複数の情報を復元できる誤り訂正符号を利用した秘密分散法

研究代表者　　古　賀　弘　樹　　筑波大学システム情報系　准教授

1 本研究の概要

秘密分散法は，秘密情報をシェアと呼ばれる複数個の分散情報に管理する方式であり，機密性の高い情報の管理に用いられる．特に，(k,n)しきい値法として知られる秘密分散法は，任意の k 個のシェアから秘密情報が復元できるが，k 個未満のシェアからは秘密情報が一切漏れないという特徴をもっている．(k,n)しきい値法の構成法として代表的なものは，有限体上のランダムな k-1 次多項式を用いる Shamir 法[1]である．

他方，誤り訂正符号は雑音のある環境下で信頼性の高い通信を行うために用いられる技術であり，深宇宙通信などの他，音楽 CD や QR コードなど，身近なところで使われている．代表的な誤り訂正符号として Reed-Solomon 符号[2]がある．McEliece and Sarwate[3]は Reed-Solomon 符号と Shamir 法の関連を指摘している．

本研究の目的は，誤り訂正符号の誤り訂正能力を利用した秘密分散法とその応用について考察し，その安全性について数理的な立場，特に情報理論的な立場から解析を加えることである．第２節では QR コードを利用した新しい(2,2)しきい値法の構成を述べる．この方式は２枚の QR コードを用いる．それぞれの QR コードを QR コードリーダで読み取ると，それぞれメッセージを読み出すことができる．さらに，２枚の QR コードを重ねてコードリーダで読み取ると，別の秘密情報が復元できる．あるゆるやかな条件のもとでは，この方式が厳密な意味で(2,2)しきい値法になっていることが示される．第３節では，Reed-Solomon 符号の検査行列を利用した(k,n)しきい値法およびランプ型(k,L,n)しきい値法を構成する．これらの方式は Shamir の方式と双対な方式であり，McEliece and Sarwate [3]の１変形になっている．また，k=n の特別な場合は，Karnin ら[4]の(n,n)しきい値法に帰着する．本研究では，分散共有される L 個の秘密情報が一般的な情報源から出力されるときに，この方式がランプ型(k,L,n)しきい値法になることを示す．

2 ２枚の二次元コードを用いた秘密分散法とその性能解析

2-1 研究の背景

近年，カメラ付き携帯電話やスマートフォンの普及により，二次元コードを用いた情報のやり取りが広く行われるようになった．中でも株式会社デンソーが開発した QR コード[5]は広く普及しており，Web ページの URL を搭載した広告や，電話番号等の連絡先の交換，飛行機の搭乗券，イベント会場の入場チケットなど，様々な用途で利用されている．QR コードには Reed-Solomon 符号(RS 符号)[2]として知られる誤り訂正符号が用いられているので，ノイズ等により一部が誤って読み取られても，その誤りを訂正して正しい情報を読み取ることができる．

この節では，QR コードの誤り訂正能力を利用した秘密分散法を提案する．提案手法では，大きさの等しい 2 枚の QR コードを用意する．これら 2 枚の QR コードは，汎用の QR コードリーダを用いて，それぞれ情報を読み出すこともできる．さらに，2 枚のうち 1 枚の QR コードを透明なシートにコピーして，もう 1 枚にぴったり重ねた状態で QR コードリーダにうまく取り込むと，別の秘密情報を読み取ることができる．また，ある条件のもとでは，どちらか一方の QR コードからは，秘密情報については一切知ることはできないことを証明することもできる．

提案手法と関連の深い技術として，Naor と Shamir により提案された視覚復号型秘密分散法[6]がある．視覚復号型秘密分散法は秘密分散法の一分野であり，1 枚の秘密の白黒 2 値画像を n 枚のシェア画像に分散符号化し，シェア画像を透明のシートに印刷して n 人のユーザに配布する．アクセス構造として(k,n)しきい値型を仮定するとき，任意の k 枚のシェア画像を重ね合わせると秘密画像を知覚できる．逆にどんな k-1 枚以下のシェア画像からは秘密画像の情報は一切得ることができない．シェア画像は通常は意味のないランダムな画像になるが，シェア画像に画像情報を入れることも可能である[7]．

視覚復号型秘密分散法を(2,2)しきい値型にして，2 枚のシェア画像にそれぞれ異なる画像情報を入れたものは提案手法に近くなる．しかしながら，秘密情報の復号に人間の視覚を用いるか，汎用のコードリーダを

用いるかが異なっている．視覚復号型秘密分散法において，シェアを重ねて画像情報を復号する場合は機器を特に必要としないが,原理的に文字列に雑音が必ず加わるので,復元される秘密情報の解像度が低くなり，秘密画像として長い文字列が入った画像を用いることは困難になる．一方，提案手法では汎用の QR コードリーダを利用することになるが，視覚復号型秘密分散法と比べると復号される文字列が機器にそのまま表示されるので可読性が高く，長い文字列が使用可能になる．QR コードリーダはスマートフォンのアプリやカメラ付き携帯電話の 1 機能として広く普及しており，目視により復号できないというデメリットは，アプリケーションによっては大きくないものと思える．提案手法は(2,2)しきい値型に限定された形ではあるが，視覚復号型秘密分散法で分散共有できる文字列を長くし可読性を上げるために，目視による復号でなくコードリーダによる復号を採用したともいえる．

