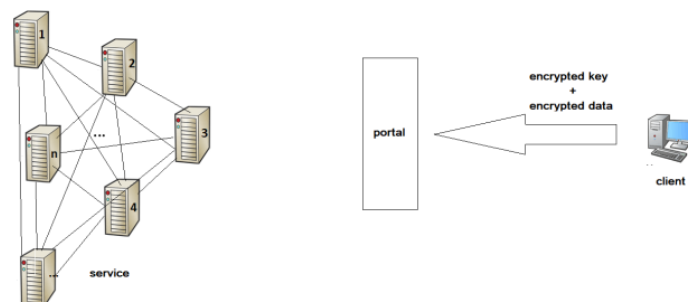


Figure 3. Step 20

- Step 21: Pr securely stores the encrypted data and encrypted key, linking them to the Cl 's ID and other parameters including the specified time mentioned in the request.
- Step 22: once the designated time specified in the request is reached, or at any point thereafter, Pr sends a request to Sr to obtain a private key, providing the Cl 's ID, public key, and time parameters. This step is illustrated in Figure 4.

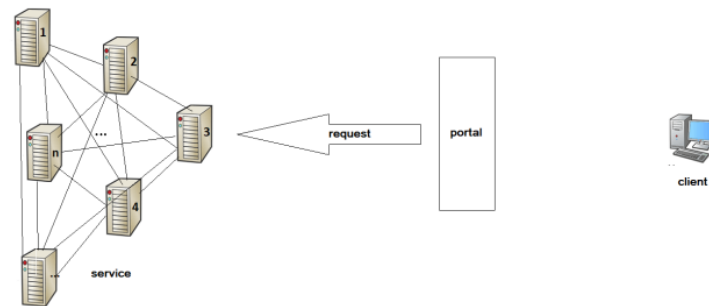


Figure 4. Step 22

- Step 23: every server receives a request and distributes its private key among the other servers.
- Step 24: each server obtains the private keys from the other servers, computes the combined private key, associates it with the corresponding public key, securely stores it in its database, and transmits the private key to Pr .
- Step 25: Pr receives the private key and decrypts the symmetric key using this key as follows. DkC_1 is calculated where Dk is private key. $-DkC_1$ is calculated (inverse element for DkC_1). $(-DkC_1) + C_2 = M$ is calculated.
- Step 26: the portal decrypts the client's data.

Note: as a component of Sr , it is possible to utilize a small network of managers who operate as a cohesive management team for overseeing Sr . The primary duty of this team is to generate a schedule of public keys and corresponding private keys produced by Sr . They also manage an internal bulletin board exclusively for Sr 's members and maintain an open bulletin board accessible to Sr 's users. Every manager will keep their individual duplicates of these boards.

The servers and users of the service will examine the messages posted on each copy of the bulletin board and determine the correct values based on the majority of entries. Each server in the service accompanies every message with a digital signature. The activities of all participants in the protocol are synchronized using a public and trusted clock, such as the ones provided by National Institute of Standards and Technology (NIST). The service has the capability to generate key structures periodically. For example, it can generate keys with a lifespan of one week every day, or keys with a duration of 4 hours for every interval of 20 minutes. Such a schedule is posted on the open bulletin board by the managers. Furthermore, Sr has the capability to accept user requests for generating new keys with designated durations. The managers receive these requests and publicly announce them on the open bulletin board. The servers then generate keys in accordance with the protocol, sign them, and publish the signed KS s on the open bulletin board. Additionally, Sr welcomes user requests for generating new keys with specific lifespans. The managers handle these requests and post them on the open bulletin board. The servers adhere to the protocol to generate keys, sign them, and make the signed KS s available on the open bulletin board.

3. RESULTS AND DISCUSSION

The main findings of the study can be summarized as follows. The present study focuses new cryptographic fault-tolerant backup storage system of confidential data based on TLC, specifically the variant known as ECTL. TLC refers to a method of encrypting data or information so that it can only be accessed or decrypted after a certain amount of time has passed. The time-lapse aspect is used as a security feature to ensure that the data remains protected until the specified time has elapsed. This technology is used in various applications, such as secure file storage or information sharing, where it is important to restrict access to sensitive information until a specified period has passed. The security of information systems created using time-lapse cryptography refers to the measures taken to protect sensitive and confidential information stored within these systems from unauthorized access, tampering, and theft. This can include techniques such as encryption, access control, and secure data storage practices. The goal of these security measures is to maintain the confidentiality, integrity, and availability of the information stored within the system and prevent any malicious attacks from compromising it [13]-[16]. The level of security in a time-lapse cryptography system depends on various factors, such as the complexity of the cryptographic algorithms used, the robustness of the underlying infrastructure, and the implementation of secure software development practices [17]-[19].

