マルチメディア通信と分散処理　85－3
（１９９７．　１１．　６）

アソシエーションスキームを用いた ゼロ知識対話証明プロトコルの提案

須賀祐治*†　　荒木啓二郎*‡
suga@k-isit.or.jp　　araki@csce.kyushu-u.ac.jp

*（財）九州システム情報技術研究所
〒８１４　福岡市早良区百道浜２丁目１番２２号　Phone:(092)852-3454, Fax:(092)852-3465
†（株）エクシーズ
‡九州大学大学院 システム情報科学研究科

概要　本報告ではアソシエーションスキームを用いたゼロ知識対話証明(以下 ZKIP) を提案する。ZKIP は相手認証やディジタル署名などといった情報セキュリティの技術へと形を変えることができる。今回提案する ZKIP は認証方式としてはまだ実用的ではないが、秘密分散方式にも対応できる点で優れている。

現在、RSA 等多くの認証方式の安全性を保証しているのは、十分大きな数の因数分解は難しいという事実である。近い将来、効率のよい因数分解のアルゴリズムが発見された時点で、これらの認証方式の安全性が失われることも想定される。本研究は RSA 等とは全く別の観点から新しい認証方式を導入することで、これらの事故が起きた場合の一つの代替方式として提案する意味合いも持つ。

A proposal for zero-knowledge interactive proofs using association schemes

Yuji SUGA*†　　Keijiro ARAKI*‡
suga@k-isit.or.jp　　araki@csce.kyushu-u.ac.jp

*Institute of Systems & Information Technologies/KYUSHU
2-1-22, Momochihama Sawara-ku, Fukuoka City 814, Japan
Phone:+81-92-852-3454　Fax:+81-92-852-3465
†Xseeds Co., Ltd.
‡Department of Computer Science and Communication Engineering, kyushu University

Abstract　This paper proposes zero-knowledge interactive proofs (ZKIPs in short) using association schemes. ZKIPs can be transformed into technologies of securities such as authentication, digital signature and so on. Proposed protocols are not practical, but are superior others because these can use as the secret sharing schemes.

The difficulties of the solution into factors assure everyone of one's securities. So if useful algorithms for the solution into factors are found, RSA forfeits confidence. This paper also proposes a new substitute method by viewing from a different angle.

1 はじめに

ゼロ知識対話証明(以下 ZKIP)は自分が保持する秘密情報を漏らすことなく、秘密情報を知っていることだけを相手に示すことのできる質疑応答型(Challenge/Response)のプロトコルである。このZKIPの概念は1985年に初めて発表され[2]、相手認証やディジタル署名など情報セキュリティの技術への応用がなされてきた。

現在、個人認証やディジタル署名に用いられている方式は RSA が主流である。RSA は公開鍵暗号方式のアルゴリズムであるので、署名だけでなく暗号化もこなす点で優れている。RSA の安全性を保証しているのは、十分大きな数の因数分解は難しいという事実である。この事実からのみの安全性に依存するのは暗号，認証方式の一極集中を引き起こすことになる。この安全性が崩れてしまう（効率のよい因数分解アルゴリズムが発見される等）前に、パラレルに様々な方式で研究を進めておくべきであろう。ある暗号方式に穴が見つかったとしても、全く別の方式と平行して運用していれば大きな混乱は免れることができる。実際、最近では離散対数問題，カオスなど、いずれも解くことが困難な数学的事実をベースにした新しい暗号方式が提案されている。

本稿では、この観点からアソシエーションスキーム（以下 AS）を用いた新しい認証方式を提案する。AS は代数的組合せ論において最も重要な概念の一つであり、有限群論，符号理論，グラフ理論などと深く関係している[1]。AS についての研究は多岐に渡っており、今でも様々な分野への広がりを見せつつある。本研究もその一つの流れになることを切望する。

本稿での構成は以下の通りである。まず 2 章で AS の定義と安全性のベースとなっている数学的事実を紹介する。次に 3 章で AS を用いた ZKIP を提案し安全性を検討した後、4 章ではその応用について触れる。最後に 5 章で本稿のまとめならびに今後の課題を述べる。

