画像の秘密共有化

2006 MI 089　久留島自翔
指導教員：小藤俊幸

1　はじめに

現代の情報社会では様々な情報がディジタル化されていて，コンピュータで処理・保存されている．しかし，それらはコンピュータの故障などの原因から損失するかのうせいがある．そのためUSBやCD-ROMなどの予備記憶装置にバックアップを保存しておく必要がある．しかし，昨今そのバックアップを紛失したり，パソコンが不正アクセスされたりすることで，情報が漏洩している．問題なのはその中には企業の重要書類や企画のデザイン，役所の住民票などのような個人情報といった見ず知らずの第3者に見られたくない，見られてはいけない情報があるということだ．そうならないために情報を見られないようにパスワードなどのロックをかけたり，暗号化の処理を行っている．しかし，これらは特定の方法をしようすることで解読することができるという欠点がある．そこでできたのがシークレット・シェアリング（Secret sharing）である．シークレット・シェアリングは情報を分けて共同保有することで，情報の漏洩を防ぐ技術である．シークレット・シェアリングは分けた情報の1つが漏洩しても情報を復元できないという特性と，情報が1つくらい欠けても復元が可能であるという特性がある．この論文ではそのシークレット・シェアリングについて論じたい．

2　シークレット・シェアリング

冒頭でも述べたとおり，シークレット・シェアリングは秘密情報を他人には見られないようにする技術の一つである．この章ではシークレット・シェアリングの基本的な仕組みを理解していきたい[1]．

p を素数とし，$s \in F_p$ を秘密にしておきたい数字とする．クレジットカードの番号やキャッシュカードの暗証番号などをイメージしておけばいいだろう．この番号を何人かで“共同”して保管することを考える．まず $s_0, s_1 \in F_p$ を適当に選んで，F_p 上の2次多項式

$$f(x) = s_0 + s_1 x + s x^2 \qquad (1)$$

を作る．さらに，$c_1, c_2, \ldots$ をF_pの相異なる元として，$d_1 = f(c_1)$, $d_2 = f(c_2)$, …を計算します．得られた対(c_1, d_1), (c_2, d_2), … をシェア(share) と呼び，秘密を共有する人たちに一つずつ渡しておく．受け取った人たちは，自分のシェアを他人には知られないように保管する．

※ここで言うシェアは，いわゆるマーケットシェア（市場占有率）のシェアではなく，株式，株券のたぐいを指す．

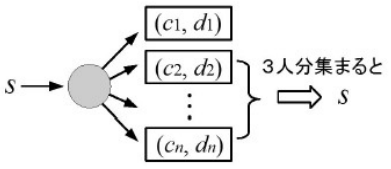

図1：Secret Sharing

秘密の共有者が（少なくとも）3人集まって，自分自身が保持しているシェアを提示しさえすれば，$s \in F_p$を復元することができる．実際，(c_i, d_i), (c_j, d_j), (c_k, d_k) を（異なる）3人のシェアとすると，$d_i = f(c_i)$, $d_j = f(c_j)$, $d_k = f(c_k)$ から，

$$\begin{bmatrix} 1 & c_i & c_i^2 \\ 1 & c_j & c_j^2 \\ 1 & c_k & c_k^2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s \end{bmatrix} = \begin{bmatrix} d_i \\ d_j \\ d_k \end{bmatrix} \qquad (2)$$

のようなs_0, s_1, s に関する連立一次方程式が得られる．左辺の行列はc_i, c_j, c_k が相異なるとき，正則（逆行列をもつこと）となり，s_0, s_1, s（特にs）が一意に定まる．なお，多項式の次数を大きくすれば，s の復元に必要な「3人」をもっと多くの人数に変えることができる．

※「正則⇔（行列式）≠ 0」は一般の体で成り立つ(行列式) ≠ 0 であることは，行列式(determinant) を実際に計算してみると分かる．$c_i \to a$, $c_j \to b$, $c_k \to c$ とおきかえて，次のように入力してみよう．このような形の行列の行列式は，ファンデルモンド(Vandermonde,1735-1796) の行列式と呼ばれている．

```
(%i1) A:matrix([1,a,a^2],[1,b,b^2],[1,c,c^2]);
(%i2) determinant(A);
(%i3) factor(%);
```

次に実際に数値をあてた例題をMaxima（今回の論文ではMaxima-5.27.0を使用した）を用いて解いてみる．

（例題）$p = 257$ とし，$s = 99$ を秘密にしたい数字とする．$s_0 = 239$, $s_1 = 228$ に取り，$f(x) = 239 + 228x + 99x^2$ とする．例えば，$c_1 = 72$ とするとき，$d_1 = f(c_1)$ の値を，次のように計算する．

```
(%i1) p:257;
(%i2) f:239+228*x+99*x^2;
(%i3) mod(subst(x=72,f),p);
```

結果として，$d_1 = 194$となる．同様に$c_2 = 89$, $c_3 = 56$, $c_4 = 240$, $c_5 = 143$ に対して，$d_i = f(c_i)$ を計算すると，$d_2 = 43$, $d_3 = 165$, $d_4 = 45$, $d_5 = 9$ となるので，シェア(72, 194), (89, 43), (56, 165), (240, 45), (143, 9) を一つずつ5人に分配する．

