半分配環上の公開鍵暗号とその応用

境理

2023 年某月某日

Abstract

半分配環とは、代数系における加法と乗法の２つの演算のうち、乗法における分配法則が左右いずれかの１つのみに限られているような代数系を指す。楕円曲線と有限体から半直積を使って新たな乗法群を構成し、更にこの代数系に加群の構造を導入して得られた半分配環上で、離散対数問題と元の３分割問題を定義し、その暗号へ応用について述べる。（草稿）

半分配環上の２つの公開鍵暗号とその応用

半直積と加法

a, b, c を素体の元、A, B, C を楕円曲線上の点とする。

半直積

半直積の演算は次のように定義されている。（ここで使うのは外部半直積の定義である。）
$(a, A)(b, B) = (ab, bA + B)$

（日本語の本だと $(a, A)(b, B) = (ab, aB + A)$ という記法をしているようだが、左右反対になるだけで基本は同じ。つまり、$(b, B)(a, A) = (ab, aB + A)$ である。）

また、半直積にはベクトル同士の積がないように加法が定義されていない。
そこで加法を次にように定義する。
$(a, A) + (b, B) = (a + b, A + B)$
普通に直和です。 以下ではこのような代数系が環であるかどうか確かめる。

環の条件

１）加法に関して結合律を満たす。

結合律

$((a, A) + (b, B)) + (c, C) = (a + b, A + B) + (c, C) = (a + b + c, A + B + C)$
$(a, A) + ((b, B) + (c, C)) = (a, A) + (b + c, B + C) = (a + b + c, A + B + C)$
よって成り立つ。

零元の存在

$(a, A) + (0, O) = (0, O) + (a, A) = (a, A)$
よって存在する。

逆元の存在

$-(a, A) = (-a, -A) + (a, A) = (a, A) + (-a, -A) = (0, O)$
となり、存在する。

可換律

$(a, A) + (b, B) = (b, B) + (a, A) = (a + b, A + B)$
よって成り立つ。

全て成り立つので、この演算は加法群である。

以下、環の条件を確かめる。

２）結合則を満足する

$(a, A)(b, B)(c, C) = (ab, bA+B)(c, C) = (abc, c(bA+B)+C) = (abc, bcA+cB+C)$
$(a, A)(bc, cB + C) = (abc, bcA + cB + C)$

よって満足する。

３）乗法単位 e が存在する

単位元 $e = (1, 0)$ とすると、$(a, A)(1, 0) = (a, A + 0), (1, 0)(a, A) = (a, 0 + A)$ となるので、e は乗法単位元である。

４）分配律を満足する

$(a, A)((b, B) + (c, C)) = (a, A)(b + c, B + C) = (ab + ac, (b + c)A + B + C)$
$((a, A)(b, B) + (a, A)(c, C)) = (ab, bA + B) + (ac, cA + C) = (ab + ac, (b + c)A + B + C)$

から積を計算するのと、積を計算してから足した結果が一致するので、左分配法則が成り立つ。

$((a, A) + (b, B))(c, C) = (a + b, A + B)(c, C) = (c(a + b), c(A + B) + C) = (ac + bc, c(A + B) + C) \neq$
$((a, A)(c, C)+(b, B)(c, C)) = (ac, cA+C)+(bc, cB+C) = (ac+bc, c(A+B)+2C)$

なので右分配法則が成り立たない数学からの物体 X。積が特殊だからかも。
つまり環ではない！

半群

半群とは、１つの演算に対して結合法則を満たす代数系である。

半分配環

更に、積に対して半群を成し、かつ加法に関して群を成す代数系であり、分配法則が左右のどちらか 1 つだけ成り立つ代数系を半分配環と言う。

しかし今、この代数系は 0 でない全ての元に逆元が存在する。
その場合を、以下で定義する。

半分配体（逆元の存在）

０以外の全ての元に対して逆元が存在する場合、半分配環の一部としてこの代数系を半分配体という
$(a, A)^{-1} = (a^{-1}, -a^{-1}A)$ なので、$(a, A)(a^{-1}, -a^{-1}A) = (1, O)$
単位元は $(1, O)$ となる。

結論

・半直積に加法を導入すると半分配環になった。
・なぜかヒル暗号に使われている。何故秘密鍵暗号なのか？？？

半直積に楕円曲線を使って、それに加法群を導入したら左分配法則しか満たさない半分配環になったというお話。
それでもきちんと動いているのは分配則を使ってないから。

結合則だけを使う分には問題なし。

半分配環と公開鍵暗号

半分配環は半分配体を含む、より大きな代数系である。この代数系にある 1 つの元を 3 つの元に分割する問題を定義して、公開鍵暗号を構成する。

目的

最初、群の問題に基づく暗号を作るうえで可換群は研究しつくされて、もうこれ以上新しい問題は出てこないと思ったので非可換群に焦点を絞った。しかし自分が知っている範囲で非可換群は少なくて、大抵、行列に還元されてしまうものであった。そこで Ushakov らの研究の中で半直積というものがあると知り、詳しく調べてみると 2 つの群を組み合わせて新しい群を作る方法だと分かった。しかも半直積は非可換だ。