2 アソシエーションスキーム

まずアソシエーションスキーム(association scheme)という概念を紹介する。AS は代数的組合せ論において最も重要な概念の一つであり、有限群論，符号理論，グラフ理論などと深く関係している[1]。この章では、AS の定義と 3.2節で提案する ZKIP で用いる補題を紹介する。

2.1 定義

AS には次の組合せ的観点からと代数的観点からの 2 つの定義がある。

定義 1 (組合せ的定義) Xをn点の有限集合、各R_i $(i=0,\ldots,d)$をX上の関係（すなわち$X\times X$の空でない部分集合）とする。この 2 つの組$\mathcal{X}=(X,\{R_i\}_{0\le i\le d})$がASであるとは次の 4 条件を満たすものとする。

(*i*) $R_0=\{(x,x)|\ x\in X\}$.

(*ii*) $R_0\cup R_1\cup\ldots\cup R_d=X\times X$でかつ
$R_i\cap R_j=\emptyset$ if $i\neq j$.

(*iii*) 各$i\in\{0,1,\ldots,d\}$に対して
$R_i^t:=\{(y,x)|(x,y)\in R_i\}$と定義すると
$R_i^t=R_j$ となる$j\in\{0,1,\ldots,d\}$が存在する。

(*iv*) 各$i,j,k\in\{0,1,\ldots,d\}$に対して
$\left|\{z\in X\mid (x,z)\in R_i,(z,y)\in R_j\}\right|$は
$(x,y)\in R_k$のもとで、x,yの取り方によらず
i,j,kのみに依存する非負整数p_{ij}^kに等しい。

グラフ理論に熟知した方には、n点完全グラフの辺全体をある条件を満たすように分割（色分け）したものととらえることができるであろう。

定義 2 (代数的定義) 定義 1 の仮定のもと各R_iに対する隣接行列A_iを次のように定義する。

$$(A_i)_{xy}:=\begin{cases}1 & \text{if } (x,y)\in R_i,\\ 0 & \text{otherwise.}\end{cases}$$

このとき$\mathcal{X}=(X,\{R_i\}_{0\le i\le d})$がASであるとは次の 4 条件を満たすものとする。

(*i*) $A_0=I$（単位行列）.

(*ii*) $A_0+\cdots+A_d=J$（成分がすべて 1 の行列）.

(*iii*) 各$i\in\{0,1,\ldots,d\}$に対して${A_i}^t=A_j$ となる
$j\in\{0,1,\ldots,d\}$が存在する。

(*iv*) 各$i,j,k\in\{0,1,\ldots,d\}$に対して

$$A_iA_j=\sum_{k=0}^{d}p_{ij}^kA_k.$$

が成立する。

定義中のパラメータdを用いて$(X, \{R_i\}_{0\le i\le d})$をclassが$d$のASと呼ぶことがある。上の2つの定義は同値であるので、AS $(X, \{R_i\}_{0\le i\le d})$は$d+1$個の$n$次正方行列の組$\{A_0(=I), A_1, \ldots, A_d\}$と同一視することができる。以後、ASはこの行列の組として考えることにする。

AS $\{A_i\}_{0\le i\le d}$がさらに$A_iA_j = A_jA_i$ for $^\forall i, j$を満たすとき可換(commutative)、$A_i^t = A_i$ for $^\forall i$を満たすとき対称(symmetric)であるという。ASが対称ならば明らかに可換である。

2.2 Fusion & Fission scheme

2つのAS間に対してfusion, fissionという関係を定義することができる。

定義 3 (fusion, fission) 2つのAS $\{A_i\}_{0\le i\le d}$, $\{B_j\}_{0\le j\le e}$ $(d<e)$に対し、任意のA_iが$\{B_j\}_{0\le j\le e}$内のいくつかの行列の和で書くことができるとき$\{A_i\}_{0\le i\le d}$を$\{B_j\}_{0\le j\le e}$のfusion schemeという。逆に$\{B_j\}_{0\le j\le e}$を$\{A_i\}_{0\le i\le d}$のfission schemeという。

