Project No.17 暗号と数理とセキュリティ

メンバー　猪股莉記　小林文太　砂子祐貴　樋口諒　満保蒼月
担当教員　白勢政明　川口聡

■テーマ説明　Theme Explanation

楕円曲線暗号による暗号資産の実現と格子暗号を用いた日本語の暗号化の実装

Realization of Cryptocurrency using Elliptic Curve Cryptography and Implementation of Japanese Encryption Using Lattice Cryptography

加速するAI事情および、量子コンピューターが実用化にむけられていることにより暗号技術の安全性が脅かされていることに伴い、本プロジェクトでは次世代の暗号技術、格子暗号の開発に挑戦することを目的としている。そしてもう一つの目的は、現在、世界中で普及している楕円曲線暗号を使い、公立はこだて未来大学で利用できる暗号資産の開発に取り組むことである。The project aims to develop a next-generation cryptographic technology, lattice cryptography, in response to the threat to the security of cryptographic technology posed by the accelerating development of AI and the practical application of quantum computers. Another objective is to develop a cryptocurrency that can be used at Future University Hakodate using elliptic curve cryptography, which is now widely used around the world.

■楕円曲線暗号　Elliptic Curve Cryptography

○楕円曲線暗号　Elliptic Curve Cryptography

楕円曲線暗号(ECC)とは公開鍵暗号の1種で、楕円曲線(図1)を用いたものである。ECCは主に、安全な通信プロトコル(SSL/TLS, SSH)やデジタル署名(ECDSA, EC-Schnorr)に用いられている。

ECC(Elliptic Curve Cryptography) is a type of public key cryptography that uses elliptic curves. ECC mainly used for secure communication protocols(i.e. SSL/TLS, SSH) and digital signatures(e.g., ECDSA, EC-Schnorr).

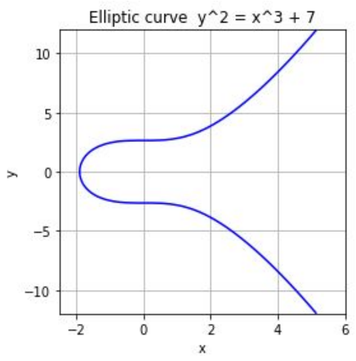


図1.楕円曲線の例

○デジタル署名とブロックチェーン

Digital signatures and Blockchain

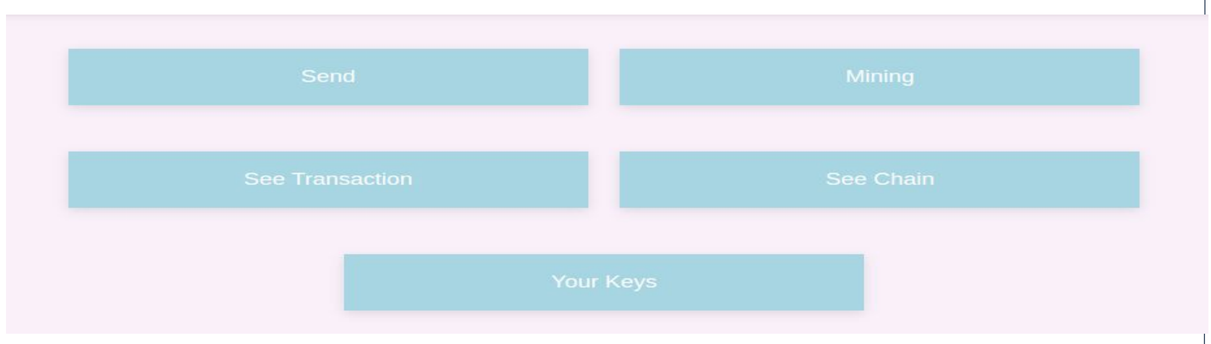
デジタル署名は、公開鍵暗号に類似した改ざん防止手法である。
デジタル署名では、署名者の秘密鍵とメッセージを用いて署名を生成するので、他のメッセージに同じデジタル署名を用いることはできない。
ブロックチェーンは、改ざんが実質的に不可能な分散型のデジタル台帳である。この台帳に記録する取引の正当性(本人確認など)を保証する手法の一つがデジタル署名であり、例えばBitcoinでは、ECDSAが用いられている。

