論　文

(k, L, n)しきい値秘密分散システム

正　員　山本　博資†

On Secret Sharing Systems Using (k, L, n) Threshold Scheme

Hirosuke YAMAMOTO†, *Member*

あらまし　(k, n)しきい値法では，情報Xがn個の部分情報に分割符号化され，そのn個から任意のk個の部分情報が得られれば，元の情報Xが完全に復元できるが，任意の$k-1$個の部分情報ではXに関して全く情報が得られない．このように，(k, n)しきい値法は情報を分散保管または分散伝送するのに適しているものの，各部分情報が元の情報Xと同じビット長を必要とし，符号化効率から考えると非常に効率が悪くなっている．本論文では，(k, n)しきい値法を拡張し，任意のk個の部分情報からは元の情報が完全に復元できるが，任意の$k-L$個では全くXの情報が得られず，任意の$k-t$個$(1 \leq t \leq L-1)$の部分情報では情報Xについて$(t/L)H(X)$のあいまいさが残るような秘密保護特性を持つ(k, L, n)しきい値法を提案する．(k, L, n)しきい値法では，各部分情報のビット長は情報Xの$1/L$でよく，非常に効率のよい符号化が行える．本論文では，(k, L, n)しきい値法を実現する(k, L, n)符号の構成法を示すと共に，その特性を明らかにする．

1. まえがき

盗聴者から情報を保護する一方式として，(k, n)しきい値法がShamir[1]により提案され，最近その実現方法や応用に関する研究が活発に行われている[2]~[11]．

(k, n)しきい値法は，情報X^Nをn個の部分情報に分割符号化して，保管または伝送する方式であり，その秘密保護特性は次のようである．n個のうち任意のk個の部分情報が得られれば情報X^Nは完全に復元できるが，任意の$(k-1)$個からではX^Nに関して全く何も情報が得られない．このように，(k, n)しきい値法を用いれば，$(k-1)$個まで部分情報が盗まれても，X^Nに関する情報が全く漏洩せず，また$(n-k)$個まで部分情報が破壊されてもX^Nを完全に復元できる特徴があり，暗号鍵の分散保管や複数の通信路を利用できる秘密情報伝送に適している．

しかし，(k, n)しきい値法を実現するためには，各部分情報のビット長は元の情報X^Nと同じだけ必要となり[3]，符号化効率から考えると非常に効率が悪くなっている．

本論文では，(k, n)しきい値法を拡張した(k, L, n)しきい値法を提案し，その実現符号化法を示す．(k, L, n)しきい値法は，n個の部分情報のうちの任意のk個が得られれば元の情報が完全に復元できるが，任意の$k-L$個では全くX^Nの情報が得られず，任意の$k-t$個$(1 \leq t \leq L-1)$の部分情報ではtが小さくなるにつれて，段階的にX^Nの情報が得られるような方式である．この(k, L, n)しきい値法を用いれば，各部分情報のビット長は元の情報X^Nの$1/L$でよく，(k, n)しきい値法に比べて，符号化効率が大きく改善される．例えば，$n=10$でしきい値をnの約1/2に設定したい場合には，$(5, 10)$しきい値法や$(6, 10)$しきい値法を用いるよりも，$(6, 2, 10)$しきい値法を用いれば，部分情報のビット長を半分にでき，かつ同程度の秘密保護特性を達成できる．

2.では(k, L, n)しきい値法を実現する符号として，(k, L, n)符号を定義し，その特性を明らかにする．**3.**では(k, n)しきい値法を実現するKarnin らの符号化法[3]を応用した(k, L, n)符号の構成法を示す．なお，秘密保護特性の評価は，従来の(k, n)しきい値法の場合と同様に，情報源を無記憶等確率とし，エントロピー関数を用いて評価している．また，**4.**では汎用計算機を用いる場合に適している2^Mを法とする剰余演算を用いて，(k, L, n)符号が実現できることを示す．

なお，$n=2, 3$の場合に関しては，各情報源出力シンボルが等確率で生起しないような，より一般的な場合において成立する符号化定理が文献[12]に示されている．また，文献[5]にはStone符号[13]を用いた拡張$(k,$

† 徳島大学工学部電子工学科，徳島市
Faculty of Engineering, Tokushima University, Tokushima-shi, 770 Japan

n)しきい値法が示されており，符号構成法に関しては，(k, L, n)しきい値法と本質的には等価なものとなっているが，文献(5)では主に誤り訂正を目的として拡張されている．

2. (k, L, n)しきい値法と(k, L, n)符号

情報源としてその出力 X_j ($j=0, \pm1, \pm2, \cdots$) が有限離散集合 $\mathcal{X}$ の値を取る離散的無記憶情報源を考える．$\mathcal{X}$ の要素数は $|\mathcal{X}|=q$ とし，簡単のため，q は素数または素数の累乗とする．また，$\mathcal{X}$ の各シンボルは全て等確率で生起するものとする．つまり，$j=0, \pm1, \pm2, \cdots$ に対して，情報源は次式を満たすものとする．

$$P_r\{X_j=x_i\}=\frac{1}{q},\quad x_i\in\mathcal{X},\quad i=1,2,\cdots,q \tag{1}$$

