1F-3

直交配列に基づく AND 結託耐性符号のレート改善法

八木 秀樹*
電気通信大学*

1 はじめに

デジタルコンテンツの著作権保護のため，デジタル指紋が重要な技術として注目されている．特にデジタル画像等のマルチメディアに対しては，拡散系列と 2 元体上で構成される AND 攻撃に耐性を持つ符号（AND-ACC）を連接させる符号化法が有用であることが示されている [3]. Trappe らは，釣合い型不完備ブロック計画 (BIBD) に基づく AND-ACC の構成法を提案した．この符号は，符号長 N に対して符号語数が N の 2 乗オーダでしか増えない点が問題点として挙げられる．そこで，安全性とブロック長を固定した元で，AND-ACC の符号語数 (符号化レート) を改善させる手法が提案されている [1, 4]. Li ら [2] は カバーフリー族を利用した AND-ACC を提案し，その具体例として直交配列を利用した符号構成法を示した．この手法は，符号長 N に対して，準指数関数的に符号語数を増大させることができる．

本論文では，線形直交配列に基づく AND-ACC [2] に対し，アルファベット拡大を適用した符号語数（符号化レート）の改善法を提案する．提案する符号構成法により，任意の線形直交配列に基づく AND-ACC の符号語数を改善できることを示す．この構成は，Reed-Solomon 符号等の最大距離分離 (MDS) 符号を外部符号，2 元 AND-ACC を内部符号とした連接符号と解釈することができる．

2 AND 結託耐性符号

2.1 デジタル指紋システム

コンテンツを配布するユーザの集合を $\Gamma = \{1, \ldots, M\}$ とする．ユーザ $i \in \Gamma$ には 2 元体上で定義される長さ N の符号語 $\boldsymbol{b}_i = (b_{i1}, \ldots, b_{iN})^{\mathrm{T}}, b_{ij} \in \{0, 1\}$ が割り当てられる．ここで，T は転置を表す．符号語の集合 $C = \{\boldsymbol{b}_i | i \in \Gamma\}$ をデジタル指紋符号と呼ぶ.

マルチメディアに対するデジタル指紋システムでは，平均化攻撃に対する耐性の重要性が示されている [3]. Trappe ら [3] は，2 元体上で AND-ACC を構成し，符号シンボルを実数体上の直交系列に連接する手法を提案した．したがって，効率良い 2 元 AND-ACC を構成することが，システム全体の性能を上げる意味で重要である．

定義 1. サイズが $\ell \geq 1$ 以下の 2 つの異なる部分集合 $S, S' \subseteq \Gamma$ に対し，$\bigwedge_{i \in S} \boldsymbol{b}_i \neq \bigwedge_{i \in S'} \boldsymbol{b}_i$ が成り立つとき，2 元符号 C は ℓ-resilient (N, M) AND-ACC と呼ばれる．ここで，演算 $\bigwedge$ は 2 元系列の成分ごとの AND を表す. □

* Hideki Yagi: Center for Frontier Science and Engineering, The University of Electro-Communications.

2.2 AND-ACC の従来構成法

AND-ACC の構成法として，BIBD を用いた手法 [3]，有限幾何に基づく手法 [4] などが提案されている．これらの手法は，Li ら [2] が示した ℓ-カバーフリー族 (ℓ-CFF) の部分クラスになる．

N 個の点の集合 $\mathcal{X}$ と M 個のブロックの集合 $\mathcal{B}$ からなる系 $(\mathcal{X}, \mathcal{B})$ を考える．任意の l 個のブロック $A_1, \ldots, A_l \in \mathcal{B}$ に対し，全てのブロック $A_0 \in \mathcal{B} \setminus \{A_1, \ldots A_l\}$ が

$$A_0 \not\subseteq \bigcup_{i=1}^{l} A_j \tag{1}$$

を満たすとき，系 $(\mathcal{X}, \mathcal{B})$ は l-CFF と呼ばれる．

定理 1 (Li et al. [2])**.** ℓ-CFF $(\mathcal{X}, \mathcal{B})$ に対し，2 元 $N \times M$ 行列 $B = [\bar{b}_{ij}]$ をその接続行列とする．ここで，点 $x_i \in \mathcal{X}$ がブロック $A_j \in \mathcal{B}$ に含まれるとき $\bar{b}_{ij} = 1$，そうでなければ $\bar{b}_{ij} = 0$ とする．行列 B の成分ごとの補数をとった（以降，単に “補数をとる” という）ものを C の符号行列とするとき，符号 C は ℓ-resilient (N, M) AND-ACC となる. □

