รหัสลายนิ้วมือดิจิทัล : สมบัติและการสร้าง
(Digital Fingerprints Codes: Property and Construction)

นางสาวณัฐนันท์ ใจสม
630510473

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์
มหาวิทยาลัยเชียงใหม่
ภาคเรียนที่ 1 ปีการศึกษา 2566

รหัสลายนิ้วมือดิจิทัล : สมบัติและการสร้าง

(Digital Fingerprints Codes: Property and Construction)

ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต
สาขาวิชาคณิตศาสตร์

คณะกรรมการควบคุมการค้นคว้าอิสระ

เป็นหญิง โรจนกุล ..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.เป็นหญิง โรจนกุล)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สุปรีดี แดงสกุล)

วันที่ 25 เดือน ตุลาคม พ.ศ. 2566

กิตติกรรมประกาศ

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์ มหาวิทยาลัยเชียงใหม่ ในกระบวนวิชา 206499 ซึ่งผู้ค้นคว้าได้ศึกษาในหัวข้อเรื่อง รหัสลายนิ้วมือดิจิทัล : สมบัติและการสร้าง (Digital Fingerprints Codes: Property and Construction)

ผู้ค้นคว้าขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.เป็นหญิง โรจนกุล อาจารย์ที่ปรึกษาการค้นคว้าอิสระที่ได้สนับสนุนในการค้นคว้าอิสระในครั้งนี้ รวมทั้งให้คำปรึกษา ช่วยตรวจสอบ และช่วยอธิบายในส่วนที่ผู้ค้นคว้าไม่เข้าใจ ตลอดจนช่วยแก้ไขข้อผิดพลาดต่าง ๆ จนงานค้นคว้าอิสระนี้สำเร็จสมบูรณ์ได้ด้วยดี และขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ สุปรีดี แดงสกุล อาจารย์กรรมการสอบงานค้นคว้าอิสระ รวมทั้งตรวจสอบความถูกต้องเหมาะสม และให้คำแนะนำที่เป็นประโยชน์ สำหรับการปรับปรุงแก้ไขงานค้นคว้าอิสระฉบับนี้ให้ดียิ่งขึ้น

ขอขอบพระคุณอาจารย์ทุกท่านที่ได้อบรมสั่งสอนและให้ความรู้แก่ผู้ค้นคว้า อันเป็นประโยชน์และสามารถนำความรู้มาประยุกต์ใช้ในงานค้นคว้าอิสระได้ สุดท้ายนี้ ขอขอบพระคุณบิดา มารดา ผู้ให้กำลังใจแก่ผู้ค้นคว้าจนสำเร็จการศึกษาระดับปริญญาตรี และอีกหลาย ๆ ท่านที่ข้าพเจ้ายังไม่ได้กล่าวถึง

หากผลงานการค้นคว้าอิสระฉบับนี้เกิดข้อผิดพลาด หรือได้รับคำติชมประการใดผู้จัดทำขออภัยมา ณ ที่นี้ด้วย

ณัฐนันท์ ใจสม

หัวข้อ (ภาษาไทย) รหัสลายนิ้วมือดิจิทัล : สมบัติและการสร้าง

หัวข้อ (ภาษาอังกฤษ) Digital Fingerprints Codes: Property and Construction

ชื่อผู้ทำการค้นคว้าอิสระ นางสาวณัฐนันท์ ใจสม รหัสนักศึกษา 630510473

ชื่ออาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.เป็นหญิง โรจนกุล

ชื่อกรรมการสอบ ผู้ช่วยศาสตราจารย์ ดร. สุปรีดี แดงสกุล

บทคัดย่อ

ในการศึกษาครั้งนี้ ผู้ค้นคว้าสนใจศึกษาสมบัติและการสร้างรหัสลายนิ้วมือดิจิทัล ซึ่งสามารถนำไปประยุกต์ใช้ป้องกันการละเมิดลิขสิทธิ์ทางดิจิทัลได้ ตรวจจับผู้ที่ทำผิดได้ โดยเราจะศึกษารหัส 4 ชนิด คือ รหัสเฟรมพรูฟ รหัสซีเคียวเฟรมพรูฟ รหัสระบุต้นกำเนิด และรหัสเทรซอะบิลลีที พร้อมทั้งสมบัติและความสัมพันธ์ระหว่างรหัสทั้ง 4 ชนิด นอกจากนี้ยังมีการค้นหาขอบเขตของรหัสต่าง ๆ และทำการสร้างรหัส 2-FP ความยาว 4 ที่มีขนาดใหญ่ที่สุดที่เป็นไปได้ รวมไปถึงการสร้างรหัสเทรซอะบิลลิที จากรหัสแก้ไขข้อผิดพลาด

Abstract

In this independent study, we are interested in properties and constructions of digital fingerprint codes, which can be used against digital piracy. We study 4 types of codes, namely frameproof codes, secureframeproof codes, parent identifying codes and traceability codes, including properties and relations between them. Moreover, we do literature review on bounds of codes and creates a 2-FP code of length 4 of the largest size possible. In addition, we construct traceability codes from error-correction codes.

สารบัญ

1 บทนำ **7**

1.1 **ความเป็นมา** 7

1.2 **วัตถุประสงค์** 8

1.3 **ประโยชน์ที่คาดว่าจะได้รับ** 8

1.4 **ขอบเขตของการศึกษา** 8

2 ความรู้พื้นฐาน **9**

2.1 **ความรู้พื้นฐานทางทฤษฎีรหัส** 9

2.2 **การกำหนดรหัสลายนิ้วมือ** 13

2.3 **ความสัมพันธ์ระหว่างรหัสลายนิ้วมือ** 20

3 ขอบเขตของรหัส **25**

3.1 **ขอบเขตของรหัสเฟรมพรูฟ (Frameproof Codes)** 25

3.2 **ขอบเขตของรหัสซีเคียวเฟรมพรูฟ (Secure Frameproof Codes)** 27

3.3 **ขอบเขตของรหัสระบุต้นกำเนิด (Identifiable Parent Property)** 28

3.4 **ขอบเขตของรหัสเทรซอะบิลลิที (Traceability)** 29

4 การสร้าง **31**

4.1 **รหัสเฟรมพรูฟ (Frameproof)** 31

4.2 **รหัสเทรซอะบิลลิที (Traceability)** 37

5 สรุปผลการศึกษา **39**

บทที่ 1

บทนำ

1.1. **ความเป็นมา**

เนื่องจากในปัจจุบันการป้องกันการละเมิดลิขสิทธิ์ทางดิจิทัลเป็นสิ่งสำคัญ แต่สามารถทำได้ยาก โดยเฉพาะตั้งแต่ยุคอินเตอร์เน็ตเป็นต้นมา ข้อมูลดิจิทัลต่าง ๆ เช่น เพลง ภาพยนตร์ เอกสาร e-book หรือซอฟต์แวร์ สามารถถูกคัดลอกและแจกจ่ายได้อย่างง่ายดาย ซึ่งทำให้เกิดการแจกจ่ายข้อมูลที่ผิดกฎหมาย หรือที่เรียกกว่า **การละเมิดลิขสิทธิ์** อย่างแพร่หลาย