$$H(X_j)=\log q \tag{2}$$

この情報源に対して，符号 (f, ϕ) を次のように定義する．ただし，$N=mL$ ($1\leq L\leq k$) とする．

$$f:\mathcal{X}^N\rightarrow\prod_{j=1}^{n}\mathcal{W}_j^m \tag{3}$$

ϕ：任意の k 個の $\mathcal{W}_j^m$ の組に対して

$$\prod_{t=1}^{k}\mathcal{W}_{j_t}^m\rightarrow\mathcal{X}^N \tag{4}$$

つまり，$(\boldsymbol{W}_1^m, \boldsymbol{W}_2^m, \cdots, \boldsymbol{W}_n^m)=f(\boldsymbol{X}^N)$† であり，任意の k 個の部分情報（以後，単に符号語と呼ぶ）の組 $(\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_k}^m)$ に対して，$\boldsymbol{X}^N=\phi(\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_k}^m)$ である．なお，符号語 $\boldsymbol{W}_j^m=(W_{j_1}, W_{j_2}, \cdots, W_{j_m})$，$j=1, 2, \cdots, n$，の各シンボル W_{ji} ($i=1, 2, \cdots, m$) は集合 $\mathcal{W}_j$ の値を取り，$|\mathcal{W}_j|=q$ とする．

この時，各符号語 $\boldsymbol{W}_j^m$ ($j=1, 2, \cdots, n$) の効率 R_j は，式(3)より全て等しく

$$R_j=\frac{N}{m}=L,\quad j=1,2,\cdots,n \tag{5}$$

である．

この符号が満たすべき秘密保護能力として，次の (k, L, n) しきい値条件を考える．

［条件1］

$0\leq t\leq L$ の t に対して，任意の $k-t$ 個の符号語の組 $(\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m)$ が次式を満たす．

$$H(\boldsymbol{X}^N|\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m)=\frac{t}{L}H(\boldsymbol{X}^N)=tm\log q \tag{6}$$

† 本論文ではベクトルは全て横ベクトルである．

［条件2］

$1\leq t\leq L$ の t に対して，任意の $k-t$ 個の符号語の組 $(\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m)$ と，$\boldsymbol{X}^N=(\boldsymbol{X}_1^m, \boldsymbol{X}_2^m, \cdots, \boldsymbol{X}_L^m)$ の任意の t 個の組 $(\boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m)$ が次式を満たす．

$$H(\boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m|\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m)=\frac{t}{L}H(\boldsymbol{X}^N)=tm\log q \tag{7}$$

条件1を満たす符号 (f, ϕ) を (k, L, n) 符号と呼び，条件2も共に満たす (k, L, n) 符号を強い (k, L, n) 符号と呼ぶことにする．

［注1］ 式(6)の $t=0$ の場合より，(k, L, n) 符号を用いれば，任意の k 個の符号語からは $\boldsymbol{X}^N$ が完全に復号できる．また，$t=L$ の場合より，任意の $k-L$ 個の符号語からは $\boldsymbol{X}^N$ に関して全く何も情報が得られない．

［注2］ $L=1$ の場合の ($k, 1, n$) 符号は，(k, n) しきい値法を実現する k-out-of-n 符号[3]となる．

［注3］ 式(5)より，秘密保護特性のスレショールド幅である L が大きいほど，符号化効率がよくなる．例として，$q=2$，$N=100$ の場合の ($k, 1, n$) 符号 (C_1)，($k-1, 1, n$) 符号 (C_2)，($k, 2, n$) 符号 (C_3) を比較すると次のようになる．

○各符号語のビット数

C_1：100　　C_2：100　　C_3：50

○秘密保護特性（可能性のある $\boldsymbol{X}^N$ の個数）

符号語数が k 以上の時，

C_1：1　　C_2：1　　C_3：1

符号語数が $k-1$ の時，

C_1：$2^{100}(\approx10^{30})$　C_2：1　　C_3：$2^{50}(\approx10^{15})$

符号語数が $k-2$ 以下の時，

C_1：2^{100}　　C_2：2^{100}　　C_3：2^{100}

この例からもわかるように，$n\gg L$ の場合には，(k, L, n) しきい値法は (k, n) しきい値法とほぼ同程度の秘密保護特性を保ちながら，符号語長を $1/L$ にすることができる．また上の例で 2^{50} 個のあいまいさが秘密保護に対して十分であると考えられる場合には，($k, 2, n$) 符号は ($k, 1, n$) 符号と実質的に同じ秘密保護能力があると見なせる．つまり，$q^{N/L}$ が十分大きい場合には，(k, L, n) しきい値法は $1/L$ の符号語長で (k, n) しきい値法と実質的に同じ秘密保護能力を達成できる．

［注4］ 弱い (k, L, n) 符号では，$t<L$ の場合に $k-t$ 個の符号語から $\boldsymbol{X}^N$ の一部が完全に復元できる可能性がある．しかし，強い (k, L, n) 符号では，式(7)より，$\boldsymbol{X}^N$ のどの部分に対しても一様に $(t/L)H(\boldsymbol{X}^N)$

のあいまいさに保つことができる．したがって，強い(k, L, n)符号の方が弱い(k, L, n)符号よりも望ましいが，X^Nが全てそろって初めて意味を持つ場合には，弱い(k, L, n)符号でもよい．

次に，符号(f, ϕ)が式(6)，(7)より大きいあいまいさを達成できないという意味で，上記の(k, L, n)符号が最適であることを示す．

［定理1］

符号(f, ϕ)が$t=0$で式(6)を満たすならば，$1\leq t\leq L$に対して，任意の$k-t$個の符号語の組($W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m$)は次式を満たす．

$$H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m) \leq (t/L)H(X^N) \quad (8)$$