というわけで半直積の材料に有限体と楕円曲線の群を組み合わせて作った代数系が今までのプラットフォームだった。まだ物足りない、何かできないだろうか？そこで新たに加法群の構造を取り入れて、その代数系は環の性質を満たすだろうか、と思い付きで試したところ分配法則が成り立たないことがわかった。

さあ、これはおかしいおかしいと分配法則が成り立たない代数系の例を調べてみたら奇跡的に半分配環の記事を見つけて、そこでようやくこの**数学からの物体 X の正体は半分配体だ**とわかったというわけです。

この先ペアリング写像なども取り入れて、新型を強化していきたいと思います。

これはどちらの材料も加法に関して群になっていたからできたというだけで、例えば置換群だと成り立ちません。しかしまだ多項式という選択肢があります。例えば有限体上定義された１変数多項式 f と有限体の元 x とのペアを考えます。$(f,x_0)(g,x_1) = (fg, g(x_0)+x_1)$ であり、更に加法＋を次のように定義する。$(f,x_0)+(g,x_1) = (f+g, x_0+x_1)$

これはこれで全く問題がないように見えます。これに関する記事は後日追加します。

準備

半直積の基本演算を定義すると、

$(c,s)(d,t) = (cd, sd+t)$：積
$(c,s)^{-1} = (c^{-1}, -sc^{-1})$：逆元
$(c,s)^{-1}(d,t)(c,s) = (d, s(e-d)+tc)$：共役元
$(c,s)^n = (c^n, c^{n-1}s + c^{n-2}s + ... + cs + s)$：べき乗公式

ここで n 項等比数列の総和が $S_n = \frac{(c^n-1)}{c-1}$ から、

$(c,s)^n = (c^n, \frac{c^{n-1}-1}{c-1}s)$
$(c,s)^{nm} = (c^n, \frac{c^{n-1}-1}{c-1}s)^m = (c^n, s')^m = (c^{nm}, \frac{c^{m-1}-1}{c-1}s')$
$(c,s)^{m+n} = (c^{m+n}, c^m\frac{c^{n-1}-1}{c-1}s + \frac{c^{m-1}-1}{c-1}s)$

半分配環と半分配体

半分配環とは、代数系における加法と乗法の２つの演算のうち、乗法における分配法則が左右いずれかの１つのみに限られているような代数系を指す。
半分配環の性質に、逆元の存在を付け合せたものが半分配体である。
楕円曲線と有限体から半直積を使って新たな乗法群を構成し、更にこの代数系に加群の構造を導入して得られた半分配体上で、離散対数問題と元の３分割問題を定義し、その暗号へ応用について述べる。

例１

定義：原始根
「p は素数であるとする。巡回群 Z_p^* の生成元 g は Z_p^* の原始根 (primitive root) または modulo p　の原始根と呼ばれる。」

秘密鍵：$s,t,u,x,y,z \in Z_p, B \in E, s > u, x > z$
公開鍵：$A,C,D,E \in E, D = A^sB^tC^u, E = A^xB^yC^z$
$p,q,r \in Z_p$ の異なる原始根。
$P,Q,R \in E$　は同じ楕円曲線上の異なる位数の点。
つまり、$A=(p,P), B=(q,Q), C=(r,R)$ である。

・ある数 g が原始根かどうかを確かめる方法
定義体がソフィー・ジェルマン素数であれば、$P-1 = 2*Q$(Q は素数) と表せる

ので、次の条件を満たすかどうかで原始根かどうか判定することができる。

判定法：ある整数 x が原始根であるとき、
$x^{(P-1)/2} \bmod P \neq 1$
かつ、
$x^2 \bmod P \neq 1$
これが安全素数に対する原始根の判定条件になります。

例えば、定義体
$P = 115792089237316195423570985008687919879869678752368678225506334468897341715723$
$p = 2, q = 4, r = 6$ の場合を考えると、4 は原始根ではなく、$2, 6$ は原始根である。

暗号１

ケーリーハミルトン攻撃を考慮した行列暗号のつもり。←これを半直積に置き換える。

秘密鍵:
整数 a, b, c, d
ただし、 $a \neq b$
素体の元と素体上で定義された楕円曲線上の点との半直積 A
公開鍵:
上と同じ半直積の元、
X,
$Y = X^a A^c X^{-a}$,
$Z = X^b A^{cd} X^{-b}$,
暗号化:
M: 平文、 r,s: 乱数
$C1 = X^r Y^s X^{-r}$
$C2 = X^r Z^s X^{-r}$
暗号文 (C1, C2 * M)

復号: $C1 = X^{(r+a)} A^{sc} X^{-(r+a)}$
$C2 = X^{(r+b)} A^{scd} X^{-(r+b)}$
より、
$C2 = X^{(b-a)} C1^d X^{-(b-a)}$
C2*M に、上で求めた C2 の逆元を掛けて M を得る。