提案手法はまた，静止画像を用いたステガノグラフィとしての側面ももち，秘密情報の存在を隠すために使うこともできる．もし提案手法で生成される 2 枚の QR コードが，一般的な他の QR コードと区別できない程度に自然に感じられれば,通常はそれら 2 枚の QR コードに別の秘密の情報が隠されているとは思わないであろう．提案手法で生成する 2 枚の QR コードのうちの 1 枚を秘密情報の入ったステゴデータ,もう 1 枚を，秘密情報を復号する鍵が埋め込まれたステゴデータとして解釈することもできる．

本節の構成は次の通りである．2.2 節では QR コードの仕様と構成について概説する．第 2.3 節で提案手法について述べ，実際の構成例を示す．第 2.4 節では提案手法の安全性についての考察し，提案手法で使用できる文字列の長さについて議論する．

2-2 QR コードを用いた秘密分散法

（１）満たすべき性質

秘密分散法でシェアとなる 2 枚の QR コードの画像を QR_X, QR_Y と書く．QR_X, QR_Y は白黒 2 値画像で同じ型であり，プリンタで正確に印刷した場合には同じ大きさになり，モジュール（画素）ごとにぴったり重なるとする．また， QR_X, QR_Y には共通のマスク処理がなされているとする．ここにマスク処理とは，QR コードのリーダによる可読性を高めるために，８種類のマスクパターンのいずれかと画素毎に排他的論理和の処理を行う処理を指す．

我々は，QR_X と QR_Y が次の 3 つの性質を満たすことを要請する．

性質 P1

QR_X を白紙に印刷し，比較的良好な条件のもとでコードリーダで読み取ると，あるメッセージ Mes_X が復号される．同様に，QR_Y を白紙に印刷し，比較的良好な条件のもとでコードリーダで読み取ると，あるメッセージ Mes_Y が復号される．

性質 P2

QR_X を白紙に印刷し，QR_Y を透明なシートに印刷して， QR_X の上に QR_Y をぴったり重ねて良好な条件のもとでコードリーダで読み取ると，別のメッセージ Mes_Z が復号される．QR_X と QR_Y が印刷される媒体を取り替えても同様に Mes_Z が復号される．

性質 P3

QR_X をどんなに解析しても Mes_Z に関する情報は一切得られない．同様に，QR_Y をどんなに解析しても Mes_Z に関する情報は一切得られない．

ここで，上述の性質 P1 における「比較的良好な条件」とは，QR コードの画像をコードリーダで取り込むときに誤る符号シンボルの数が，QR コードのもつランダム誤り訂正能力の範囲内に収まる状況を指す．また性質(P2)における「良好な条件」とは，QR コードの取り込み時にすべての符号語シンボルが正しく読み取れる状況を指す．

なお，QR コードではランダム誤り訂正能力の上限 t は[5,表 12]に記載されており，4 型で誤り訂正レベルが L の(以下簡単のため 4L 型という)場合は t=10 となる．提案手法では,3 つのメッセージ Mes_X, Mes_Y, Mes_Z はいずれも，適当なモード（英数字モードなど）で記述した場合に必要なヘッダと終端パターンを連接したときのビット長が 8t 以下であることを仮定する．実際，4L 型の場合に英数字モードを用いて情報を記述する場合は Mes_X, Mes_Y, Mes_Z はいずれも 11 文字以下ならこの仮定は満たされる．また，符号語長 n と t は $n-9t \geqq 0$ を満たすことも仮定する．4L 型の場合は n=100, t=10 であるのでこの仮定は満たされる．

（２）符号語のブロック分割

以下，2 枚の QR コード画像 QR_X，QR_Y に対応する短縮 RS 符号の符号語をそれぞれ $\mathbf{c}_X, \mathbf{c}_Y$ と表す．$\mathbf{c}_X, \mathbf{c}_Y$ の符号語長は n である．いま t をこの短縮 RS 符号のランダム誤りを訂正できるシンボル数の上限として，符号語 $\mathbf{c}_X$ を $\mathbf{c}_X = (X_1, X_2, \ldots, X_{10})$ と表す．ここに $X_I, i=1,2,\ldots,9$ は符号語 $\mathbf{c}_X$ を前から順に t シンボルずつに区切って得られるブロックであり，X_{10} は残りの n-9t シンボルを指す．仮定から n-9t≧0 であり，Mes_X はヘッダ，終端パターンとともに X_1 に含まれるとしてよい．

