啟動研究列車

主講人：李崇道

創新研究之方法、寫作與倫理

方法

- 廣交人才與掌握資源
  實作工具與善用網路
- 研究歷程與經驗分享
- 進步成長與計較短利

寫作

- 文句與數據表達
- 架構組織
- 期刊特性
- 全球趨勢

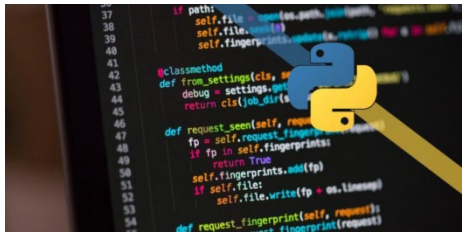
倫理

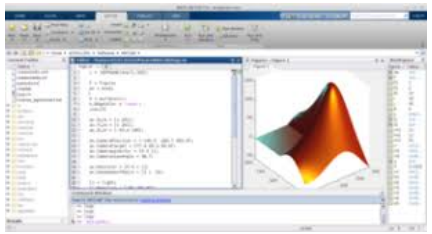
- ✓ 抄襲、實驗數據造假
- ✓ 掠奪性期刊、研討會

廣交人才、實作工具、掌握資源、善用網路

01
教授、學長姐

02
軟體、硬體





03
產官學單位

MOST 科技部
Ministry of Science and Technology

工業技術研究院
Industrial Technology Research Institute

04
電子資料庫

ELSEVIER

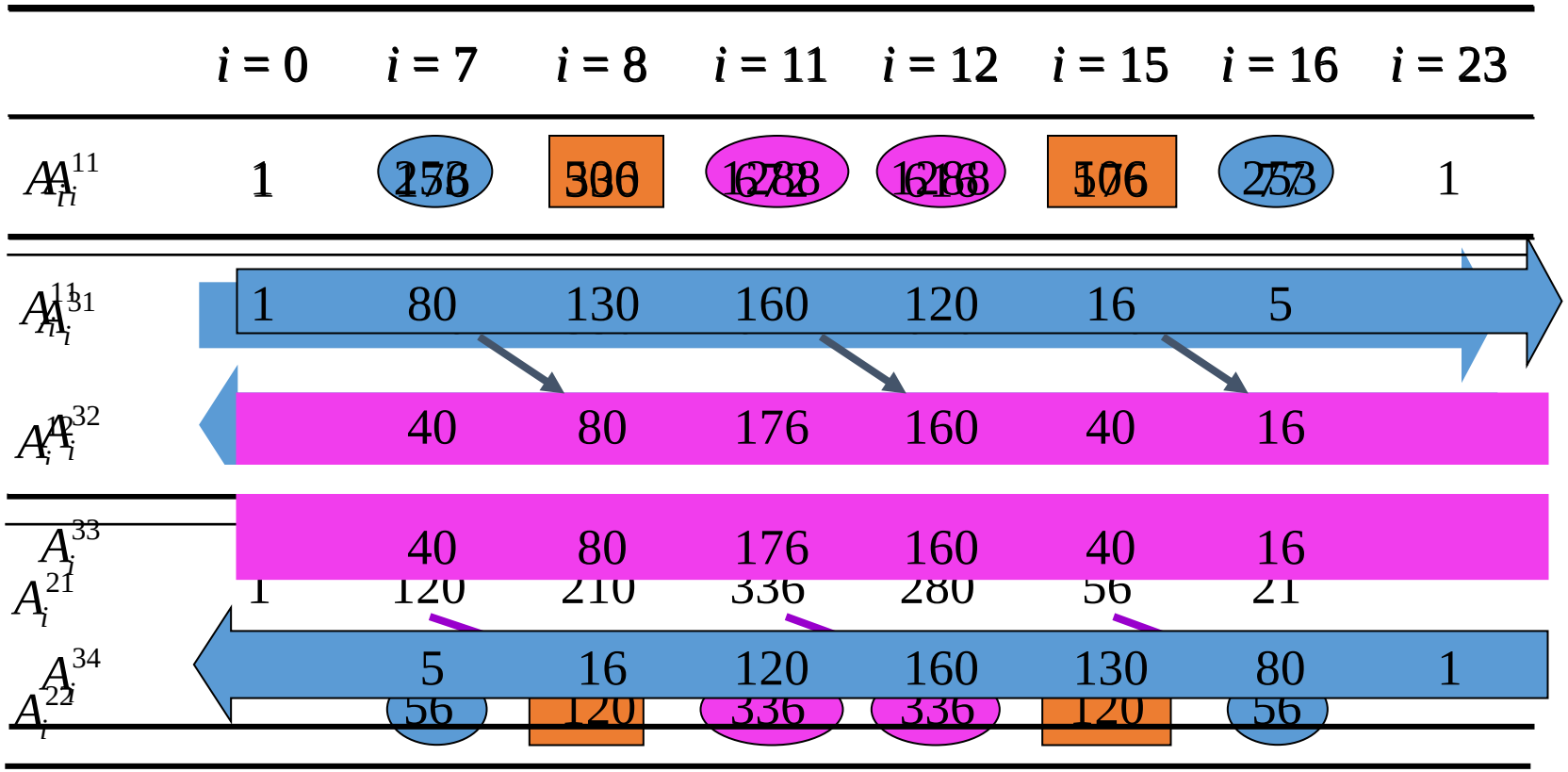
IEEE Xplore® Digital Library

研究歷程與經驗分享(案例1)

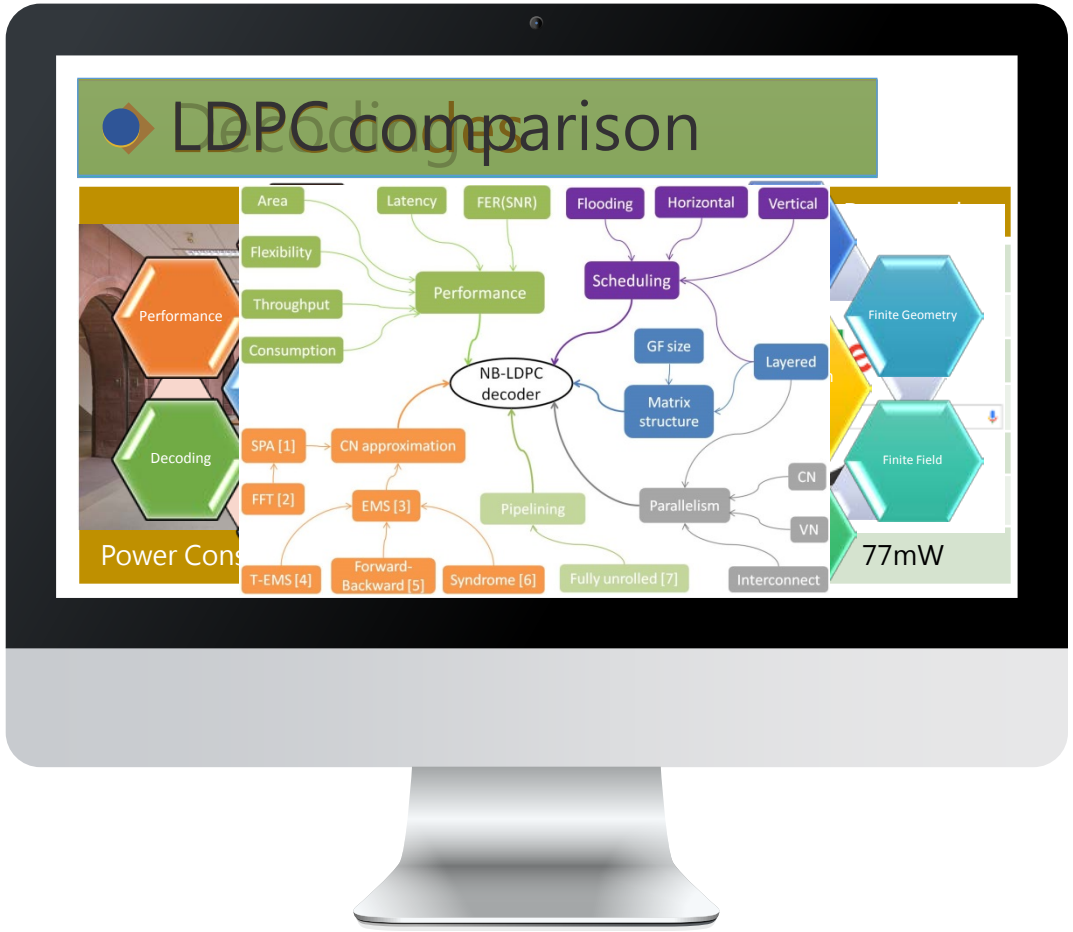
實驗數據有感再深入

- ✓ 無心插柳柳成蔭
- ✓ 1961年結果
- ✓ 理論證明用到三種數學
- ✓ 250台電腦
- ✓ 同時間研究

➢ Weight Distribution of (23, 12, 7) Golay code



研究歷程與經驗分享(案例2)



