Vol.2020-MPS-131 No.24
2020/12/18

「橋をかけろ」を用いた電子認証の提案

芳賀陸雄[1]　安細勉[1]

概要：本発表では、ペンシルパズル「橋をかけろ」の NP 完全性を用いたゼロ知識証明による電子認証への応用の方法を提案する．現在使用されている RSA ベースの電子認証方法は量子コンピュータに対する耐量子性を持っていない．そこで、耐量子性を持つ新たな電子認証の方法を考える必要がある．他のペンシルパズルを用いた電子認証においては、認証局の責任の重さ、証明者と認証局とのゼロ知識性に問題があり、本発表では、その 2 点について改善する方法を提案する．

キーワード：NP 完全、耐量子計算機暗号、ゼロ知識証明、電子認証、ペンシルパズル

A New Electronic Authentication Using “Hashiwokakero”

RIKUO HAGA[†1] TSUTOMU ANSAI[†1]

Abstract: We propose a new electronic authentication by zero knowledge proof using “Hashiwokakero”. The RSA-based electronic authentication currently be used is not tolerant of Quantum computer. So, we need to consider alternative method. Previous study about electronic authentication using other Pencil Puzzles had some problem that are insufficient Zero knowledge and momentousness of Certification Authority responsibility. This study will improve them.

Keywords: NP-complete, Post Quantum Cryptography, Zero Knowledge proof, Electronic Authentication, Pencil Puzzle.

1. はじめに

近年、量子コンピュータ(QC)の開発研究が盛んに行われており、大規模な QC が数十年後には実現する可能性が高まってきている．公開鍵暗号や、電子認証、電子署名等で主に使用されている RSA の安全性の根拠とする素因数分解問題は QC によって効率的に解くことができるアルゴリズムが見つかっており、大規模な QC が実用化されると現在使用されている暗号方式のほとんどで安全性を保障できなくなってしまう．そこで、QC に対しても耐性をもつような新しい暗号方式の研究開発が課題となっている．また、公開鍵暗号を応用した電子認証、デジタル署名なども同様に QC に対する耐性が求められている．以上から、耐量子性のある NP 完全問題を情報セキュリティ技術へ応用する研究テーマの着想に至った．本研究の先行研究として、NP 完全問題である「バトルシップ問題」を用いたゼロ知識認証による電子認証方式の研究[1]があるが、ゼロ知識認証のステップにおける認証局とのゼロ知識性、責任の重さに問題があった．そこで、NP 完全問題から「橋をかけろ」を選び上記問題を解決する電子認証の研究を行っている．

2. 橋をかけろ

「橋をかけろ」はパズル通信ニコリ[2]にて発表され、数字を線でつなぎ合わせるペンシルパズルである．また、2009 年には「ハミルトン路問題」へと帰着可能なことから NP 完全問題であることが証明[3]されている．図 1 に問題の例と解を示す．

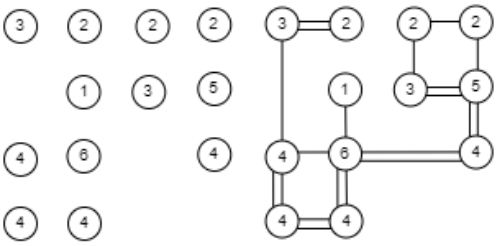

図1 問題の例と解
Figure 1 Example of "Hashiwokakero" Problem and Solution

2.1 ゲームルール

(1)数字同士を線で結び、全ての数字を線で繋げる．
(2)線は他の線と交差したり、数字を横切ったりできない．
(3)線は水平方向か垂直方向のみに引かれる．
(4)どの数字の間にも 2 本までしか線は引くことができない．
(5)数字はその数字から引かれる線の数を表す．

2.2 Hashi Solving Techniques

「橋をかけろ」には線を引ける箇所が直ちに定まるテクニックがいくつか存在[4]し、解を求めるための計算量を大幅に減少させることができる．

(1) Just Enough Neighbor Techniques

引くことができる線の数と数字が一致している時は、線を引ける箇所がその箇所だけに定まる．

(2) One Unsolved Neighbor Techniques

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

数字 1 の隣に 1 つだけしか数字が存在しない時は、線を引ける箇所がその箇所だけに定まる.

(3) Few Neighbor Techniques

ルール(4)より､線を引ける箇所が少なくとも 1 本定まる場合が存在する.

(4) Leftover Techniques

線を引ける箇所が N で隣り合う数字の数が N の時、隣の数字が 1 と(N-1)の時は(N-1)の方から線を引く.

