International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-11| 2023 Published: |22-11-2023|

ELLIPTIC CURVE CRYPTOGRAPHY

https://doi.org/10.5281/zenodo.10144011

V.A.Obuxov
Fergana branch of TUIT named after Muhammad al-Kharizmi,
assistant of "Information Technology"

Introduction

The safety of your data during storage and transfer from one device to another is of great importance. There are a number of measures aimed at ensuring the security of your digital assets. One of the proven ways to ensure the security of your data during storage and transmission is cryptography.

In cryptography, you can encrypt and decrypt your file using special keys. An excellent technique in cryptography is elliptic curve cryptography. Thanks to elliptic curve cryptography, it will replace your file with a smaller key size and provide faster transfer.

Blockchain applications such as BITCOIN use a type of ECC called the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions.

The exchange and transmission of information via the Internet has become commonplace. The security of this information becomes a priority for everyone and this is where the need for cryptography comes into play. Cryptography refers to the security of messages that you intend to store or transmit, and also consists of encrypting and decrypting messages.

When you encrypt and decrypt messages, you make them unreadable and inaccessible to unauthorized users. Encryption means converting text in its natural language into ciphertext using an algorithm. You can use several methods to encrypt data and information over the Internet. One of them is elliptic curve cryptography.

What is Elliptic Curve Cryptography?

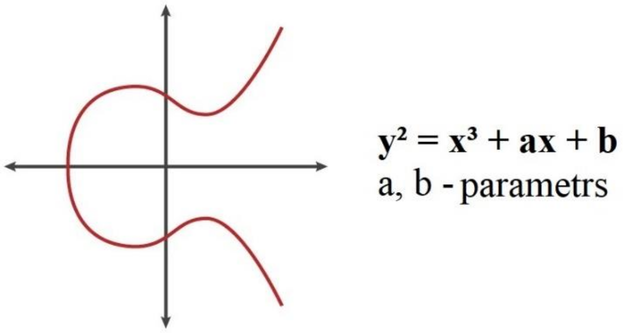

Figure 1. Elliptic curve.

Elliptic curve cryptography (ECC) is a key-based data security technique. ECC uses public and private keys to encrypt and decrypt web traffic. Over the years, ECC has distinguished itself as a powerful cryptographic approach. When you use elliptic curve cryptography to secure your web traffic, it will generate a security key between decision pairs (public and private) using elliptic curve mathematics.

The advantage of ECC over other cryptography methods is its smaller key size and high level of security/privacy. The elliptic curve cryptography approach to public keys is based on algebraically structured elliptic curves over finite fields. This structure shows that ECC generates very complex and mathematically intensive keys to crack.

Due to its superior performance and security, more and more sites and applications continue to use elliptic curve cryptography.

Blockchain platforms such as Bitcoin and Ethereum use the Elliptic digital signature algorithm Curve Digital Signature Algorithm (ECDSA) for signing transactions. The planar curve depicts an elliptic curve for the current ECC target over a finite field, consisting of points satisfying this equation "$y^2 = x^3 + ax + b$."

Using this ECC equation, any point on the curve can be mirrored along the x-axis and the curve will remain unchanged. Likewise, a non-vertical line will intersect the curve in three places or less.

Besides encryption, some other features of the elliptic curve function include key distribution and digital signature algorithm. You can use the ECC digital signature algorithm to authenticate the signer and verify the integrity of the message. This digital signature algorithm is being adapted into cryptocurrency . Having defined the meaning of elliptic curve cryptography, let's dive into how cryptography works and the benefits of using this technology.

How Elliptic Curve Cryptography Works in Cryptocurrency .

Elliptic curve cryptography is a technique for implementing digital signatures in cryptocurrency. This implementation technique is called the Elliptic Curve Digital Signature Algorithm. Curve Digital Signature Algorithm , ECDSA).

The Elliptic Curve Digital Signature Algorithm (ECDSA) was standardized in 2005, compared to its close replacement, the Rivest -Shamir- Adleman Algorithm (RSA), standardized in 1995. Blockchain applications such as Bitcoin and Ethereum use the Elliptic digital signature algorithm Curve Digital Signature Algorithm (ECDSA) when signing transactions due to its efficiency. ECDSA uses ECC keys to ensure the uniqueness of each user (signer and validator) in a transaction and guarantees the security of the transaction.