（証明）

$1\leq t\leq L$のtに対して，次式が成り立つ．

$$\begin{aligned}
&H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m)\\
&\quad = H(X^N, W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m)\\
&\qquad - H(W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m)\\
&\quad \geq H(X^N, W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m)\\
&\qquad - H(W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m)\\
&\qquad - H(W_{j_{k-t}}^m \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m)\\
&\quad = H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m)\\
&\qquad - H(W_{j_{k-t}}^m \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m)\\
&\quad \geq H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m) - H(W_{j_{k-t}}^m)\\
&\quad \geq H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t-1}}^m) - m\log q \quad (9)
\end{aligned}$$

したがって

$$H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_k}^m) = 0 \quad (10)$$

の時，$1\leq t\leq L$のtに対して，次式が成り立つ．

$$\begin{aligned}
&H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m)\\
&\quad \leq H(X^N \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_k}^m) + tm\log q\\
&\quad = tm\log q = (t/L)H(X^N) \quad (11)
\end{aligned}$$

（証明終）

条件2に関しても，

$$\begin{aligned}
&H(X_{s_1}^m, X_{s_2}^m, \cdots, X_{s_t}^m \mid W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_{k-t}}^m)\\
&\quad \leq (t/L)H(X^N) \quad (12)
\end{aligned}$$

が成立することは式(8)より明らかである．

3. (k, L, n)符号の構成法

強い(k, L, n)符号には，文献(3)で示されているL個の情報を一度に符号化する$k-\text{out}-\text{of}-n$符号を利用することができる†．

まず，次のような符号を考える．GF(q)上の$km\times m$行列A_s($s=1, 2, \cdots, L$)とB_j($j=1, 2, \cdots, n$)を用意する．与えられた$X^N=(X_1^m, X_2^m, \cdots, X_L^m)$に対して，

$$X_s^m = U^{km}A_s, \quad s=1, 2, \cdots, L \quad (13)$$

を満たす範囲内でランダムにkm次元ベクトルU^{km}を決定する．符号語W_j^mは

$$W_j^m = U^{km}B_j, \quad j=1, 2, \cdots n \quad (14)$$

により定められる．A_s($s=1, 2, \cdots, L$)，B_j($j=1, 2, \cdots, n$)は公開されているものとする．

$$G=[A_1, A_2, \cdots, A_L, B_1, B_2, \cdots, B_n] \quad (15)$$

とすると

$$(X_1^m, X_2^m, \cdots, X_L^m, W_1^m, W_2^m, \cdots, W_n^m) = U^{km}G \quad (16)$$

と表わせる．この符号をUG型符号と呼ぶ．このUG型符号に関して次の定理が成り立つ．

［定理2］

UG型符号が強い(k, L, n)符号であるための必要十分条件は，$\{A_1, A_2, \cdots, A_L, B_1, B_2, \cdots, B_n\}$から選んだ任意の$k$個の行列$\{C_{j_1}, C_{j_2}, \cdots, C_{j_k}\}$が

$$\text{rank}[C_{j_1}, C_{j_2}, \cdots, C_{j_k}] = km \quad (17)$$

を満たすことである．また，弱い(k, L, n)符号となるための必要十分条件は，$\{B_1, B_2, \cdots, B_n\}$から選んだ任意の$k$個の行列$\{B_{j_1}, B_{j_2}, \cdots, B_{j_k}\}$が

$$\text{rank}[B_{j_1}, B_{j_2}, \cdots, B_{j_k}] = km \quad (18)$$

を満たし，かつ$\{B_1, B_2, \cdots, B_n\}$から選んだ任意の$k-L$個の行列$\{B_{j_1}, B_{j_2}, \cdots, B_{j_{k-L}}\}$が

$$\text{rank}[A_1, A_2, \cdots, A_L, B_{j_1}, B_{j_2}, \cdots, B_{j_{k-L}}] = km \quad (19)$$

を満たすことである．

（証明）

まず，式(18)，(19)が満たされれば条件1が成り立つことを示す．

任意のk個の行列の組$\{B_{j_1}, B_{j_2}, \cdots, B_{j_k}\}$が式(18)を満たすことより，

$$U^{km} = [W_{j_1}^m, W_{j_2}^m, \cdots, W_{j_k}^m][B_{j_1}, B_{j_2}, \cdots, B_{j_k}]^{-1} \quad (20)$$

でU^{km}が求まり，式(13)を用いてX^Nが求まる．ゆえに，式(6)が$t=0$の場合に成り立つ．

次に$1\leq t\leq k$の場合を考える．式(13)を満たすU^{km}の個数は，各$x^N\in\mathcal{X}^N$に対して$q^{(k-L)m}$個存在し，かつそれらが等確率でランダムに選ばれる．ゆえに，

$$H(U^{km} \mid X^N) = \sum_{x^N} P_r(x^N)H(U^{km} \mid x^N) = (k-L)m\log q$$

が成り立つ．式(13)よりX^NはU^{km}から一意に定まるので，

$$\begin{aligned}
H(U^{km}) &= H(U^{km}X^N) = H(X^N) + H(U^{km} \mid X^N)\\
&= H(X^N) + (k-L)m\log q \quad (21)
\end{aligned}$$