เราสามารถใช้เทคนิคของฮาร์ดแวร์ที่ป้องกันการคัดลอกทรัพย์สินทางปัญญามาช่วยป้องกันการละเมิดลิขสิทธิ์ได้ แต่อย่างไรก็ตามเทคนิคเหล่านี้อาจลดความสะดวกของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงข้อมูล ไม่ให้ทำสิ่งที่ถูกต้องตามกฎหมาย เช่น การทำสำเนาของซีดีหรือดีวีดี หรือการใช้สื่อที่มีลิขสิทธิ์เพื่อการวิจัยและการศึกษาภายใต้กฎหมายการใช้งานโดยชอบ ดังนั้น เราจึงสนใจเทคนิคซึ่งทำการสอดแทรกลักษณะเฉพาะรูปแบบใดรูปแบบหนึ่งเข้าไปในข้อมูลดิจิทัลแต่ละชุด ทำให้สามารถรวบรวมหลักฐานเพื่อให้สามารถสืบทราบไปถึงกลุ่มเจ้าของไฟล์ต้นฉบับ แม้ว่าข้อมูลดิจิทัลแต่ละชุดจะถูกดัดแปลงและเอาผิดผู้แจกจ่ายสำเนาข้อมูลซ้ำอย่างผิดกฎหมาย เทคนิคเหล่านี้เรียกกันทั่วไปว่า **ลายนิ้วมือดิจิทัล** ในการค้นคว้าอิสระนี้เราสนใจคุณสมบัติของคณิตศาสตร์เชิงการจัด ที่อยู่เบื้องหลังเทคนิคดังกล่าว เรียกว่า **รหัสลายนิ้วมือ**

รหัสลายนิ้วมือคล้ายกับลายนิ้วมือของมนุษย์ ซึ่งลายนิ้วมือของมนุษย์แต่ละคนจะมีเอกลักษณ์เฉพาะตัว และสามารถใช้ระบุเจ้าของลายนิ้วมือได้ ลายนิ้วมือดิจิทัลจะระบุเอกลักษณ์ของข้อมูลดิจิทัลโดยเฉพาะ และช่วยให้เราสามารถระบุไปถึงเจ้าของไฟล์ดิจิทัลได้ ลายนิ้วมือในแต่ละระบบอาจแตกต่างกันไปตั้งแต่ตัวเลขหลักเดียวไปจนถึงกุญแจเข้ารหัส

1.2. วัตถุประสงค์

1. เพื่อศึกษาคุณสมบัติของรหัสลายนิ้วมือดิจิทัล
2. เพื่อศึกษาวิธีการสร้างรหัสลายนิ้วมือดิจิทัล
3. เพื่อค้นหาวิธีการระบุต้นฉบับลายนิ้วมือดิจิทัลจากลายนิ้วมือดิจิทัลดัดแปลง

1.3. ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ทราบคุณสมบัติของรหัสลายนิ้วมือดิจิทัล
2. ได้ทราบวิธีการสร้างรหัสลายนิ้วมือดิจิทัล
3. ได้ทราบวิธีการระบุต้นฉบับลายนิ้วมือดิจิทัลจากลายนิ้วมือดิจิทัลดัดแปลง

1.4. ขอบเขตของการศึกษา

1. ศึกษาเกี่ยวกับรหัสลายนิ้วมือดิจิทัล
2. ศึกษารหัสเฟรมพรูฟ (frameproof)
3. ศึกษารหัสซีเคียวเฟรมพรูฟ (secure frameproof)
4. ศึกษารหัสระบุต้นกำเนิด (identifiable parent property)
5. ศึกษารหัสเทรซอะบิลลิที (traceability)
6. ศึกษาความสัมพันธ์ระหว่างรหัสลายนิ้วมือดิจิทัลทั้ง 4 แบบ
7. การสร้างรหัสลายนิ้วมือดิจิทัล

รายงานฉบับนี้ประกอบไปด้วย 5 บท โดยประกอบได้ด้วยเนื้อหาดังต่อไปนี้ ความรู้พื้นฐานในเรื่องทฤษฎีรหัส ขอบเขตของรหัส และการสร้างรหัส โดย บทที่ 2 จะกล่าวถึง ความรู้พื้นฐานทางทฤษฎีรหัสและบทนิยามของรหัสลายนิ้วมือดิจิทัล บทที่ 3 จะกล่าวถึงขอบเขตของรหัส บทที่ 4 จะกล่าวถึงการสร้างรหัสเฟรมพรูฟ และรหัสเทรซอะบิลลีที และสรุปผลในบทที่ 5

บทที่ 2

ความรู้พื้นฐาน

ในบทนี้จะกล่าวถึงความรู้พื้นฐานที่สำคัญในการค้นคว้าอิสระ โดยช่วงแรกจะกล่าวถึงความรู้พื้นฐานทางทฤษฎีรหัส แล้วจึงตามด้วยนิยามของรหัสลายนิ้วมือชนิดต่าง ๆ ปิดท้ายด้วยความสัมพันธ์ระหว่างรหัสลายนิ้วมือแต่ละชนิด

2.1. ความรู้พื้นฐานทางทฤษฎีรหัส

บทนิยาม 2.1.1 : ให้ q และ n เป็นจำนวนนับใด ๆ *เซตอักษรฐาน* q (q-ary alphabet) คือเซตจำกัดที่ประกอบไปด้วยสมาชิก q ตัว เรียกสมาชิกของเซตอักษรว่า *สัญลักษณ์* (symbols)

บทนิยาม 2.1.2 : ให้ q และ n เป็นจำนวนนับใด ๆ ให้ A เป็นเซตอักษรฐาน q
เรียก $\emptyset \neq C \subseteq A^n$ ว่า *รหัส (Code)* ฐาน q ความยาว n เหนือ A
เรียกจำนวนสมาชิกของ C ว่า *ขนาด (size)* ของ C เขียนแทนด้วย $|C|$
สมาชิกของ A^n เรียกว่า *คำ (words)* และสมาชิกของ C เรียกว่า *คำรหัส (codewords)*

หมายเหตุ 2.1.3 : เพื่อง่ายต่อการอธิบายในการค้นคว้าอิสระนี้ บางครั้งเราเรียกทั้ง คำและคำรหัส ว่า *ลายนิ้วมือ (fingerprints)*

เพื่อป้องกันการละเมิดลิขสิทธิ์ทางดิจิทัล ลายนิ้วมือจากรหัส C จะถูกนำมาใช้ดังนี้ ข้อมูลดิจิทัลแต่ละชุดจะถูกฝังลายนิ้วมือที่แตกต่างกันไว้เพื่อเป็นเอกลักษณ์เฉพาะของข้อมูลแต่ละชุด เมื่อชุดข้อมูลแต่ละชุดถูกขายหรือแจกจ่ายออกไป ลายนิ้วมือที่ซ่อนอยู่จะทำให้เรารู้ว่าข้อมูลแต่ละชุดเป็นของใคร ใครเป็นผู้ซื้อ ดังนั้น เมื่อไรก็ตามที่เราเจอการเผยแพร่ข้อมูลแบบผิดกฎหมาย เราก็สามารถใช้กฎหมายกับ