暗号２：半分配体上の離散対数問題（乗法に関する）

秘密鍵：$s, t, u, x, y, z \in Z_p, B \in E, s > u, x > z$
公開鍵：$A, C, D, E \in E, D = A^s B^t C^u, E = A^x B^y C^z$
$p, q, r \in Z_p$ の異なる原始元。
$P, Q, R \in E$　は同じ楕円曲線上の異なる位数の点。
つまり、半直積に使う元、A, B, C は、それぞれ有限体の元 p, q, r と楕円曲線の異なる点 P, Q, R とを任意に取り、
$A = (p, P), B = (q, Q), C = (r, R)$
である。

定義：原始根
「p は素数であるとする。巡回群 Z_p^* の生成元 g は Z_p^* の原始根 (primitive root) または modulo p　の原始根と呼ばれる。」

秘密鍵：$s,t,u,x,y,z \in Z_p, B \in E, s > u, x > z$
公開鍵：$A,C,D,E \in E, D = A^s B^t C^u, E = A^x B^y C^z$
$p,q,r \in Z_p$ の異なる原始根。
$P,Q,R \in E$　は同じ楕円曲線上の異なる位数の点。
つまり、$A = (p,P), B = (q,Q), C = (r,R)$ である。

・ある数 g が原始根かどうかを確かめる方法
定義体がソフィー・ジェルマン素数であれば、$P-1 = 2*Q(Q$ は素数) と表せるので、次の条件を満たすかどうかで原始根かどうか判定することができる。

$D' = (p,P)^s(q,Q)^t(r,R)^u = (p^s q^t r^u, q^t r^u \frac{p^{s-1}-1}{p-1}P + r^u Q + \frac{r^{u-1}-1}{r-1}R)$
$E' = (p,P)^x(q,Q)^y(r,R)^z = (p^x q^y r^z, q^y r^z \frac{p^{x-1}-1}{p-1}P + r^z Q + \frac{r^{z-1}-1}{r-1}R)$

この半直積の左側成分は通常の多元離散対数問題であり、右側は楕円曲線の多元離散対数問題である。
２つの異なる原始根を使った離散対数問題は、「多元離散対数問題（Multiple Discrete Logarithm Problem）」と呼ばれます。これは、異なる原始根に対する離散対数を求める問題です。

暗号文：
$C1 = A^r DC^{r'} = A^{(s+r)} BC^{(u+r')}$
$C2 = A^r EC^{r'} = A^{(x+r)} BC^{(z+r')}$

復号
アリスは $s-x, u-z$ を知っているので以下を計算できる。
$X = A^{(s-x)} C2C^{(u-z)} = A^{(x+r)} BC^{(y+r')} = C1$

暗号化に関する指数にはなんの制約もないので、むしろこっちの設定のほうが自然だと思います。秘密鍵が増えるということ以外、特に問題はなさそうです。

この暗号は一見して難しそうに見えます。
というのも右要素も左要素も構造が複雑だからです。
2 つ以上の原始根、それも 2 つ以上の秘密指数がある場合には、互いに混ざり合ってしまうので、単純には計算できません。これはもう少し論文を理解する必要があるので簡単には言い切れないですが、解読ができてもできなくても、ここで公開する予定です。
原始根 q は秘密鍵であり、更に両側の原始根を秘密指数でべき乗しているので簡単には指数を計算できません。ただ、p,r は小さなサイズの原始根、q は大きなサイズの原始根であるとします。
ただ左半分は、右の楕円曲線を計算するためのものであって、楕円曲線の 521bit 以上の大きさにはなりません。そして見たことのない 3 つの原始根の離散対数問題になっています。
これが解ければ楕円半直積の離散指数も分かるということなので、この暗号の安全性は半直積の離散対数問題にある可能性が濃くなります。
素数 p,q,r がそれぞれ異なる原始根であることから、簡単な指数関数としてみる

こともできません。
同じような方式がないか調べる必要があります。（それが今日多元離散対数問題であるということが解った）

暗号文解析：

$X = A^{(x-z)}C2C^{(y-w)} = A^{(x+r)}BC^{(y+r')} = (p^{x+r'}qr^{y+r'}, qr^{y+r'}\frac{p^{x+r'}-1}{p-1}P + r^{y+r'}Q + \frac{r^{y+r'}-1}{r-1}R)$

暗号文は最終的にこの形に収まります。
この暗号の計算には、楕円曲線の点の素数位数 n を使います。
行列の場合、未知変数が 2 つだったから解読できただけで 4 つにしたら安全だったのかもしれません。
暗号化に使う点のスカラー倍は半直積のべき乗で等比級数の総和で決まりますが、これは半直席の特徴です。
この点のスカラー倍は、秘密指数が分からなければ決定できないので、ここはやはり半直積の離散対数に依存していると言えるような気がします。
暗号文から秘密鍵や平文の情報が漏れているようには見えません。
行列じゃないからケーリーハミルトンも使えないし、総合してみると、A, C を公開しても全く問題がなさそうなので、早速実装してみました。