また，$\mathbf{c}_X$ と同じブロック分割のもとで，マスクパターンを $\mathbf{f} = (F_1, F_2, \ldots, F_{10})$ と表す． QR_X の n 個のシンボル部分に対応するのは，$\mathbf{c}_X$ の各ブロックをマスク処理したブロック

$$X_i' = X_i \oplus F_i, \quad i=1,2,\ldots,10$$

を用いて定義される $\mathbf{c}_X' = (X_1', X_2', \ldots, X_{10}')$ が表すビットパターンである．ここに⊕ はビットごとの排他的論理和を表す．さらに $\mathbf{c}_Y = (Y_1, Y_2, \ldots, Y_{10})$，$\mathbf{c}_Y' = (Y_1', Y_2', \ldots, Y_{10}')$ も同様に定義する．QR_X と QR_Y はマスクパターンが共通であるので，

$$Y_i' = Y_i \oplus F_i, \quad i=1,2,\ldots,10$$

であることにも注意する．

次に 2 枚の QR コード画像の重ね合わせについて述べる．性質 P2 のように，2 枚の QR コード画像の一方を白紙に，他方を透明なシートに印刷してぴったり重ね合わせることは，2 枚の QR コード画像のモジュール（画素）ごとの OR をとることに相当する．ゆえに，2 枚の QR コード画像 QR_X と QR_Y の OR をとって得られる画像 QR_Z のシンボル部分 $\mathbf{c}_Z' = (Z_1', Z_2', \ldots, Z_{10}')$ は

$$Z_i' = X_i' \vee Y_i', \quad i=1,2,\ldots,10$$

を満たす．ここに∨はビット単位の OR 演算を表す．$\mathbf{c}_Z'$ のマスクを外したものを $\mathbf{c}_Z = (Z_1, Z_2, \ldots, Z_{10})$ と書く．性質(P2)は，$\mathbf{c}_Z$ を短縮 RS 符号の復号器で復号した結果， Mes_Z が得られることを要請している．

（３）符号語の構成手順

マスクパターン f は固定であるので，QR_X と QR_Y を構成するためには符号語 $\mathbf{c}_X$,$\mathbf{c}_Y$ を決定すればよい．本稿では，$\mathbf{c}_X$,$\mathbf{c}_Y$ の決定に先立ち，別の符号語 $\mathbf{c}_Z^* = (Z_1^*, Z_2^* \ldots, Z_n^*)$ を構成する． $\mathbf{c}_Z^*$ は，対応する QR コード画像 QR_Z* を比較的良好な条件のもとでコードリーダに取り込んだときに Mes_Z が復号されるように定める．$\mathbf{c}_X$ $\mathbf{c}_Y$ のブロックの一部は，$\mathbf{c}_Z^*$ のブロックを用いて構成する．

<u>符号語 $\mathbf{c}_Z^*$ の構成手順</u>

(1) Z_1^* を Mes_Z より生成する．具体的には，Mes_Z を適当なモードのビット列で表し，モード指示子と文字数指示子をヘッダとして連接し，末尾に終端パターンを連接する．得られたビット列の長さが 8t より短かければ，一様乱数列を連接して 8t ビットにする．

(2) $Z_i^*, i=2,3,4,5$ は，B'をすべて 1(黒)から成るブロック，$B_i = B' \oplus F_{i+1}, i=1,2,3,4$ として，$Z_2^* = B_1$，$Z_3^* = B_2$，$Z_4^* = B_3$，$Z_5^* = B_4$，と順に定める．

(3) $Z_6^* = R_1$，$Z_7^* = R_2$ と定める．ここに R_1, R_2 は独立な t シンボルの一様乱数である．

(4) Z_{10}^* は，長さ n-9t のシンボル列 U として任意に定める．

(5) Z_8^*, Z_9^* は $\mathbf{c}_Z^*$ に対して消失訂正を行って定める．$Z_8^* = P_{Z^*,1}$，$Z_9^* = P_{Z^*,2}$ とおく．

<u>符号語 $\mathbf{c}_X$ の構成手順</u>

(1) X_1 を Z_1^* と同様に Mes_X より生成する．

(2) $X_2 = B_1$，$X_3 = B_2$ とし，また $X_6 = R_1$，$X_8 = P_{Z^*,1}$ と定める．

(3) X_7, X_9 は W'をすべて 0（白）から成るブロックとして，$X_7 = W_{X,1} = W' \oplus F_7$，$X_9 = W_{X,2} = W' \oplus F_9$ と定める．

(4) $X_{10} = U$ と定める．

(5) X_4, X_5 は $\mathbf{c}_X$ に対して消失訂正を行って定める．$X_4 = P_{X,1}$，$X_5 = P_{X,2}$ とおく．

<u>符号語 $\mathbf{c}_Y$ の構成手順</u>

(1) Y_1 を Z_1^* と同様に Mes_Y より生成する．

(2) $Y_4 = B_3$，$Y_5 = B_4$ とし，また $Y_7 = R_2$，$Y_9 = P_{Z^*,2}$ と定める．

(3) Y_6, Y_8 は W'をすべて 0（白）から成るブロックとして，$Y_6 = W_{Y,1} = W' \oplus F_6$，$Y_8 = W_{Y,2} = W' \oplus F_8$ と定める．