เจ้าของข้อมูลชุดนั้นได้

สำหรับแต่ละ $x \in A^n$ คำ เราเขียน x_i แทนสัญลักษณ์ในตำแหน่งที่ i ของ x ยกตัวอย่างเช่น $x = 0110$ จะได้ว่า $x_1 = 0, x_2 = 1, x_3 = 1$ และ $x_4 = 0$

สำหรับจำนวนเต็มบวก n ใช้สัญลักษณ์ $[n]$ แทนเซตของจำนวนเต็มจาก 1 ถึง n นั่นคือ $[n] = \{1, 2, 3, .., n\}$

นิยามต่อไปจะกล่าวถึงระยะแฮมมิงซึ่งเป็นจำนวนตำแหน่งที่ต่างกันของสองคำใด ๆ

<u>บทนิยาม 2.1.4</u> : ให้ A เป็นเซตอักษรฐาน q และให้ $x, y \in A^n$
กำหนด *ระยะแฮมมิง (hamming distance)* ระหว่าง x, y แทนด้วยสัญลักษณ์ $d_H(x, y)$ ดังนี้

$$d_H(x, y) = |\{i \in [n] : x_i \neq y_i\}|$$

สำหรับเซตย่อย $X \subseteq A^n$ ใด ๆ ที่ไม่เป็นเซตว่าง *ระยะที่น้อยที่สุด (minimum distance)* ของ X กำหนดจากระยะต่ำสุดระหว่าง 2 ลายนิ้วมือใด ๆ ใน X แทนด้วยสัญลักษณ์ดังนี้

$$d_H(X) = \min_{\substack{x,y \in X \\ x \neq y}} d_H(x, y)$$

สำหรับทุก ๆ $X \subseteq A^n$ และ $y \in A^n$ กำหนด

$$d_H(X, y) = \min_{x \in X} d_H(x, y)$$

<u>ตัวอย่าง 2.1.5</u> : ให้ $X = \{a, b, c\}$ ถ้าให้ $a = 1111, b = 1100, c = 0001$ และ $y = 0110$ แล้ว จงหา $d_H(X)$

วิธีทำ

พิจารณา $d_H(a, b) = |\{3, 4\}| = 2$, $d_H(b, c) = |\{1, 2, 4\}| = 3$ และ $d_H(a, c) = |\{1, 2, 3\}| = 3$
ดังนั้น $d_H(X) = 2$ □

<u>บทนิยาม 2.1.6</u> : ให้ C เป็นรหัส กำหนด *ระยะ (distance)* ของ C เป็นระยะที่น้อยที่สุดของ C แทนด้วยสัญลักษณ์ $d(C)$ กล่าวคือ

$$d(C) = \min\{d_H(x, y) : x, y \in C, x \neq y\}$$

ตัวอย่าง 2.1.7 : ให้ $C = \{00000, 00111, 11111\}$ เป็นรหัสฐาน 2 จงหา $d(C)$

วิธีทำ พิจารณา

$$d_H(00000, 00111) = 3$$

$$d_H(00000, 11111) = 5$$

$$d_H(11111, 00111) = 2$$

ดังนั้น $d(C) = 2$ □

บทนิยาม 2.1.8 : ให้ F เป็นเซตภายใต้การดำเนินการบวก + และการคูณ $\cdot$ ที่สอดคล้องกับสมบัติดังต่อไปนี้

สัจพจน์สำหรับการบวก (Axioms of addition)

(A1) สมบัติปิด : $x + y \in \mathbb{F}$ สำหรับทุก $x, y \in F$

(A2) สมบัติการสลับที่ : $x + y = y + x$ สำหรับทุก $x, y \in F$

(A3) สมบัติการจัดหมู่ : $(x + y) + z = x + (y + z)$ สำหรับทุก $x, y, z \in F$

(A4) สมบัติการมีเอกลักษณ์ : มี $0 \in F$ เพียงตัวเดียวเท่านั้นที่ทำให้ $x + 0 = x = 0 + x$ สำหรับทุก $x \in F$ เรียก 0 ว่าเอกลักษณ์การบวกของ F

(A5) สมบัติการมีตัวผกผัน : สำหรับแต่ละ $x \in F$ จะมี $-x \in F$ เพียงตัวเดียวเท่านั้นที่ทำให้ $x+(-x) = 0 = (-x) + x$ เราเรียก $-x$ ว่าตัวผกผันการบวกของ x

สัจพจน์สำหรับการคูณ (Axioms of multiplication)

(M1) สมบัติปิด : $x \cdot y \in F$ สำหรับทุก $x, y \in F$

(M2) สมบัติการสลับที่ : $x \cdot y = y \cdot x$ สำหรับทุก $x, y \in F$

(M3) สมบัติการจัดหมู่ : $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ สำหรับทุก $x, y, z \in F$

(M4) สมบัติการมีเอกลักษณ์ : มี $1 \in \mathbb{F}$ เพียงตัวเดียวเท่านั้นที่ทำให้ $x \cdot 1 = x = 1 \cdot x$ สำหรับทุก $x \in F$ เรียก 1 ว่าเอกลักษณ์การคูณของ F

(M5) สมบัติการมีตัวผกผัน : สำหรับแต่ละ $x \in F$ ที่ $x \neq 0$ จะมี $x^{-1} \in F$ เพียงตัวเดียวเท่านั้นที่ทำให้ $x \cdot x^{-1} = 0 = x^{-1} \cdot x$ เราเรียก x^{-1} ว่าตัวผกผันการคูณของ x

สัจพจน์แห่งการแจกแจง (Axioms of distribution)

(D) $x \cdot (y + z) = x \cdot y + x \cdot z$ สำหรับทุก $x, y, z \in F$

แล้วจะเรียก F ว่า *ฟิลด์ (Field)*

ตัวอย่าง 2.1.9 : จากสมบัติของฟิลด์ จะได้ว่าข้อความนี้เป็นจริง สำหรับทุก $x, y, z \in F$
ตัวอย่างเช่น $\mathbb{R}$ เป็นฟิลด์ เนื่องจากมีสัจพจน์สำหรับการบวก และสัจพจน์สำหรับการคูณ รวมไปถึงการมีสัจพจน์แห่งการแจกแจง

บทนิยาม 2.1.10 : ให้ C เป็น *รหัสแก้ไขข้อผิดพลาด (error-correcting codes)* คือรหัสที่มีการเพิ่มตำแหน่งตรวจสอบสภาวะคู่หรือคี่เข้าไป เพื่อให้สามารถตรวจจับและแก้ไขข้อผิดพลาดที่เกิดขึ้นได้ ภายใต้ขั้นตอนวิธีใด ขั้นตอนวิธีหนึ่ง โดยไม่ต้องส่งข้อความซ้ำ