解答已經存在

- 世界之大，找得到嗎?
- 關鍵字、聯結性
- 題目本質
- 優劣分析

研究歷程與經驗分享(案例3)

- 移地研究

- ✓ 廈門大學
- ✓ 新題目
- ✓ 序列設計
- ✓ 工具、實驗研究室
- ✓ 建立新團隊

PERFECT GAUSSIAN INTEGER SEQUENCES

$$[6-j, 4+j, 1-j, -1+j, 1-j, 4+j, -4-j, -1+j, 1-j, -1+j]$$

$$[2-3j, 2-2j, 2+2j, 2-2j, -3+2j, 2+3j, 2+2j, 2-2j, 2+2j, -3-2j]$$

$$[3, -2, 3, -2, -2, 3, -2, -7, -2, -2] \text{ (real-valued)}$$

$$[-3j, -3j, 2j, 2j, 2j, -3j, 7j, 2j, 2j, 2j] \text{ (purely-imaginary)}$$

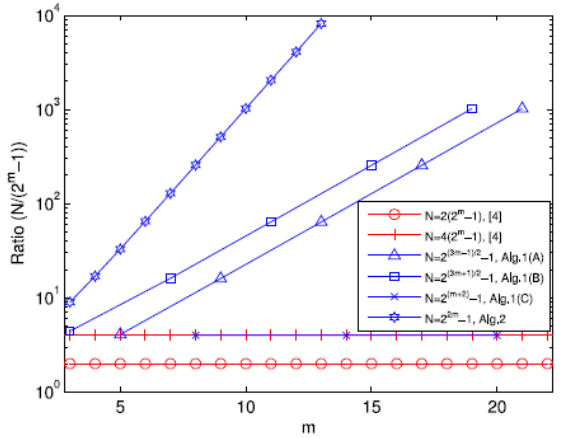
July 2014

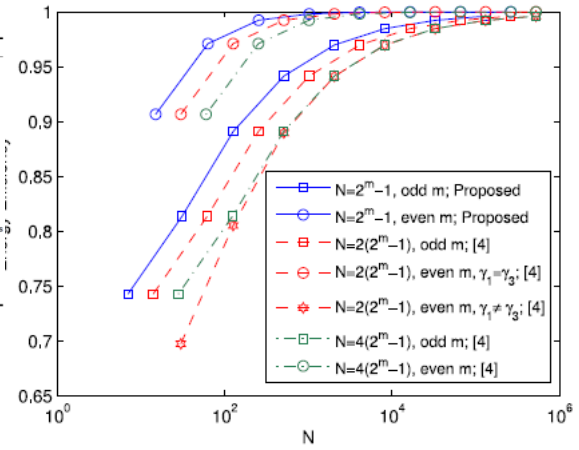
July 2015

n	amount	hexadecimal representation
31	6	96e36750, 1ae6c761, 9c0da8b7, 719a1ec6, 73785986, fd15b031
127	6	9ca56e134be73af0a3d4c7d372665500, 735091a23c9aceca50279eee05ef0fc6, 10aa664ecbe32bc50f5ce7d2c876a531, 73f0f7a07779e40a5373593c45890ac6, fd1f987d940c5137bca92805bb90f271, 9e4f09dda014953dec8a3029be19f8b7

Period	References	Degree	Theorem	Approach
$N = 0 \pmod 2$	[1]	3,4,6	Theorem 1	base sequences
$N = 0 \pmod 4$	[1]	3,4,5,6	Theorem 2	base sequences
	[4]	–	Theorem 2	interleaving
$N = 2 \pmod 4$	[4]	–	Theorem 1	interleaving
$N = 4$	[5]	2,3,4	Theorems 7,12,13	un-sampling
$N = 2^m,\ m \geq 3$	[5]	4	Theorem 13	un-sampling
$N = kp$, even k, prime p	[5]	3	Theorems 8,9,10	un-sampling
$N = \theta^2 + \theta^2 + \theta + 1$, odd $\theta = p^r,\ r \geq 1$	proposed	2	Theorem 5	cyclic difference sets
$N = p$, prime p	[2]	3,5	Theorems 1,4	cyclotomic classes
	[7]	–	–	Gaussian sum
$N = p(p+2)$, primes $p,\ p+2$	[3]	3,5	Theorems 1,4	Whiteman's generalised cyclotomy
$N = kp$, odd k, prime p	[5]	3	Theorems 8,9,10	un-sampling
$N = kp,\ (k, p) = 1$	[7]	–	–	zero padding, Legendre symbol
$N = 2^m - 1$, prime $N,\ m \geq 3$	[6]	2	Theorem 1	Legendre sequences
$N = 2^m - 1,\ m = 5,7,17$	[6]	2	Theorem 2	Hall's sixtic residue sequences
$N = 2^m - 1,\ m \geq 3$	[6]	2	Theorem 3	m-sequences
$N = 2^m - 1$, composite m	[6]	2	Theorem 4	GMW sequences
$N = 2^m - 1,\ m \geq 5,\ m = 0 \pmod 2$	proposed	2	Theorems 1,2	three-term, Segre, Glynn Type II sequences
$N = 2^m - 1,\ m \geq 5,\ m = 1, 2 \pmod 3$	proposed	2	Theorem 1	five-term, Welch-Gong sequences
$N = 2^m - 1,\ m \geq 5,\ m = 1, 3 \pmod 4$	proposed	2	Theorem 2	Glynn Type I sequences
$N = p = 3(\bmod 4)$, square or prime $\frac{p-3}{4}$	proposed	2	Theorem 3	cyclic difference sets
$N = (t^r + t + 1,\ t = p^r \neq 3 \pmod 4,\ r \geq 1$ [4]	proposed	2	Theorem 4	cyclic difference sets
$N = \theta^2 + \theta^2 + \theta + 1$, even $\theta = 2^r,\ r \geq 1$	proposed	2	Theorem 5	cyclic difference sets
$N = p(3p+2)$, primes $p, 3p+2$	proposed	2	Theorem 6	cyclic difference sets
$N = 133$	proposed	2	Theorem 7	cyclic difference sets

- **BALANCED BINARY SEQUENCES**
- **COMBINATORIAL DESIGN**
- **FINITE FIELD**





April 2017

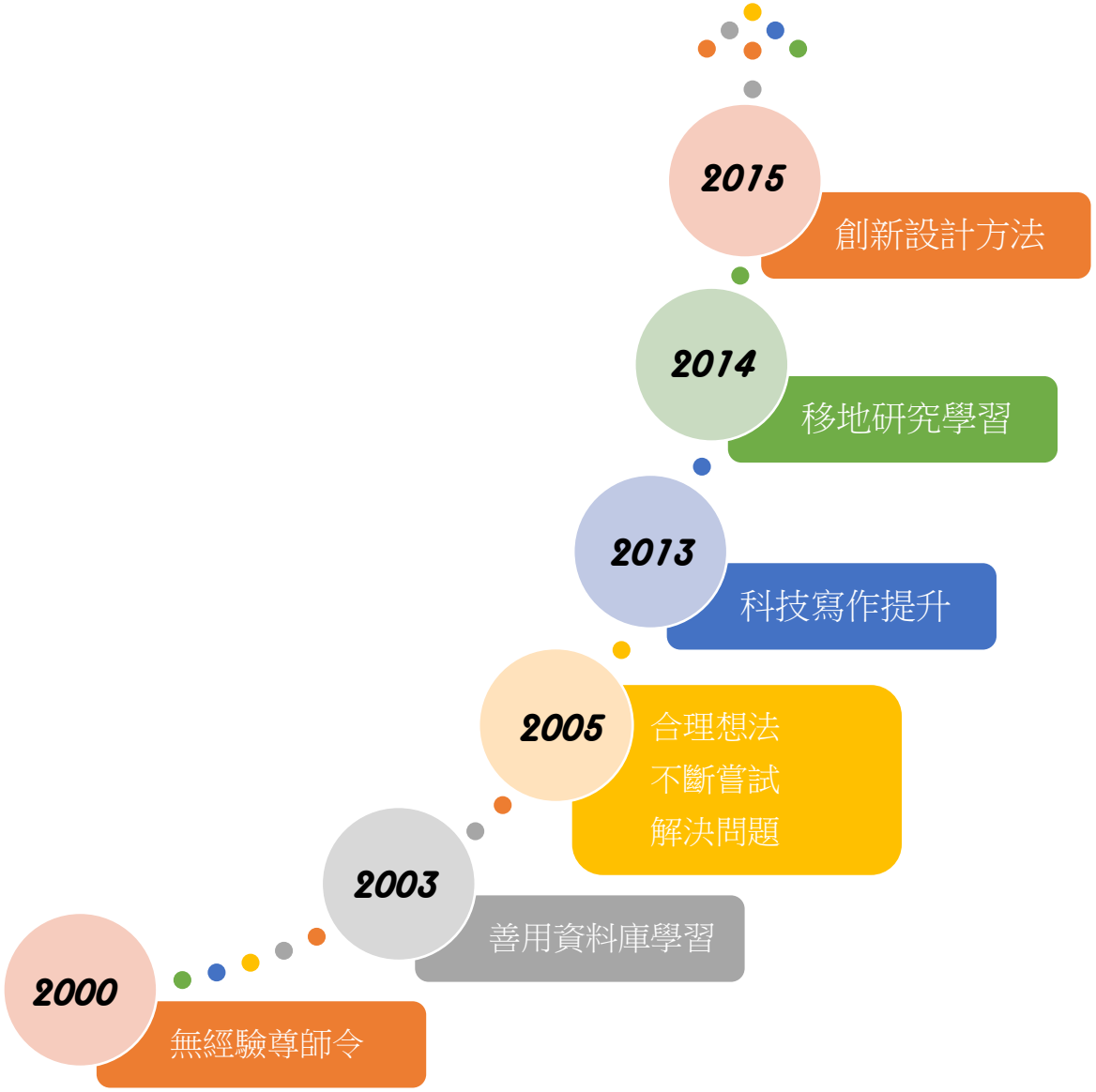
研究歷程與經驗分享(案例4)