(y, P, g_i) が公開パラメータとして、素数 P、互いに素な i 個の原始元 g_i、i 個の秘密指数 x_i があった時、

$$y = \Sigma_{i=0}^{n} g_i^{x_i}$$

(y, P, g_i) から $(x_0, x_1, ..., x_n)$ を求める問題を（加法的）多元離散対数問題：(Additive Multi Discrete Logarithm Problem) と呼ぼう。

ベクトル同士の積が定義されてないように、半直積の和も定義次第でどうにかなりそうな気がするが、どうすれば矛盾なく計算できるのか、或いは左側だけ演算を変えることができるのか、しばらく時間が必要である。
もしこれがうまく行けば、難しい問題になる可能性あり。

暗号３：離散対数問題に加法を定義する

ここで、半直積同士に加法を定義してみる。つまり、
$(p, P) + (q, Q) = (p + q, P + Q)$
$(a, A)^n + (b, B)^m = (a^n + b^m, \frac{a^{n-1}-1}{a-1}A + \frac{b^{m-1}-1}{b-1}B)$
よって、加法に関しては、可換である。
逆元は、$(a, A)^{-1} = (-a, -A)$ である。

定義：多元離散対数問題（加法と乗法に関する）

1st step と同じように材料を定義する。
秘密鍵：$s, t, u, x, y, z \in Z_p, B \in E, s > u, x > z$
公開鍵：$A, C, D, E \in E, D = A^s B^t C^u, E = A^x B^y C^z$

$p, q, r \in Z_p$ の異なる原始元。
$P, Q, R \in E$　は同じ楕円曲線上の異なる位数の点。
つまり、半直積に使う元、A, B, C は、それぞれ有限体の元 p, q, r と楕円曲線の異なる点 P, Q, R とを任意に取り、
$A = (p, P), B = (q, Q), C = (r, R)$
である。

$(c, s)^n = (c^n, \frac{c^{n-1}-1}{c-1}s)$

であるから、公開鍵を D, E とすると、
$D = (p, P)^s + (q, Q)^t + (r, R)^u = (p^s + q^t + r^u, \frac{p^{s-1}-1}{p-1}P + \frac{q^{t-1}-1}{q-1}Q + \frac{r^{u-1}-1}{r-1}R)$
$E = (p, P)^x + (p, P)^s + (q, Q)^t + (r, R)^u + (r, R)^y = (p^x + p^s + q^t + r^u + r^y, (\frac{p^{x-1}-1}{p-1} + \frac{p^{s-1}-1}{p-1})P + \frac{q^{t-1}-1}{q-1}Q + (\frac{q^{y-1}-1}{q-1} + \frac{r^{u-1}-1}{r-1})R)$

暗号文：
$C1 = A^r + D + C^{r'} = A^r + A^s + B^t + C^u + C^{r'}$
$C2 = A^r + E + C^{r'} = A^r + A^x + A^s + B^t + C^{r'} + C^y + C^u$

復号
アリスは x, y を知っているので以下を計算できる。
$X = A^{(x)} + C1 + C^{(y)} = A^s + A^x + A^r + B^t + C^{r'} + C^y + C^u = C2$

問題

$Z = A^s + B^t + C^u$ から
$W = \frac{p^{s-1}-1}{p-1}P + \frac{q^{t-1}-1}{q-1}Q + \frac{r^{u-1}-1}{r-1}R$
を満たすような指数 s, t, u を求めよ。

例：
$1575 = (7^x + 11^y + 13^z) \bmod 2039$
これなら x, y, z はどうなりますか？

ただし、$A = (p, P), B = (q, Q), C = (r, R)$ なる左側要素を素体の元、右側要素を素体上定義された楕円曲線の点であるような半直積とし、B は秘密であるとする。

解読法（以下の記事より既出ですが）

https://qiita.com/fumumue/items/55b61f63a005f290a2c6

今、加法的多元離散対数問題を解読しようとする。
$D = (p, P)^s + (q, Q)^t + (r, R)^u = (p^s + q^t + r^u, \frac{p^{s-1}-1}{p-1}P + \frac{q^{t-1}-1}{q-1}Q + \frac{r^{u-1}-1}{r-1}R)$

このように書けるところから、異なる原始根に対するべき乗の線形結合が線形代数の手法で簡単に破られるかもしれないという潜在的な危険性がある。つまり A, B, C に関するベクトル空間があったときに、D が線形独立であるか従属であるかという問題と、ベクトルとして考えたときにガウスの消去法のような手法を使って簡単に解けるかもしれないという可能性です。まあ、隠すべきは冪指数な

