Vol.2020-MPS-131 No.21
2020/12/18

ぬりかべパズルの NP 完全性を利用した暗号技術への応用

飛田翔哉 [1]　安細勉 [1]

概要：近年，買い物や行政手続きなどはインターネット上で行われることが一般的になり，クレジットカード番号や個人名，住所などの個人情報がインターネットを介してやり取りされている.その中で公開鍵暗号系の技術は現在のインターネットセキュリティにおいて基礎となる技術であり，RSA 暗号は公開鍵暗号方式として主流となっている.しかし，量子コンピュータの登場により，公開鍵暗号系の技術の安全性は脅かされることになる.そこで，量子コンピュータでは効率的に解くことができない NP 完全問題に注目し，比較的最近 NP 完全であることが証明されたぬりかべパズルと呼ばれるペンシルパズルを用いて，ゼロ知識証明を用いた電子認証などの暗号モデルへの応用を試みた.

キーワード：ぬりかべパズル，電子認証，ゼロ知識証明

Application to cryptography using Nurikabe puzzle with NP completeness

SHOYA TOBITA[†1]　TSUTOMU ANSAI[†1]

Abstract: In recent information society, shopping and administrative procedures are generally performed on the Internet, and personal information that should not be known to third parties is exchanged via the Internet. In order to securely communicate such information, RSA encryption using a public key cryptosystem, which is a basic technology in current Internet security, is widely used. However, with the advent of quantum computers, the security of public key cryptosystems such as RSA cryptography has been lost. In this research, I tried to application to cryptographic model such as electronic authentication using zero-knowledge proof, using Nurikabe puzzles that were proved to be NP-complete relatively recently.

Keywords: Nurikabe puzzles，electronic authentication，zero-knowledge proof

1. はじめに

昨今の情報化社会において，買い物や行政手続きなどはインターネット上で行われることが一般的になり，様々な個人情報がインターネットを介してやり取りされている.これらの情報を安全に通信するために一般的には通信の暗号化を行い，万が一第三者にインターネット上を行き交うパケットを盗聴されても情報の漏洩を防ぐことができる.特に公開鍵暗号系の技術は現在のインターネットセキュリティにおいて基礎となる技術であり，RSA 暗号は公開鍵暗号方式として主流となっている.

しかし，このような暗号技術を脅かす存在として量子コンピュータが挙げられる.現在実用的な量子コンピュータは実現していないが，将来的に量子コンピュータが実現した場合，RSA 暗号などの公開鍵暗号系は安全性を失われてしまう.

そこで本研究では，比較的最近に NP 完全であることが証明されたぬりかべパズルというペンシルパズルを用いた暗号モデルへの応用を試みた.

2. ぬりかべパズル

ぬりかべは株式会社ニコリ出版のパズル通信ニコリによって発表されたペンシルパズルである.

プレイヤーは四角形の盤面とその盤面のマス目の所々に記された数字が与えられ，プレイヤーはその数字を元に盤面を黒マスで塗りつぶさなければならない.なお盤面の数字は，その数字が含まれる，黒マスによって分断されたところのマス（ルール上シマと呼ぶ）の数を表し，以下の制約を守らなくてはいけない.

- すべてのシマに数字が１つずつ入るようにし，数字が入っているマスを黒くぬってはいけない
- すべての黒マスはタテヨコにひとつながりになっていなければならない
- 黒マスを２×２以上のカタマリにしてはいけない

以下，図 1 に問題の例とその解答を示す.

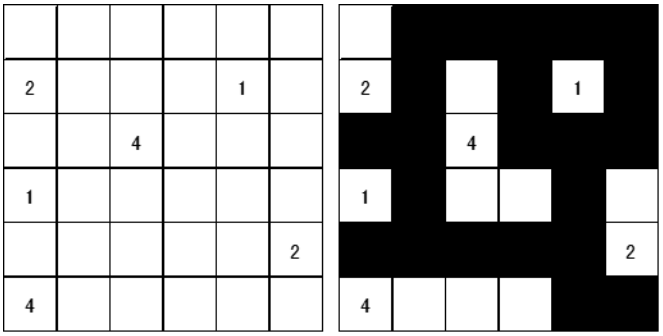

図 1　問題の例(左)とその解答(右)

1 茨城工業高等専門学校
National Institute of Technology，Ibaraki College

また，ぬりかべは 2004 年に，クラス NP に属する決定問題で，任意のクラス NP に属する問題から多項式時間帰着可能な問題である NP 完全性が証明されている[1].