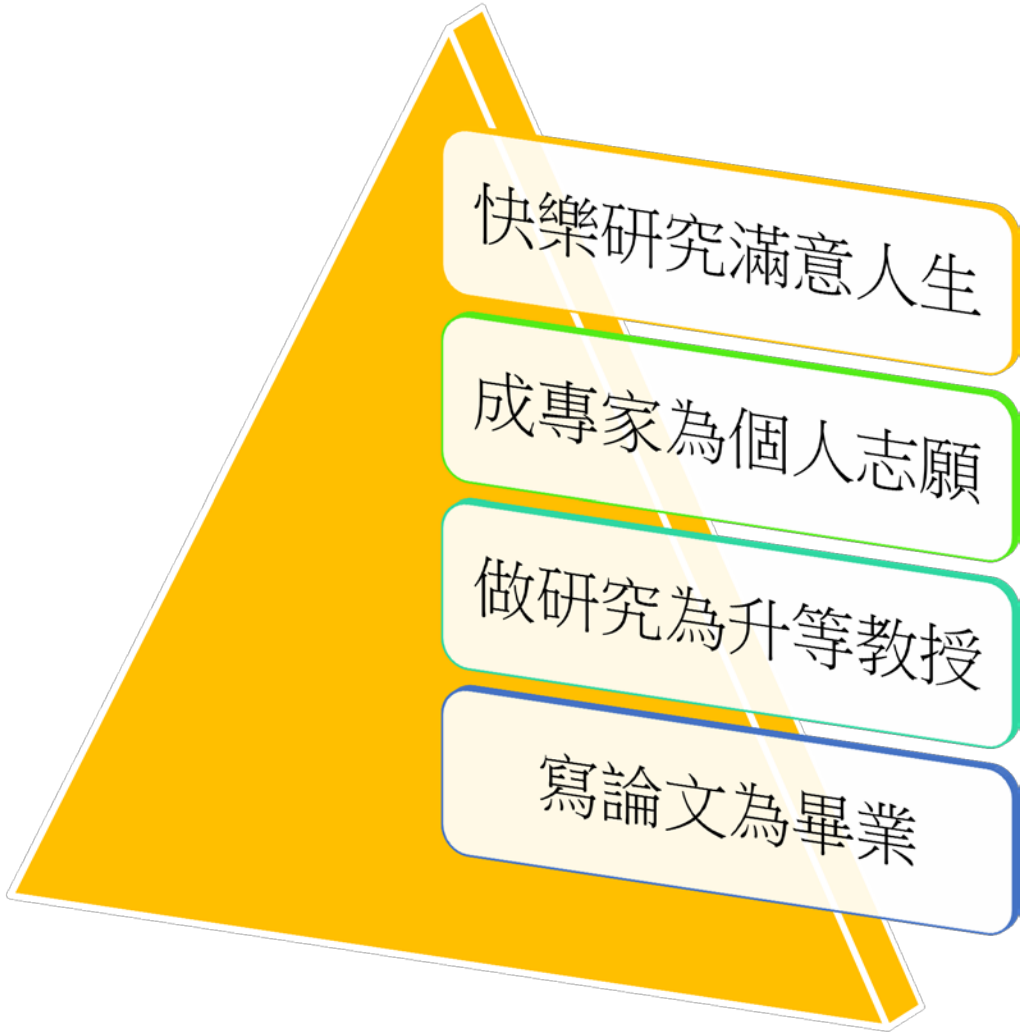
大論文方法

- 演算法
- 架構改變
- 數學定義、步驟修正
- 合理化、應用化說服
- 創新方法、理論證明難度高

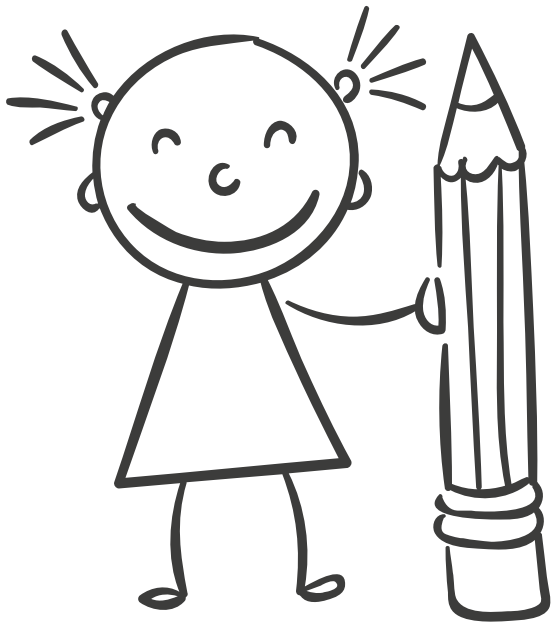
- 貢獻度高
- 期刊論文
- 研究熱度
- 被引用高

進步成長與計較短利


2015
創新設計方法
2014
移地研究學習
2013
科技寫作提升
2005
合理想法
不斷嘗試
解決問題
2003
善用資料庫學習
2000
無經驗尊師令


快樂研究滿意人生
成專家為個人志願
做研究為升等教授
寫論文為畢業

寫作是一門藝術



1

文句與數據表達

單字、句子、段落、表格、圖。

2

架構組織

摘要、介紹、章節、實驗結果、分析比較、
參考文獻。

3

期刊特性

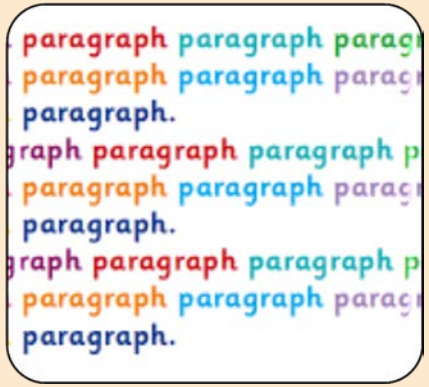
理論、實驗、雜誌、Survey。

4

全球趨勢

一頁研討會論文、幾頁期刊論文、長短篇期刊論文、
長篇期刊論文、 Open Access論文。

文句與數據表達



propose

present

new

novel

prove

Demonstrate

NG---We have

the newly proposed method

more widely and flexibly

thruoghout this paper

play an important role

Chen *et al.*

倒裝句

主被動

smooth

關聯性

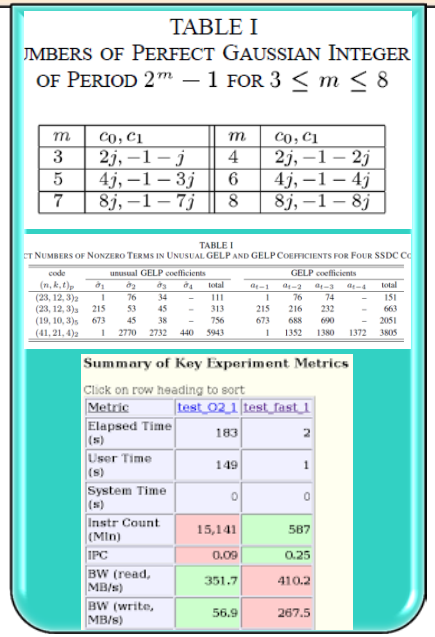


TABLE I
UMBERS OF PERFECT GAUSSIAN INTEGER OF PERIOD $2^m - 1$ FOR $3 \leq m \leq 8$

m	c_0, c_1	m	c_0, c_1
3	$2j, -1-j$	4	$2j, -1-2j$
5	$4j, -1-3j$	6	$4j, -1-4j$
7	$8j, -1-7j$	8	$8j, -1-8j$