が成立する．さらに，この不等式より次式が得られる．

† 文献(3)では$t=0$と$t=1$の場合に条件1，2を満たすことが示されている．

$$
\begin{aligned}
&H(\boldsymbol{X}^N \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\quad \geq I(\boldsymbol{X}^N ; \boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\quad = H(\boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\qquad - H(\boldsymbol{U}^{km} \mid \boldsymbol{X}^N, \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
(*1)\quad &\quad = H(\boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\quad \geq H(\boldsymbol{U}^{km}) - \sum_{s=1}^{k-t} H(\boldsymbol{W}_{j_s}^m) \\
&\quad \geq H(\boldsymbol{U}^{km}) - (k-t) m \log q \\
(*2)\quad &\quad \geq H(\boldsymbol{X}^N) + (L-t) m \log q \\
&\quad = t m \log q \\
&\quad = (t/L) H(\boldsymbol{X}^N)
\end{aligned}
\qquad (22)
$$

ここで，（*1）は式(18)に，また（*2）は式(21)による．式(8)，(22)より式(6)が成り立つ．

同様に式(17)が満たされていれば次式が成り立つ．

$$
\begin{aligned}
&H(\boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\quad \geq I(\boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m ; \boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\quad = H(\boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\qquad - H(\boldsymbol{U}^{km} \mid \boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m, \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
(*3)\quad &\quad = H(\boldsymbol{U}^{km} \mid \boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m) \\
&\qquad \geq t m \log q \\
&\qquad = (t/L) H(\boldsymbol{X}^N)
\end{aligned}
\qquad (23)
$$

ここで(*3)は式(17)による．式(12)，(23)より式(7)が成り立つ．

また逆に，式(18)，(19)が成立しなければ，式(6)を満たさない（$\boldsymbol{W}_{j_1}^m, \boldsymbol{W}_{j_2}^m, \cdots, \boldsymbol{W}_{j_{k-t}}^m$）が存在し，式(17)が成立しなければ式(7)を満たさない（$\boldsymbol{X}_{s_1}^m, \boldsymbol{X}_{s_2}^m, \cdots, \boldsymbol{X}_{s_t}^m$）が存在することを容易に示せる．　（証明終）

さらに行列 $\{A_1, A_2, \cdots, A_L, B_1, B_2, \cdots, B_{k-L}\}$ の選び方に関して次の定理が成り立つ．

［定理3］

一般性をなくすことなく

$$
A_s = \begin{bmatrix} 0_m \\ \vdots \\ 0_m \\ I_m \\ 0_m \\ \vdots \\ 0_m \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} 0_m \\ \vdots \\ 0_m \end{matrix}}\right\} s-1 \text{個} \\ \\ \\ \\ \\ \end{matrix}, \quad B_j = \begin{bmatrix} 0_m \\ \vdots \\ 0_m \\ I_m \\ 0_m \\ \vdots \\ 0_m \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} 0_m \\ \vdots \\ 0_m \end{matrix}}\right\} L+j-1 \text{個} \\ \\ \\ \\ \\ \end{matrix} \qquad (24)
$$

$s = 1, 2, \cdots, L$　　$j = 1, 2, \cdots, k-L$

とできる．ここで，0_m および I_m は $m \times m$ のゼロ行列および単位行列である．

（証明）　省略（文献(3)のTh. 3と同様）

定理3より，$\boldsymbol{U}^{km}$ は $\boldsymbol{U}^{km} = (\boldsymbol{X}_1^m, \boldsymbol{X}_2^m, \cdots, \boldsymbol{X}_L^m, \boldsymbol{Z}_1^m, \boldsymbol{Z}_2^m, \cdots, \boldsymbol{Z}_{k-L}^m)$ とできる．ただし，$\boldsymbol{Z}_j^m = (Z_{j_1}, Z_{j_2}, \cdots, Z_{j_m})$，$j = 1, 2, \cdots, k-L$，の Z_{j_l}，$l = 1, 2, \cdots, m$ は GF(q) 上の一様乱数である．

定理2より（k, L, n）符号を求めるには，式(17)または式(18)，(19)を満たす行列の組 $\{A_1, A_2, \cdots, A_L, B_1, B_2, \cdots, B_n\}$ を求めればよい．k，L，q，mが与えられた時の可能なnの最大値を$n_{\max}$とすると，強い（k, L, n）符号に関しては文献(3)のTh. 4より，$n_{\max}$は次の定理を満たす．

［定理4］

UG型符号を用いて強い（k, L, n）符号を構成した時，$n_{\max}$は次式を満たす．

$q^m > k$ の時，　$q^m - L + 1 \leq n_{\max} \leq q^m + k - L - 1$　(25)

$q^m \leq k$ の時，　$n_{\max} = k - L + 1$　(26)

（証明）　省略（文献(3)のTh. 4より明らか）

式(26)で示された$n_{\max}$の下限は $G = [A_1, A_2, \cdots, A_L, B_1, B_2, \cdots, B_n]$ を式(27)のように選べば達成できる†．ただし，$m = 1$ としてある．$m > 1$ の場合は式(27)の各要素 β ($= 0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-1}$) の代わりに，$\beta I_m$を用いればよい．また，$\alpha$ は GF(q) の原始元である．

$$
G = \begin{bmatrix}
1 & 0 & 1 & 1 & \cdots\cdots & 1 \\
0 & 0 & \alpha & \alpha^2 & \cdots\cdots & \alpha^{q-1} \\
0 & 0 & \alpha^2 & \alpha^4 & \cdots\cdots & \alpha^{(q-1)2} \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots\cdots & \alpha^{(q-1)(k-1)}
\end{bmatrix} \qquad (27)
$$