ので係数を求めるような方法では簡単に解けないと思うのですが、それでも例えば $A^s = (p, P)^s = y$ のとき、$log(y) = s(log(A))$ として指数 s を線形代数の手法で解けるかもしれないという危険性です。いくら加法で誤魔化したつもりでも、代数的構造が線形では単純すぎて簡単に解読できるかもしれないということです。しかし今の時点では、A, B, C の個々の値は分かっていても、その真数 y が分からない状態なので、できるかもしれないしできないかもしれない。それは暗号解析に当たって、条件を満たすような暗号文や、選択平文の関係から導き出されるものなので、解読できる可能性が大きいと思います。このように１つの鍵に対する安全性は確立できても、暗号化したデータにはその保証がないというべきでしょう。幸いなのは B が秘密であることです。１つでもわからない値があれば LWE のようなエラーが入った多元１次連立多項式の回を計算する問題にうまく関連付けることができるかもしれない。（この辺り何も理解しないで考えているというのがわかります・・・）

今のところは鍵交換に使っていますが、ここで今後公開鍵暗号方式を設計するときに必要なことは、線形代数に気をつけることと、LWE 問題のような（未知の値はエラーが入って０になったと考えればいいので）別の問題に帰着できるようにすることです。（考察中）

section

20230623

MDLP に関する記述に疑問を持って、半直積に加法を定義してみました。
すると魔法のように難しい問題になって６４ビット整数なら４つ秘密指数を知らないと解けない暗号になりました。
実装はまだです。

section-1

20230620

楕円曲線の半直積でできた多元離散対数問題に基づく公開鍵暗号と分割問題に基づく暗号（いずれもオリジナル）を実装しました。
名前は、「離散対数とハードボイルドワンダーランド」に決めましたw
ec.cpp の ehw 関数がそれです。
この方式は勢いと思いつきで作ったのですが、幸運なことに量子計算機で解読する方法がまだ見つかっていないそうです。

新型暗号はもう出来てるので ec.cpp の中に混在しています。
これは謎のようなものですが（エニグマ？）、まだやりたいことがあるので chatGPT を使って説明を穴埋めしたいと思います。
つまり、MDLP と Decomposition Problem を使った暗号が混在しているということです。
いまは巨大整数ライブラリである NTL を使っていますが、これも GPT を使って C のコードに置き換えていきたい。

それとも Rust がいいのか、C++のままでいいのか・・・（迷ってます）

詳しくは以下のサイトをご覧ください。

https://qiita.com/fumumue/items/5f622ee6ea83cbd4a7f9

行列以外の群に対する鍵交換

この問題は、私が離散対数でもなく共役元探索問題でもない、非可換群を用いた鍵交換で初めて経験した方法です。
世の中非可換群を使ったプロトコルなんて山のようにあるけど、本当は可換になる部分群を使ってたりしてがっかりすることが多いのですが、そんな偽物ではなく本当に非可換な元同士を組み合わせて鍵交換をしようというのが動機です。
行列を使った暗号は色々攻撃法があって危険かもしれませんが、そのときは半直積にしてお好きな群を非可換にしてみるのも手だと思います。
ちなみに置換群は行列なので解読できる可能性が高いです。
今度記事を書くときには、置換群と数ベクトルの半直積を作って、その弱点を調べたいと思います。
今まで置換群で共役元探索問題をやろうとして線形代数攻撃に悩まされてきたのですが、今度こそその攻撃を交わすことができればいいと思います。
ちなみに行列の３分割問題への攻撃法は先程思いつきましたので、整数行列は絶対に使わないでください。
多変数多項式を要素に持つベクトルと、整数ベクトルの半直積などをやってみたいです。
例えば、１変数多項式をｎ本持つベクトルと、ｎこの整数を持つベクトルとの半直積を考える。
ベクトルを v, x、多項式を f, g とすると $(v, f)(x, g) = (f_n(x_n) + v_n, f_n g_n)$（ここで Z/mZ は整数環,$I(x)$ は多項式の法となる既約多項式）のような演算を定義します。

３分割問題（Triple Decomposition Problem）

定義：(Decomposition Problem) とは

ある $v = x_0 x_1 x_2$ と x_1 が与えられた時、を満たすような x_1, x_2 を求める問題です。
ここで、x_0, x_1, x_2 は互いに冪等元でないとする。

ここでは 3 分割のうち 1 つが公開されている問題になっているはずです。
見た感じ行列を使った暗号によく使われるようです。

鍵設定

アリスは 6 個の異なる元を取ります。
$a, b, c, d, x, y \in S_n$
ボブも同様に 6 個の元を取ります。
アリスはそのうち x, y だけを公開し、アリスとボブとの間で共有します。

公開する鍵はボブが決めても問題ありません。
つまりボブの秘密鍵は、
$e, f, g, h \in S_n$
の４つだけです。

アリスは次のようにして公開鍵を作ります。
まず $d^{-1}a = h'^{-1}e = \phi$ であるように決めます。
これは後で述べるビットパターンの分離記号としての役割を果たす元です。