ECTLC is a modification of TLC that is based on elliptic curves. The security of ECTLC is based on the hardness of the discrete logarithm problem (DLP) over elliptic curves. As long as this problem remains hard, the encrypted information will be secure against unauthorized access. However, it is crucial to emphasize that the security of ECTLC is only as strong as the weakest link in the system, and various factors such as implementation errors, side-channel attacks, or weaknesses in the underlying cryptographic primitives can affect the overall security of the system. It is important to properly implement and deploy ECTLC in order to ensure its security. This includes proper selection of cryptographic parameters, secure implementation of cryptographic primitives, and proper handling of keys and encrypted information. Additionally, it is important to regularly assess the security of this protocol in light of new developments in cryptography and computer science to ensure that it continues to provide a high level of security [20]-[22].

The DKG protocol based on the DLP on EC, used in ECTLC, is a cryptographic algorithm for generating shared secret keys between multiple parties in a secure and efficient manner. The security of such a protocol relies on the computational hardness of the DLP over EC. In these protocols, each participant generates a public-private key pair, and the public keys are combined to generate a shared secret key. The security of the shared secret key relies on the intractability of the DLP over EC. As long as this problem remains hard, the shared secret key will be secure against unauthorized access.

Pedersen verifiable threshold secret sharing protocol, used in ECTLC, is a cryptographic protocol for securely sharing a secret among multiple parties in such a way that a threshold of parties must cooperate to reconstruct the secret. The security of the Pedersen's threshold VSS protocol relies on the hardness of the DLP and the computational indistinguishability of the commitment scheme used. In this protocol, a dealer distributes shares of the secret to each participant, and any threshold number of participants can cooperate to reconstruct the secret. The protocol also includes a verifiable reconstruction process, in which any participant can verify the correctness of the reconstructed secret, ensuring that the secret has not been tampered with or reconstructed incorrectly. The security of the protocol is considered to be strong as long as the underlying cryptographic assumptions hold.

The ElGamal encryption algorithm on elliptic curves, used in TLC, is a public-key encryption algorithm that is based on the mathematical problem of computing discrete logarithms over elliptic curves. The security of ElGamal encryption on elliptic curves is based on the computational hardness of the DLP over elliptic curves. In the ElGamal encryption algorithm, a sender encrypts a message using the recipient's public key, and the recipient can then decrypt the message using their private key. The security of the encrypted message relies on the intractability of the DLP over elliptic curves, making it computationally infeasible for an attacker to compute the private key from the public key [23]-[25].

In this model, the client performs a standard login to the portal. This step is a standard login process that is generally considered secure, provided the portal has implemented secure authentication mechanism. It is important to ensure that the authentication mechanisms used by the portal are strong enough to prevent unauthorized access to the system. This may include methods such as multi-factor authentication, strong password policies, and encryption of sensitive user data. Additionally, within the model, Cl submits a request to Pr to encrypt specific information, denoted as message m . The security of this step depends on the encryption algorithm used, as well as the secure transmission of the message to the portal. If the encryption algorithm used is strong and the transmission of the message is secure (eg., using SSL/TLS), then this step can be considered secure. In this step, Pr forwards the Cl 's request to Sr , including essential details such as Cl 's unique ID, the timestamp of the request, and the designated timeframe during which Cl 's data must remain encrypted and inaccessible for decryption. The security of this step depends on the security of the transfer of the request from the portal to the service, as well as the secure storage of metadata by the portal and the service. It is important to secure the transmission of the request and the secure storage of the metadata. In addition, the use of a unique customer ID and decryption time limits can help prevent unauthorized access to customer data. In general, the security of the steps in the considered model depends on various factors, such as the security of the authentication mechanisms, the strength of the encryption algorithm used, and the secure transmission and storage of data. It is important to ensure that all these factors are carefully considered and implemented to ensure the security of the system.