TABLE I
CT NUMBERS OF NONZERO TERMS IN UNUSUAL GELP AND GELP COEFFICIENTS FOR FOUR SSDC C

code	unusual GELP coefficients					GELP coefficients				
$(n, k, \ell)_p$	σ_1	σ_2	σ_3	σ_4	total	$a_{\ell-1}$	$a_{\ell-2}$	$a_{\ell-3}$	$a_{\ell-4}$	total
$(23, 12, 3)_5$	1	76	34	–	111	1	76	74	–	151
$(23, 12, 3)_5$	215	53	45	–	313	215	216	232	–	663
$(19, 10, 3)_5$	673	45	38	–	756	673	688	690	–	2051
$(41, 21, 4)_2$	1	2770	2732	440	5943	1	1352	1380	1372	3805

Summary of Key Experiment Metrics

Click on row heading to sort

Metric	test_O2_1	test_fast_1
Elapsed Time (s)	183	2
User Time (s)	149	1
System Time (s)	0	0
Instr Count (Mln)	15,141	587
IPC	0.09	0.25
BW (read, MB/s)	351.7	410.2
BW (write, MB/s)	56.9	267.5

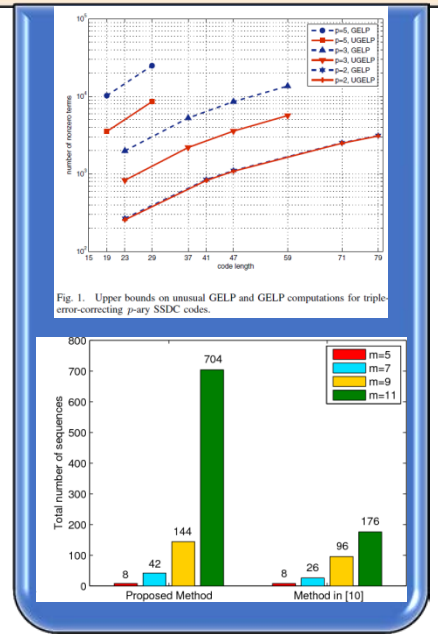
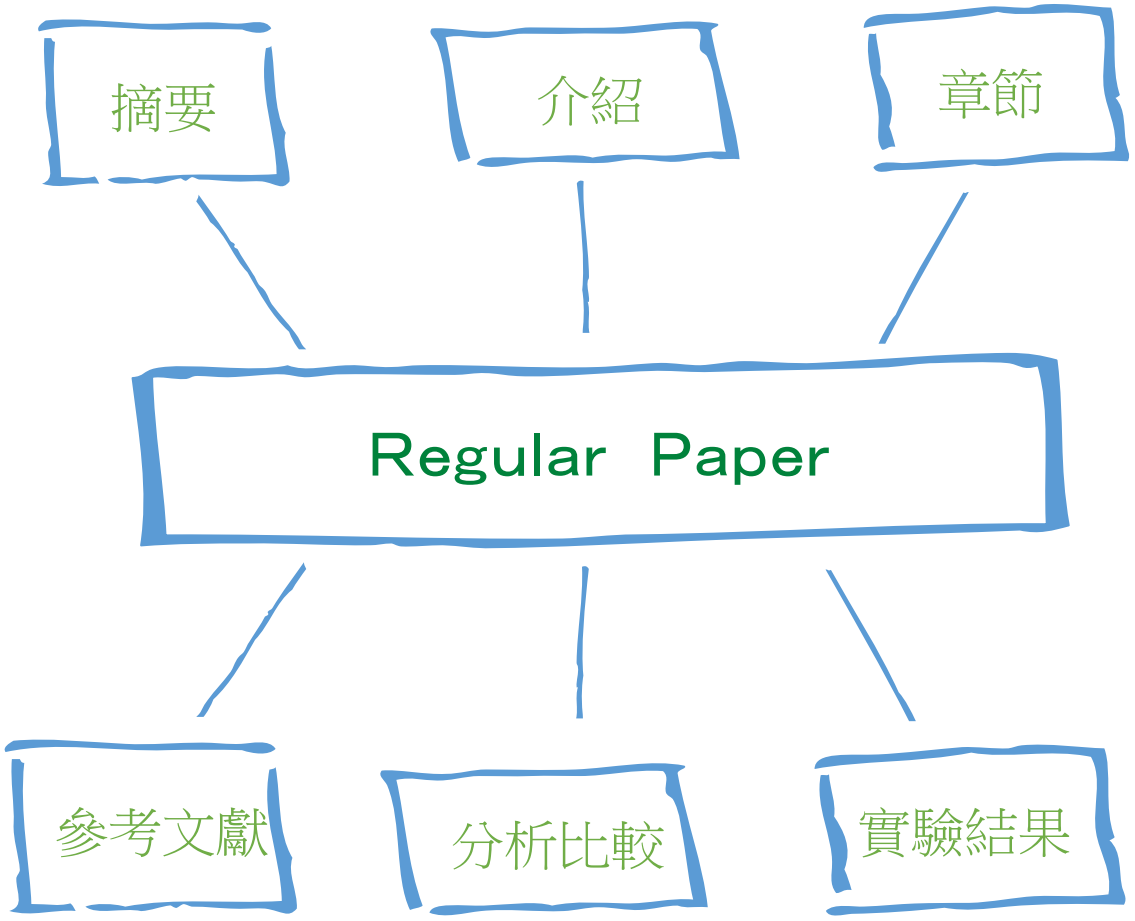


Fig. 1. Upper bounds on unusual GELP and GELP computations for triple-error-correcting p-ary SSDC codes.

Writing

架構組織



Algebraic Decoding of Cyclic Codes Using Partial Syndrome Matrices

Chong-Dao Lee, *Senior Member, IEEE*

***Abstract*— Cyclic codes have been widely used in many applications of communication systems and data storage systems. This paper proposes a new procedure for decoding cyclic codes up to actual minimum distance. The decoding procedure consists of two steps: 1) computation of known syndromes and 2) computation of error positions and error values simultaneously. To do so, a matrix whose all entries are syndromes is called *syndrome matrix*. A matrix whose entries are either syndromes or the elements of a finite field is said to be *partial syndrome matrix*. In this paper, two novel methods are presented to determine error positions and error values simultaneously and directly. The first method uses a new partial syndrome matrix along with Gaussian elimination. The partial syndrome matrices for binary (respectively, ternary) cyclic codes of lengths from 69 to 99 (respectively, 16 to 37) are tabulated. For some cyclic codes, the partial syndrome matrices contain unknown syndromes; the second method constructs a matrix from a system of equations, which is generated by the determinants of different partial syndrome matrices and makes use of Gaussian elimination to determine its row rank. Many more cyclic codes beyond the Bose–Chaudhuri–Hocquenghem bound can be decoded with these methods.**

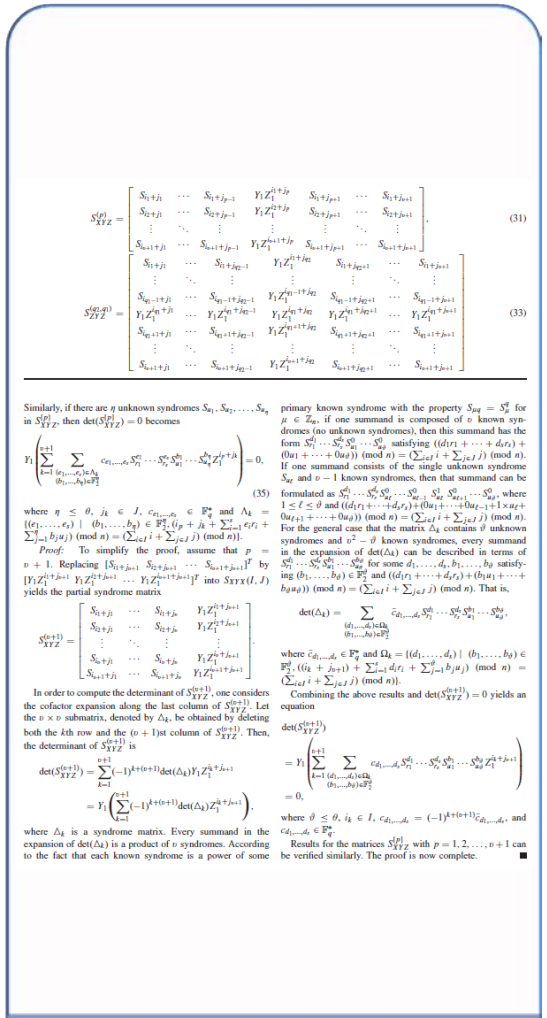
***Index Terms*— Cyclic codes, decoding, Gaussian elimination, partial syndrome matrices, unknown syndromes.**