You can use ECDSA to generate certificates in electronic format.

This certificate will contain information about the encryption key, the owner of the certificate, information about the owner of the certificate, and the signature of the issuer of the certificate.

The issuer of an ECDSA certificate is a verified trustee, and at any time you can trace the certificate back to the issuer through the chain of trust. The issuer is called a certificate authority.

Moreover, due to the ease of ECC, Bitcoin uses elliptic curve cryptography as an asymmetric cryptosystem.

Benefits of ECC

Elliptic curve cryptography stands out among other encryption keys due to its robust capabilities. ECC is more powerful than its close substitute, RSA. For example, an ECC key size of 256 bits is equivalent to a 3072-bit RSA key. The ECC key size is 10,000 times stronger than the equivalent RSA key size.

The significant shortcomings that users find with RSA and DSA are well addressed in ECC. ECC developers always strive to identify weaknesses specific to replacement keys and strengthen those areas in ECC.

These weaknesses are significant causes of unauthorized access and data breaches, and size and ability to function may also be weaknesses.

Elliptic curve cryptography is faster than all cryptographic platforms. Reasons why ECC is fast include:

- ECC uses more minor keys, which means that less data will be transferred from the server to the client during the SSL handshake.
- Another reason for its speed is that ECC requires less processing power. The processor and memory consume less power during data transfer, resulting in faster response times.

Conclusion

Elliptic curve cryptography (ECC) is an improvement and improvement on the cryptography used in SSL. Undoubtedly, ECC ranks highly compared to other cryptographic protocols.

The benefits of using ECC are enormous and include improved safety, increased durability and increased productivity. However, not all browsers and patents support the ECC certificate. Some of these browsers still use outdated RSA and DSA cryptographic technologies.

REFERENCES:

1. Обухов, В. А. (2023). Цифровая безопасность данных в блокчейн-сетях. PEDAGOG, 6(10), 304-308.

2. Обухов Вадим Анатольевич, Ахунова Таманнохон Зокир кизи, & Сиддиков Муродали Йулдошали угли. (2023). АДАПТИВНЫЕ АЛГОРИТМЫ РАСПОЗНАВАНИЯ ТЕКСТОВ. Ta'lim Innovatsiyasi Va Integratsiyasi, 7(1), 58–61. Retrieved from http://web-journal.ru/index.php/ilmiy/article/view/750

3. Обухов Вадим Анатольевич, Тохирова Сарвиноз Гайратжон кизи, & Исахонов Хушнидбек Муродилжон угли. (2023). ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТА. Ta'lim Innovatsiyasi Va Integratsiyasi, 7(1), 52–57. Retrieved from http://web-journal.ru/index.php/ilmiy/article/view/749

4. Обухов Вадим Анатольевич, Тохирова Сарвиноз Гайратжон кизи, & Сотволдиев Асадбек Аброржон угли. (2023). МЕТОДЫ РАСПОЗНАВАНИЯ И ЭТАПЫ ОБРАБОТКИ ИЗОБРАЖЕНИЯ. Ta'lim Innovatsiyasi Va Integratsiyasi, 7(1), 40–44. Retrieved from http://web-journal.ru/index.php/ilmiy/article/view/757

5. Обухов, В. А. Тохирова Сарвиноз Гайратжон кизи, & Исахонов Хушнидбек Муродилжон угли.(2023). ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТА. Ta'lim Innovatsiyasi Va Integratsiyasi, 7 (1), 52–57. ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТА. Ta'lim Innovatsiyasi Va Integratsiyasi, 7(1), 52-57.

6. Обухов, В. (2023). 5 СПОСОБОВ, КОТОРЫМИ БЛОКЧЕЙН ПОВЛИЯЕТ НА ИНДУСТРИЮ ОБРАЗОВАНИЯ. Engineering problems and innovations.

7. Набижонов , Р., & Обухов , В. (2023). ДАЛЬНЕЙШИЙ ВКЛАД БЛОКЧЕЙН-СЕТЕЙ В РАЗВИТИЕ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ. Research and Implementation. извлечено от https://fer-teach.uz/index.php/rai/article/view/772

8. Обухов, В., Эльнур, Х., & Набижонов, Р. (2023). ПОЭТАПНОЕ ВНЕДРЕНИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН. Research and implementation.