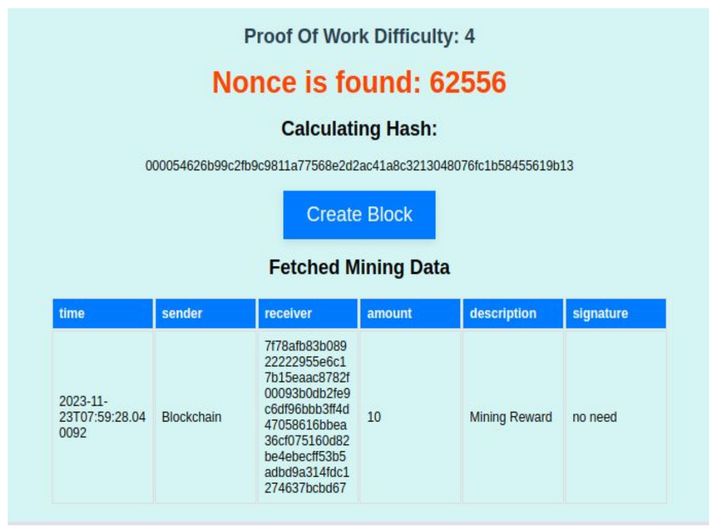
A digital signatures is a tamper-resistant method similar to public key cryptography.
In digital signatures, the signer's private key and message are used to generate the signature, so the same digital signature cannot be used for other messages.
A blockchain is a distributed digital ledger that is virtually impossible to tamper with. A digital signatures is one of the methods used to guarantee the legitimacy (e.g., identity verification) of transactions recorded in this ledger.

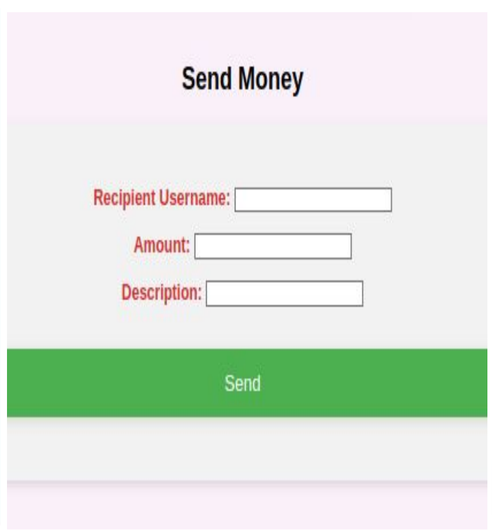
○成果物

*Azure*を用いてクラウドとブロックチェーン技術を融合させ,学内で使用できる暗号資産Webアプリケーションを開発した. 仕組みとしては金額を送金するために(1)トランザクションデータをトランザクションプールに登録する.(2)ユーザーが*JavaScript*によって*Nonce*を発見し,ブロックを作成する.(3)トランザクションデータがブロックに取り込まれる. この過程では,改ざん不可能であり,データの透明性を保持するためにトランザクションプールとブロックのデータは常に*Accessible*にしている.クラウド上でブロックチェーンを実装することにより,ユーザーはソフトウェアをダウンロードすることなく*Immutable*な*暗号資産*サービスを体験することができる.

This web service, hosted on a Microsoft Azure Virtual Machine, aims to provide a *transparent*, *decentralized*, and *immutable* blockchain system on the cloud. Accessible from anywhere, including outside of Future University Hakodate, it enables client-side mining using JavaScript. To guarantee transparency, this site allows you to monitor transaction pools and the data of blocks in the chain. Connections are secured with HTTPS encryption. This service offers the fundamental algorithm of the blockchain, *facilitating those unfamiliar with blockchain technology*. Additionally, by implementing blockchain on the cloud, user can experience an *immutable* cryptocurrency system without needing to downloading any software.