$\{A_i\}$を$\{B_j\}$のfusion schemeとするとき、厳密には$\{A_i\}$と同型なAS(左右から置換行列Pを施して行，列の成分を入れ替えたもの$\{P^tA_iP\}$)もfusionと定義することができる。しかし本報告でのfusion, fissionは定義3のように狭義の概念のみを指すとする。

互いにfusion, fissionの関係にあるASの例を紹介する。ASを表示する際に簡略化のためRelation matrixという表示形式を用いることが多い。AS $\{A_i\}_{0\le i\le d}$のRelation matrix $\mathcal{R}(\{A_i\})$を$\sum_{k=0}^{d} kA_k$と定義する。

例 4

$$\mathcal{R}(\{A_i\}_{0\le i\le 5}) = \begin{bmatrix} 0&1&2&3&4&5\\ 5&0&1&2&3&4\\ 4&5&0&1&2&3\\ 3&4&5&0&1&2\\ 2&3&4&5&0&1\\ 1&2&3&4&5&0 \end{bmatrix}$$

$$\mathcal{R}(\{B_j\}_{0\le j\le 3}) = \begin{bmatrix} 0&1&2&3&1&2\\ 2&0&1&2&3&1\\ 1&2&0&1&2&3\\ 3&1&2&0&1&2\\ 2&3&1&2&0&1\\ 1&2&3&1&2&0 \end{bmatrix}$$

$$\mathcal{R}(\{C_k\}_{0\le k\le 2}) = \begin{bmatrix} 0&1&1&2&1&1\\ 1&0&1&1&2&1\\ 1&1&0&1&1&2\\ 2&1&1&0&1&1\\ 1&2&1&1&0&1\\ 1&1&2&1&1&0 \end{bmatrix}$$

$\{B_j\}$は$\{A_i\}$の*fusion scheme*であり、$\{C_k\}$は$\{B_j\}$の*fusion scheme*である。もちろん$\{C_k\}$は$\{A_i\}$の*fusion scheme*でもある。

補題5は*AS*が与えられたとき、その*AS*の*fusion scheme*を構成する際にとても有用である。

補題 5 $\{A_i\}_{0\le i\le d}$を非対称かつ可換なASとする。ここで$\{A_i\}$内で対称でない(i.e. $A_i \neq A_i^t$)行列をsymmetrizeする(i.e. $B_j = A_i + A_i^t$として対称行列を作る)ことで新しい行列の集合$\{B_j\}_{0\le j\le e}$を構成する。このとき、$\{B_j\}$はASとなり$\{A_i\}$の(symmetric) fusion schemeになる。

例4では$\{B_j\}$から$\{C_k\}$を補題5を用いて構成している。また$\{A_i\}$からは

$$\begin{bmatrix} 0&1&2&3&2&1\\ 1&0&1&2&3&2\\ 2&1&0&1&2&3\\ 3&2&1&0&1&2\\ 2&3&2&1&0&1\\ 1&2&3&2&1&0 \end{bmatrix}$$

をRelation matrixとして持つ$\{D_l\}$が構成できる。

このように、非対称かつ可換なASについてはfusion schemeを見い出すことは容易である。しかし逆に対称なASからfission schemeを見つけることは困難になる。詳細は3.3節で触れる。

3 ゼロ知識対話証明

ZKIPは証明者(Prover)と検証者(Verifier)間の質疑応答型(Challenge/Response)のプロトコルで

ある。検証者の確率的振る舞いをする質問に対し、証明者が返答するといった双方向の対話を繰り返し、証明が正しいことを検証者に納得させることができる。それに加え、双方のやりとり間では証明が正しいこと以外一切情報を漏らさない。