(5) Isolation Techniques

ルール(1)より､数字は孤立しないように線を引く必要があるので、引ける箇所が定まる場合が存在する.

2.3 解の唯一性

パズルを生成時に Hashi Solving Techniques を使用して、その箇所以外に線を引くことができないことをチェックしながら数字を決めることで、パズルの解が唯一となるように生成することができる.

3. 提案手法

本研究では「橋をかけろ」と対話式ゼロ知識証明を用いた電子認証方式を提案する. 本研究における電子認証では正しい通信相手であることを証明する側を証明者、確かめる側を検証者とする.

3.1 認証の準備

証明者は認証の前に以下の準備を行う必要がある.

・問題のサイズを決めるパラメータを N とする.

・サイズ 2N(N-1)の盤のうち線を引く箇所を 1, 引かない箇所を 0 としてハミルトン路を生成し、H とする.

・H のサイズを 2(2N-1)(2N-2)に拡大し、B_1 とする.

・線を 1 本引く箇所を 0, 2 本引く箇所を 1 として、{0,1}を一様分布から $2(N^2-1)$個選び、B_2 とする.

・B_1 と B_2 を組み合わせたものを B とする.

・解が唯一となるように線を引く箇所を増やし、パズルを生成し G とする. G の解を A とする.

・できた G を公開し、A を知っていることを正しい証明者であることの根拠とする.

3.2 認証の手順

1. 検証者は公開されている G を、解が唯一となるように、サイズ$(2N+1)^2$ に拡大し、exG として証明者へ送信する. 拡大して増えた線を引く箇所を exB とする.
2. 証明者は G の解から解の唯一性判定を行うことで exG の解を求める. ここで求まったものを exA'とする.
3. 証明者は exA'から A を引いた部分を exB'とし､検証者へ送信する.
4. 検証者は exB と exB'が等しければ認証をパスする.

1~4 を n 回繰り返すと、n 回連続で認証をパスできる確率は$(1/2)^n$となり、n を十分に大きくすると A を知らずに認証をパスできる確率は十分に小さくなり、A を知っていると証明することができる.

3.3 ゼロ知識証明の性質

ゼロ知識証明を用いる際は次の 3 つの性質を満たす必要がある. A を証明者、B を検証者とする.

・完全性(Completeness)

A が本当に命題 P を知っているときに検証が通ること.

提案手法では､パズル G から exG への拡大の際に唯一解を持つように拡大するから A を知っている者は exA を求めることができるので完全性を満たす.

・健全性(Soundness)

検証が通れば本当に A が命題 P を知っていることを保証すること.

提案手法では、NP 完全問題であることから問題のサイズを決める N が十分に大きければ exG から解を求めることは難しいので健全性を満たす.

・ゼロ知識性(Zero knowledge)

検証過程で命題 P に関する情報が洩れていないこと.

提案手法では､認証の過程で証明者は検証者に exB'しか与えないから A に関する情報は全く漏れていないのでゼロ知識性を満たす.

4. 結論

本研究では「橋をかけろ」を用いたゼロ知識証明による電子認証の手法を提案した. 先行研究[1]ではゼロ知識性に問題があり、認証局を利用することで証明者と検証者とのゼロ知識性を確保していたが証明者と認証局との間のゼロ知識性が問題であった. 提案手法では、ゼロ知識性を高めたことにより認証局の必要性を無くし先行の問題を解決した.

5. 今後の課題

現段階では、問題のサイズの大きさをどれだけ大きくすれば安全性を確保できるかという検証ができていないので、問題のサイズによる安全性の検証を行う必要がある. また、本研究で用いたゼロ知識証明の手法は対話式ゼロ知識証明であるが、一般的に非対話ゼロ知識証明の方が通信回数が 1 回で済むので使い勝手が良いとされている. 今後は非対話ゼロ知識証明での実現が望まれる.

参考文献

佐藤哲平, 安細勉.バトルシップ問題を用いたゼロ知識証明による電子認証. 平成 29 年度電気学会東京支部茨城支所研究発表会. p.114-115.

"nikoli 橋をかけろ". https://www.nikoli.co.jp/ja/puzzles/hashiwokakero/, (参照 2020-11-15).

Anderson, D. Hashiwokakero is NP-complete. Information Processing Letters 109(19). p.1145-1146.

Malik, R.F., R.Efendi, A.P.Eriska. Solving Hashiwokakero puzzle game with hashi solving techniques and depth first search. Bulletin of Electrical Engineering ad Informatics 1(1). p.61-68