I. Introduction

CYCLIC codes are an important class of error-correcting codes, e.g., Bose-Chaudhuri-Hocquenghem (BCH) codes of small lengths. Unfortunately, however, the (47, 24, 11) binary quadratic residue code can not be decoded up to actual minimum distance. To solve this problem, He *et al.* [13] developed a syndrome matrix to calculate the unknown syndrome needed in the decoder. Later, the Berlekamp-Massey algorithm was utilized to find the error-locator polynomials for binary quadratic residue decoders [14]–[16] with lengths 71, 79, 89, 97, 103, and 113. In 2005, Orsini and Sala [17] proved that every cyclic code admits a general error-locator polynomial. Particularly for double-error-correcting binary cyclic codes [18] of length less than 63, the general error-locator polynomials have only a few nonzero terms so that their decoding is very fast. In addition, some researches on ternary quadratic residue decoders have been investigated in [19]–[24]. Recently, the weak-locator polynomials [23], [25] derived from two partial syndrome matrices were proposed to decode the (61, 30, 12) ternary quadratic residue code. More recently, a novel partial syndrome matrix [24] which can be transformed into the matrix in row echelon form was presented to determine error positions directly for decoding the (47, 23, 15) ternary quadratic residue code up to seven errors. Once those error positions are known, the corresponding error values can also be found by Gaussian-Jordan elimination for a linear system with respect to known syndromes. This decoder requires

Writing

期刊特性



$$S_{XYZ}^{(p)} = \begin{bmatrix} S_{i_1+j_1} & \cdots & S_{i_1+j_{p-1}} & Y_1 Z_1^{i_1+j_p} & S_{i_1+j_{p+1}} & \cdots & S_{i_1+j_{v+1}} \\ S_{i_2+j_1} & \cdots & S_{i_2+j_{p-1}} & Y_1 Z_1^{i_2+j_p} & S_{i_2+j_{p+1}} & \cdots & S_{i_2+j_{v+1}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{i_{v+1}+j_1} & \cdots & S_{i_{v+1}+j_{p-1}} & Y_1 Z_1^{i_{v+1}+j_p} & S_{i_{v+1}+j_{p+1}} & \cdots & S_{i_{v+1}+j_{v+1}} \end{bmatrix}, \quad (31)$$

$$S_{XYZ}^{(q),(q')} = \begin{bmatrix} S_{i_1+j_1} & \cdots & S_{i_1+j_{q-1}} & Y_1 Z_1^{i_1+j_q} & S_{i_1+j_{q+1}} & \cdots & S_{i_1+j_{v+1}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{i_{q'-1}+j_1} & \cdots & S_{i_{q'-1}+j_{q-1}} & Y_1 Z_1^{i_{q'-1}+j_q} & S_{i_{q'-1}+j_{q+1}} & \cdots & S_{i_{q'-1}+j_{v+1}} \\ Y_1 Z_1^{i_{q'}+j_1} & \cdots & Y_1 Z_1^{i_{q'}+j_{q-1}} & Y_1 Z_1^{i_{q'}+j_q} & Y_1 Z_1^{i_{q'}+j_{q+1}} & \cdots & Y_1 Z_1^{i_{q'}+j_{v+1}} \\ S_{i_{q'+1}+j_1} & \cdots & S_{i_{q'+1}+j_{q-1}} & Y_1 Z_1^{i_{q'+1}+j_q} & S_{i_{q'+1}+j_{q+1}} & \cdots & S_{i_{q'+1}+j_{v+1}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{i_{v+1}+j_1} & \cdots & S_{i_{v+1}+j_{q-1}} & Y_1 Z_1^{i_{v+1}+j_q} & S_{i_{v+1}+j_{q+1}} & \cdots & S_{i_{v+1}+j_{v+1}} \end{bmatrix}. \quad (33)$$

Similarly, if there are η unknown syndromes $S_{\theta_1}, S_{\theta_2}, \ldots, S_{\theta_\eta}$ in $S_{XYZ}^{(p)}$, then $\det(S_{XYZ}^{(p)}) = 0$ becomes

$$Y_1 \left(\sum_{k=1}^{v+1} \sum_{\substack{(e_1,\ldots,e_\eta)\in\Lambda_k \\ (b_1,\ldots,b_\eta)\in\mathbb{F}_2^\eta}} c_{e_1,\ldots,e_\eta} S_{r_1}^{e_1} \cdots S_{r_\eta}^{e_\eta} S_{a_1}^{b_1} \cdots S_{a_\eta}^{b_\eta} Z_1^{\rho+\mathrm{j}_k} \right) = 0, \quad (35)$$

where $\eta \le \theta$, $\mathrm{j}_k \in J$, $c_{e_1,\ldots,e_\eta} \in \mathbb{F}_q^*$ and $\Lambda_k = \{(e_1,\ldots,e_\eta) \mid (b_1,\ldots,b_\eta) \in \mathbb{F}_2^\eta, (i_p + \mathrm{j}_k + \sum_{i=1}^{\eta} e_i r_i + \sum_{j=1}^{\eta} b_j u_j) \pmod n = (\sum_{i\in I} i + \sum_{j\in J} j) \pmod n\}$.

Proof: To simplify the proof, assume that $p = v+1$. Replacing $[S_{i_1+j_{v+1}} \ S_{i_2+j_{v+1}} \ \cdots \ S_{i_{v+1}+j_{v+1}}]^T$ by $[Y_1 Z_1^{i_1+j_{v+1}} \ Y_1 Z_1^{i_2+j_{v+1}} \ \cdots \ Y_1 Z_1^{i_{v+1}+j_{v+1}}]^T$ into $S_{XYZ}(I,J)$ yields the partial syndrome matrix

$$S_{XYZ}^{(v+1)} = \begin{bmatrix} S_{i_1+j_1} & \cdots & S_{i_1+j_v} & Y_1 Z_1^{i_1+j_{v+1}} \\ S_{i_2+j_1} & \cdots & S_{i_2+j_v} & Y_1 Z_1^{i_2+j_{v+1}} \\ \vdots & \ddots & \vdots & \vdots \\ S_{i_v+j_1} & \cdots & S_{i_v+j_v} & Y_1 Z_1^{i_v+j_{v+1}} \\ S_{i_{v+1}+j_1} & \cdots & S_{i_{v+1}+j_v} & Y_1 Z_1^{i_{v+1}+j_{v+1}} \end{bmatrix}.$$

In order to compute the determinant of $S_{XYZ}^{(v+1)}$, one considers the cofactor expansion along the last column of $S_{XYZ}^{(v+1)}$. Let the $v \times v$ submatrix, denoted by Δ_k, be obtained by deleting both the kth row and the $(v+1)$st column of $S_{XYZ}^{(v+1)}$. Then, the determinant of $S_{XYZ}^{(v+1)}$ is

$$\det(S_{XYZ}^{(v+1)}) = \sum_{k=1}^{v+1} (-1)^{k+(v+1)} \det(\Delta_k) Y_1 Z_1^{i_k+j_{v+1}} = Y_1 \left(\sum_{k=1}^{v+1} (-1)^{k+(v+1)} \det(\Delta_k) Z_1^{i_k+j_{v+1}} \right),$$

where Δ_k is a syndrome matrix. Every summand in the expansion of $\det(\Delta_k)$ is a product of v syndromes. According to the fact that each known syndrome is a power of some primary known syndrome with the property $S_{\mu q} = S_\mu^q$ for $\mu \in \mathbb{F}_{q^n}$, if one summand is composed of v known syndromes (no unknown syndromes), then this summand has the form $S_{r_1}^{d_1} \cdots S_{r_\ell}^{d_\ell} S_{a_1}^{b_1} \cdots S_{a_\theta}^{b_\theta}$ satisfying $((d_1 r_1 + \cdots + d_\ell r_\ell) + (b_{\theta 1} + \cdots + b_{\theta\theta})) \pmod n = (\sum_{i\in I} i + \sum_{j\in J} j) \pmod n$. If one summand consists of the single unknown syndrome S_{a_ℓ} and $v-1$ known syndromes, then that summand can be formulated as $S_{r_1}^{d_1} \cdots S_{r_{\ell'}}^{d_{\ell'}} S_{r_{\ell'+1}}^{d_{\ell'+1}} \cdots S_{r_{\theta-1}}^{d_{\theta-1}} S_{a_\ell}^{b_\ell} S_{a_{\ell+1}}^{d_{\ell+1}} \cdots S_{a_\theta}^{d_\theta}$, where $1 \le \ell \le \theta$ and $((d_1 r_1 + \cdots + d_{\ell'} r_{\ell'}) + (b_{\theta 1} + \cdots + b_{\theta\ell-1}) \times a_\ell + (b_{\theta\ell+1} + \cdots + b_{\theta\theta})) \pmod n = (\sum_{i\in I} i + \sum_{j\in J} j) \pmod n$. For the general case that the matrix Δ_k contains ϑ unknown syndromes and $v^2 - \vartheta$ known syndromes, every summand in the expansion of $\det(\Delta_k)$ can be described in terms of $S_{r_1}^{d_1} \cdots S_{r_\ell}^{d_\ell} S_{a_1}^{b_1} \cdots S_{a_\vartheta}^{b_\vartheta}$ for some $d_1, \ldots, d_\ell, b_1, \ldots, b_\vartheta$ satisfying $(b_1, \ldots, b_\vartheta) \in \mathbb{F}_2^\vartheta$ and $((d_1 r_1 + \cdots + d_\ell r_\ell) + (b_1 a_1 + \cdots + b_\vartheta a_\vartheta)) \pmod n = (\sum_{i\in I} i + \sum_{j\in J} j) \pmod n$. That is,

