Vol.2021-MPS-135 No.7
2021/10/18

カードベースプロトコルを用いた情報セキュリティの検討

國井 大[1]　安細 勉[1]

概要：インターネットは匿名性が高く、自分と通信している相手が本当に自分の想定している相手かどうかわからないことも多々ある。匿名性を利用したなりすましや盗聴を防ぐために、情報セキュリティ技術が重要になる。また、急な災害等が発生し、コンピュータが使えなくなると、通信が行えなくなってしまうので、日常生活に支障をきたしてしまう。そのため、デジタルではなくアナログな技術での通信も必要になってくると考えられる。これらの事から、近年カード組による秘密計算を用いた情報セキュリティ技術が開発されているが、その改良について発表する。

キーワード：カードベースプロトコル、　公開鍵暗号、　電子認証

A investigate of Information Security Using Card-Based Protocols

DAI KUNII[1]　TSUTOMU ANSAI[1]

Abstract: The Internet has anonymity, and it is often difficult to know if the person you are communicating with is who you think they are. Information security technology will be important to prevent identity theft and eavesdropping using anonymity. And if a sudden disaster or other event were to occur and computers were not available, communication would not be possible, which would interfere with daily life. Therefore, it will be necessary to communicate using analog technology instead of digital. For these reasons, information security technology using secret computation with card pairs has been developed in recent years, and I will present improvements to this technology.

Keywords : Card-based protocol, Public key encryption, Electronic authentication

1 はじめに

近年、スマートフォンやウェアラブル端末の急速な普及によって、インターネットを介してのやりとりが生活の一部になってきている。最近ではインターネットを使った遠隔での授業や仕事、会議などが増えてきている。だがインターネットは匿名性が高く、自分と通信している相手が本当に自分の想定している相手かどうかわからないことも多々ある。匿名性を利用したなりすましや盗聴を防ぐために、情報セキュリティ技術が重要になる。また、急な災害等が発生し、コンピュータが使えなくなると、通信が行えなくなってしまうので、日常生活に支障をきたしてしまう。そのため、デジタルではなくアナログな技術での通信も必要になってくると考えられる。今回はカード組による秘密計算を用いた情報セキュリティ技術の向上についての提案、及び作成を行う。

2 カードベース暗号の排他的論理和の演算

入力 a と b が図 1 のように示されているとする。

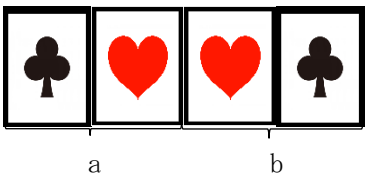

図 1 入力 a と b の位置(クローバーが黒、ハートが赤のカードを表す)
Figure1. Position of input a and b(clover:black heart:red)

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

カードを裏返し、図 2 のようにカードの位置を入れ替える。

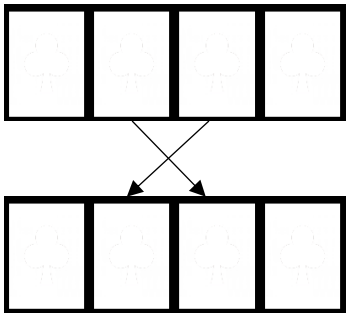

図 2　カードの入れ替え
Figure2. Replacing cards

ランダム二等分カット(カードの列を左右で同じ枚数になるように分割し、任意の回数、左右を入れ替える)を行い、再び図 2 のようにカードの位置を入れ替える。左の二枚のカードをめくったときに図 3 のようになっていれば、右側の二枚は a と b の排他的論理和になっており、図 4 のようになっていたら、右側の二枚は a と b の排他的論理和の否定になっている。

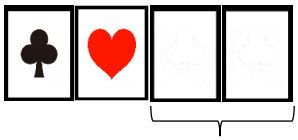

図 3　演算結果その 1
Figure3. Result1

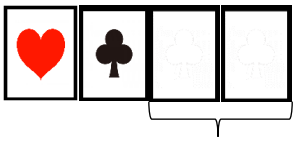

図 4　演算結果その 2
Figure4. Result2

3　カードを用いたゼロ知識証明

ゼロ知識証明は認証によく用いられ、1 から 9 までの数字が書かれたカードを用いて数独パズルを解いたことを証明するゼロ知識証明の方法[6]がある。しかし、この方法を行おうとすると、カードの枚数が 3×9×9 = 243 枚のカードが必要になってしまう。また、この数独をはじめとするペンシルパズルを用いた認証技術は、秘密鍵にペンシルパズルの答えを用いる事が多く[4][5]、その問題の作成に時間がかかってしまう。また、このゼロ知識証明の方法は 1 から 9 までの数字が書かれたカードを合計 243 枚用意しなければならず、実現するには少々手間がかかる。本研究では 2 種類の記号が書かれたカードを用いれば実現できる（記号でなくても見分けが付くものなら実現可能。）ため、上記のカードを用いた認証技術よりもカードな枚数が少なく、実現がさらに容易な新しいカードを用いた認証技術を提案する。

4　情報セキュリティ技術への応用

カード組による数列を秘密鍵(以下、秘密カード列とする)とし、その数列に使ったカードの枚数を公開鍵とする。公開鍵をもとに相手に、秘密鍵と同様の方法で数列(以下、公開カード列とする)を作成してもらい、その数列を自分と第三者に送ってもらう。自分と第三者が秘密カード列と公開カード列で排他的論理和を取り、お互いの結果をもとにもう一度、排他的論理和を計算する。もし、自分が相手の想定している人物なら、最終的な排他的論理和の演算結果はすべて 0 になる。

5　今後の課題

- 提案した技術のパラメータ(カードの枚数やランダム二等分カットの回数)を変え、計算速度[2]がどのように変化していくかのデータを取る。
- 認証に応用する際の適切なカードの枚数を調査する。

6　参考文献

[1] 水木敬明(2015)「カード組を用いた秘密計算」電子情報通信学会 基礎・境界ソサイエティ Fundament review 9 巻 3 号

[2] 上田 格・林 優一・水木 敬明・曽根 秀昭(2017)「実行時間に基づいたカードベースプロトコルの評価手法」コンピュータセキュリティシンポジウム 2017 論文集 2 号

[3] 田口 渉(2018)「立体ピクロスの情報セキュリティへの応用」平成 30 年度 電気学会東京支部茨城支所研究発表会. 2018. 124-124

[4] 芳賀 陸雄(2020)「「橋をかけろ」を用いた電子認証の提案」Vol.2020-MPS-131,No.24,1-2 (WEB ONLY)

[5] 飛田翔哉(2020)「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」Vol.2020-MPS-131,No.21,1-2 (WEB ONLY)

[6] “イメージで理解できる-ゼロ知識証明”
https://note.com/strictlyes/n/n4566802b2830
(参照:2021-09-13)