ตัวอย่าง 2.1.11 : ให้ $C = \{000, 111\}$ เป็นรหัสฐาน 2 ความยาว 3 จะได้ว่า C เป็นรหัสแก้ไขข้อผิดพลาดถึง 1 ตำแหน่ง
พิสูจน์ เราจะพิจารณาคำรหัสทั้งหมดใน C
ในกรณีที่เกิดข้อผิดตลาด 1 ตำแหน่ง
คำรหัส 000 ผิดพลาดเป็น 100
$d_H(100, 000) = 1 \qquad d_H(100, 111) = 2 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 000
คำรหัส 000 ผิดพลาดเป็น 010
$d_H(010, 000) = 1 \qquad d_H(010, 111) = 2 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 000
คำรหัส 000 ผิดพลาดเป็น 001
$d_H(001, 000) = 1 \qquad d_H(001, 111) = 2 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 000
คำรหัส 111 ผิดพลาดเป็น 011
$d_H(011, 000) = 2 \qquad d_H(011, 111) = 1 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 111
คำรหัส 111 ผิดพลาดเป็น 101
$d_H(101, 000) = 2 \qquad d_H(101, 111) = 1 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 111
คำรหัส 111 ผิดพลาดเป็น 110
$d_H(110, 000) = 2 \qquad d_H(110, 111) = 1 \longrightarrow$ ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 111
เนื่องจาก ถ้า 000 ผิดพลาด 2 ตำแหน่งเป็น 011 จะได้ว่า $d_H(000, 011) = 2$
ถอดรหัสเป็นคำรหัสที่ใกล้เคียงที่สุดได้เป็น 111
ทำให้ไม่เป็นรหัสแก้ไขข้อผิดพลาด 2 ตำแหน่ง
ดังนั้น C เป็น รหัสแก้ไขข้อผิดพลาด 1 ตำแหน่ง □

2.2. **การกำหนดรหัสลายนิ้วมือ**

ในหัวข้อนี้จะกล่าวถึงนิยามของรหัสลายนิ้วมือทั้งสี่ชนิด โดยเริ่มจากแรงบันดาลใจที่ทำให้เกิดนิยามเหล่านี้ขึ้นมา Naor และ Fiat [2] นำเสนอ แบบแผนการเข้ารหัสออกอากาศ (Broadcast encryption schemes) ครั้งแรกในงาน Eurocrypt ปี 1993 มีสถานการณ์เบื้องต้นดังนี้ สถานีโทรทัศน์ต้องการถ่ายทอดสัญญาณโทรทัศน์ในรูปแบบเข้ารหัสไปตามเครือข่าย โดยสัญญาณจะถูกเข้ารหัสด้วยกุญแจหลัก K จากเซต $\mathcal{K}$ ซึ่งใช้งานได้แค่ภายในระยะเวลาใดเวลาหนึ่งและมีการเปลี่ยนอย่างสม่ำเสมอ กุญแจหลัก K จะถูกแบ่งออกเป็น n ส่วน และแต่ละส่วนจะถูกเข้ารหัสด้วยกุญแจที่แตกต่างกันและส่งไปยังผู้ใช้ระบบในแต่ละช่วงเวลา แต่ละส่วนของ K จะสามารถถอดรหัสได้ด้วยกุญแจ q แบบ เรียกกุญแจที่ใช้ในการถอดรหัสกุญแจหลักส่วนที่ i ว่า กุญแจชนิดที่ i ผู้ใช้ในเครือข่ายจะจ่ายเงินซื้อกล่อง TV เพื่อรับและถอดรหัสสัญญาณโดยในกล่องจะมีกุญแจ n ชนิด ชนิดละ 1 ดอก กุญแจเหล่านี้จะใช้ในการถอดรหัสส่วนย่อยของกุญแจหลัก เพื่อประกอบให้ได้ K เพื่อใช้ในการถอดรหัสสัญญาณโทรทัศน์ต่อไป

ในสถานการณ์นี้การกระจายสัญญาณที่ถอดรหัสแล้วออกไป ต้องอาศัยทรัพยากรจำนวนมาก ทั้งต้องถอดรหัสสัญญาณโทรทัศน์ตลอดเวลา และต้องส่งสัญญาณดังกล่าวออกไปด้วย ดังนั้น ผู้ที่ต้องการส่งต่อสัญญาณโทรทัศน์ให้ผู้ใช้นอกระบบอย่างผิดกฎหมายมักเลือกที่จะทำสำเนาของกล่อง TV และชุดกุญแจแทน หรือบางครั้งกลุ่มของผู้ใช้ในระบบอาจรวมตัวกันเพื่อสร้างชุดกุญแจดัดแปลง โดยนำกุญแจของทุกคนในกลุ่มมารวมกันแล้วสร้างชุดกุญแจดัดแปลงโดยให้มีกุญแจ n ชนิด ชนิดละ 1 ดอก จากกุญแจที่มีอยู่เดิมของคนในกลุ่ม

จากสถานการณ์ข้างต้นผู้เผยแพร่สัญญาณอาจมีเป้าหมายที่จะสืบทราบบสมาชิกของกลุ่มผู้ใช้ที่รวมกันสร้างชุดกุญแจดัดแปลง จากชุดกุญแจดัดแปลงที่พบ แล้วนำไปสู่การจับกุมสมาชิกที่เหลือ หรือผู้เผยแพร่สัญญาณ อาจต้องการเพียงจะแน่ใจว่า ไม่มีผู้บริสุทธิ์ถูกใส่ร้ายจากชุดกุญแจดัดแปลงที่กลุ่มผู้ใช้สร้างขึ้น

ก่อนที่จะกำหนดรหัสลายนิ้วมือ เราจะกล่าวถึงแนวคิดของดีเซนแดนท์ ซึ่งเป็นชุดกุญแจดัดแปลงทั้งหมดที่สามารถรับได้จากชุดกุญแจของกลุ่มสมาชิก

<u>บทนิยาม 2.2.1</u> : ให้ A เป็นเซตที่ไม่ใช่เซตว่าง สำหรับ $X \subseteq A^n$ เซตของ *ดีเซนแดนท์ (descendants)* ของ X แทนด้วยสัญลักษณ์ $\mathrm{desc}(X)$ คือ

$$\mathrm{desc}(X) = \{d \in A^n : \forall i \in [n], \exists x \in X \text{ ที่ } d_i = x_i\}$$

สังเกตได้ว่าดีเซนแดนท์มีหลักการเดียวกับ DNA ของลูกซึ่งแต่ละตำแหน่งจะตรงกับพ่อหรือแม่เท่านั้น เพียงแต่พ่อและแม่ของรหัสจะไม่ได้จำกัดไว้ที่ 2 คำ