(4) $Y_{10} = U$ と定める．

(5) Y_2, Y_3は$\mathbf{c}_Y$に対して消失訂正を行って定める．$Y_2 = P_{Y,1}$，$Y_3 = P_{Y,2}$とおく．

さて，2 枚の QR コード画像 QR_X, QR_Y を重ね合わせて得られる画像 QR_Z を考える．QR_X, QR_Y の形式情報は完全に一致するので，ビット単位で OR をとってもビットパターンは変化せず，そのまま QR_Z の形式情報になる．一方，シンボル部分は$\mathbf{c}_X$'と$\mathbf{c}_Y$'のビットごとの OR をとることになるので，図２より一番左のブロックを除いて$\mathbf{c}_Z$*にマスク処理を施したものに一致する．QR コードは t シンボル以下のランダム誤りの訂正が可能であるので，コードリーダは良好な条件のもとではこの左端のブロックに生じた高々t シンボルの誤りを訂正することができる．$\mathbf{c}_Z$の誤りを訂正した結果得られる符号語は$\mathbf{c}_Z$*であり，左端のブロック Z_1*から Mes_Z を読み出すことができる．

（４）構成例

上記のアルゴリズムに基いて生成された 4L 型の QR コード画像 QR_X, QR_Y をそれぞれ図 1 に示す．マスクはマスク参照子 011 のものを用いた．比較的良好な条件のもとでコードリーダで取り込むと，QR_X から文字列「IEICE TRANS」が，QR_Y から文字列「U. TSUKUBA」が読み出せる．QR_X と QR_Y のビットごとの OR をとった画像 QR_Z を図に示す．良好な条件のもとで QR_Z をコードリーダで取り込むと，文字列「SECRET INFO」が読み出せる．図は$\mathbf{c}_Z$*をもとに作成した QR コード画像 QR_Z*である． QR_Z と QR_Z*を比較すると，ほとんどが同じであるが，右端の誤りが生じる部分だけビットパターンが異なる．QR_Z*からは，比較的良好な条件のもとで文字列「SECRET INFO」が読み出せる．

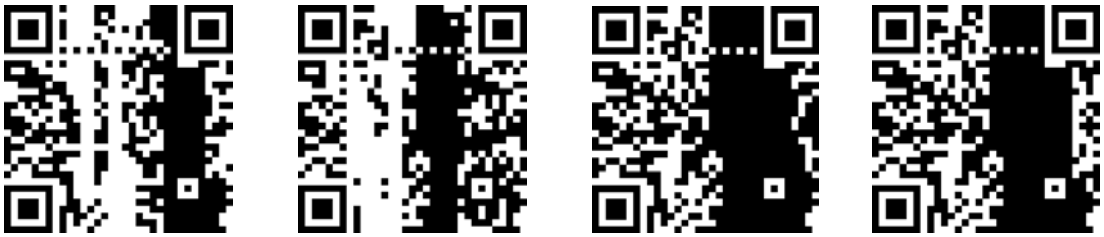

図１　生成された QR_X, QR_Y とそれらの OR および QR_Z*（左から順に）

4L 型の場合は t=10 であるので，ブロック X_1, Y_1, Z_1*は 80 ビットから成る．ヘッダが 9 ビット，終端パターンが 4 ビットであるので，メッセージに使えるビット数は高々63 ビットである．英数字モードの場合は 11 ビットで 2 文字を記述することになる(奇数長の文字列の場合は最後の 1 文字を 6 ビットで記述する)ので，記述できる文字列の長さの上限は 11 になる．

（５）シンボルの配置順序の変更

前節で述べた方式で生成したシンボル列をそのまま QR コードに配置した場合は,図のように黒のモジュールと白のモジュールが連続して現れる領域が存在する．こうした領域によって，コードリーダによる QR コード自体の可読性が低下するおそれがある．また QR コードとしてはいささか不自然であり，通常とは異なる何らかのメッセージが QR コードの中に埋め込まれている可能性を示唆するので,ステガノグラフィ的な用途には向かない．

そこで，黒のモジュールと白のモジュールを QR コード画像全体に分散して配置することを考える．具体的には，前節の 2 枚の QR コードの生成に用いる符号語$\mathbf{c}_X$，$\mathbf{c}_Y$，$\mathbf{c}_Z$*の構成法において，ステップ(4)まで進めた後，X_1, Y_1, Z_1*以外のブロックを 1 つのブロックに統合して共通の置換を施したあと，値が決まっていない残りの 2t シンボルの値を消失訂正により決定するという方法をとる．

図２は，節で示した QR コードのシンボル配置を，黒と白が交互に配置されるような順序に入れ替えた例である．図２からはそれぞれ図１と同じ文字列を読み取ることができる．