In comparison with other studies, the present study contributes by specifically focusing on the application of TLC and its variant, ECTLC, based on elliptic curves. While other studies may have explored different cryptographic methods or variants, this study delves into the security aspects, underlying protocols, and algorithms specific to ECTLC. The findings of this study have significant implications for the field of cryptography and information security. TLC, especially ECTLC, offers an additional layer of security by leveraging the time factor for data access. The use of elliptic curves and the reliance on the hardness of the DLP provide strong security guarantees, but proper implementation and deployment are crucial for maintaining the overall security of the system. The DKG protocol and the Pedersen's threshold VSS protocol provide secure ways of generating shared secret keys and sharing secrets among multiple parties. These protocols offer robust security as long as the underlying cryptographic assumptions hold, ensuring that

sensitive information remains protected and tamper-proof. The ElGamal encryption algorithm on elliptic curves provides secure communication through public-key encryption. The intractability of the DLP over ECs ensures the confidentiality of the encrypted messages, protecting them from unauthorized access. The strengths of this study lie in its focus on time-lapse cryptography, specifically ECTL, and its detailed exploration of the underlying protocols and algorithms. The study provides a comprehensive understanding of the security aspects of ECTL, including the distributed key generation protocol, the Pedersen's threshold VSS protocol, and the ElGamal encryption algorithm.

It is important to note that, as with any cryptographic protocol, the security of these algorithms is only as strong as the weakest link in the system, and various factors such as implementation errors, side-channel attacks, or weaknesses in the underlying cryptographic primitives can affect the overall security of the system. It is important to properly implement and deploy such protocols in order to ensure its security. This includes proper selection of cryptographic parameters, secure implementation of cryptographic primitives, and proper handling of keys and encrypted messages. Additionally, it is important to regularly assess the security of this algorithm in light of new developments in cryptography and computer science to ensure that it continues to provide a high level of security.

In conclusion, TLC, particularly the variant ECTL, offers an innovative approach to securing data and information. The use of elliptic curves and the reliance on the hardness of the DLP provide a strong foundation for security. However, proper implementation, secure software development practices, and regular security assessments are essential to maintain the overall security of the system. Recommendations for future research include conducting empirical studies to evaluate the real-world effectiveness and performance of ECTL, including its resistance to potential attacks. Furthermore, staying updated with new developments in cryptography and computer science is crucial to ensure that ECTL continues to provide a high level of security. Additionally, exploring potential applications and use cases for TLC and ECTL in various domains can help further understand their practical implications and benefits.

4. CONCLUSION

In this paper, a model of functioning of a fault-tolerant backup data storage system for a given time is considered. The model is based on the cryptographic encryption protocol for a given time ECTL. The protocol effectively combines the DKG protocol that relies on the discrete logarithm on ECs, the Pedersen's threshold VSS protocol, an ElGamal encryption on ECs, and an electronic DS. The protocol permits the usage of predefined parameters, which include the prime number modulus (p) of the EC, the equation and coefficients (a and b) of the EC from the field (Fp), and a point (G) on the EC with a prime order (q) specifically for the ElGamal encryption on EC. A fault-tolerant backup storage system for confidential data in distributed servers based on ECTL is a specialized solution designed to provide both data protection and fault tolerance while incorporating cryptographic techniques that take into account the passage of time. This type of system utilizes distributed storage architecture, where data is replicated across multiple servers or nodes. The redundancy ensures that even if one or more servers fail, the confidential data remains accessible and intact. The distributed nature of the system also enhances fault tolerance and resilience to hardware failures. By combining fault tolerance mechanisms with ECTL, the system ensures the protection and availability of confidential data stored in distributed servers. It addresses potential hardware failures and provides secure transmission of sensitive information over extended periods, all while maintaining the confidentiality and integrity of the data.

It is worth noting that further research and evaluation are necessary to assess the efficiency, security, and effectiveness of the fault-tolerant backup storage system based on time-lapse cryptography. Ongoing studies can help refine the protocols, algorithms, and parameters used and ensure that the system remains resistant to known attacks and meets the evolving security requirements for safeguarding confidential data in distributed environments. Hence, it will be essential to conduct a study in the future to evaluate and choose the most efficient algorithms and parameters mentioned earlier for the developed protocol. The ECTL protocol, which is derived from TLC, presents a solution for transmitting confidential messages to future recipients. However, instead of the distributed key generation, verifiable thresholding, and encryption algorithms used in TLC, algorithms based on elliptic curve cryptography are used, which suggests greater efficiency. At the same time, it is assumed that these changes do not affect the resistance to known attacks.





