Vol.2021-MPS-135 No.8
2021/10/18

ヘルゴルフパズルの情報セキュリティ技術への応用

藤家一夢 [1]　安細勉 [1]

概要：現在，公開鍵暗号系の技術は，インターネットセキュリティでも基礎となる技術の一つであり，特に RSA 暗号は主流となっている．しかし，このような暗号技術を脅かす存在がある．それは量子コンピュータであり，従来のコンピュータと比べて非常に高い計算性能を持つため素因数分解問題や離散対数問題を効率的に解くことができてしまい，素因数分解を効率的にできないことを安全性の根拠とした RSA 暗号は，将来量子コンピュータが実現した場合，安全性を失ってしまう．そこで本研究では，近年 NP 完全性が証明されたヘルゴルフパズルを用いて，量子コンピュータに対しても安全性の確保が可能である情報セキュリティ技術の開発を目標とする．

キーワード：ヘルゴルフパズル，NP 完全問題，公開鍵暗号

Applying of Herugolf Puzzle into information security technology

KAZUMU FUJIIE[†1]　TSUTOMU ANSAI[†1]

Abstract: Currently, public key cryptosystem is one of the fundamental technologies in Internet security, and RSA cryptosystem in particular has become a mainstream cryptosystem. However, there is an entity that threatens these cryptosystems. This is the quantum computer, which can efficiently solve prime factorization problems and discrete logarithm problems due to its extremely high computational performance compared to conventional computers. The RSA cryptosystem, whose security is based on its inability to efficiently solve prime factorization, will lose its security when quantum computers are realized in the future. In this research, we aim to develop an information security technology that can be secured against quantum computers by using the Herugolf puzzle, whose NP-completeness has recently been proven.

Keywords: Herugolf puzzle, NP-Complete problem, cryptosystem

1. はじめに

現在，公開鍵暗号系の技術は，インターネットセキュリティでも基礎となる技術の一つであり，特に RSA 暗号は主流となっている．近年ではインターネット上で買い物や行政手続きなどを行うことが一般的になってきていることや，また昨今の COVID-19 の影響により，リモートワーク等の今までインターネット上で行われる機会がなかったことが一般的に行われるようになっていることもあり，公開鍵暗号系の技術は特に社会にとって必要な技術となっている．

しかし，このような暗号技術を脅かす存在がある．それは量子コンピュータであり，従来のコンピュータと比べて非常に高い計算性能を持つ．また，素因数分解問題や離散対数問題を効率的に解くことができてしまうため，素因数分解を効率的にできないことを安全性の根拠とした RSA 暗号は，将来量子コンピュータが実現した場合，安全性を失ってしまうことになる．

そこで本研究では，近年 NP 完全性が証明されたヘルゴルフパズルを用いて，量子コンピュータに対しても安全性の確保が可能となる情報セキュリティ技術のうち，公開鍵暗号系の開発を目標とする．

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

2. ヘルゴルフパズル

ヘルゴルフパズル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．[1]

以下にヘルゴルフパズルのルールを示す．

（1）すべての丸（球）を何回か移動させ，H（ホール）のマスに運ぶ．各 H のマスに球が 1 つずつ運ばれる
各回の移動は矢印で表し，矢印の先端はマスの中央になる．
（2）矢印の線が他の球や H のマスを通過したり，線どうしで交差したり重なったりしてはいけない
（3）1 回の移動は縦か横にまっすぐ，球の数字分のマスだけ移動する．1 回の移動を終えるごとに球の数字は 1 減り，再度移動可能となる．移動方向は各回で変えてもかまわない
（4）数字が 0 になった球や，H のマスで停止した球はそれ以上移動が不可能となる
（5）球が盤面の外に出たり（OB），灰色のマス（池）で停止したりするような移動はできない

また，ヘルゴルフパズルは 2018 年に NP 完全性が証明されている．[2]