$$\det(\Delta_k) = \sum_{\substack{(d_1,\ldots,d_\ell)\in\Omega_k \\ (b_1,\ldots,b_\vartheta)\in\mathbb{F}_2^\vartheta}} \tilde{c}_{d_1,\ldots,d_\ell} S_{r_1}^{d_1} \cdots S_{r_\ell}^{d_\ell} S_{a_1}^{b_1} \cdots S_{a_\vartheta}^{b_\vartheta},$$

where $\tilde{c}_{d_1,\ldots,d_\ell} \in \mathbb{F}_q^*$ and $\Omega_k = \{(d_1,\ldots,d_\ell) \mid (b_1,\ldots,b_\vartheta) \in \mathbb{F}_2^\vartheta, ((i_k + \mathrm{j}_{v+1}) + \sum_{i=1}^{\ell} d_i r_i + \sum_{j=1}^{\vartheta} b_j u_j) \pmod n = (\sum_{i\in I} i + \sum_{j\in J} j) \pmod n\}$.

Combining the above results and $\det(S_{XYZ}^{(v+1)}) = 0$ yields an equation

$$\det(S_{XYZ}^{(v+1)}) = Y_1 \left(\sum_{k=1}^{v+1} \sum_{\substack{(d_1,\ldots,d_\ell)\in\Omega_k \\ (b_1,\ldots,b_\vartheta)\in\mathbb{F}_2^\vartheta}} c_{d_1,\ldots,d_\ell} S_{r_1}^{d_1} \cdots S_{r_\ell}^{d_\ell} S_{a_1}^{b_1} \cdots S_{a_\vartheta}^{b_\vartheta} Z_1^{i_k+j_{v+1}} \right) = 0,$$

where $\vartheta \le \theta$, $i_k \in I$, $c_{d_1,\ldots,d_\ell} = (-1)^{k+(v+1)} \tilde{c}_{d_1,\ldots,d_\ell}$, and $c_{d_1,\ldots,d_\ell} \in \mathbb{F}_q^*$.

Results for the matrices $S_{XYZ}^{[p]}$ with $p = 1, 2, \ldots, v+1$ can be verified similarly. The proof is now complete. ■

IEEE Trans. Inf. Theory

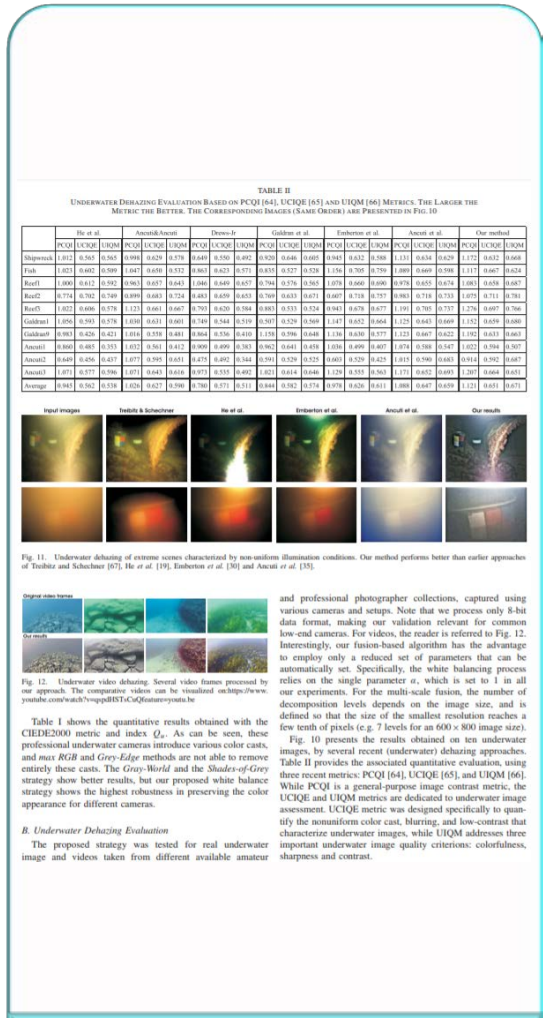


TABLE II
UNDERWATER DEHAZING EVALUATION BASED ON PCQI [64], UCIQE [65] AND UIQM [66] METRICS. THE LARGER THE METRIC THE BETTER. THE CORRESPONDING IMAGES (SAME ORDER) ARE PRESENTED IN FIG. 10

	He et al.			Ancuti&Ancuti			Drews-Jr			Galdran et al.			Emberton et al.			Ancuti et al.			Our method		
	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM	PCQI	UCIQE	UIQM
Shipwreck	1.012	0.565	0.565	0.998	0.629	0.578	0.649	0.550	0.492	0.920	0.646	0.605	0.945	0.632	0.588	1.131	0.634	0.629	1.172	0.632	0.668
Fish	1.023	0.602	0.599	1.047	0.650	0.532	0.865	0.623	0.571	0.835	0.527	0.528	1.156	0.705	0.759	1.089	0.669	0.598	1.117	0.667	0.624
Reef1	1.000	0.612	0.592	0.963	0.657	0.643	1.046	0.649	0.657	0.794	0.576	0.565	1.078	0.660	0.690	0.978	0.655	0.674	1.083	0.658	0.687
Reef2	0.774	0.702	0.749	0.899	0.683	0.724	0.483	0.659	0.653	0.769	0.633	0.671	0.607	0.718	0.757	0.983	0.718	0.733	1.075	0.711	0.781
Reef3	1.022	0.606	0.578	1.123	0.661	0.667	0.793	0.620	0.584	0.883	0.533	0.524	0.943	0.678	0.677	1.191	0.705	0.737	1.276	0.697	0.766
Galdran1	1.056	0.593	0.578	1.030	0.631	0.601	0.749	0.544	0.519	0.507	0.529	0.569	1.147	0.652	0.664	1.125	0.643	0.669	1.152	0.659	0.686
Galdran8	0.983	0.426	0.421	1.014	0.558	0.481	0.864	0.536	0.410	0.158	0.596	0.648	1.136	0.630	0.577	1.123	0.667	0.622	1.192	0.633	0.663
Ancuti1	0.860	0.485	0.353	1.032	0.561	0.412	0.809	0.499	0.383	0.962	0.641	0.458	1.036	0.499	0.407	1.074	0.588	0.547	1.022	0.594	0.507
Ancuti2	0.649	0.456	0.437	1.077	0.595	0.651	0.475	0.492	0.344	0.591	0.529	0.525	0.601	0.529	0.425	1.015	0.590	0.683	0.914	0.592	0.687
Ancuti3	1.071	0.577	0.596	1.071	0.643	0.616	0.973	0.535	0.492	1.021	0.614	0.646	1.129	0.555	0.563	1.171	0.652	0.693	1.207	0.664	0.651
Average	0.945	0.562	0.538	1.026	0.627	0.590	0.780	0.571	0.511	0.844	0.582	0.574	0.978	0.626	0.611	1.088	0.647	0.659	1.121	0.651	0.671

Fig. 11. Underwater dehazing of extreme scenes characterized by non-uniform illumination conditions. Our method performs better than earlier approaches of Treibitz and Schechner [67], He *et al.* [19], Emberton *et al.* [30] and Ancuti *et al.* [35].

Fig. 12. Underwater video dehazing. Several video frames processed by our approach. The comparative videos can be visualized on:https://www.youtube.com/watch?v=upqvBHSTsCuQfeature=youtu.be

Table I shows the quantitative results obtained with the CIEDE2000 metric and index Q_u. As can be seen, these professional underwater cameras introduce various color casts, and *max RGB* and *Grey-Edge* methods are not able to remove entirely these casts. The *Gray-World* and the *Shades-of-Grey* strategy show better results, but our proposed white balance strategy shows the highest robustness in preserving the color appearance for different cameras.