一方，弱い（k, L, n）符号に関しては次の限界が成り立つ．

［定理5］

UG型符号を用いて弱い（k, L, n）符号を作った時，$n_{\max}$は次式を満たす．

$L = k$，

$q^m > k$ の時，　$q^m + 1 \leq n_{\max} \leq q^m + k - 1$　(28)

$q^m \leq k$ の時，　$n_{\max} = k + 1$　(29)

$L = k - 1$，

$q^m > k$ の時，　$q^m \leq n_{\max} \leq q^m + k - 1$　(30)

$q^m \leq k$，

$q^m \neq 2$ の時，　$n_{\max} = k + 1$　(31)

$q^m = 2$，kが奇数の時，　$n_{\max} = k + 1$　(32)

$q^m = 2$，kが偶数の時，　$n_{\max} = k$　(33)

$1 < L < k - 1$，

$q^m > k$ の時，　$q^m + 1 \leq n_{\max} \leq q^m + k - 1$　(34)

$k - 1 \leq q^m \leq k$ の時，　$k \leq n_{\max} \leq k + 1$　(35)

$\max(L, k-L) < q^m < k - 1$ の時，　$n_{\max} \leq k + 1$

† 式(27)を用いて構成できるUG型符号はShamirの多項式補間法による符号[1]を包含している[3],[6]．

(36)

$q^m \leq \max(L, k-L)$ の時，存在しない．

$L=1$，

$q^m > k$ の時，　$q^m+1 \leq n_{\max} \leq q^m+k-1$　(37)

$q^m \leq k$ の時，　$n_{\max}=k$　(38)

（証明）　付録に記す．

4. 2^Mを法とする剰余演算による(k, L, n)符号および疑似(k, L, n)符号

式(27)や式(A·3)～(A·9)などの行列を用いれば(k, L, n)符号を作れるが，演算は全てGF(q)上の演算を行わなければならない．Nが大きい場合にはかなり複雑な演算となる．(k, L, n)符号では復号器を ${}_nC_k$ 通り用意する必要があり，符号化・復号化の演算はより容易なことが望まれる．

そこで本章では，実用上重要な$q=2^M$の場合に対して，汎用計算機などで容易に計算できる2^Mを法とする剰余演算のみを用いた(k, L, n)符号の構成法を考える．簡単のために$m=1$とする．$m>1$の場合も同様に行える．

例として最も簡単な(2, 1, 2)符号，すなわち2-out-of-2符号を考える．この時，定理3，4より，行列Gとして

$$G=\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix} \quad (39)$$

を，また$\boldsymbol{U}$として$\boldsymbol{U}=(X, Z)$を用いることができる．ただし，情報XはX∈GF(2^M)であり，ZはGF(2^M)上の一様乱数である．この時，符号化は次のようになる．

$$W_1=Z \quad (40)$$

$$W_2=X+Z \quad (41)$$

ここで，＋はGF(2^M)上の加算である．復号は

$$X=W_2-W_1 \quad (42)$$

で行える．ただし，－はGF(2^M)上の減算である．この例のように行列Gが{0, 1}の要素のみで構成されている時は，加減算のみが用いられるので，体でなく加法群でも十分である．そこで，加法群をなす2^Mを法とする剰余演算を用いると(2, 1, 2)符号は次のように構成できる．ただし，$X, Z \in \mathcal{J}_{2^M} \triangleq \{0, 1, 2, \cdots, 2^M-1\}$で，Zは$\mathcal{J}_{2^M}$上の一様乱数である．

符号化：
$$\begin{cases} W_1=Z & (43)\\ W_2=(X+Z) \bmod 2^M & (44)\end{cases}$$

復号化：　$X=(W_2-W_1) \bmod 2^M$　(45)

このように2^Mを法とする剰余演算による強いあるいは弱い(k, L, n)符号が存在するためには，GF(2)の上で式(17)あるいは式(18)，(19)を満たす行列Gが存在すればよい．

強い(k, L, n)符号に関しては，定理4の式(26)より，

$$k \leq n_{\max}=k-L+1 \quad (46)$$

を満たさなければならないので，

$$n=k, \quad L=1 \quad (47)$$

の場合に存在する．また，弱い(k, L, n)符号に関しては，定理5より次の場合に存在する．

$L=1$，$2 \leq k$の時，　$n=k$　(48)

$L=k-1$が偶数の時，　$n=k, k+1$　(49)

$L=k-1$が奇数の時，　$n=k$　(50)

$L=k \geq 2$の時，　$n=k, k+1$　(51)

このように式(47)～(51)を満たす(k, L, n)に対しては2^Mを法とする剰余演算による(k, L, n)符号が構成できるが，その他の(k, L, n)に対しては2^Mを法とする剰余演算による(k, L, n)符号の構成は困難であると思われる．しかし，式(47)～(51)以外の(k, L, n)に対しても以下に示すように，ほぼ(k, L, n)符号の条件を満たす符号を，2^Mを法とする剰余演算を用いて構成できる．