図２　シンボルの順序を置換した QR_X, QR_Y とそれらの OR および QR_Z*（左から順に）

2-3 考察

（１）メッセージの可読性

節，節で生成した QR_X，QR_Y，QR_Z*は，Denso Wave 社製の iPhone/iPad アプリ``QRdeCode''，Android アプリ``QR コードスキャナー''，シャープ社製携帯電話 SH-02A，SH-08A でいずれも正しく復号できることを確認した．これらの実験では，機器に付属しているカメラを用いて各 QR コードを取り込んだ．

また，Windows 上のソフトウェア``Q 太郎''，``QR Code Editor''に QR コードのデータを直接処理させた場合にも，3 つの QR コードはいずれも復号できることを確認した．

一般には，QR_X，QR_Y は QR コードのもつ誤り訂正能力がそのまま残っているので，汎用のコードリーダを用いて素早く復号できるが，QR_Z*は誤り訂正能力を Mes_Z の復号のために使っていることもあり，復号に時間がかかる場合がある．特に上に載せる透明なシートの光の反射は大きな雑音要因となる．一般には，カメラの画素数が多く，タブレット端末など画像処理能力が高い機器を用いた方が，QR_Z から Mes_Z を安定して復号できる傾向が見られた．

以上の結果をもとに，節で述べた性質 P1，性質 P2 はともに満たされていると判断した．

（２）安全性

ここでは節で述べた性質 P3 について議論する．ここで想定する攻撃者は，QR_X または QR_Y のどちらか一方の QR コード画像を手に入れたと仮定し，これら 2 枚の生成方式について知っているとする．例えば，QR_X を入手した攻撃者は，符号語 $\mathbf{c}_Z$*で使われている Z_1*, R_2, $P_{Z*,2}$以外の値をすべて知ることができる．$P_{Z*,1}$, $P_{Z*,2}$ は Z_1*, R_1, R_2を用いて生成されるので，この攻撃者は自分がもつ $P_{Z*,1}$から Mes_Z に関する情報を得られる可能性がある．

本節では符号語 $\mathbf{c}_X$, , $\mathbf{c}_X$, が節で述べた方法で構成されているとする．また Mes_X，Mes_Y，Mes_Z は長さも含めて確率的に生成されるとする．このとき X_1, Y_1, Z_1*は確率変数になり，R_1, R_2も確率変数と見なす．$\mathbf{c}_X$, , $\mathbf{c}_X$, に共通に現れる文字列 U は固定であるとする．

次の定理は，性質 P3 がある条件のもとで満たされることを示している．エントロピー等の定義は[7]を参照のこと．証明は省略する．

定理１：$(X_1, Y_1), Z_1$*, (R_1, R_2)が独立であり，R_1,R_2 が独立で一様分布に従うとすると，提案手法について

$$H(Z_1^*|X_1\ R_1\ P_{Z*,1}) = H(Z_1^*)$$

$$H(Z_1^*|Y_1\ R_2\ P_{Z*,2}) = H(Z_1^*)$$

が成り立つ．ここに H(・)はエントロピー，H(・|・)は条件つきエントロピーを表す．

（３）埋め込み可能な情報量

QR コードから読み出せる文字数は，採用するモード，すなわち扱うことのできる文字の種類によって異なる．提案手法ではメッセージを書き込めるシンボルは t シンボルに限られるので，英数字モードを用いた場合に読み出すことができる文字数の上限は，3L 型で 7，4L 型で 11，5L 型で 15 となる．

5 型より大きい型の場合は，RS ブロックが 2 以上(符号語シンボル列が 2 つ以上の符号語をなす)になってより詳細な検討が必要になるが，データ列は複数の符号語のシンボルにインタリーブされるので各符号語を並列に考えることができ，原理的には読み出せる情報量の増加が見込める．英数字モードを用いた場合の文字数の上限は 6L 型で 20，7L 型で 23，8L 型で 29，9L 型で 37 になる．

提案手法で読み出すことのできる文字数は，通常の QR コードと比べると 10%程度に減少する(英数字モードの場合，3L～9L 型に埋め込める文字数はそれぞれ 77，114，154，195，224，279，335[5,表 7])．しかしながら，QR コードにはホームページの URL の情報を入れることが多く，2 つの異なる QR コードを重ねて復号

することで非公開の URL をもつホームページに誘導することも可能である．したがって，アプリケーションによっては情報量の少なさはあまり問題にならないこともある．

QR コードから読み出せる文字数を増やすためには，型を大きくせずに誤り訂正レベルを上げるという選択肢もある．ところが，M 型を用いると n-9t ≧0 の仮定が満たされず(4M 型の場合は RS ブロック数 2，n=50，t=9)，誤り訂正レベルを上げて読み出せる文字数を増やすアプローチをとることは，QR コードの仕様上，提案手法では不可能である．