ACKNOWLEDGEMENTS

This work is supported by the SC of the MSHE of the Republic of Kazakhstan, grant No. AP14869013.





REFERENCES

- [1] D. Arivudainambi and K. A. V. Kumar, "Performance analysis of security framework for software defined network architectures," *International Journal of Advances in Applied Sciences (IJAAAS)*, vol. 8, no. 3, pp. 232-242, 2019, doi: 10.11591/ijaas.v8.i3.pp232-242.
- [2] W. Hassan, T. -S. Chou, X. Li, P. A. -Kubi, and T. Omar, "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks," *The International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no. 3, pp. 162-183, 2019, doi: 10.11591/ijict.v8i3.pp162-183.
- [3] H. J. Muhasin, A. Y. Gheni, and H. A. Yousif, "Proposed model for data protection in information systems of government institutions," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 3, pp. 1715-1722, 2022, doi: 10.11591/eei.v11i3.3727.
- [4] L. Hoti, K. Dermaku, S. Klaiqi, and H. Dermaku, "Protection and Exchange of Personal Data on the Web in the Registry of Civil Status," *Emerging Science Journal*, vol. 7, no. 1, 2023, doi: 10.28991/ESJ-2023-07-01-03.
- [5] O. Farion, A. Balendr, O. Androshchuk, A. Mostovyi, and V. Grinchenko, "Methods of Extraction and Analysis of Intelligence to Combat Threats of Organized Crime at the Border," *Journal of Human, Earth, and Future*, vol. 3, no. 3, 2022, doi: 10.28991/HEF-2022-03-03-07.
- [6] M. Riasetiawan and A. Ashari, "A Proposed Framework of Knowledge Management for COVID-19 Mitigation based on Big Data Analytic," *Emerging Science Journal*, vol. 7, 2023, doi: 10.28991/ESJ-2023-SPER-015.
- [7] Z. D. Abbass, J. S. Maatooq, and M. M. Al-Mukhtar, "Monitoring and Modelling Morphological Changes in Rivers Using RS and GIS Techniques," *Civil Engineering Journal*, vol. 9, no. 3, 2023, doi: 10.28991/CEJ-2023-09-03-03.
- [8] M. O. Rabin and C. A. Thorpe, "Method and apparatus for time-lapse cryptography," *U.S. Patent*, 2007. [Online]. Available: <https://patents.google.com/patent/US8526621B2/en>
- [9] M. O. Rabin, and C. A. Thorpe, "Time-lapse cryptography," *Technical report TR-22-06*, 2006. [Online]. Available: <https://dash.harvard.edu/handle/1/26506434>
- [10] B. Yergaliyeva, Y. Seitkulov, D. Satybaldina, and R. Ospanov, "On some methods of storing data in the cloud for a given time," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 20, no. 2, pp. 366-372, 2022, doi: 10.12928/TELKOMNIKA.v20i2.21887.
- [11] H. Sun, X. Zheng, and Y. Yu, "A Proactive Secret Sharing Scheme Based on Elliptic Curve Cryptography," *2009 First International Workshop on Education Technology and Computer Science*, 2009, pp. 666-669, doi: 10.1109/ETCS.2009.408.
- [12] D. J. Bernstein and T. Lange, "SafeCurves: choosing safe curves for elliptic-curve cryptography," *SafeCurves*. [Online]. Available: <https://cr.ypt.to/talks/2014.01.18/slides-dan+tanja-20140118-a4.pdf>
- [13] S. K. Ibrahim and S. A. Abdulhussien, "Improved storage area network method for backup approach," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1493-1498, 2020, doi: 10.11591/ijeecs.v17.i3.pp1493-1498.
- [14] I. M. Sukarsa, I. K. A. M. Antara, P. W. Buana, I. P. A. Bayupati, N. W. Wisswani, and D. W. Puteri, "Data storage model in low-cost mobile applications," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 1128-1138, 2022, doi: 10.11591/ijeecs.v28.i2.pp1128-1138.
- [15] V. Kuklin, I. Alexandrov, D. Polezhaev, and A. Tatarkanov, "Prospects for developing digital telecommunication complexes for storing and analyzing media data," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 3, pp. 1536-1549, 2023, doi: 10.11591/eei.v12i3.4840.
- [16] V. Kaviani J., P. A. D. Amiri, F. Z. Brujeni, and N. Akhlaghi, "Modification data attack inside computer systems: A critical review," *Computer Science and Information Technologies*, vol. 1, no. 3, pp. 98-105, 2020, doi: 10.11591/csit.v1i3.p98-105.
- [17] P. Nadee and P. Somwang, "Efficient incremental data backup of unison synchronize approach," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2707-2715, 2021, doi: 10.11591/eei.v10i5.2212.
- [18] M. M. Trung, L. P. Do, D. T. Tuan, N. V. Tanh, and N. Q. Tri, "Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1734-1743, 2023, doi: 10.11591/ijece.v13i2.pp1734-1743.
- [19] S. Deb and M. M. Haque, "Elliptic curve and pseudo-inverse matrix based cryptosystem for wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4479-4492, 2019, doi: 10.11591/ijece.v9i5.pp4479-4492.
- [20] E. T. Oladipupo and O. C. Abikoye, "Improved authenticated elliptic curve cryptography scheme for resource starve applications," *Computer Science and Information Technologies*, vol. 3, no. 3, pp. 169-185, 2022. [Online]. Available: <https://iaesprime.com/index.php/csit/article/view/218/84>
- [21] B. S. B. Gowda, "Implementation of Elliptic Curve Cryptography over a Server-Client network," *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 2020, pp. 116-119, doi: 10.1109/ICDCS48716.2020.243562.
- [22] D. Maimut and A. C. Matei, "Speeding-Up Elliptic Curve Cryptography Algorithms," *Mathematics*, vol. 10, no. 19, 2022, doi: 10.3390/math10193676.
- [23] A. Malik, M. Aggarwal, B. Sharma, A. Singh, and K. K. Singh, "Optimal Elliptic Curve Cryptography-Based Effective Approach for Secure Data Storage in Clouds," *International Journal of Knowledge and Systems Science (IJKSS)*, vol. 11, no. 4, 2020, doi: 10.4018/IJKSS.2020100105.
- [24] V. G. Martínez, L. H. Encinas, A. M. Muñoz, and R. D. Díaz, "Secure elliptic curves and their performance," *Logic Journal of the IGPL*, vol. 27, no. 2, 2019, doi: 10.1093/jigpal/jzy035.
- [25] S. S. Dhandu, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463-470, 2020, doi: 10.1080/09720502.2020.1731959.