この章では「グラフの同型を証明するプロトコル」(3.1節) をベースに、AS を用いる方式を提案する。

3.1 グラフの同型を証明するZKIP

古典的な例としてグラフ理論に基づく ZKIP を紹介する [4][5][6]。$G_1 = (V, E_1), G_2 = (V, E_2)$ を n 頂点のグラフとする。辺の関係を不変にするような G_1 の頂点集合から G_2 の頂点集合への全単射写像 π が存在 ($i.e\ G_2 = \pi(G_1)$) するとき、G_1 と G_2 が同型であるという。「同型」を行列の言葉に置き換えて考えることもできる。グラフ G_1, G_2 の隣接行列をそれぞれ A_1, A_2 とするとき、G_1 と G_2 が同型であることは $A_2 = P^t A_1 P$ となるような置換行列 P が存在することである。

RSA 等で安全性を保証しているのは、十分大きな数の因数分解は難しいという事実である。これと同様に、十分大きな頂点数の 2 つのグラフの同型を判定することは困難であることが知られている。この詳細は 3.3節で触れる。

次がグラフ同型問題に基づく ZKIP である。

【入力】グラフ G_1, G_2 の隣接行列の対 (A_1, A_2)
【証明すること】$\mathcal{P}$(証明者) は、G_1 と G_2 が同型であること (i.e $A_2 = P^t A_1 P$ となるような置換行列 P が存在) を $\mathcal{V}$(検証者) に証明する。
Step 1: $\mathcal{P}$はランダムな置換行列 Q を生成し、G_2 と同型なグラフの隣接行列 $H = Q^t A_2 Q$ を $\mathcal{V}$に送る。
Step 2: $\mathcal{V}$は $b \in \{1, 2\}$ を二者択一的にランダムに選び、b を$\mathcal{P}$に送る。
Step 3: $\mathcal{P}$は置換行列 R を$\mathcal{V}$に送る。

$$R := \begin{cases} PQ & \text{if } b = 1 \\ Q & \text{if } b = 2 \end{cases}$$

Step 4: $\mathcal{V}$は $H = R^t A_b R$ かどうか検証する。不合格ならば停止する。
以上のStepを k回繰り返して、すべてのラウンドで検証に合格すれば、受理する。

このプロトコルの完全性 (証明が正しければ、$\mathcal{V}$は1または圧倒的確率で受理すること)、健全性 (証明が誤っていれば、$\mathcal{V}$は圧倒的確率で棄却すること) は明らかである。

このプロトコルがゼロ知識性 (証明が正しければ、証明の正しさ以外の情報は一切漏れないこと) を満たしている理由は、$\mathcal{V}$が与えられた2つのグラフが同型であることに納得したとしても、$\mathcal{V}$が2つのグラフを入れ替える置換行列 P を見つけるためのどんな「知識」も得ることができない (ランダムな置換行列が施された行列 R しかわからない) からである。

つまり、偽の証明者が検証者を騙し続けることのできる確率は $1/2^k$である。繰り返す回数 kは、どのくらいの安全性を要求するかという検証者のポリシーによって決めればよい。

3.2 ASを用いたZKIP

3.1節で紹介したグラフ同型問題に基づく ZKIP をベースに、次のような AS を用いる方式を提案する。

【入力】対称な AS $\{A_i\}_{0 \le i \le d}$ と行列 $D^t D$
【証明すること】$\mathcal{P}$(証明者) は、$\{A_i\}_{0 \le i \le d}$ の非対称かつ可換な fission scheme を知っていること (i.e fission scheme 内の非対称な行列 D を知っていること) を $\mathcal{V}$(検証者) に証明する。
Step 1: $\mathcal{V}$は $i \in \{1, \ldots, d\}$ をランダムに選び、i を$\mathcal{P}$に送る。以下、K_i を次のように定める。

$$\underline{K_1 = A_i},\ \underline{K_2 = D^t A_i D (= D^t D A_i)}$$

Step 2: $\mathcal{P}$はランダムな置換行列 Q を生成し、K_2と同型な行列 $H = Q^t K_2 Q$ を$\mathcal{V}$に送る。
Step 3: $\mathcal{V}$は $b \in \{1, 2\}$ を二者択一的にランダムに選び、b を$\mathcal{P}$に送る。
Step 4: $\mathcal{P}$は置換行列 R を$\mathcal{V}$に送る。

$$R := \begin{cases} DQ & \text{if } b = 1 \\ Q & \text{if } b = 2 \end{cases}$$

Step 5: $\mathcal{V}$は $H = R^t K_b R$ かどうか検証する。不合格ならば停止する。
以上のStepを k回繰り返して、すべてのラウンドで検証に合格すれば、受理する。