Trappe ら [3] による AND-ACC は符号長 N に対し，符号語数 M は $O(N^2)$ となる．文献 [4] では，$N = q^m$（q は素数のべき，m は任意の正数）に対し，符号語数を $M = O(N^{\frac{1}{4}(m+2)})$ とできることが示された．一方，直交配列を利用した手法 [2] は，$M = O(q^{\sqrt{N}}) = O(2^{\frac{1}{2}\sqrt{N}\log N})$ とできる点で魅力的である．

定義 2. q 元 $n \times M$ 配列（ここで，$M = q^k$）において，任意の k 行の中に，各 q 元 k 次元ベクトルが列として 1 回ずつ現れるとき，この配列を直交配列 $OA(k, n, q)$ と呼ぶ. □

任意の素数べき q と $k < q$, $n \leq q + 1$ に対し，線形な直交配列 $OA(k, n, q)$ が存在することが知られている．この直交配列の列集合はガロア体 GF(q) 上で定義された MDS 符号を成す.

定理 2. 線形直交配列 $OA(k, n, q)$ の列 $\boldsymbol{a}_i = (a_{1i}, \ldots, a_{ni})^{\mathrm{T}}$ に対し，ブロック A_i を $\{(1, a_{1i}), (2, a_{2i}), \ldots (n, a_{ni})\}$ とする．このブロック計画の接続行列の補数をとった行列は，$\lfloor \frac{n-1}{k-1} \rfloor$-resilient (nq, q^k) AND-ACC の符号行列となる. □

3 提案する AND-ACC の構成法

3.1 線形直交配列の性質

素数べき q に対し，線形な直交配列 $OA(k, n, q)$ を考える．$OA(k, n, q)$ はガロア体 GF(q) の元を成分にとる

と仮定できる．このとき，配列の各列はMDS符号の符号語となるため，各列のHamming重みは$d = n-k+1$以上，任意の2列は高々$n-d = k-1$個の同一成分を持つ．

体GF(q)の原始元をαとする．このとき，GF(q)の全ての元は$0 = \alpha^{-\infty}, 1 = \alpha^0, \alpha^1, \ldots, \alpha^{q-2}$と表される．元$\alpha^i$の位置ベクトルを$\boldsymbol{z}(\alpha^i) = (z_{-\infty}, z_0, z_1, \ldots, z_{q-2})^{\mathrm{T}} \in \{0,1\}^q$とする．ただし，$z_j$は$i = j$で1，それ以外の$j$で0を取る．$\pi$は行列の各行の1ビット左巡回シフトを表し，$I_{q-1}$は$(q-1) \times (q-1)$の単位行列とする．また，$J_{q-1} := \left[\frac{\mathbf{0}}{I_{q-1}}\right]$を第1行が全零ベクトルの$q \times (q-1)$行列とする．任意の非零元$\beta = \alpha^j \in \mathrm{GF}(q)$に対し，$\{\alpha^0\beta, \alpha^1\beta, \ldots, \alpha^{q-2}\beta\}$を位置ベクトル表現すると，$\pi^j(J_{q-1})$と表現されることに注意しよう．また，便宜的に$\pi^{-\infty}(J_{q-1})$を第1行が全1ベクトル，第$j$行$(j = 2 \ldots, q)$は全零ベクトルとなる$q \times (q-1)$行列と定義する．

直交配列の非零列ベクトル$\boldsymbol{c}_i = (c_{1i}, \ldots, c_{ni})^{\mathrm{T}}$に対し，$W_i := \{\alpha^j \boldsymbol{c}_i | j = 0, \ldots, q-2\}$は乗法群を成す．直交配列の線形性より，全ての$\alpha^j \boldsymbol{c}_i$もまた直交配列の列ベクトルとなる．直交配列において，最小インデックスの非零成分が$\alpha^0 = 1$となる列ベクトルの集合を$\tilde{C}_0 = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_{A_q}\}$とする．ただし，$A_q := q^{k-1} + q^{k-2} + \cdots + 1$である．$W_0 = \{\mathbf{0}\}$と定義すると，直交配列の列ベクトル集合$\tilde{C}$は$\tilde{C} = \bigcup_{i=0}^{A_q} W_i$とパーティションに分けられることに注意されたい．位置ベクトル表現を用いると，W_iは$qn \times (q-1)$行列

$$Z(W_i) := \begin{bmatrix} \pi^{c_{1i}}(J_{q-1}) \\ \pi^{c_{2i}}(J_{q-1}) \\ \vdots \\ \pi^{c_{ni}}(J_{q-1}) \end{bmatrix} \tag{2}$$

により表される．したがって，直交配列全体の位置ベクトルによる表現は

$$\left[\boldsymbol{z}(\mathbf{0}) \middle| Z(W_1) \middle| \cdots \middle| Z(W_{A_q})\right] \tag{3}$$