$A1 = (a_1 = axb, a_2 = b^{-1}xc, a_3 = c^{-1}xd^{-1})$
$A2 = (b_1 = ayb, b_2 = b^{-1}yc, b_3 = c^{-1}yd^{-1})$

$B1 = (c_1 = exf, c_2 = f^{-1}xg, c_3 = g^{-1}xh'^{-1})$
$B2 = (d_1 = eyf, d_2 = f^{-1}yg, d_3 = g^{-1}yh'^{-1})$

$A1, A2$ はアリスの公開鍵、$B1, B2$ がボブの公開鍵、a, b, c, d がアリスの秘密鍵、e, f, g, h' がボブの秘密鍵です。

ビットパターンと鍵共有

（ややこしいのでじっくり読みましょうw）

ここで 1 つ制約条件をつけます。
それはアリスとボブの秘密のバイナリ列の長さが偶数であるという仮定です。
その仮定のもとにこの鍵交換は成り立ちます。
ビットパターンを
$h = (0,0), i = (0,1), j = (1,0), k = (1,1)$ とします。
長さ 2 のバイナリ列にはこの 4 パターンしかないので、これだけ定義できれば十分です。

この時、各 2 ビット列が、アリストボブの間でどのように組み合わせられるのか見ていきます。
まず、パターン h のとき、アリスの鍵の組み合わせは、
$h = a_1a_2a_3 = ax^3d^{-1}$ と決めます。
同様にパターン i の場合は、
$i = a_1b_2a_3 = axyxd^{-1}$
$j = b_1a_2b_3 = ayxyd^{-1}$
$k = b_1b_2b_3 = ay^3d^{-1}$

となるように決めます。
同様にボブも、
$h1 = c_1c_2c_3 = ex^3h'^{-1}$ と決めます。
同様にパターン i の場合は、
$i1 = c_1d_2c_3 = exyxh'^{-1}$
$j1 = d_1c_2d_3 = eyxyh'^{-1}$
$k1 = d_1d_2d_3 = ey^3h'^{-1}$

これは行ってしまえば、０と１を 2 つの元の対応関係で表現しているということです。

3 つの異なる元を組み合わせると同時に、ビット列を共有したいという要求を実現できます。

ここで $d^{-1}a = h^{-1}e = \phi$ と決めた事を思い出してください。
あとはパターン通りに鍵の組み合わせを並べるだけです。

アリスのビットパターンが 1010 のときは、
$K_{a_1} = jj = b_1a_2b_3b_1a_2b_3 = ayxy\phi yxyd^{-1}$
$K_{a_2} = j1j1 = c_1d_2c_1b_1d_2b_3 = eyxy\phi yxyh'^{-1}$
1111 の場合は、
$K_{b_1} = kk = b_1b_2b_3b_1b_2b_3 = ay^3\phi y^3d^{-1}$
$K_{b_2} = k1k1 = ey^3\phi y^3h'^{-1}$

$K_{alice} = K_{a_1}K_{b_1} = ayxy\phi yxy^4\phi y^3d^{-1}$
$K_{bob} = K_{a_2}K_{b_2} = eyxy\phi yxy^4\phi y^3h'^{-1}$

であり、鍵に割り当てられた番号同士をつなぎ合わせて、K_{alice}, K_{bob} からそれぞれアリスとボブの秘密鍵を取り除けば鍵共有は出来上がりです。
これは非可換でなければならないという要請に答えるための鍵共有ができる元の 3 分割問題 (triple decomposition problem) を利用したものとなると思います。(不安)

ここで問題が。
ϕ が公開されることで、特定の位置に ϕ があることがわかるというのはどの程度問題になるだろうか？
かと言って 1 にしてしまうと 3 つのパーツを全部揃えれば線形代数攻撃に弱くなるし、何かいい方法があるかもう少し考えます。

成功したら大発見です。

以下の記事の続きです。
オリジナルバージョンの公開鍵暗号を使ってシュノア署名を実現します。

https://qiita.com/fumumue/items/5f622ee6ea83cbd4a7f9

ここで言う非可換群を、楕円曲線の点群を要素に持つに持つ半直積と呼ぶことにする。
半直積については上記アドレスに書いてあります。

鍵の設定

公開鍵：$D = A^xBC^y, E = A^zBC^w, A, C$
秘密鍵：x, y, z, w, B

署名作成

$P = DE^{-1} = A^xBC^{(y-w)}B^{-1}A^{-z} = A^xQA^{-z}$
と置く。
r, r' を乱数とし、次を計算する。

$e = H(m||A^rQA^{r'})$
$y_1 = r - xe$
$y_2 = r' + ze$

$sig = (y_1, y_2, e)$

署名検証

$P = A^xQA^{-z}$
なので、
$c = A^{y_1}A^ePA^{y_2}A^e = A^{r-ex}A^ePA^{r'-ze}A^e = A^{r-ex}A^e(A^xQA^{-z})A^eA^{r'+ze} = A^rQA^{r'}$
と置くと、
$e' = H(m||c)$
もし、$e = e'$ なら正しい署名である。