各 i に対して行列の対 $(A_i, D^t A_i D)$ を公開して、行列 D を秘密情報としていると考えれば、グラフ

同型問題に基づくZKIPと対比してとらえることができるであろう。大きく異なるのは秘密情報として置換行列 P の代わりにバイナリ行列 D を扱う点である。

D を秘密にする際に行列の対 (A_i, D^tA_iD) を公開する主な理由は次の点にある。D^tAD は対称行列 $((D^tAD)^t = D^tA^t(D^t)^t = D^tAD)$ であるから AS $\{A_i\}_{0\leq i\leq d}$ の線形結合で書けるため、送信情報量を大幅に減らすことができる。行列そのものを送る代わりに係数だけを送信すればよいからである。

グラフ同型問題に基づくZKIPと同様に、このプロトコルが完全性，健全性，ゼロ知識性を満たしていることは明らかである。

3.3 計算量的側面

この節では、3.2節で提案したZKIPの安全性について検討する。3.1節で紹介したグラフ同型問題に基づくZKIPの安全性を保証する数学的事実は、十分大きな頂点数の2つのグラフの同型を判定することは困難であることであった。グラフの同型性判定の問題はクラスNPに属しているが、クラスPに属する問題かどうかについては知られていない。すなわち入力サイズの多項式時間で解くことのできるアルゴリズムが存在するかどうかは未解決である。

同様に行列の対 (A, D^tAD) が与えられたときバイナリ行列 D を求める問題を考える。

この問題がクラスNPに属していることは明らかである。一方、しらみつぶしに D になり得る行列の候補を数え上げると $({}_{2d}C_d)^n$ (ただし n は行列のサイズ、d はバイナリ行列 D の valency (各行，各列の1の個数)) になる。D の満たすべき条件から実際にはもっと少ない候補数にはなるが、多項式ステップで解けるアルゴリズムには程遠い。グラフの同型性判定問題と同様、入力サイズの多項式時間で解くことのできるアルゴリズムが存在するかどうかは未解決である。

補足であるが、バイナリ行列 D として valency が1 (i.e. 各行，各列の1の個数が1) の行列 (= 置換行列) は扱うことができない。なぜなら $D^tD = I$ を満たすことから、すべての D^tA_iD が A_i と一致してしまうからである。

4 ASを用いたZKIPの応用例

一般にZKIPは、相手認証（個人認証）を可能にする。この章では、3.2節で提案したZKIPを用いた他の応用例とその可能性について検討する。

4.1 ディジタル署名

ディジタル署名は、電子データがある能力を持つ者によって正しく生成されたということを確認するための手段である。現在広く使用されている署名方式にはRSA署名があるが、公開鍵暗号方式を用いるため処理に時間がかかる。

それに比べ、ZKIPを応用したFiat-Shamir方式[3]はRSA署名に比べ非常に効率的であることが知られている。

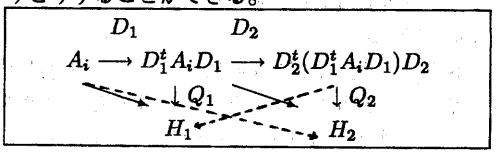
同様にしてASを用いたZKIPを用いてディジタル署名することができる。署名の仕組みは対話的でないが、MD5等の一方向ハッシュ関数を検証者の代わりに用いることで署名を可能にする。しかし、この方式はFiat-Shamir方式に比べ署名部分の情報量が多くなる欠点がある。

4.2 秘密分散法

ASを用いたZKIPの最大の特徴は、秘密分散が可能な点である。秘密分散法とは、ある秘密情報を複数に分割しておき、分割したままで元の秘密を復元できるという方式である。ASを用いてこれを次のように実現する。