3 Reed-Solomon 符号の検査行列に基づく秘密分散法とその安全性解析

3-1 研究の背景

Shamir の(k,n)しきい値法[1]は最も基本的な秘密分散法の 1 つであり，ディーラはランダムな k-1 次多項式を利用して，1 個の秘密情報から n 個のシェアを生成する．Shamir の(k,n)しきい値法は，任意の k 個のシェアから秘密情報が復元でき，逆にどんな k-1 個のシェアからも秘密情報が全く漏れない．McEliece and Sarwate[3]は Shamir の(k,n)しきい値法と Reed-Solomon 符号[2]の関連を指摘し，Karnin ら[4]は(k,n)しきい値法の情報理論的な定式化を行い，簡単な(n,n)しきい値法および行列形式の(k,n)しきい値法を提案している．

Shamir の(k,n)しきい値法はこれまで様々な形に拡張されてきた．1 つの代表的な拡張は，L 個(2 ≦ L ≦ k-1)の秘密情報から一括して n 個のシェアを生成するランプ型の秘密分散法であり，Blakley and Meadows [10]は Shamir 法を拡張したランダムな k-1 次の多項式を用いた方式を提案している．ランプ型秘密分散法については，従来から様々な研究が行われている．

本節では，ある種の連立 1 次方程式を用いた秘密分散法を定義し解析する．実際，本稿では，秘密情報 S と n 個のシェア $X_1, X_2, \ldots, X_n$ を連接した n+1 次元のベクトルが，ある(n+1)×(n-k+1)行列 B に対して $[S\ X_1 \cdots X_n]\ B = 0$ を満たすようにシェアを生成する．k-1 個のシェア $X_1, X_2, \ldots, X_{k-1}$ を一様乱数を用いて生成すれば，残りの n-k 個のシェアは n-k+1 次の連立 1 次方程式を解くことで計算できる．同様に，任意の k 個のシェアからも，n-k+1 次の連立 1 次方程式を解くことで S および残りのシェアを計算できる．

本方式は(k,n)しきい値法になることが容易に示され，Karnin らの(n,n)しきい値法[4]を特別な場合として含む．行列 B は短縮化 Reed-Solomon 符号(以下 RS 符号)で組織符号化を行う場合の検査行列に相当し，本方式は Shamir の(k,n)しきい値法の 1 つの双対な形式であると考えられる．

さらに，提案方式は L 個(2 ≦ L ≦ k-1)の秘密情報 S^Lを一括符号化するランプ型の方式に拡張することができる．拡張方式では，S^Lと $X_1, X_2, \ldots, X_n$ を連接した n+L 次元のベクトルと，ある行列 B の積が 0 になるように n 個のシェアを生成する．この拡張方式では，S^Lの分布によらず，任意の k 個のシェアから S^Lが復元されること，およびどの k-L 個のシェアからも S^Lの情報が一切漏れないこと，が示される．また，k-L+l 個(l=1,2,...,L-1)のシェアを与えたときの S^Lの条件つきエントロピーも，広い S^Lの分布クラスに対して解析できる．特に，秘密情報が一様分布に従い独立に生成されるときは，拡張方式は強ランプ型(k,L,n)しきい値法になることが示される．

3-1 (k,n)しきい値法

（1）定義

本節では(k,n)しきい値法を議論する．参加者集合を $\mathbf{P}=\{P_1, P_2, \ldots, P_n\}$ とし，n ≧ 2 を任意整数，k を 2 ≦ k ≦ n を満たす任意整数であるとする．本稿を通じて n と k は任意に固定しておく．また秘密情報を S，n 個のシェアを $X_1, X_2, \ldots, X_n$ と表す．$S, X_1, X_2, \ldots, X_n$ はいずれも有限体 GF(q)に値をとる確率変数である．シェア $X_1, X_2, \ldots, X_n$は，ディーラによって S および乱数を用いて生成される．各 i=1,2,...,n に対して，シェア X_i は参加者 P_iに，他の参加者に知られないように秘密裡に配布される．

(k,n)しきい値法を次のように定義する．k 個未満のどんなシェアからも秘密情報が全く漏れないこと，k 個以上のどんなシェアからも秘密情報が必ず復元できることを要請する．

定義 1 ((k,n)しきい値法)：秘密分散法が(k,n)しきい値法をなすとは，任意の $\{i_1, i_2, \ldots, i_m\} \subseteq \{1,2,\ldots,n\}$ に対して

$H(S|X_{i1}\ X_{i2} \cdots X_{im}) = H(S)$　(m＜k のとき)

$H(S|X_{i1}\ X_{i2}\ \cdots\ X_{im}) = 0$　　(m≧k のとき)
が成り立つことをいう.

（２）シェア生成・秘密情報復元のアルゴリズムと安全性

さて，秘密分散法を定義しよう．S と X_i, i=1,2,...,n が値をとる有限体のサイズ q は n<q-1 を満たすように選んでおく.

シェアの生成手順

(1) 与えられた秘密情報 S に対し，S と独立で一様分布に従う k-1 個の独立な確率変数 $U_1, U_2, ..., U_{k-1}$を生成する.

