バイト列を公開鍵にもつ認証方式

Lema Savaktani †
E-mail: †vu37e5@bma.biglobe.ne.jp

あらまし 巡回セールスマン問題では経路の距離の総和の最小値が問題であったが､経路の距離の総和が一定値になるように変形した問題を用いてゼロ知識証明を提案する。この文章では、経路と置換群を決定することが同じであることを示した後、有向グラフ上での巡回セールスマン問題の変形を考え、バイト列を用いた認証方式の提案を行う。

キーワード 認証，巡回セールスマン問題，ゼロ知識証明。

Keyword authentication，TSP，zero-knowledge

概要

０．動機

WEB で認証を行う場合、多くはパスワード方式が用いられる｡然しこの方法はそれほど安全とはいえない。より暗号学的な強度の安全性を得るために、公開鍵暗号を用いたゼロ知識証明を導入したい。しかし、CGI で使われるスクリプト言語では従来方式にある巨大素数を扱うことはそのままでは出来ない。そこで、誤り訂正符号など小さな値の集まりを計算させる問題に帰着させる公開鍵暗号系を使うのが望ましい。ここで誤り訂正符号の公開鍵が大きいことが、実装上のデメリットである。より効率的な認証を行うために、新しい方式を考えなければならない。G を任意のｎ個の頂点を持つグラフの外周とする。新しい認証方式の安全性は、各頂点の差分の総和を a とし、各頂点に対して置換πを作用させた結果新しく得られた差分の総和を a’とする。この時、認証の安全性は a’から置換πを求める問題の困難性に基づいている。

１．TSP の変形

巡回セールスマン問題とは与えられた都市全てを通る最短の経路を求める問題である。計算機による数値実験では､異なる経路で同じ値を取る場合が存在し、距離の総和が最小値なのか極小値なのかを識別することは難しい。今２都市間の全ての経路を辺とするｎ個の頂点をもつ完全グラフを考えると、全ての頂点を一度だけ通る経路は閉路を構成する。この時巡回セールスマン問題は探索問題になる。巡回セールスマン問題における、二点間の距離の定義を少し変える。頂点に数字を割り当て､各頂点同士の差分を距離と定義して、全ての点を通る最小な距離の経路を求める問題に変形する。今巡回セールスマン問題で、最小の距離を求めるのではなく、特定の距離になる経路を決定する問題に置き換えることを考える。すると統計的な分布の偏りにより、同じ距離になる経路が複数存在する。この時、経路は各頂点間の差分の和に等しいので、経路の違いは頂点を並べ替える置換群に等しくなる。ランダムに異なる自然数を割り当てた頂点の初期状態から、ある置換群を作用させた状態をｓと置き、その時の差分の和を a と置く。更に、置換πを繰り返し作用させたときの距離 a_i を差分和の系列と呼ぶ。以下では単に系列と呼ぶ。ここで系列とは同じ置換を繰り返し作用させて出来た差分の構成列を言う。

巡回セールスマン問題を次のように変形する。

有限体上の元を頂点に持ち、各頂点間の差分を辺の重みとする重み付完全グラフを考える。この時、外周は閉路である。ランダムな置換を取って頂点を置き換えると、可能な全ての頂点間の差分全てと経路が表現できる。つまりこの場合、閉路として外周のみを考えることができる。外周の向きに関わらず（加法和は対称なので)､頂点の並び方が閉路を構成するために必要な順序を与える。探索問題とした方が系列の順序を効率よく求められるが、TSP はこのように外周を考えたときの頂点間に生じる差分の和が最小になる置換群を求める問題と考えられる。よって以下のような認証系が考えられる。

有限体上定義された重み付完全グラフの頂点間の差分の総和がある値になるような順序を求めることとする。今異なる経路をたどって総和が同じ値になる場合を考える。初期状態を与えておき、この二つに置き換わる置換群をそれぞれπ、π’と置くと、各置換のべき乗によって新たに生じる置換と距離の総和には以下のような関係がみられる。全ての置換のべき乗は有限巡回群になるので、総和の値もある周期をもって変化する。ある置換のべき乗がそれまでの総和と一致するときは、ある時点で置換を作用させた時の頂点の並び方が等しいか、差分の要素の構成が等しくなる時であ

る。頂点の重みを十分にランダムにとれば、グラフの対称性は取り除けるので繰り返し置換により差分の構成が等しくなる確率は無視できる。従って十分多くの要素から頂点の重みを選べば、系列が同じになる確率は無視できる。置換のべき乗によって生じる系列は個々の置換特有のものになるだろうか？全ての差分が異なるので構成が同じになる場合は選び方が同じの時か平文が置換によって移った先が等しくなる時のみである。グラフが非対称で、このグラフに作用させる置換群の位数が十分な大きさであれば、系列は置換により固有であり､系列が等しい時､二つの置換は等しい。計算機による実験では差分の排他的論理和を系列としたときには、置換に対する固有の値にはなり得ない。というのも、差分の構成が異なっていても排他的論理和の場合は異なる値の和が同じ値になりうるからである。更に、系列を差分の加法和に取ると固有の値になった。これは差分の構成が異なるとき、その和も異なる値を取るからである。異なる置換の系列が一致する場合は存在しないのか、それとも見つけるのが難しいだけだろうか？同じ系列を生成する置換は存在しない。今問題にしているのは頂点間の距離が同じものを含まないグラフである。同じ系列を生成する置換が存在すれば任意の二つの経路は等しくなる場合がある。これは同じ経路を持たないという仮定に矛盾する。よって経路は置換に固有である。ここに系列を使って順序を識別する認証方法が構成可能となる。このとき、系列からは置換の具体的操作に関する情報が消えていることが望ましい。すなわち公開されている系列の部分情報からは、元の置換が復元できないか非常に難しくなければならない。