2^Mを法とする剰余演算を行った時，乗算の逆元は一意に決まらない．しかし，

$$a \cdot b \mod 2^M=c \quad (52)$$

においてa, c ($\in \mathcal{J}_{2^M}$)が与えられた時，上式を満たす可能性のあるbの個数はa以下である．そこで{0, 1}以外にはなるべく小さな自然数を要素として持ち，式(17)または式(18)，(19)を満たす行列Gを用いれば，2^Mを法とする剰余演算を用いてもほぼ(k, L, n)符号の条件（式(6)または式(7)）を満たす符号を構成できることが期待できる．

例として(2, 1, 3)符号，つまり2-out-of-3符号を考える．G，$\boldsymbol{U}$として次のものを用いる．

$$G=\begin{bmatrix}1&0&1&1\\0&1&1&2\end{bmatrix} \quad (53)$$

$$\boldsymbol{U}=[X, Z] \quad (54)$$

ただし，情報XはX∈$\mathcal{J}_{2^M}$で，Zは$\mathcal{J}_{2^M}$上の一様乱数とする．この時，符号化は次式で行なわれる．

$$W_1=Z \quad (55)$$

$$W_2=(X+Z) \bmod 2^M \quad (56)$$

$$W_3=(X+2Z) \bmod 2^M \quad (57)$$

この符号は次式のあいまいさを満たす．

$$H(X|W_1)=H(X|W_2)=M \quad (58)$$

$$H(X|W_3)=M-1 \quad (59)$$

$$H(X|W_iW_j)=0 \quad i \neq j, \quad i, j=1, 2, 3 \quad (60)$$

式(59)を除き，他は全て（2，1，3）符号の条件を満たしている．$H(X|W_3)$は$M-1$とMより1だけ小さくなっているが，Mがある程度以上大きければ実質的に（2，1，3）符号と同じ秘密保護能力を有している．

このような（k，L，n）符号の条件を完全には満たしてはいないが，実用上（k，L，n）符号として使える符号を疑似（k，L，n）符号と呼ぶ．

疑似（k，L，n）符号を用いれば式(47)～(51)以外のいろいろな（k，L，n）に対しても，2^Mを法とする剰余演算を用いて符号が構成できる．しかし，行列Gの選び方によっては条件1の式(6)を$t=0$で完全に満たさないことがある．そのような場合には，あるk個の符号語を用いてもX^Nが一意に求まらない．必ず任意のk個の符号語でX^Nが完全に復号できるような疑似（k，L，n）符号を求めるためには，Gの決め方に注意を要する．

以下に，2^Mを法とした剰余演算を用いた（k，L，n）符号および疑似（k，L，n）符号用の行列Gを，kが5以下の場合に対して示す．ただし，疑似（k，L，n）符号に関しては任意のk個の符号語で一意に復号できるものを選んであり，行列の要素には{0，1}以外に{2，3}を許してある．G^S_{kL}は強い（k，L，n）符号用であり，G^W_{kL}は弱い（k，L，n）符号用である．また，各G_{kL}に対して適用可能なnの長さも合せて示してある．＊印が付いたものは疑似（k，L，n）符号となる．これらの行列から（k，L，n）符号を作るには，G_{kL}の第$L+1$列から第$L+n$列までの小行列をgとした時，符号語は

$$[W_1, W_2, \cdots, W_n] = [X_1, X_2, \cdots, X_L, Z_1, Z_2, \cdots, Z_{k-L}]\,g \qquad (61)$$

で求まる．ただし，加算は2^Mを法とする剰余をとる．また，$X_i, Z_i \in \mathcal{S}_{2^M}$であり，$Z_i$は$\mathcal{S}_{2^M}$上の一様乱数である．

$$G^S_{21}=\begin{bmatrix}1&0&1&1\\0&1&1&2\end{bmatrix}\quad(n=2,3^*)\qquad G^S_{22}=\begin{bmatrix}1&0&1&1&2\\0&1&1&2&1\end{bmatrix}\quad(n=2^*,3^*)$$

$$G^W_{22}=\begin{bmatrix}1&0&1&0&1\\0&1&0&1&1\end{bmatrix}\quad(n=2,3)$$

$$G^S_{31}=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}\quad(n=3)\qquad G^S_{32}=\begin{bmatrix}1&0&0&1&1\\0&1&0&1&2\\0&0&1&1&3\end{bmatrix}\quad(n=3^*)$$

$$G^S_{33}=\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&2&3\\0&0&1&1&3&2\end{bmatrix}\quad(n=3^*)$$

$$G^W_{32}=\begin{bmatrix}1&0&1&0&0&1\\0&1&0&1&0&1\\0&0&1&1&1&1\end{bmatrix}\quad(n=3,4)$$

$$G^W_{33}=\begin{bmatrix}1&0&0&1&0&0&1\\0&1&0&0&1&0&1\\0&0&1&0&0&1&1\end{bmatrix}\quad(n=3,4)$$

$$G^S_{41}=\begin{bmatrix}1&0&0&0&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&1&1\end{bmatrix}\quad(n=4)$$

$$G^W_{42}=\begin{bmatrix}1&0&0&0&1&1\\0&1&0&0&1&2\\0&0&1&0&1&1\\0&0&0&1&1&2\end{bmatrix}\quad(n=4^*)$$