B. Underwater Dehazing Evaluation

The proposed strategy was tested for real underwater image and videos taken from different available amateur and professional photographer collections, captured using various cameras and setups. Note that we process only 8-bit data format, making our validation relevant for common low-end cameras. For videos, the reader is referred to Fig. 12. Interestingly, our fusion-based algorithm has the advantage to employ only a reduced set of parameters that can be automatically set. Specifically, the white balancing process relies on the single parameter a, which is set to 1 in all our experiments. For the multi-scale fusion, the number of decomposition levels depends on the image size, and is defined so that the size of the smallest resolution reaches a few tenth of pixels (e.g. 7 levels for an 600 × 800 image size).

Fig. 10 presents the results obtained on ten underwater images, by several recent (underwater) dehazing approaches. Table II provides the associated quantitative evaluation, using three recent metrics: PCQI [64], UCIQE [65], and UIQM [66]. While PCQI is a general-purpose image contrast metric, the UCIQE and UIQM metrics are dedicated to underwater image assessment. UCIQE metric was designed specifically to quantify the nonuniform color cast, blurring, and low-contrast that characterize underwater images, while UIQM addresses three important underwater image quality criterions: colorfulness, sharpness and contrast.

IEEE Trans. Image Proc.

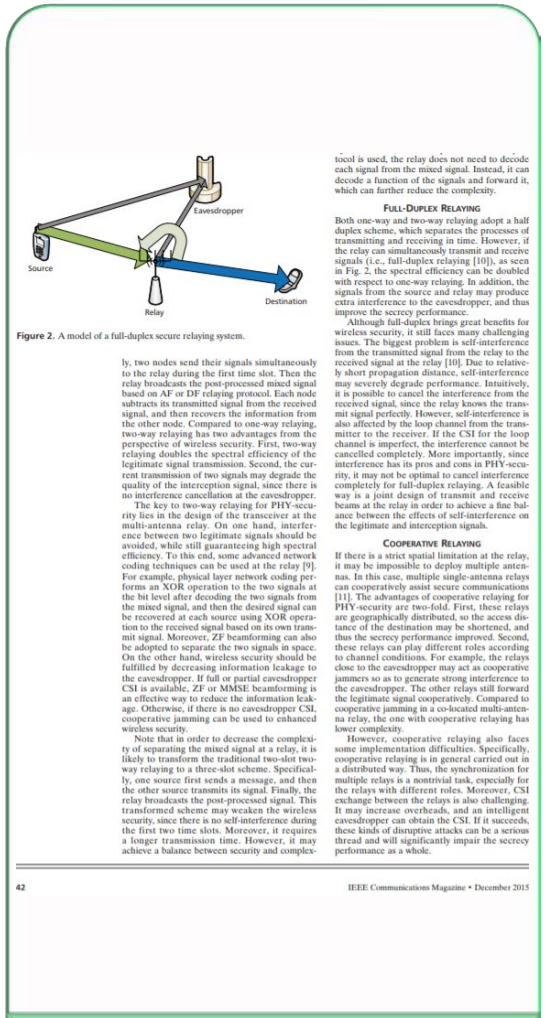


Figure 2. A model of a full-duplex secure relaying system.

ly, two nodes send their signals simultaneously to the relay during the first time slot. Then the relay broadcasts the post-processed mixed signal based on AF or DF relaying protocol. Each node subtracts its transmitted signal from the received signal, and then recovers the information from the other node. Compared to one-way relaying, two-way relaying has two advantages from the perspective of wireless security. First, two-way relaying doubles the spectral efficiency of the legitimate signal transmission. Second, the current transmission of two signals may degrade the quality of the interception signal, since there is no interference cancellation at the eavesdropper.

The key to two-way relaying for PHY-security lies in the design of the transceiver at the multi-antenna relay. On one hand, interference between two legitimate signals should be avoided, while still guaranteeing high spectral efficiency. To this end, some advanced network coding techniques can be used at the relay [9]. For example, physical layer network coding performs an XOR operation to the two signals at the bit level after decoding the two signals from the mixed signal, and then the desired signal can be recovered at each source using XOR operation to the received signal based on its own transmit signal. Moreover, ZF beamforming can also be adopted to separate the two signals in space. On the other hand, wireless security should be fulfilled by decreasing information leakage to the eavesdropper. If full or partial eavesdropper CSI is available, ZF or MMSE beamforming is an effective way to reduce the information leakage. Otherwise, if there is no eavesdropper CSI, cooperative jamming can be used to enhanced wireless security.

Note that in order to decrease the complexity of separating the mixed signal at a relay, it is likely to transform the traditional two-slot two-way relaying to a three-slot scheme. Specifically, one source first sends a message, and then the other source transmits its signal. Finally, the relay broadcasts the post-processed signal. This transformed scheme may weaken the wireless security, since there is no self-interference during the first two time slots. Moreover, it requires a longer transmission time. However, it may achieve a balance between security and complexity and is used, the relay does not need to decode each signal from the mixed signal. Instead, it can decode a function of the signals and forward it, which can further reduce the complexity.

FULL-DUPLEX RELAYING

Both one-way and two-way relaying adopt a half duplex scheme, which separates the processes of transmitting and receiving in time. However, if the relay can simultaneously transmit and receive signals (i.e., full-duplex relaying [10]), as seen in Fig. 2, the spectral efficiency can be doubled with respect to one-way relaying. In addition, the signals from the source and relay may produce extra interference to the eavesdropper, and thus improve the secrecy performance.

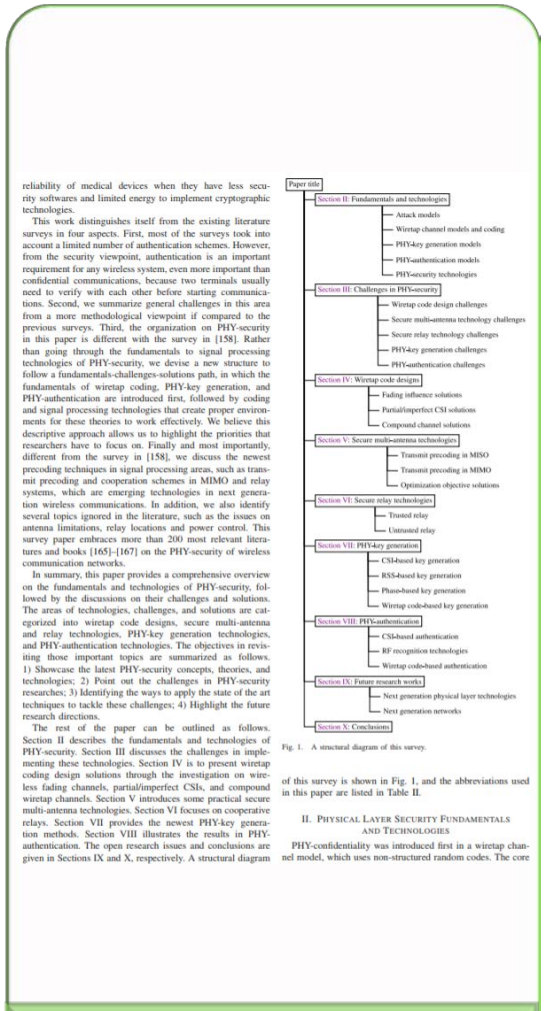
Although full-duplex brings great benefits for wireless security, it still faces many challenging issues. The biggest problem is self-interference from the transmitted signal from the relay to the received signal at the relay [10]. Due to relatively short propagation distance, self-interference may severely degrade performance. Intuitively, it is possible to cancel the interference from the received signal, since the relay knows the transmit signal perfectly. However, self-interference is also affected by the loop channel from the transmitter to the receiver. If the CSI for the loop channel is imperfect, the interference cannot be cancelled completely. More importantly, since interference has its pros and cons in PHY-security, it may not be optimal to cancel interference completely for full-duplex relaying. A feasible way is a joint design of transmit and receive beams at the relay in order to achieve a fine balance between the effects of self-interference on the legitimate and interception signals.

COOPERATIVE RELAYING

If there is a strict spatial limitation at the relay, it may be impossible to deploy multiple antennas. In this case, multiple single-antenna relays can cooperatively assist secure communications [11]. The advantages of cooperative relaying for PHY-security are two-fold. First, these relays are geographically distributed, so the access distance of the destination may be shortened, and thus the secrecy performance improved. Second, these relays can play different roles according to channel conditions. For example, the relays close to the eavesdropper may act as cooperative jammers so as to generate strong interference to the eavesdropper. The other relays still forward the legitimate signal cooperatively. Compared to cooperative jamming in a co-located multi-antenna relay, the one with cooperative relaying has lower complexity.

However, cooperative relaying also faces some implementation difficulties. Specifically, cooperative relaying is in general carried out in a distributed way. Thus, the synchronization for multiple relays is a nontrivial task, especially for the relays with different roles. Moreover, CSI exchange between the relays is also challenging. It may increase overheads, and an intelligent eavesdropper can obtain the CSI. If it succeeds, these kinds of disruptive attacks can be a serious thread and will significantly impair the secrecy performance as a whole.