以下，図 1 に問題例とその解答を示す．

ⓒ2021 Information Processing Society of Japan

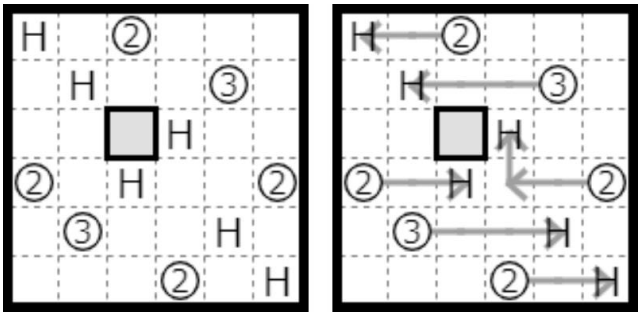

図 1　問題の例(左)と解答(右)
Figure 1　Problem(left) and Solution(right) of Herugolf Puzzle

3. 提案手法

前提として，ここから取り扱うヘルゴルフパズルは池がない場合に限るものとする．

3.1 ダミー球

本研究の目標である情報セキュリティ技術への応用となる公開鍵暗号の開発のため，ダミー球というものを定義する．定義は以下のとおりである．

- ダミー球とは暗号化の際, 通常の球と混ぜて置くダミーの球のことである
- ダミー球は通常の球と見分けはつけられず, 動きも通常の球と同様であるとする
- ダミー球に対応するホールはないものとする
- ダミー球は少なくとも 1 回は移動させることとする
- ダミー球およびダミー球の経路となる矢印は平文の情報を埋め込まないものとする
- 上記以外については 2 項にあるルールを適用する

3.2 具体例

図 2 は，ダミー球を用いたヘルゴルフパズルの具体例とその解答である．今回の例では，球が 3 つに対し H のマスが 2 つしかないため，ダミー球が 1 つあることが分かる．ここで，不正解の例として図 3 を示す．このとき，どちらも 2 つの球は H のマスまで移動できているが，残った球は 1 回も移動することができない．これは 3.1 項で述べた定義に反するため，不正解となる．実際，図 2 にある解答はダミー球の定義をすべて満たしていることが分かる．

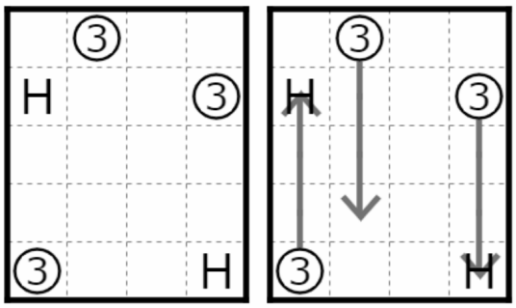

図 2 ダミー球があるヘルゴルフの問題例(左)と解答(右)
Figure 2　Herugolf Puzzle with a Dummy Ball

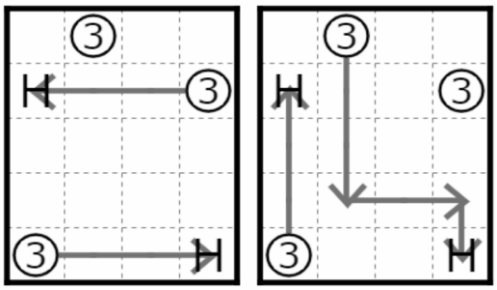

図 3　図 2 の問題における不正解の例
Figure 3　Example of Incorrect Answer in the Problem in Fig. 2

4. 検討

4.1 ダミー球の期待される効果

公開鍵暗号系を構成する要素として，秘密鍵，公開鍵，平文，暗号文がある．これらをヘルゴルフパズルの要素と対応させることで，暗号が完成する．現在，ダミー球に関する全ての情報を秘密鍵，盤面上にあるダミー球の経路となる矢印の一部を含んだ複数の矢印を公開鍵，H のマスに移動し終わった時点での球の数字を平文，図 2 の左にあるようなダミー球を混ぜた問題を暗号文として考えている．

この時に期待されるダミー球の効果については以下が考えられる．

4.1.1 復号における計算量の減少

暗号化の際，ダミー球を通常の球と混ぜて置くことで，ダミー球の情報を持っていた場合，ダミー球は 2 項にあるルール（2）によって，境界線のような役割をもつようになる．これにより，復号の際に計算量を減らすことができると考えられる．

4.1.2 解読における計算量の増加

通常の球とダミー球を混ぜて暗号化した暗号文に対し，攻撃者はダミー球の情報を持っていない．このとき，どの球がダミー球かが分からないため，ルールおよび定義上成立するすべてのダミー球と通常の球の組み合わせを検証しなければならず，結果，同じサイズで通常の球だけで構成された場合と比べて，計算量が増加すると考えられる．

5. 今後の課題

今後，本研究を行うに際しての課題は以下となる．

- 考案した公開鍵暗号の検証および改良
- 計算量的安全性と実際の計算シミュレーション
- 電子署名・電子認証への応用

参考文献

[1] Chuzo IWAMOTO, Masato HARUISHI, Tatsuaki IBUSUKI. Computational Complexity of Herugolf and Makaro. IEICE, Vol.E102-A, No.9, pp.1118-1125.
[2] “nikoli ヘルゴルフ”. https://www.nikoli.co.jp/ja/puzzles/herugolf/, (参照：2021-09-15).

ⓒ2021 Information Processing Society of Japan