一例として，シェア(89, 43), (56, 165), (143, 9) から$s = 99$ を復元することを考えよう．対応する(2) の方程式をガウスの消去法で解けばよい．特に，s は階段化して得られる最後の式から直ちに求められる．次の計算例では，A0 を (2) の（Maxima流ではない）通常の拡大係数行列としている．

```
(%i4) modulus:p;
(%i5)A0:radcan(matrix([1,89,89^2,43],[1,56,56^2,165],[1,143,143^2,9]));
(%i6) A1:radcan(matrix(A0[1],A0[2]-A0[1],A0[3]-A0[1]));
(%i7)A2:radcan(matrix(A1[1],A1[2],A1[3]+(54/33)*A1[2]));
(%i8) s:mod(radcan(-68/72),p);
```

3　画像のシークレット。シェアリング

前章ではシークレット・シェアリングの基本的なことにつ

いて述べたので，この章ではこの論文の題目にもなっている画像のシークレット・シェアリングについて述べたい．今回は白黒の二値画像（白黒画像のように色が2色しかない画像）をサンプル画像として使用して 2 人にシェアした場合の画像のシークレット・シェアリングをする[2]．

画像のシークレット・シェアリングをする手順としては，まず，1 ピクセルを 4 ピクセル分の正方形に置き換える．次に 2 つの分散画像に分割する．元々が黒だったピクセルの場合は図 2.1 のようにそれぞれ左端と右端を互い違いに黒くして，重ねたときに黒い部分が重ならないようにする．右を黒くするか左を黒くするかはランダムで決める．また元々が白だったピクセルの場合は図 2.2 のようにそれぞれ右端と左端の同じ側を黒くして，2 つを重ねた時に黒い部分が重なるようにする．なお，ここでは見やすくするため灰色で表示する．

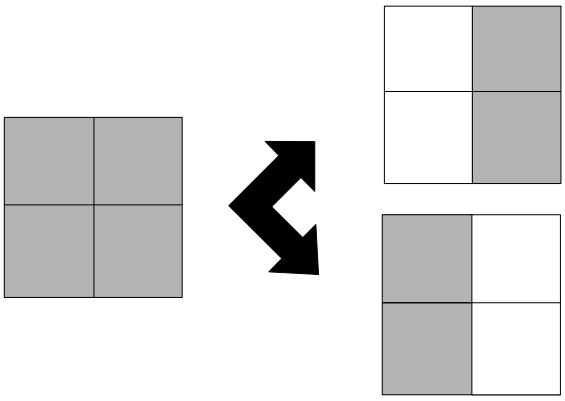

図 2.1　黒の場合

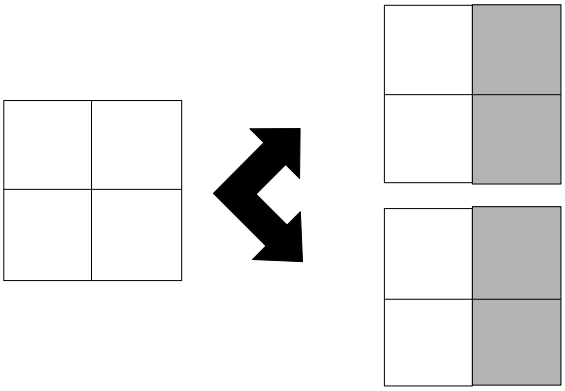

図 2.2　白の場合（右端を黒くする場合）

このようにして今述べた手順に従って，図 3.1 の画像サンプルを実際にシークレット・シェアリングの処理を行ってみる．

図 3.1

これを先ほど述べた手順でシークレット・シェアリングをして，2 つに分けると次の図 3.2 と図 3.3 のように分割する前，どんな画像であったかわからない 2 つの画像が出来上がる．

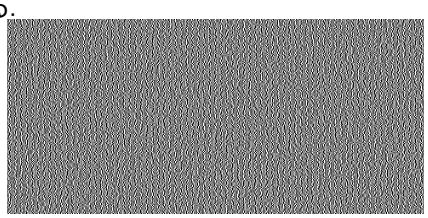

図 3.2

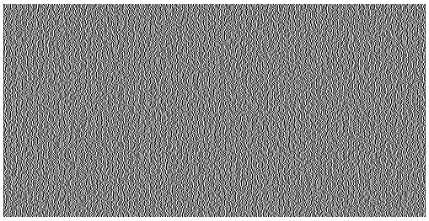

図 3.3

しかし，実際にこの 2 つの画像を OHP シートのような透明なシートに印刷して，それらを重ね合わせてみると，図 3.4 のようになる．

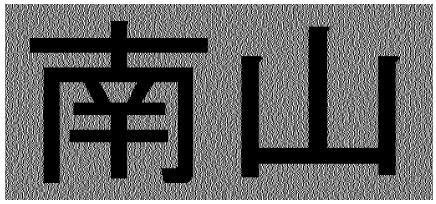

図 3.4

図 3.4 を見てみると，元々は「南山」という文字が書かれていた画像であることがわかる．このようにして画像を見たいときには今のように保持している画像を提示して，重ね合わせることで元々の画像を見ることができるということがわかった．

4．おわりに

今回の論文で，シークレット・シェアリングによって画像を分けてそれを秘密にすることができた．今回は画像を二つ（二人分）に分けたが，実際に行われているシークレット・シェアリングの場合は，始めに述べたとおり，画像だけではなく様々な情報があり，共有する人数はもっと多くなるし，情報を暗号化した上でシークレット・シェアリングをする．なので今度はそういった処理も行った上でシークレット・シェアリングをしたい．

5．参考文献

[1]小藤俊幸，情報システム数理実習資料，2011.
[2]S.Cimate,C.-N.Yang(ed.),"Visual Cryptography and Secret Image Sharing",CRC Press,Boca Raton,2012.