２．最小差分和問題の困難性

向きのないグラフを考えた場合、頂点間の差分は加法和に取ることができる。この場合頂点数ｎの場合並べ替えのパターンは n!となる。ｎ個の値をランダムにｎ個の頂点に割り当てた場合取り得る差分の値はｎ(n+1)/2 個である。従って十分な数の頂点を用意し、十分ランダムに置換群を取れば、全ての結果が重複する確率は限りなく小さくできる。例えばｎ＝６４の時、各頂点の持つ確率は 1.54 である。12 回連続して置き換えた結果が重複する可能性は無視できる。一方、系列から置換を求める問題は困難だろうか？総和の系列からは順序に関する情報をどのように記述できるだろうか？順序に関する情報は差分の構成に含まれる。つまり総和と差分の構成が一対一に結び付けられていれば解析できる。しかし加法和の場合多くの異なる置換が異なる値を持ちうる。全ての系列に対して置換と構成が紐づけられていればいいが、頂点の重みをランダムに取った時、対応はランダムになるのですべてを記憶しなければならない。これは置換の総当たりをするのと同じである。系列から置換を決定するような多項式時間アルゴリズムは存在するだろうか？

３．認証

鍵生成

１．バイト列ｂ、バイト列間の差分βの和 a、秘密の置換πをとる。

2. π（ｂ）＝B を計算する。

3.（B、a）を公開する。

１．送信者はランダムに置換Πを取って、Π（B）＝B'を計算し、その差分の和Σβ'=αを計算して受信者にαを送る。

２．受信者はランダムに 0 か 1 を送信する。

３．

もし０なら、送信者はランダム置換Πを送信する。

もし１なら、送信者は（B’+b）を送信する。受信者はΣ（β’+β）＝（α+a）であることを検証する。

４．考察

最小差分和問題を使ったゼロ知識証明を考えた。この問題は次のように一般化できる。ある値 A を決めたとき、有限体上の元を決まった数だけ並べてやり、隣り合った要素ごとの差分の和がある値 A になるような置換Πは存在するか？という問題である。これを定数差分和問題と呼ぼう。置換をランダムに取ると、差分の和が a に一致する確率は無視できないほど多い。これは差分和の絶対値が置換群の位数に対して相対的に小さいためで、固有な置換を決定しているわけではない。この状況は認証にとって良くない。バイト列に対する置換を追加して改善できる。置換の累乗を計算し、それぞれの置換について差分和を計算しそれを公開する。送信者は置換に対する証拠を増やすだけでよい。定義から、最小差分和問題は距離の定義を少し変えた場合の巡回セールスマン問題であることがわかる。拘束条件である距離の最小和をある特定の距離に変えた場合、定量的な決定問題は探索問題に置き換わる。しかし今此処で問題なのは、距離よりも経路の一意性である。特定の距離になる経路は他にもあるかもしれないが、ある都市の巡回経路から置換群を作用させた数ある経路の中から、特定の経路を一意に決定する困難さは巡回セールスマン問題の変形である。経路を表すために置換群が用いられ、それは秘密鍵に相当する。逆順は同じ結果を出すので、向きの無いグラフ上の巡回セールスマン問題の変形になる。

５．更なる進展

最小差分和問題が巡回セールスマン問題の変形であることを示した。結合文字列を用いた認証方式の安全性が、巡回セールスマン問題の非可換な場合であることを示す。この問題は向き付けのあるグラフ上の巡回セールスマン問題である。

非可換とは、演算の順序を変えたとき結果が異なる性質のことを言う。置換群や行列の積は非可換である。上の文章で２頂点間の順序を示すのに差分を用いたが、今度は２頂点間の積の和を考える事にし、各頂点に２次の正方行列を割り当てる事にする。ここで差分に相当するものは行列の積の和である。経路を示すのに、全ての行列の積の和を考える。この結果得られる行列は順序を変えると変わる。頂点に割り当てられた行列と、特定の経路を選択した場合得られる行列の積の和を公開鍵とする。今経路に相当する置換を秘密鍵とすると、ランダムに選んだ置換を初期状態に作用させた経路を通った場合に出来る行列の積の和を証拠として、対話証明を行うことが出来る。検証者のチャレンジが０の場合、証明者はランダム置換を返す。一方、チャレンジが１の場合、証明者は秘密の経路を通ったときの行列と、予め送信しておいたランダム経路の行列の排他的論理和を送信する。検証者はその結果を、公開情報と予め証明者から送られてきた行列との排他的論理和を計算して一致すれば合格とみなす。

しかしながらこの方法は、公開情報の増大という好ましくない結果をもたらす。結論から言えばこの状況を改善するのに文字列を使うことが出来る。系列の代わりに、行列を異なる文字で置き換え、更に結合してしまえば元に戻すのは組み合わせ論的問題と等しく難しいので、認証に使えて効率も良い。実装が楽なのでこの方式はとても実用的である。

６．今後の課題

置換群を秘密鍵に、文字や行列、そしてバイト列を公開鍵にしたゼロ知識証明を提案した。この方式の安全性は巡回セールスマン問題の困難性に基づいている。巡回セールスマン問題を用いた暗号は構成可能だろうか？鍵交換は出来るだろうか？数論的暗号が万能であるように、このような任意の問題から暗号学的関数を作り出すのは個人的趣味であるが、暗号に関する一般的な事実を見出すためには重要な作業である。

参　考　文　献

[1] Oliver Prezel, Finite fields and Codes, Oxford University Press, London, 1992.

[2] Oblivious Verification of Common String、Claude Cr´epeau and Louis Salvail
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.17.9227