(2) $X_i = U_i$, i=1,2,...,k-1 とする.

(3) X_i, i=k,k+1,...,n を次式を満たすように定める.

$[\ S\ X_1\ \cdots\ X_n]\ B = [\ 0\ 0\ \cdots\ 0\ ]$

ここに B は，α を GF(q)の原始元として

$$B = \begin{vmatrix} 1 & 1 & \mathsf{L} & 1 \\ 1 & \alpha & \mathsf{L} & \alpha^{n-k} \\ \mathsf{M} & \mathsf{M} & \mathsf{O} & \mathsf{M} \\ 1 & \alpha^{n} & \mathsf{L} & \alpha^{n(n-k)} \end{vmatrix}$$

により定義される(n+1)×(n-k+1)行列であり，右辺は n-k+1 次元のゼロベクトルである.

(4) ステップ 2, 3 で求めた $X_1, X_2, ..., X_n$を出力する.

秘密情報の復元手順

(1) 与えられた k 個のシェア $X_{i1}\ X_{i2}\ \cdots\ X_{ik}$に対し，S および残りのシェアを$[\ S\ X_1\ \cdots\ X_n]\ B = [\ 0\ 0\ \cdots\ 0\ ]$を満たすように定める．行列 B の第 2 列は n < q-1 の仮定からすべて相異なるので，k 個の変数が既知ならば残りの n-k+1 個の変数は連立 1 次方程式を解くことにより求まる.

(2) ステップ 1 で求めた S を出力する.

この方式は定義１の意味で(k,n)しきい値法をなすことを示すことができる.

３-２ ランプ型秘密分散法への拡張

（１）ランプ型(k,L,n)しきい値法の定義

本節では，前節で述べた(k,n)しきい値法を，L 個の秘密情報 $S^L=(S_1, S_2, ..., S_L)$を一括して分散符号化する形に拡張し，その安全性を解析する．L は 1 ≦ L ≦ k-1 を満たす任意整数であり，n, k と同様に固定であるとする．以下ではS^Lについて，任意の 1≦ 1 ≦ L-1 と$\{j_1, j_2\ ...,\ j_L\}=\{1,2,...,L\}$に対して

$H(S_{j1+1}...S_{jL}|\ S_{j1}...S_{j1}) > 0$

を満たすことを仮定する．この仮定のもとでは，S^Lのいかなる部分情報からも S^L全体を決定することはできず，ランプ型秘密分散法の１つの健全性条件になっている.

我々は，ランプ型(k,L,n)しきい値法を次で定義する.

定義２ （ランプ型(k,L,n)しきい値法）：秘密分散法がランプ型(k,L,n)しきい値法をなすとは，任意の$\{i_1, i_2, ..., i_m\} \subseteq \{1,2,...,n\}$に対して次の３条件を満たすことをいう.

(C1) 0 ≦ m ≦ k-L のとき

$H(S^L|X_{i1}, X_{i2}, ..., X_{im}) = H(S^L)$.

(C2) k-L+1 ≦ m ≦ k-1 のとき

$0 < H(S^L|X_{i1}, X_{i2}, ..., X_{im}) < H(S^L)$.

(C3) k ≦ m のとき

$H(S^L|X_{i1}, X_{i2}, ..., X_{im}) = 0$.

条件(C1)は k-L 個以下のどんなシェアからも秘密情報が全く漏れないことを，条件(C3)は k 個以上のどんなシェアからも秘密情報が必ず復元できることを，それぞれ意味する．条件(C2)はシェアの数が n-L+1 個以上 k-1 個以下のときの要請であるが，この場合は S^Lが完全に復元できるわけでも，全く漏れないわけでもない．

（２）シェア生成・秘密情報復元のアルゴリズムと安全性

ディーラは次の手順に従って，S^Lと k-L 個の一様乱数 $U_1, U_2, \ldots, U_{k-L}$から n 個のシェア $X_1, X_2, \ldots, X_n$を生成する．有限体のサイズ q は n+L<q を満たすとする．

シェアの生成手順

(1) 与えられた秘密情報 S に対し，S と独立で一様分布に従う k-1 個の独立な確率変数 $U_1, U_2, \ldots, U_{k-L}$を生成する．

(2) $X_i = U_i$, i=1,2,...,k-L とする．

(3) X_i, i=k-L+1,k+1,...,n を次式を満たすように定める．

[S X_1 … X_n] B = [0 0 … 0]

ここに B は，α を GF(q)の原始元として

$$B = \begin{bmatrix} 1 & 1 & \mathsf{L} & 1 \\ 1 & \alpha & \mathsf{L} & \alpha^{n-k+L-1} \\ \mathsf{M} & \mathsf{M} & \mathsf{O} & \mathsf{M} \\ 1 & \alpha^{n+L-1} & \mathsf{L} & \alpha^{n(n-k+L-1)} \end{bmatrix}$$