この暗号自体がエルガマル暗号のような離散対数問題と、群の元を 3 つに分解する分解問題の合体のようなものなので、どちらの問題の困難性に基づいているのかはまだ明らかではない。
ところで、RSA が鍵を大きくすることで生き残れるとしたら、ECDLP もそうなるはずで、どちらも一時しのぎに過ぎないかもしれないけど、今から楕円曲線やペアリングを始める価値も十分にある。暗号の応用としては、私は決定不可能性を用いた暗号（要するに計算機には解けない）や、非可換群を用いた暗号で IBE（ID ベース暗号）などが作れればいいのにと思っている。でも今回、非可換群を使うことでエルガマル型の電子署名ができたので、他の応用にも使えるのではないかと期待している。

すでに実装はしてたんですが、ちょっと驚いてます。対応策として以下の 3 つを考えました。

その１：共役元探索問題を用いた公開鍵暗号

定義：共役元探索問題とは、y, A が公開されているとき $y = xAx^{-1}$ から x を求める問題である。鍵：$y = xAx^{-1}, z = xBx^{-1}, A, B, y, z$ を公開鍵とし、x を秘密鍵とする。暗号化：S をバイナリ列とし、0 を y、1 を z と置き換えて S を表した元を $tr(S, y, z)$ とする。この時、$U = tr(S, y, z) = xABAB...x^{-1}$ であると同時に $V = tr(S, A, B) = ABAB...$ なので、暗号文を C, メッセージを M と置くと、$C = (H(U) * M, V)$ である。ここで H はハッシュ関数であるとする。復号：$U = x^{-1}Vx$ とすると $M = H(U) * M/H(U)$ となる。

攻撃：x が未知である時、$yx = xA, zx = xB$ なので、$y = (p, P), z = (q, Q)$ とすると、$(p, P)(x, X) = (x, X)(a, A), (q, Q)(x, X) = (x, X)(b, B)$ $(px, xP + X) = (ax, aX + A), (qx, xQ + X) = (xb, bX + B)$ $px - ax = 0 \rightarrow x(p - a) = 0$??? アフィン群の定義から連立一次方程式が導けるので線形代数攻撃ができるかもしれない。**追記 (20230820)：鍵を合成するときの計算がすでに非可換群のなす準同型写像（内部自己同型写像）であることから、この暗号が準同型暗号になる可能

性がある。** 例えば、別の暗号化法が使えることが分かる。今、乱数をバイナリ表現したものを R と置き、平文をバイナリ表現したものを M と置くと、暗号化は $C_1 = xRMx^{-1}, C_2 = xRx^{-1}, C = (C_1, C_2)$ というように書くことができる。復号は $C' = (m_1 = x^{-1}C_1x = RM, m_2 = x^{-1}C_2x = R)$ ゆえに $M = m_2^{-1}m_1$ である。これは足すというよりは継ぎ足している感じである。つまり平文と乱数をかけて結果を得るというところである。これの発展形は後日別記事にしようと思います。群準同型の勉強をしている間に気が付きました。勉強は大事w

その２：元の分割問題を用いた公開鍵暗号

定義：y, z が公開、n, m, x が秘密とされているとき、$y = x^m zx^n = x_1 zx_2$ から x_1, x_2 を求める問題である。公開鍵：$y = x^{-n+m}zx^{2n}, w = x^{-n+l}zx^{2n}, X = a^{-1}zx^{n+m}a, Y = a^{-1}zx^{n+l}a$、が公開鍵、$x, m, l, n, a = x^c$ が秘密鍵とする。暗号化：まず、s, t をランダムにとり

$$W = a^{-1}y^s w^t a = a^{-1}x^{-n+m}zx^{m+n}...zx^{n+l}zx^{n+l}...zx^{2n}a = x^{m-n}a^{-1}X^{s-1}Y^{t+1}azx^{2n}$$

(が、x は分からない) とする。次に乱数 r をとり、$R = (Y^{-1}X)^r = a^{-1}x^{(m-l)r}a$ と置く。更に

$$W' = RW = a^{-1}x^{(m-l)r}x^{-n+m}X^{s-1}Y^{t+1}azx^{2n}$$

として乱数化する。ここで $Z = x^{(m-l)r}X^{s-1}Y^{t+1}$ とする。平文を M とし、ハッシュ関数を H と置くと、暗号化は $C = (H(Z) * M, W')$ である。復号：$Z = x^{n-m}aWa^{-1}x^{-2n}z^{-1}$ である。ここから $H(Z)$ を計算し、$M = C/H(Z)$ となり平文 M が求まる。攻撃：共役元探索問題が解けると仮定する。$X = zx^{n+m}, y = x^{-n+m}zx^{2n}$ の場合 $(z^{-1}X)^{-1}y = z^{-1}zx^{-n-m}x^{-n+m}zx^{2n} = x^{-2n}zx^{2n}$ となり、共役元探索問題が解ければ解読できる。しかし、a があるので攻撃は防げると思う。