$$G^W_{43}=\begin{bmatrix}1&0&0&1&0&0&0&1\\0&1&0&0&1&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&1&1&1&2\end{bmatrix}\quad(n=4,5^*)$$

$$G^W_{44}=\begin{bmatrix}1&0&0&0&1&0&0&0&1\\0&1&0&0&0&1&0&0&1\\0&0&1&0&0&0&1&0&1\\0&0&0&1&0&0&0&1&1\end{bmatrix}\quad(n=4,5)$$

$$G^S_{51}=\begin{bmatrix}1&0&0&0&0&1\\0&1&0&0&0&1\\0&0&1&0&0&1\\0&0&0&1&0&1\\0&0&0&0&1&1\end{bmatrix}\quad(n=5)$$

$$G^W_{52}=\begin{bmatrix}1&0&0&0&0&1&1&2\\0&1&0&0&0&1&2&1\\0&0&1&0&0&1&1&3\\0&0&0&1&0&1&2&2\\0&0&0&0&1&1&3&1\end{bmatrix}\quad(n=5^*,6^*)$$

$$G^W_{53}=\begin{bmatrix}1&0&0&0&0&1&1&0\\0&1&0&0&0&1&0&1\\0&0&1&0&0&1&0&0\\0&0&0&1&0&1&1&1\\0&0&0&0&1&1&2&2\end{bmatrix}\quad(n=5^*)$$

$$G^W_{54}=\begin{bmatrix}1&0&0&0&1&0&0&0&0&1\\0&1&0&0&0&1&0&0&0&1\\0&0&1&0&0&0&1&0&0&1\\0&0&0&1&0&0&0&1&0&1\\0&0&0&0&1&1&1&1&1&1\end{bmatrix}\quad(n=5,6)$$

$$G_{55}^{W}=\begin{bmatrix}1&0&0&0&0&1&0&0&0&0&1\\0&1&0&0&0&0&1&0&0&0&1\\0&0&1&0&0&0&0&1&0&0&1\\0&0&0&1&0&0&0&0&1&0&1\\0&0&0&0&1&0&0&0&0&1&1\end{bmatrix}\quad(n=5,\ 6)$$

5. むすび

本論文では情報を分散保管または分散伝送するのに適している(k, n)しきい値法を拡張した(k, L, n)しきい値法を提案し，それを実現する(k, L, n)符号の構成方法を示した．(k, L, n)しきい値法を用いれば，(k, n)しきい値法と実用上ほぼ同じ程度の秘密保護特性を保ちながら各部分情報のビット長を$1/L$にすることができ，非常に効率のよい符号化が行える．

(k, L, n)符号は(k, n)しきい値法を実現するk-out-of-n符号と同じ程度の複雑さで符号化・復号化が行えるため，現在(k, n)しきい値法の応用が考えられている分野にそのまま(k, L, n)しきい値法が適用できるものと思われる．

文　献

(1) A. Shamir: "How to share a secret", Commun. ACM, 22, pp. 612-613 (Nov. 1979).
(2) R. J. McEliece and D.V. Sarwate: "On sharing secrets and Reed-Solomon codes", Commun. ACM, 24, pp. 583-584 (Sept. 1981).
(3) E.D. Karnin, J.W. Greene and M.E. Hellman: "On secret sharing systems", IEEE Trans. Inf. Theory, IT-29, 1, pp. 35-41 (Jan. 1983).
(4) C. Asmuth and J. Bloom: "A modular approach to key safeguarding", IEEE Trans. Inf. Theory, IT-29, 2, pp. 208-210 (March 1983).
(5) 松見，常盤，笠原，滑川，田中："代数的誤り訂正符号を用いた情報分散保管問題に関する理論的，実験的検討"，信学技報，IT84-8(昭59-05).
(6) 松見，常盤，笠原，滑川："(K, N)しきい値法に関する諸考察"，情報理論とその応用研究会，第7回シンポジウム資料，pp. 158-163 (昭59-11).
(7) 山口，今井："Stone符号に関する一考察"，信学技報，IT84-27 (昭59-07).
(8) 山口，今井："Stone符号の復号法とその応用"，情報理論とその応用研究会，第7回シンポジウム資料，pp. 36-40 (昭59-11).
(9) 小山謙二："複数グループ間の暗号鍵共有法とその解析"，情処学論，22, 2, pp. 81-88 (昭56-03).
(10) K. Koyama: "Cryptographic key sharing methords for multi-groups and security analysis", Trans. IECE Japan (Section E), E66, 1, pp. 13-20 (Jan. 1983).
(11) 松井甲子雄："k-out-of-N個人識別方式によるファイル管理システム"，情処学論，25, 3, pp. 351-356 (昭59-05).
(12) H. Yamamoto: "On secret sharing communication systems with two or three channels", IEEE Trans. Inf. Theory (to apper).
(13) J. J. Stone: "Multiple-furst error correction with the Chinese remainder theorem", J. SIAM, 11, 1, pp. 74-81 (March 1963).