となる．ただし，$\boldsymbol{z}(\mathbf{0}) \in \{0,1\}^{nq}$は全零ベクトル$\mathbf{0} \in \mathrm{GF}(q)^n$の位置ベクトル表現である．

3.2 提案構成法

定理2から，$OA(k,n,q)$から得られる式(3)の行列の補数をとったものは，$\lfloor \frac{n-1}{k-1} \rfloor$-resilient (nq, q^k) AND-ACCを与える．そこで，$\lfloor \frac{n-1}{k-1} \rfloor$以上の結託耐性を持つ$\ell$-resilient (q,m) AND-ACCを用意し，その符号行列の補数をとったものをQとする（任意の$\ell \leq q$に対し，符号語数mがq以上のℓ-resilient AND-ACCが必ず存在する）．以下では，行列Qを直交配列の部分行列$\pi^{c_{ji}}(J_{q-1})$と置き換えることで配列のアルファベット拡大を行い，符号長と結託耐性を同一に保ったまま符号語数を増大させる手法を提案する．

整数mが正整数fと$g \leq q-2$により$m = f(q-1)+g$と表現されることに注意し，2元$q \times m$行列Qをf個の$q \times (q-1)$部分行列Q_l $(l = 1, \ldots, f)$と$q \times g$部分行列Q_{f+1}に分ける (i.e., $Q = [Q_1|Q_2|\cdots|Q_{f+1}]$)．式(2)で表されるパーティション$W_i$の位置ベクトル表現を

$$\tilde{Z}(W_i) := \left[\begin{array}{c|c|c|c} \pi^{c_{1i}}(Q_1) & \pi^{c_{1i}}(Q_2) & \cdots & \pi^{c_{1i}}(Q_{f+1}) \\ \pi^{c_{2i}}(Q_1) & \pi^{c_{2i}}(Q_2) & \cdots & \pi^{c_{2i}}(Q_{f+1}) \\ \vdots & \vdots & & \vdots \\ \pi^{c_{ni}}(Q_1) & \pi^{c_{ni}}(Q_2) & \cdots & \pi^{c_{ni}}(Q_{f+1}) \end{array}\right]$$

のように置き換える．ここでも便宜的に$\pi^{-\infty}(Q_l)$ $(l = 1, \ldots, f+1)$を第1行が全1ベクトル，第j行$(j = 2 \ldots, q)$が全零ベクトルとなる行列を表すことにする．結果として得られる行列

$$\left[\boldsymbol{z}(\mathbf{0}) \middle| \tilde{Z}(W_1) \middle| \cdots \middle| \tilde{Z}(W_{A_q})\right] \tag{4}$$

の補数をとったものを符号行列にとると，この2元符号は以下の性質を持つ．

Theorem 1. $OA(k,n,q)$と$\lfloor \frac{n-1}{k-1} \rfloor$-resilient (q,m) AND-ACCを元に提案手法で構成される2元符号は長さ$N = nq$, 符号語数$M = A_q m + 1$の$\lfloor \frac{n-1}{k-1} \rfloor$-resilient (N,M) AND-ACCを与える． □

定理1から，結託耐性と符号長を同一に保ったまま，直交配列に基づくAND-ACCの符号語数を必ず増大できることが示される．ここで，直交配列から構成される符号語数をM_{OA}と表すと，提案する符号構成法により得られる符号語数は$M = m/(q-1)M_{\mathrm{OA}} + 1$と表現できる．したがって，$Q$として用いるAND-ACCの符号語数$m$が大きいほど，提案手法の有効性は大きくなる．素数べきpに対して$q = p^m$が成り立つとき，文献[4]で提案された有限幾何EG(m,p)に基づく$(p-1)$-resilient AND-ACCをQとして用いれば，符号語数は$M = \Omega(q^{k+\frac{1}{4}(m+2)})$となる．直交配列から得られる符号の符号語数が$M = q^k$となるのに比べて，提案手法の有効性が分かる．

参考文献

[1] I.K. Kang, K. Sinha, and H.-K. Lee, "New digital fingerprint code construction scheme using group-divisible design," *IEICE Trans. Fundamentals*, vol. E89-A, no. 12, pp. 3732–3735, Dec. 2006.

[2] Q. Li, X. Wang, Y. Li, Y. Pan, and P. Fan, "Construction of anti-collusion codes based on cover-free families," *Proc. 2009 6th Int. Conf. on Information Technology: New generations*, pp. 362–365, Apr. 2009.

[3] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Processing*, vol. 51, pp. 1069–1087, Apr. 2003.

[4] H. Yagi, T. Matsushima, and S. Hirasawa, "Fingerprinting codes for multimedia data against averaging attack," *IEICE Trans. Fundamentals*, vol. E92-A, no. 1, pp. 207-216, Jan. 2009.