3. 暗号技術への応用

3.1 ゼロ知識証明による電子認証

パズルの性質を利用し，二者間の通信において，通信相手が本人かどうか検証する中立で安心できる通信を保証する認証局を介して電子認証を行う.通信する二者間の内，相手が本人かどうかを確認することを認証局に要請する人物を検証者，自分が本人であることを認証局に証明する人物を証明者とする.この時，証明者のみがパズルの解を持っているものとし，その解を知っている事を証明する事で自身が証明者本人である事を証明する.しかし，証明者がパズルの解をそのまま認証局に送信してしまうと，悪意ある第三者が通信を傍受した際に，パズルの解を知りなりすましが可能になってしまう．その際に，ゼロ知識証明を用いて証明者がパズルの解を持っている事を証明する．

3.2 具体例

3.1 項で前述した認証局において，証明者がいくつかのパズルの問題と，それぞれのパズルの解から切り取った一部分，パズルを解いた際の縦と横の行のそれぞれのシマの数を認証局に送信し保管しておく．

今回は図１のパズルをもとに認証を行うと想定する.図２は，図１のパズルから切り取った一部分と，パズルを解いた際の縦と横の行のそれぞれのシマの数を表す.

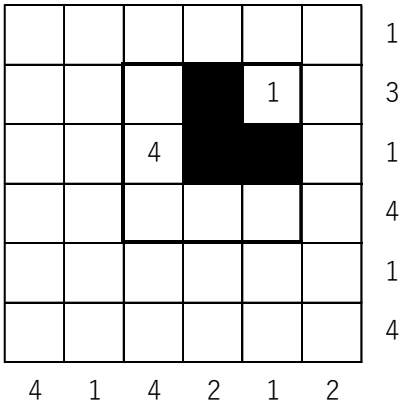

図 2　図１のパズルから切り取った一部分と，パズルを解いた際の縦と横の行のそれぞれのシマの数

検証者から要請を受けた認証局は証明者に対し事前に受けとったパズルの問題を提示し，パズルの解の切り取った部分がどこかを質問する.証明者は提示された問題のパズルの内，図３のような切り取った一部分以外のパズルの解を認証局へ送信する.認証局はあらかじめ保管されているパズルの解の一部分と証明者から送られてきた穴の開いたパズルを組み合わせ，同様に保管されている縦と横のシマの数を確認し，そのパズルの問題の解となっているかを確認し，証明者が正当な証明者であるか判断する.

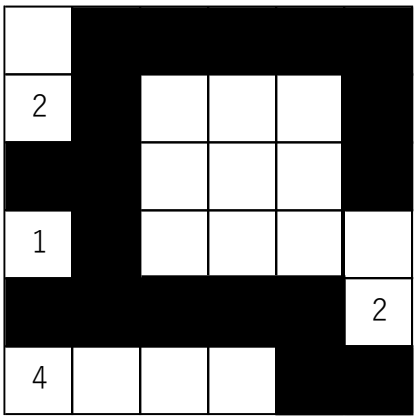

図 3　切り取った一部分以外のパズルの解

認証局は，検証者に対して証明者が認証を通過したかを yes/no の二値で知らせる．

3.3 安全性

この認証システムの安全性は，ぬりかべパズルの解を持つ正当な証明者と，パズルの解をもたない者が認証を通過しようとする場合について考えることで検証する.

3.3.1 正当な証明者が認証を通過しようとする場合

ぬりかべパズルの解を持つ正当な証明者にとって，認証局から送られてきた問題を解くことは容易である.よって，検証者が複数回認証を繰り返しても証明者は問題を解くことができ，認証を拒否されることはない.

3.3.2 パズルの解をもたない者が認証を通過しようとする場合

ぬりかべパズルの解を持つ正当な証明者以外の者は問題を解くことができない.また，検証者が認証を複数回繰り返すことによって正当な証明者以外の者が認証を通過する確率を低くすることができる.

4. 今後の課題

今後本研究を行う際に発生する課題を以下に示す.

- 計算量的安全性と実際の計算シミュレーション
- 電子認証の電子署名への発展
- 電子署名における平文の定義

参考文献

[1] Markus Holzer，Andreas Klein，Martin Kutrib . On The NP-Completeness of The Nurikabe Pencil Puzzle and Variants Thereof. In Proceedings of the 3rd International Conference on FUN with Algorithms ,pages 77–89，Isola d’Elba, Italy， May 2004.