ตัวอย่าง 2.2.2 : ถ้าให้ $P = \{1100, 2102, 1122\}$ แล้ว

$$\mathrm{desc}(P) = \{1100, 1102, 1120, 1122, 2100, 2102, 2120, 2122\}$$

เนื่องจาก ลายนิ้วมือใน $\mathrm{desc}(P)$ สร้างจากสัญลักษณ์ของลายนิ้วมือใน P ซึ่งสัญลักษณ์ในตำแหน่งแรกสามารถเป็นได้เพียง 1 หรือ 2 เท่านั้น ในขณะที่สัญลักษณ์ในตำแหน่งสองสามารถเป็นได้แค่ 1 และสัญลักษณ์ในตำแหน่งสามและสี่เป็นได้เพียง 0 หรือ 2 เท่านั้น

ถ้าเราเชื่อมโยงตัวอย่างนี้กลับไปสู่สถานการณ์การกระจายสัญญาณโทรทัศน์เมื่อตอนต้น เราพิจารณา P เป็นชุดกุญแจที่ได้จากกลุ่มผู้ใช้ 3 คน แล้วชุดลายนิ้วมือ $\mathrm{desc}(P)$ เป็นเซตของชุดกุญแจที่เป็นไปได้ทั้งหมดที่กลุ่มคนนี้สามารถผลิตได้ ภายใต้เงื่อนไขการสร้างชุดกุญแจดัดแปลงที่กำหนด

บทนิยาม 2.2.3 : ให้ k เป็นจำนวนเต็มบวก ให้ A เป็นเซตที่ไม่ใช่เซตว่าง สำหรับ $C \subseteq A^n$ เซตของ *รหัส k-ดีเซนแดนท์ (k–descendant code)* ของ C แทนสัญลักษณ์ $\mathrm{desc}_k(C)$ คือ

$$\mathrm{desc}_k(C) = \bigcup_{\substack{X \subseteq C \\ |X| \leq k}} \mathrm{desc}(X)$$

$\mathrm{desc}_k(C)$ เป็นเซตที่รวมดีเซนแดนท์ทั้งหมดที่สร้างจากสับเซตที่มีขนาดไม่เกิน k ของ C นั่นคือ $\mathrm{desc}_k(C)$ เป็นเซตของชุดกุญแจดัดแปลงที่เป็นไปได้ทั้งหมด ซึ่งสร้างขึ้นโดยกลุ่มคนที่ไม่เกิน k คน และชุดกุญแจที่นำมาใช้ก็จะไม่เกิน k คำ

พิจารณาเซต P เหมือนในตัวอย่างก่อนหน้านี้และกลับมาที่สถานการณ์ของเราอีกครั้ง เราอาจคิดว่า P เป็นชุดกุญแจทั้งหมดในกล่องถอดรหัสสัญญาณโทรทัศน์ของผู้ใช้ในระบบ สมมติว่าธุรกิจพึ่งเริ่มจนถึงตอนนี้มีผู้ใช้ในระบบเพียงแค่ 3 คนเท่านั้น และชุดกุญแจที่อยู่ในกล่องถอดสัญญาณเหล่านั้นคือลายนิ้วมือ 3 ชุดของ P สมมติว่าสถานการณ์ของเราไม่เลวร้ายจนเกินไปเนื่องจากผู้ใช้ของเราอย่างน้อย 1 คนมีความซื่อสัตย์ และจะมีผู้ใช้อย่างมาก 2 คน ที่พยายามสร้างชุดกุญแจละเมิดลิขสิทธิ์ ดังนั้น $\mathrm{desc}_2(\mathrm{P})$ เป็นชุดของลายนิ้วมือที่เป็นไปได้ทั้งหมดที่ใช้ในชุดกุญแจละเมิดลิขสิทธิ์ ซึ่งสร้างโดยกลุ่มคนที่ไม่เกิน 2 คนดังตัวอย่างนี้

ตัวอย่าง 2.2.4 : ให้ $P = \{1100, 2102, 1122\}$ แล้ว

$$\mathrm{desc}_2(P) = \{1100, 1102, 1120, 1122, 2100, 2102, 2122\}$$

พิสูจน์ เซตย่อยที่ไม่เป็นเซตว่างที่เป็นไปได้ทั้งหมดที่มีขนาดไม่เกิน 2 ของ P
หรืออีกนัยหนึ่งคือเซตของลายนิ้วมือทั้งหมดจากกลุ่มคนที่ไม่เกิน 2 คน
ได้แก่ $\{1100\}, \{2102\}, \{1122\}, \{110, 2102\}, \{1100, 1122\}$ และ $\{2102, 1122\}$

พิจารณาเซตของดีเซนแดนท์ทั้งหมด
เราจะได้ $\mathrm{desc}(\{1100\}) = \{1100\}$,
$\mathrm{desc}(\{2102\}) = \{2102\}$
$\mathrm{desc}(\{1122\}) = \{1122\}$,
$\mathrm{desc}(\{1100, 2102\}) = \{1100, 1102, 2100, 2102\}$,
$\mathrm{desc}(\{1100, 1122\}) = \{1100, 1102, 1120, 1122\}$
และ $\mathrm{desc}(\{2102, 1122\}) = \{1102, 1122, 2102, 2122\}$
ดังนั้น

$$\begin{aligned}
\mathrm{desc}_2(P) &= \bigcup_{\substack{X \subseteq C \\ |X| \leq 2}} \mathrm{desc}(X) \\
&= \{1100\} \cup \{2102\} \cup \{1122\} \cup \{1100, 1102, 2100, 2102\} \\
&\cup \{1100, 1102, 1120, 1122\} \cup \{1102, 1122, 2102, 2122\} \\
&= \{1100, 1102, 1120, 1122, 2100, 2102, 2122\}
\end{aligned}$$

□

ต่อไปเราจะกำหนดรหัสลายนิ้วมือทั้ง 4 ชนิด ที่เราสนใจศึกษาในการค้นคว้าอิสระนี้ ได้แก่ รหัสเฟรมพรูฟ (Frameproof:FP), รหัสซีเคียวเฟรมพรูฟ (Secure Frameproof:SFP) ,รหัสระบุต้นกำเนิด (Identifiable Parent Proppety:IPP) และ รหัสเทรซอะบิลลิที (Traceability:TA)

<u>บทนิยาม 2.2.5</u> : ให้ C เป็นรหัสฐาน q ความยาว n และให้ k เป็นจำนวนเต็มบวก

(i) C มีสมบัติ k–*เฟรมพรูฟ* $(k-frameproof)$ หรือเป็น k–FP ก็ต่อเมื่อ ถ้า $X \subseteq C$ โดยที่ $|X| \leq k$ แล้ว

$$\mathrm{desc}(X) \cap C \subseteq X$$

(ii) C มีสมบัติ k–*ซีเคียวเฟรมพรูฟ* $(k-secure\ frameproof)$ หรือเป็น k–SFP ก็ต่อเมื่อถ้า $X_1, X_2 \subseteq C$ ที่ $|X_1|, |X_2| \leq k$ ถ้า $\mathrm{desc}(X_1) \cap \mathrm{desc}(X_2) = \emptyset$ แล้ว $X_1 \cap X_2 = \emptyset$