IEEE Commun. Maganization



reliability of medical devices when they have less security softwares and limited energy to implement cryptographic technologies.

This work distinguishes itself from the existing literature surveys in four aspects. First, most of the surveys took into account a limited number of authentication schemes. However, from the security viewpoint, authentication is an important requirement for any wireless system, even more important than confidential communications, because two terminals usually need to verify with each other before starting communications. Second, we summarize general challenges in this area from a more methodological viewpoint if compared to the previous surveys. Third, the organization on PHY-security in this paper is different with the survey in [158]. Rather than going through the fundamentals to signal processing technologies of PHY-security, we devise a new structure to follow a fundamentals-challenges-solutions path, in which the fundamentals of wiretap coding, PHY-key generation, and PHY-authentication are introduced first, followed by coding and signal processing technologies that create proper environments for these theories to work effectively. We believe this descriptive approach allows us to highlight the priorities that researchers have to focus on. Finally and most importantly, different from the survey in [158], we discuss the newest precoding techniques in signal processing areas, such as transmit precoding and cooperation schemes in MIMO and relay systems, which are emerging technologies in next generation wireless communications. In addition, we also identify several topics ignored in the literature, such as the issues on antenna limitations, relay locations and power control. This survey paper embraces more than 200 most relevant literatures and books [165]–[167] on the PHY-security of wireless communication networks.

In summary, this paper provides a comprehensive overview on the fundamentals and technologies of PHY-security, followed by the discussions on their challenges and solutions. The areas of technologies, challenges, and solutions are categorized into wiretap code designs, secure multi-antenna and relay technologies, PHY-key generation technologies, and PHY-authentication technologies. The objectives in revisiting those important topics are summarized as follows. 1) Showcase the latest PHY-security concepts, theories, and technologies; 2) Point out the challenges in PHY-security researches; 3) Identifying the ways to apply the state of the art techniques to tackle these challenges; 4) Highlight the future research directions.

The rest of the paper can be outlined as follows. Section II describes the fundamentals and technologies of PHY-security. Section III discusses the challenges in implementing these technologies. Section IV is to present wiretap coding design solutions through the investigation on wireless fading channels, partial/imperfect CSIs, and compound wiretap channels. Section V introduces some practical secure multi-antenna technologies. Section VI focuses on cooperative relays. Section VII provides the newest PHY-key generation methods. Section VIII illustrates the results in PHY-authentication. The open research issues and conclusions are given in Sections IX and X, respectively. A structural diagram of this survey is shown in Fig. 1, and the abbreviations used in this paper are listed in Table II.

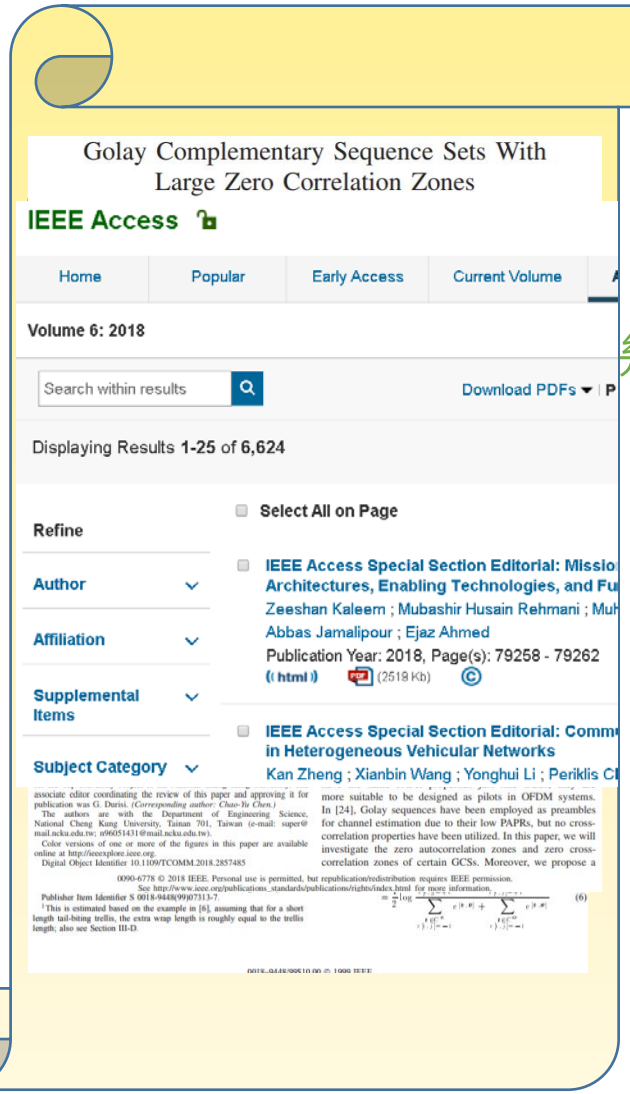
Fig. 1. A structural diagram of this survey.

II. PHYSICAL LAYER SECURITY FUNDAMENTALS AND TECHNOLOGIES

PHY-confidentiality was introduced first in a wiretap channel model, which uses non-structured random codes. The core

IEEE Commun. Surveys Tutorials

全球趨勢


Golay Complementary Sequence Sets With Large Zero Correlation Zones

IEEE Access

Home | Popular | Early Access | Current Volume

Volume 6: 2018

Search within results

Download PDFs

Displaying Results 1-25 of 6,624

Refine

Author

Affiliation

Supplemental Items

Subject Category

Select All on Page

IEEE Access Special Section Editorial: Missio
Architectures, Enabling Technologies, and Fu
Zeeshan Kaleem ; Mubashir Husain Rehmani ; Mu
Abbas Jamalipour ; Ejaz Ahmed
Publication Year: 2018, Page(s): 79258 - 79262
(2518 Kb)

IEEE Access Special Section Editorial: Comm
in Heterogeneous Vehicular Networks
Kan Zheng ; Xianbin Wang ; Yonghui Li ; Periklis C

01 1960 幾頁期刊論文

02 1994 一頁研討會論文

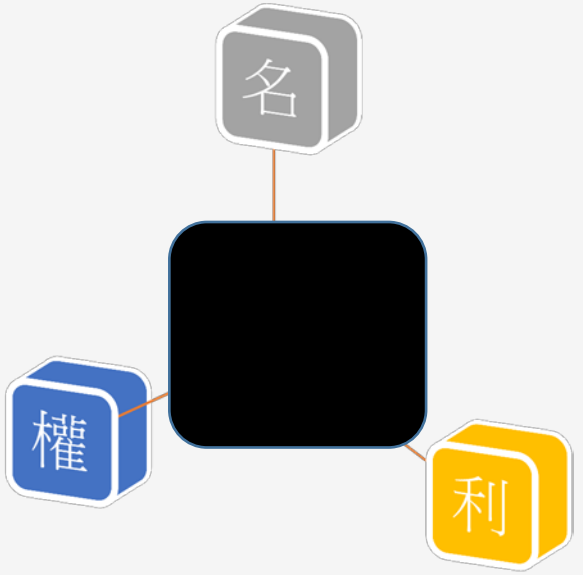
03 1996 長短篇期刊論文

04 2010 長篇期刊論文

05 2015 Open Access論文

研究社群保衛科學倫理

單元名稱	大學部 核心課程	大學部進階 核心課程	研究所 核心課程	教研人員 推薦課程	IRB / REC 相關課程	英文版本
0117_認識學術誠信	○	○	○	○		○
0101_研究倫理定義與內涵		○	○	○		○
0102_研究倫理專業規範與個人責任			○	○		○
0103_研究倫理的政府規範與政策			○	○		○
0104_不當研究行為：定義與類型		○	○	○		○
0105_不當研究行為：捏造與篡改資料		○	○	○		○
0106_不當研究行為：抄襲與剽竊		○	○	○		○
0107_不當研究行為：自我抄襲		○	○	○		○
0108_學術寫作技巧：引述		○	○	○		○
0109_學術寫作技巧：改寫與摘寫		○	○	○		○
0110_學術寫作技巧：引用著作		○	○	○		○
0111_論文作者定義與掛名原則		○	○	○		○
0112_著作權基本概念	○	○	○	○		○
0113_個人資料保護法基本概念		○	○	○	○	○
0114_隱私權基本概念		○	○	○	○	○
0115_受試者保護原則與實務		○	○	○	○	○
0116_研究資料管理概述	○	○	○	○		○
0201_研究中的利益衝突			○	○	○	○
0118_為什麼不能作弊？	○	○				○
0119_不當研究行為及學術寫作技巧	○	○				○
0120_網路著作權	○	○				○



臺灣學術倫理教育資源中心

抄襲、實驗數據造假

掠奪性期刊、研討會

謝謝聆聽

I-Shou University
Office of Library & Information Services