BIOGRAPHIES OF AUTHORS

Olzhas Tasmagambetov     He is a doctoral student on the specialty “Information Security”, Gumilyov ENU, Astana, Kazakhstan. He is a specialist in the field of cybersecurity, has publications in domestic journals. He has extensive practical experience in law enforcement. In addition, he works at the Institute of Information Security and Cryptology as a leading researcher. He can be contacted at email: 5999452@mail.ru.







Yerzhan Seitkulov     Ph.D, Professor at the Department of Information Security, the Gumilyov ENU, Astana, Kazakhstan. Research interests - cryptography, coding theory, cloud computing, voice information protection, supercomputer technologies, distributed computing. He is also the head of a number of scientific and technical projects and programs through line ministries. Over the past 10 years, he has led 8 scientific projects in the field of information security. He can be contacted at email: yerzhan.seitkulov@gmail.com.



Ruslan Ospanov     He is a doctoral student on the specialty “Information Security”, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. His research interests are cryptology, blockchain technology, big data, coding theory, the Internet of things. He is the author of the development of a new hash function, and he also developed new methods for generating optimal s-boxes used in symmetric cryptographic algorithms. He can be contacted at email: ospanovrm@gmail.com.



Banu Yergaliyeva     She is a doctoral student on the specialty “Information Security”, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. She is a leading researcher at the Scientific Institute of Information Security and Cryptology. Research interests - applied cryptography, cloud technologies, Internet of things, secure processing in the cloud, secure storage of big data in the cloud. She can be contacted at email: banu.yergaliyeva@gmail.com.