(iii) C มีสมบัติ k–*ระบุต้นกำเนิด* $(k-identifiable\ parent\ property)$ หรือเป็น k–IPP ก็ต่อเมื่อ ถ้า $x \in \mathrm{desc}_k(C)$ แล้ว

$$\bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \mathrm{desc}(X)}} X \neq \emptyset$$

(iv) C มีสมบัติ k–*เทรซอะบิลลิที* $(k-traceability)$ หรือเป็น k–TA ก็ต่อเมื่อ สำหรับทุก $X \subseteq C$ ที่ $|X| \leq k$ และ ทุก $x \in \mathrm{desc}(X)$ จะได้ว่า ทุก $z \in C$ ถ้า $d_H(x,z) = \min_{y \in C} d_H(x,y)$ แล้ว $z \in X$

ที่มาของรหัสแต่ละชนิดมีแรงบันดาลใจดังนี้ สำหรับ **รหัสเฟรมพรูฟ** กลุ่มคนใด ๆ ที่มีจำนวนไม่เกิน k คน จะไม่สามารถสร้างลายนิ้วมือของผู้ใช้ที่ไม่ได้เป็นสมาชิกนอกกลุ่มได้ ตรงตามชื่อของรหัส รหัสเฟรมพรูฟ รับประกันว่าไม่มีกลุ่มคนใดสามารถใส่ร้ายผู้ใช้นอกกลุ่มได้ โดยสร้างชุดกุญแจดัดแปลงที่เหมือนกับชุดกุญแจของผู้ใช้รายนั้น ใน **รหัสซีเคียวเฟรมพรูฟ** ชุดของลายนิ้วมือดีเซนแดนท์ที่สร้างโดยกลุ่มคน 2 กลุ่ม ที่ไม่มีสมาชิกร่วมกันจะไม่มีลายนิ้วมือใดเหมือนกัน นั่นคือ กลุ่มผู้ใช้ 2 กลุ่มที่ไม่มีสมาชิกร่วมกันจะไม่สามารถสร้างลายนิ้วมือเดียวกันได้ ดังนั้น พวกเขาจึงไม่สามารถใส่ร้ายซึ่งกันและกันหรือสร้างชุดกุญแจชุดใหม่ชุดเดียวกันได้ ใน **รหัสระบุต้นกำเนิด** หากกลุ่มคน 2 กลุ่มขึ้นไป สามารถสร้างดีเซนแดนท์เดียวกันได้ ต้องมีผู้ใช้อย่างน้อย 1 คนที่เป็นสมาชิกของทุกกลุ่ม หมายความว่า จากการพิจารณาชุดกุญแจที่จัดทำขึ้นโดยกลุ่มคน เราก็สามารถติดตามย้อนกลับไปยังสมาชิกคนกลุ่มนั้นอย่างน้อย 1 คนได้เสมอ ประการสุดท้าย ใน **รหัสเทรซอะบิลลิที** เจ้าของชุดกุญแจที่คล้ายกับดีเซนแดนท์ที่กำหนดมากที่สุด จะเป็นสมาชิกของกลุ่มคนที่สร้างดีเซนแดนท์เสมอ เรามั่นใจว่าผู้ใช้ที่เป็นเจ้าของชุดกุญแจที่คล้ายกับชุดกุญแจละเมิดลิขสิทธิ์มีความผิด

เราจะแสดงตัวอย่างของรหัสลายนิ้วมือชนิดต่าง ๆ ดังต่อไปนี้

ตัวอย่าง 2.2.6 : ให้ $C = \{1100, 1001, 1010\} \subseteq \{0,1\}^4$ จะได้ว่า C เป็น รหัส 2-FP

พิสูจน์ เนื่องจาก $\text{desc}(\{1100, 1001\}) \cap C = \{1100, 1001\}$

$\text{desc}(\{1100, 1010\}) \cap C = \{1100, 1010\}$

และ $\text{desc}(\{1001, 1010\}) \cap C = \{1001, 1010\}$ □

ตัวอย่างต่อไปเป็นตัวอย่างของรหัส 2-SFP

ตัวอย่าง 2.2.7 : ให้ $C = \{1001, 1200, 0010, 2211\} \subseteq \{0,1,2\}^4$ จะได้ว่า C เป็นรหัส 2-SFP

พิสูจน์ เนื่องจาก $\text{desc}(\{1001, 1200\}) \cap \text{desc}(\{0010, 2211\}) = \emptyset$

$\text{desc}(\{1001, 0010\}) \cap \text{desc}(\{1200, 2211\}) = \emptyset$

และ $\text{desc}(\{1001, 2211\}) \cap \text{desc}(\{1200, 0010\}) = \emptyset$ □

ตัวอย่าง 2.2.8 : ให้ $C = \{1111111111, 1111000000, 1000111000, 0100100110,$
$0010010101, 0001001011\} \subseteq \{0,1\}^{10}$ จะได้ว่า C เป็นรหัส 3-SFP

พิสูจน์ เซตย่อยที่มีขนาดไม่เกิน 3 ทั้งหมด ($\binom{6}{1} + \binom{6}{2} + \binom{6}{3}$=41 กรณี) ของ C ได้แก่
$\{1111111111\}, \{1111000000\}, \{1000111000\}, \{0100100110\}, \{0010010101\}, \{0001001011\},$
$\{1111111111, 1111000000\}, \{1111111111, 1000111000\}, \{1111111111, 0100100110\},$
$..., \{0100100110, 0010010101, 0001001011\}$ เนื่องจากคู่ของ $X_1, X_2 \subseteq C$ ซึ่ง $X_1 \cap X_2 = \emptyset$ มีเป็นจำนวนมาก เราจึงเลือกทำเฉพาะบางกรณี

กรณี $X_1 = \{1111111111\}$, $X_2 = \{1111000000\}$

จะได้ว่า $\text{desc}(X_1) = \{1111111111\}$ และ $\text{desc}(X_2) = \{1111000000\}$

ทำให้ $\text{desc}(X_1) \cap \text{desc}(X_2) = \emptyset$ และ $X_1 \cap X_2 = \emptyset$ สอดคล้องกับนิยาม

กรณี $X_1 = \{1111111111\}$ $X_2 = \{1000111000\}$

จะได้ว่า $\text{desc}(X_1) = \{1111111111\}$ และ $\text{desc}(X_2) = \{1000111000\}$

ทำให้ $\text{desc}(X_1) \cap \text{desc}(X_2) = \emptyset$ และ $X_1 \cap X_2 = \emptyset$ สอดคล้องกับนิยาม

.

.

.

กรณี $X_1 = \{1111111111, 1111000000\}$, $X_2 = \{1000111000, 0100100110\}$
จะได้ว่า $\mathrm{desc}(X_1) = \{1111000000, 1111100000, ..., 1111111111\}$
และ $\mathrm{desc}(X_2) = \{0000100000, 0000100010, ..., 1100111110\}$
ทำให้ $\mathrm{desc}(X_1) \cap \mathrm{desc}(X_2) = \emptyset$ และ $X_1 \cap X_2 = \emptyset$ สอดคล้องกับนิยาม

.