付　録

定理5の証明

○ n_{max}の上界式

式(18)が成立するためには，文献(3)のTh. 4とCor. 1の証明より，n_{max}は次式を満たさなければならない(文献(3)のTh. 4の$n_{max}+1$をn_{max}に置き換えればよい)．

$q^m > k$の時，　$n_{max} \leq q^m + k - 1$　(A·1)

$q^m \leq k$の時，　$n_{max} \leq k + 1$　(A·2)

○ n_{max}の下界式

n_{max}の下界は行列Gを次のように選ぶことで達成できる．ただし，$m=1$としてある．$m>1$の場合は行列Gの各要素β($=0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-1}$)の代わりに$\beta I_m$を用いればよい．

$L=k$,

$q^m > k$の時，

$$G=\begin{bmatrix}&0&1&\\&0&0&\\I_k&\vdots&\vdots&H_{00}\\&0&0&\\&1&0&\end{bmatrix}\qquad(A\cdot3)$$

ただし，H_{st}は次の行列である．

$$H_{st}=\begin{bmatrix}1&1&\cdots\cdots\cdots\cdots&1\\\alpha&\alpha^2&\cdots\cdots\cdots\cdots&\alpha^{q-1-t}\\\alpha^2&\alpha^4&\cdots\cdots\cdots\cdots&\alpha^{(q-1-t)2}\\\vdots&\vdots&&\\\alpha^{k-1-s}&\alpha^{2(k-1-s)}&\cdots\cdots&\alpha^{(q-1-t)(k-1-s)}\end{bmatrix}\qquad(A\cdot4)$$

$q^m \leq k$の時，

$$G=\begin{bmatrix}&&1\\&&1\\I_k&I_k&\vdots\\&&1\end{bmatrix}\qquad(A\cdot5)$$

$L=k-1$,

$q^m > k$の時，

$$G=[\,I_k\ \ H_{00}\,]\qquad(A\cdot6)$$

$q^m \leq k$の時，

$$G=\begin{bmatrix} & & 0\ 1 \\ & & 0\ 1 \\ I_{k-1} & I_{k-1} & \\ & & 0\ 1 \\ 0\ 0\cdots\cdots 0\ 1\ 1\cdots\cdots 1\ 1\ X \end{bmatrix} \qquad (A\cdot 7)$$

ここで，Xは0および1+1+…+1（L回1を加算）以外のGF(q)の元．$q=2$でかつkが偶数（Lが奇数）の時は，そのような元Xは存在しない．その他の場合は必ず存在する．

$1<L<k-1$，

$q^m>k$の時，

$$G[\ I_k\ \ H_{00}\ ] \qquad (A\cdot 8)$$

$q^m=k$の時，

$$G=\left[\begin{array}{c|cc} I_L & I_L & \begin{matrix}0\cdots\cdots 0\\ \vdots\quad\ \vdots\\ 0\cdots\cdots 0\end{matrix} \\ \hline \begin{matrix}0\cdots\cdots 0\\ \vdots\quad\ \vdots\\ \vdots\quad\ \vdots\\ \vdots\quad\ \vdots\\ 0\cdots\cdots 0\end{matrix} & \begin{matrix}1\ 0\\ 0\ 0\\ \vdots\ \vdots\\ 0\ 0\\ 0\ 1\end{matrix} & H_{L1} \end{array}\right] \qquad (A\cdot 9)$$

$q^m=k-1$の時，

$$G=\left[\begin{array}{c|cc} I_L & I_L & \begin{matrix}0\cdots\cdots 0\\ \vdots\quad\ \vdots\\ 0\cdots\cdots 0\end{matrix} \\ \hline \begin{matrix}0\cdots\cdots 0\\ \vdots\quad\ \vdots\\ \vdots\quad\ \vdots\\ \vdots\quad\ \vdots\\ 0\cdots\cdots 0\end{matrix} & \begin{matrix}1\ 0\\ 0\ 0\\ \vdots\ \vdots\\ 0\ 0\\ 0\ 1\end{matrix} & H_{L0} \end{array}\right] \qquad (A\cdot 10)$$

$q^m\leq\max(L, k-L)$の時，

定理3より次のような行列を考えればよい．

$$G=\left[\begin{array}{c|c} I_L & A \\ \hline \begin{matrix}0\cdots\cdots 0\\ \vdots\quad\ \vdots\\ 0\cdots\cdots 0\end{matrix} & B \end{array}\right] \qquad (A\cdot 11)$$

式(19)を満たすためには，式(A・11)の部分行列Bの任意の$k-L$列が一次独立でなければならないが，文献(3)のTh. 3より，$q^m\leq k-L$の時，Bの一次独立な列の最大個数は$k-L+1$個となり

$$n_{\max}\leq k-L+1<k \qquad (A\cdot 12)$$

となる．また，$q^m\leq L$の時には，Bの一次独立な列の最大個数は$q^m+k-L-1$個以下となり

$$n_{\max}\leq q^m+k-L-1\leq k-1<k \qquad (A\cdot 13)$$

となる．これは

$$n_{\max}\geq k \qquad (A\cdot 14)$$

に矛盾する．よって，式(19)を満たす行列Gは存在しない．

$L=1$，

この場合は強い(k, L, n)符号と一致するので，

$q^m>k$の時，　$q^m\leq n_{\max}\leq q^m+k-2$　(A・15)

$q^m\leq k$の時，　$n_{\max}=k$　(A・16)

となる．　（証明終）

（昭和60年1月9日受付，4月15日再受付）

山本　博資

昭50静岡大学工学部電気工学科卒業．昭55東京大学大学院工学系研究科博士課程修了．同年徳島大学工学部電子工学科助手．現在，同助教授．主に，通信路符号，情報源符号，暗号などにおけるシャノン理論の研究，および電子回路，マイコン応用などの研究に従事．IEEE会員，工学博士．