その２の代替案（半分配体を使う）

上記の半直積に加法を定義する。つまり $(a, P)(b, Q) = (a+b, P+Q)$ である。そこで、

$$(c, s)^n = (c^n, \frac{c^{n-1}-1}{c-1}s)$$

であるから、公開鍵を D, E とすると、

$$D = (p, P)^s + (q, Q)^t + (r, R)^u = (p^s, \frac{p^{s-1}-1}{p-1}P) + (q^t, \frac{q^{t-1}-1}{q-1}Q) + (r^u, \frac{r^{u-1}-1}{r-1}R)$$

$$= (p^s + q^t + r^u, \frac{p^{s-1}-1}{p-1}P + \frac{q^{t-1}-1}{q-1}Q + \frac{r^{u-1}-1}{r-1}R)$$

$$E = (p, P)^x + (p, P)^s + (q, Q)^t + (r, R)^u + (r, R)^y$$

$$= (p^x, \frac{p^{x-1}-1}{p-1}P) + (p^s, \frac{p^{s-1}-1}{p-1}P) + (q^t, \frac{q^{t-1}-1}{q-1}Q) + (r^y, \frac{r^{y-1}-1}{r-1}R) + (r^u, \frac{r^{u-1}-1}{r-1}R)$$

$$= (p^x+p^s+q^t+r^u+r^y, (\frac{p^{x-1}-1}{p-1}+\frac{p^{s-1}-1}{p-1})P+\frac{q^{t-1}-1}{q-1}Q+(\frac{q^{y-1}-1}{q-1}+\frac{r^{u-1}-1}{r-1})R)$$

暗号文：

$$C1 = A^r + D + C^{r'} = A^r + A^s + B^t + C^u + C^{r'}$$
$$C2 = A^r + E + C^{r'} = A^r + A^x + A^s + B^t + C^{r'} + C^y + C^u$$

復号アリスは x, y を知っているので以下を計算できる。

$$X = A^{(x)} + C1 + C^{(y)} = A^s + A^x + A^r + B^t + C^{r'} + C^y + C^u = C2$$

その３：原始元を暗号化し離散対数問題を解く関数を復号関数に持つような暗号方式

定義：原始元を暗号化する。共役元探索問題が難しいと仮定する。

公開鍵：$D = A^a X A^{-a}, A$、$E = A^b X A^{-b}, A, X^c$、秘密鍵 a, b, c, X

暗号化１：$C = A^r D^{m_1} E^{m_2} A^{-r} = A^{r+a} X^m A^{b-a} X^m A^{-b-r}, R = A^r X^c A^{-r}$

暗号化２：$S = A^r D^m A^{-r} = A^{r+a} X^m A^{-a-r}, T = A^r X A^{-r}$、

復号：$U = A^a T A^{-a} = A^{a+r} X A^{-a-r}, S = U^m$ より、S, U から離散指数 m を求める方法により平文 m を得る。

攻撃：鍵から秘密指数を計算できれば解読できる。**追記 (20230820)：問題は、S, T から $T' = A^{a+r} X A^{-r-a}$ もしくは秘密指数 a を見つけることである。論文にある攻撃法は原始元となるべき任意の元 $Z = (m, P)$ と、その n 乗された元 $A = Z^n = (x^n, [\frac{m^n-1}{m-n}P])$ が与えられればShor のアルゴリズムを使って $[m-1]A+P = [m^n]P$ から m^n を計算することができ、更にもう一度 m^n に対して Shor のアルゴリズムを繰り返すことで最終的に n が計算できるという２段階の処理になります。**

復号１：まず、共役元探索問題を解くアルゴリズムがあると仮定する。この時、R, X^c, から A^r がわかる。すると、$G = A^{-r} C A^r = D^m E^m = A^a X^m A^{b-a} X^m A^{-b}$ である。次に、A^a, A^b は既知なので、$H = A^{-a} G A^b = X^m A^{b-a} X^{-m}$ となり、A^{b-a} は既知なのでここでも共役元探索問題が解け、A^m が求まる。復号２：$S = U^m, U = A^a T A^{-a} = A^{a+r} X A^{-a-r}$ なので、ここでは原始元に相当する元を暗号化することでこの攻撃を回避しています。なんだか合気道みたいですねw

ああでも復号関数に Shor を使うなんて効率悪すぎますね。そもそもそれって量子計算機が出てきたらの話だし。あ、でも**mが小さい場合なら復号できそう。しかも積に関して準同型を満たす。**

ついに離散対数を求める方法を使うときが来たのよ！とばかりに昔の方式をいじってみたりする。これをやっていてよく理解できたんですが、やはり暗号の多様性が大事なのだという事。最初に暗号の多様性をいい出したのはパタリンだと思うけど違うのだろうか？脱！離散対数！

この記事の続きでは、楕円曲線だけでなく、置換群とベクトルの半直積やその他決定不可能な問題を利用した暗号系をやる予定である。

参考文献

付録：プログラム