非対称かつ可換な AS $\{B_j\}_{0\leq j\leq e}$ を生成し、$\{B_j\}$ 内の m 個の異なる非対称行列の組を $\{D_1, D_2, \ldots, D_m\}$ $(D_i \neq D_j^t \ if \ i \neq j)$ と列挙する。そしてこれらを一つずつ m 人に分配しておく。また、補題5を用いて構成した $\{B_j\}_{0\leq j\leq e}$ の fusion scheme $\{A_i\}_{0\leq i\leq d}$ を共通の公開情報としておく。

ここで、秘密 D_1 を持っている人と秘密 D_2 を持っている人の2人が協力することにより、$(A_i, (D_1D_2)^tA_iD_1D_2)$ を公開してあたかも D_1D_2 を知っている1人のように振る舞って検証者とやりとりすることができる。



前ページの図の実線の部分は個人のみで証明できるが、点線の部分は2人が協力して証明する必要がある。例えば、検証者が A_i から H_2 への写像を要求した場合には、D_1 と D_2 が必要となるため、2人が協力しないと証明できない。

プロトコルの詳細については触れていないが、これが多人数の場合にも同様にも適用できる。

4.3 実装の方法案

これまで非対称かつ可換な AS の存在を仮定してきたが、実は補題6のようにして構成できる[1]。

補題 6 $\Omega = \{1, \ldots, n\}$, S_nをΩ上の対称群とする。群 G として S_n の部分群で Ω 上可移に作用するものとする。ここで、群 G を $\Omega \times \Omega$ に作用させたときの共役類を$\Lambda_0, \Lambda_1, \ldots, \Lambda_d$ とする。このとき $(\Omega, \{\Lambda_i\}_{0 \leq i \leq d})$ は AS となる。

詳細については触れないが、実装する際には有用な補題であろう。また Hamming scheme や Johnson scheme から fission scheme といった古典的な AS からも構成することができる[8]。

5 今後の課題

本報告では、グラフ同型問題に基づく ZKIP をベースに、AS を用いる ZKIP を提案した。そしてこの ZKIP は相手認証やディジタル署名だけでなく、秘密分散が可能な方式であることを述べた。

しかし、このプロコトルの安全性は理論的にしか考察していない。そこで、GAP(Groups, Algorithms and Programming)[7] による実装を試み、このプロトコルがどのくらいの強度を持ち、行列のサイズとしてどの位大きくすれば (現段階で) 十分安全とみなすことができるのか検討したいと考えている。その結果次第で、実用可能かどうか判断できるであろう。

また、このプロトコルを拡張して次の2つが実現できるか検討したい。一つは、文書の内容を秘密にしつつ署名をつけるブラインド署名である。ブラインド署名は、電子投票などへの応用が期待される技術である。

もう一つは、公開鍵暗号方式のように「署名」だけでなく、文書の「暗号化」が可能かどうかである。AS は符号理論と深く関連があり、また符号化と暗号化は同一視できる点からも研究の余地があると考えられる。

参考文献

[1] E. Bannai and T. Ito, Algebraic Combinatorics I : Association schemes, Benjamin/Cummings, Menlo Park, California, 1984.

[2] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, The knowledge complexity of interactive proof systems, Proc. of STOC, 291-304, 1985, SIAM J. on Computing, 18(1) 186-208, 1989.

[3] Feige, U., Fiat, A., and Shamir, A., Zero-knowledge proofs of identity, Proceeding of the ACM Symp. on the Theory of Computing, Acm Press, New York, 210-217, 1987.

[4] 藤原良、神保雅一：符号と暗号の数理, 共立出版, 1993.

[5] D.Stinson、櫻井幸一監訳：暗号理論の基礎, 共立出版, 1996.

[6] 岡本龍明、山本博資：現代暗号, 産業図書, 1997.

[7] http://www-math.math.rwth-aachen.de /gap/index.html

[8] Y.Suga, On the fission association schemes of the Johnson and Hamming schemes, master's thesis, Graduate School of Mathematics, Kyushu Univ., 1997