■格子暗号　Lattice Cryptography

○格子暗号とは？ What is lattice cryptography?

1次独立なベクトルの組(格子基底)を整数倍した点の集合が格子である(図1)。また、格子基底が異なる場合でも同じ格子を生成できることがある(図2)。本プロジェクトでは、以下に示す格子問題を解く困難さを安全性の根拠にした格子暗号を研究した。

A lattice is a set of points that are integer multiples of a pair of first-order independent vectors (lattice basis) (Figure 1). The same lattice can also be generated for different lattice bases (Figure 2). In this project, we studied lattice cryptography based on the security of the difficulty of solving the following lattice problem.

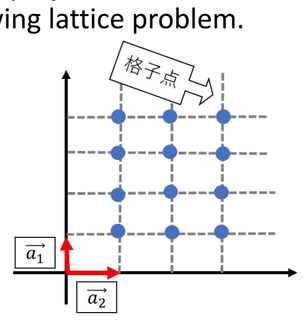


図1. 格子

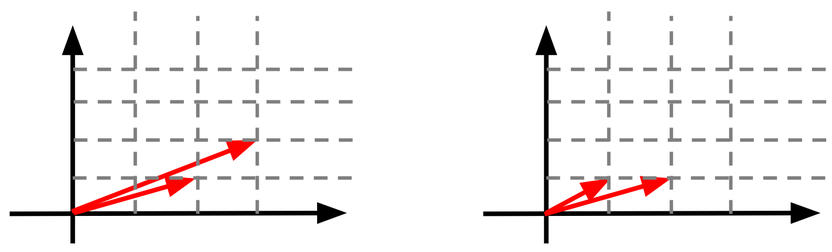


図2. 同じ格子を生成する格子基底の例

○格子暗号の安全性の根拠 Basis for security of lattice ciphers

格子暗号の安全性を担保しているのは格子問題という数学問題である。格子問題の例として最近ベクトル問題、LWE問題、最短ベクトル問題が存在する。この時、最近ベクトル問題とは与えられた点に対して一番近い格子点を求める問題であり、LWE問題とは未知数が式の数よりも多い連立合同式を解く問題である。本グループで用いたGGH方式では最近ベクトル問題を利用しており、LWE方式ではLWE問題を利用している。また、3つめの最短ベクトル問題は与えられた格子に対して最も原点からの距離が短い非零ベクトルを求める問題である。

The security of lattice cryptography is ensured by a mathematical problem called the lattice problem. Examples of lattice problems are the nearest neighbor vector problem, the LWE problem, and the shortest vector problem. The nearest neighbor vector problem is the problem of finding the nearest lattice point to a given point, and the LWE problem is the problem of solving a congruence equation where the number of unknowns is greater than the number of equations. The GGH method used in this group uses the nearest neighbor vector problem, while the LWE method uses the LWE problem. The third shortest vector problem is to find the shortest non-zero vector for a given lattice.

○成果物

格子暗号の暗号方式であるGGH方式とLWE方式を用いてネットワーク上で安全に暗号化/復号ができるwebページを作成した。このwebページの暗号化/復号は公開鍵暗号方式に則って作成した。本ページの機能としては、「encryption」ページで自分が打ち込んだテキストを公開鍵で暗号化し、その暗号化情報をテキストファイルとして保存する。そして、「decryption」ページで秘密鍵を使って暗号化した情報を復号するというものである。

We created a web page that can be securely encrypted/decrypted over a network using the GGH and LWE methods, which are lattice-based cryptographic schemes. The encryption/decryption of this web page was created in accordance with public key cryptography. The function of this page is to encrypt the text you type on the "encryption" page with the public key and save the encrypted information as a text file. Then, on the "decryption" page, the encrypted information is decrypted using the private key.