により定義される(n+L)×(n-k+L)行列であり，右辺は n-k+L 次元のゼロベクトルである．

(4) ステップ 2, 3 で求めた $X_1, X_2, \ldots, X_n$を出力する．

秘密情報の復元手順

(1) 与えられた k 個のシェア X_{i1} X_{i2} … X_{ik}に対し，S および残りのシェアを[S X_1 … X_n] B = [0 0 … 0]を満たすように定める．行列 B の第 2 列は n+L < q の仮定からすべて相異なるので，k 個の変数が既知ならば残りの n-k+1 個の変数は連立 1 次方程式を解くことにより求まる．

(2) ステップ 1 で求めた S を出力する．

このアルゴリズムについて，我々は次の定理を示すことができる．

定理２：S^Lが上述の仮定を満たすとき，提案方式はランプ型(k,L,n)しきい値法をなす．

４．まとめ

本稿では，第２節でシェア画像として 2 枚の QR コードを用いる秘密分散法を構成した．汎用の QR コードリーダを用いることで，2 枚のシェア画像からはそれぞれのメッセージを，シェア画像を重ねて得られる画像からは秘密のメッセージを，それぞれ読み出すことができる．提案方式の安全性を議論し，ある条件のもとでは 1 枚のシェアからは秘密のメッセージは情報理論的な意味で全く漏れないことを示した．また提案手法において，埋め込むことができる文字数についても上限を与えた．

提案手法は QR コードを 2 枚のシェアとする秘密分散法の 1 つの実現法であるので，埋め込める文字数が多いより効率的な方式が存在する可能性は残されている．また，RS ブロック数が 2 以上の場合の性能を実験的に確認することも今後の研究課題となる．

第３節では短縮化 Reed Solomon 符号の組織符号化における検査行列を用いた(k,n)しきい値法を議論した．また，この(k,n)しきい値法を拡張し，L 個の秘密情報 S^Lを一括してシェアに分散符号化するランプ型の秘密分散法が構成できることを示した．議論した方式は[8]により言及された方式ではあるが，一般の S^Lの分布に対して，性能を詳細に解析したところに意義がある．

シェア生成および秘密情報復元のための計算量についての評価は今後の課題であるが,(k,n)しきい値法においてkとnが非常に近い（定数程度）場合に限れば，秘密情報復元のための計算量は，Karninらの方式[3]と同じくnの線形オーダとなり,Shamir法においてラグランジュの補間公式を用いた場合よりも高速になる．また，k個より多いシェアが集まった場合であってもそれらすべてのシェアを使うことでk個の場合よりも一般には高速に復号できるという特徴をもっている．

【参考文献】

[1] A. Shamir, ``How to share a secret,'' Communications of the ACM, vol.22, pp. 612--613, 1979.

[2] I. S. Reed and G.~Solomon, ``Polynomial codes over certain finite fields,'' J. SIAM, vol. 8, no. 2, pp. 300--304, 1960.

[3] R. J. McEliece and D. V. Sarwate, ``On sharing secrets and Reed-Solomon codes,'' Comm. of ACM, vol. 24, no. 9. pp. 583--584, 1981.

[4] E. D. Karnin, J. W. Greene, and M. E. Hellman, ``On secret sharing schemes,'' IEEE Trans. Inf. Theory, vol. IT-29, no. 1, pp. 35--41, 1983.

[5] JIS X 0510 ``二次元コードシンボル —QRコード— 基本仕様,'' 日本規格協会, 2004.

[6] M. Naor and A. Shamir, ``Visual cryptography,'' Advance in Cryptology-Eurocrypt '94, LNCS 950, pp. 1--12, Springer-Verlag, 1995.

[7] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, ``Extended capabilities for visual cryptography,'' Theoretical Computer Science, vol. 250, pp. 143--161, 2001.

[8] T. M. Cover and J. A. Thomas, Elements of Information Theory (2nd Ed.), Wiely-Interscience, 2006.

[9] G. R. Blakley and C. Meadows, ``Security of ramp schemes,'' Advances in Cryptology -- CRYPT0' 84, LNCS 196, pp.~242--269, 1985.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
H. Koga and S. Honjo, “A Secret Sharing Scheme Based on a Systematic Reed-Solomon Code and Analysis of its Security for a General Class of Sources	Proceedings of 2014 IEEE International Symposium on Information Theory	2014年7月
古賀，本庄，“短縮化 Reed-Solomon 符号の検査行列に基づく秘密分散法とその安全性解析”	第３６回情報理論とその応用シンポジウム予稿集	2013年11月
本庄，古賀，“２枚の二次元コードを用いた秘密分散法の一実現法”	電子情報通信学会和文論文誌 A, Vol. J98-A, no.2	2015年2月
坂下，古賀，本庄，“LT 符号を用いた高速なランプ型しきい値秘密分散法の検討”	電子情報通信学会研究技術報告（情報理論）	2014年3月
本庄，古賀，坂下，“MRD 符号を用いた強いランプ型秘密分散法の構成とその安全性評価”	電子情報通信学会研究技術報告（情報理論）	2014年3月