.

.

ดังนั้น เมื่อตรวจสอบทุกกรณี จะพบว่า C เป็น 3-SFP □

ตัวอย่างต่อไปนี้เป็นรหัส 2-IPP

ตัวอย่าง 2.2.9 : ให้ $C = \{0000, 0111, 0222, 1012, 1120, 1201, 2021, 2102, 2210\} \subseteq \{0, 1, 2\}^4$ เป็นรหัส 2-IPP

พิสูจน์ เซตย่อยขนาดไม่เกิน 2 ทั้งหมดของ C ($\binom{9}{0} + \binom{9}{1} + \binom{9}{2}$=45 กรณี) ได้แก่ $\{0000\}, \{0111\}, \{0222\}, ..., \{0000, 0111\}, ..., \{2102, 2210\}$
ต่อไปจะเป็นดีเซนแดนท์ของเซตย่อย

$\mathrm{desc}(0000) = \{0000\}$

$\mathrm{desc}(0111) = \{0111\}$

$\mathrm{desc}(0222) = \{0222\}$

.

.

.

$\mathrm{desc}(0000, 0111) = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111\}$

.

.

.

$\mathrm{desc}(2102, 2210) = \{2100, 2102, 2110, 2112, 2200, 2202, 2210, 2212\}$
ดังนั้น $\mathrm{desc}_2(C) = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, ..., 2100, 2102, 2110, 2112, 2200, 2202, 2210, 2212\}$
เนื่องจากคำรหัสใน $\mathrm{desc}_2(C)$ มีเป็นจำนวนมาก เราจึงยกตัวอย่างการพิจารณาเพียงกรณีเดียว พิจารณา $x = 0110$ จะได้ว่า $x \in \{0000, 0111\}, x \in \{0111, 1120\}, x \in \{0111, 2210\}$

และ $\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ x\in \mathrm{desc}(X)}} X = \{0111\} \neq \emptyset$ สอดคล้องกับนิยาม □

ตัวอย่างสุดท้ายเป็นของรหัส 2-TA

ตัวอย่าง 2.2.10 : $C = \{000, 111, 222\} \subseteq \{0,1,2\}^3$ เป็นรหัส 2-TA

พิสูจน์ เซตย่อยขนาดไม่เกิน 2 ทั้งหมดของ C ได้แก่ $\{000\}, \{111\}, \{222\}, \{000, 111\}, \{000, 222\}, \{111, 222\}$
พิจารณา บางกรณี
กรณี $X = \{000\}$ ได้ $\mathrm{desc}(X) = \{000\}$
พิจารณา $000 \in \mathrm{desc}(X)$
จะได้ว่า $d_H(C, 000) = d_H(000, 000) = 0$ และ $000 \in X$
$d_H(C, 000) = d_H(111, 000) = 3$ และ $000 \in X$
$d_H(C, 000) = d_H(222, 000) = 3$ และ $000 \in X$
.
.
.
กรณี $X = \{111, 222\}$ จะได้ว่า $\mathrm{desc}(X) = \{111, 112, 121, 211, 122, 212, 221, 222\}$
และพิจารณาระยะระหว่างคำรหัส และ C ทีละคำรหัสใน $\mathrm{desc}(X)$
จะได้ว่า $d_H(C, 111) = d_H(111, 111) = 0$ และ $111 \in X$
$d_H(C, 112) = d_H(111, 112) = 1$ และ $111 \in X$
$d_H(C, 121) = d_H(111, 121) = 1$ และ $111 \in X$
.
.
.
$d_H = (C, 222) = d_H(222, 222) = 0$ และ $222 \in X$ □

2.3. **ความสัมพันธ์ระหว่างรหัสลายนิ้วมือ**

จากแรงบันดาลใจ ซึ่งเป็นที่มาของรหัสเห็นได้ว่า รหัสระบุต้นกำเนิด กับ รหัสเทรซอะบิลลิที มีสมบัติในการตรวจจับผู้ใช้ที่ละเมิดลิขสิทธิ์ ในขณะที่รหัสเฟรมพรูฟ กับ รหัสซีเคียวเฟรมพรูฟ มีสมบัติป้องกันไม่ให้ผู้ใช้ที่ละเมิดลิขสิทธิ์ใส่ร้ายผู้ใช้อื่นได้ จะเห็นว่า รหัสระบุต้นกำเนิด กับ รหัสเทรซอะบิลลิที จะมีสมบัติเข้มกว่า รหัสเฟรมพรูฟ กับ รหัสซีเคียวเฟรมพรูฟ ดังนั้น เราจะกล่าวถึงความสัมพันธ์ระหว่างรหัสประเภทต่าง ๆ ต่อไปนี้

เราอาจตรวจสอบจากนิยามว่ารหัสประเภทต่าง ๆ มีความสัมพันธ์กัน ดังนี้ รหัส $k-$TA เป็นรหัส $k-$IPP , รหัส $k-$IPP เป็นรหัส $k-$SFP และรหัส $k-$SFP เป็นรหัส $k-$FP ซึ่งจะพิสูจน์และยกตัวอย่างในบทแทรกและทฤษฎี ดังต่อไปนี้

บทแทรก 2.3.1 : รหัส $k-$TA เป็นรหัส $k-$IPP

พิสูจน์ ให้ C เป็นรหัส $k-$TA และ ให้ x เป็นคำใน $\mathrm{desc}_k(C)$
ให้ z เป็นคำรหัสใน C ที่ $d_H(x,z)$ มีค่าต่ำสุด นั่นคือ $d_H(x,z) = \min_{y \in C} d_H(x,y)$
โดยสมบัติ $k-TA$
ถ้า $X \subseteq C$ โดยที่ $x \in \mathrm{desc(X)}$ แล้ว $z \in X$
ดังนั้น

$$z \in \bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \mathrm{desc(X)}}} X$$

กล่าวคือ

$$\bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \mathrm{desc(X)}}} X \neq \emptyset$$

ดังนั้น C เป็นรหัส $k-$IPP □

ต่อไปเป็นตัวอย่างที่สอดคล้องกับบทแทรก 2.3.1

ตัวอย่าง 2.3.2 : รหัส 2-TA ได้ $C = \{000, 111, 222\}$ เป็นรหัส 2-IPP

พิสูจน์ เราคำนวณเซตดีเซนแดนท์ของเซตย่อยทั้งหมดที่มีขนาดไม่เกิน 2 ของ C

$\mathrm{desc}(\{000\}) = \{000\}$

$\mathrm{desc}(\{111\}) = \{111\}$

$\mathrm{desc}(\{222\}) = \{222\}$

$\mathrm{desc}(\{000, 111\}) = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$\mathrm{desc}(\{000, 222\}) = \{000, 002, 020, 022, 200, 202, 220, 222\}$

$\mathrm{desc}(\{111, 222\}) = \{111, 112, 121, 122, 211, 212, 221, 222\}$

ดังนั้น $\mathrm{desc}_2(\mathrm{C}) = \{000, 001, 002, 010, 011, 020, 022, 100, 101, 110, 111, 112, 121, 122,$

$200, 202, 211, 212, 220, 221, 222\}$

การพิจารณาคำทั้งหมดใน $\mathrm{desc}_2(\mathrm{C})$ เราจะได้

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 000\in \mathrm{desc(X)}}} X = \{000\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 001\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 002\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 010\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 011\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 020\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 022\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 100\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 101\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 110\in \mathrm{desc(X)}}} X = \{000, 111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 111\in \mathrm{desc(X)}}} X = \{111\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 112\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 121\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 122\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 200\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 020\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 211\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 212\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 220\in \mathrm{desc(X)}}} X = \{000, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 221\in \mathrm{desc(X)}}} X = \{111, 222\} \neq \emptyset$

$\bigcap_{\substack{X\subseteq C:|X|\leq 2 \\ 222\in \mathrm{desc(X)}}} X = \{222\} \neq \emptyset$

ดังนั้น C เป็น 2-IPP □

อย่างไรก็ตาม บทกลับของบทแทรกนี้ไม่เป็นความจริงเสมอไป ตัวอย่างขัดแย้งของรหัส C ในตัวอย่างที่ 2.2.9 ที่เป็น 2-IPP แต่ไม่เป็น 2-TA เนื่องจาก $2110 \in \mathrm{desc}(\{2102, 2210\})$ แต่ $d_H(C, 2110) = d_H(0111, 2110) = 2$ และ $0111 \notin \{2102, 2210\}$

ทฤษฎีบท 2.3.3 : รหัส $k-$IPP เป็นรหัส $k-$SFP

พิสูจน์ ให้ C เป็นรหัส $k-$IPP ให้ X_1, X_2 เป็นเซตย่อยของ C ขนาดไม่เกิน k
สมมติให้ $\mathrm{desc(X_1)} \cap \mathrm{desc(X_2)} \neq \emptyset$
ถ้าให้ $x \in \mathrm{desc(X_1)} \cap \mathrm{desc(X_2)}$ แล้ว $x \in \mathrm{desc}_k(C)$
โดยสมบัติ $k-$IPP

$$\bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \mathrm{desc(X)}}} X \neq \emptyset$$

และ

$$\bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \mathrm{desc(X)}}} X \subseteq X_1 \cap X_2$$

ดังนั้น

$$X_1 \cap X_2 \neq \emptyset$$

ดังนั้น C เป็นรหัส $k-$SFP

ต่อไปเป็นตัวอย่างที่แสดงให้เห็นว่าขากลับของทฤษฎีบท 2.3.3 ไม่เป็นจริง

ตัวอย่าง 2.3.4 : $C = \{1001, 1200, 0010, 2211\} \subseteq \{0,1,2\}^4$ เป็นรหัส 2-SFP
แต่ไม่เป็นรหัส 2-IPP

พิสูจน์ เนื่องจาก $1201 \in \mathrm{desc}\{1001, 2211\}$, $1201 \in \mathrm{desc}\{1001, 1200\}$ และ $1201 \in \mathrm{desc}\{1200, 2211\}$
แต่ $\{1001, 2211\} \cap \{1001, 1200\} \cap \{1200, 2211\} = \emptyset$
ดังนั้น C เป็นรหัส $2-$SFP แต่ไม่เป็น $2-$IPP □

ทฤษฎีบท 2.3.5 : รหัส $k-$SFP เป็นรหัส $k-$FP

พิสูจน์ ให้ C เป็นรหัส $k-$SFP ให้ X_0 เป็นเซตย่อยของ C ที่มีขนาดที่ไม่เกิน k
และให้ $x \in \mathrm{desc(X_0)} \cap C$
ดังนั้น $\mathrm{desc(X_0)} \cap \{x\} = \mathrm{desc(X_0)} \cap \mathrm{desc(\{x\})} \neq \emptyset$
โดยสมบัติ $k-$SFP , $X_0 \cap \{x\} \neq \emptyset$ ทำให้ $x \in X_0$
ดังนั้น C เป็นรหัส k-FP □

ตัวอย่างต่อไปจะแสดงให้เห็นว่า รหัส $k-$FP ไม่จำเป็นต้องเป็นรหัส $k-$SFP

ตัวอย่าง 2.3.6 : $C = \{1100, 1001, 1010, 0100\} \subseteq \{0,1\}^4$ เป็นรหัส 2-FP แต่ไม่เป็นรหัส 2-SFP

พิสูจน์ เห็นได้ว่า C เป็นรหัส 2-FP เนื่องจาก $\mathrm{desc}(\{1100, 1001\}) \cap C = \{1100, 1001\}$

$\mathrm{desc}(\{1100, 1010\}) \cap C = \{1100, 1010\}$

$\mathrm{desc}(\{1100, 0100\}) \cap C = \{1100, 0100\}$

$\mathrm{desc}(\{1001, 1010\}) \cap C = \{1001, 1010\}$

$\mathrm{desc}(\{1001, 0100\}) \cap C = \{1001, 0100\}$

และ $\mathrm{desc}(\{1010, 0100\}) \cap C = \{1010, 0100\}$

แต่ C ไม่ใช่รหัส 2-SFP

เนื่องจาก $\mathrm{desc}(\{1100, 1001\}) \cap \mathrm{desc}(\{1010, 0100\}) = \{1000, 1100\} \neq \emptyset$

แต่ $\{1100, 1001\} \cap \{1010, 0100\} = \emptyset$ □

บทที่ 3

ขอบเขตของรหัส

เมื่อทราบตัวแปรที่เกี่ยวข้องกับรหัส เช่น ฐาน q ความยาว n และทราบสมบัติที่เกี่ยวข้องแล้ว ในทางทฤษฎีรหัสมักศึกษาเพื่อหาขนาดที่ใหญ่ที่สุดที่เป็นไปได้ของรหัสเหล่านั้น โดยทั่วไป ขนาดที่ใหญ่ที่สุดที่เป็นไปได้ของรหัสเป็นสิ่งที่หาได้ยาก ในงานวิจัยต่าง ๆ จึงพบเพียงขอบเขตบนและขอบเขตล่างของขนาดที่ใหญ่ที่สุดที่เป็นไปได้ของรหัส เรียกย่อ ๆ ว่าขอบเขตของรหัส ขอบเขตบนมักได้มาจากการพิสูจน์ในขณะที่ขอบเขตล่างมักได้จากการสร้าง

ในบทนี้จึงจะกล่าวถึงขอบเขตของขนาดของรหัสทั้ง 4 ชนิด ที่ผู้ศึกษาได้รวบรวมมาจากงานวิจัยต่าง ๆ ตลอดหัวข้อนี้ให้ n, q, k เป็นจำนวนเต็มบวกที่มีค่าอย่างน้อย 2

3.1. ขอบเขตของรหัสเฟรมพรูฟ (Frameproof Codes)

ในปี 2017 Shangguan และคณะ [15] ได้ศึกษาขอบเขตของรหัสเฟรมพรูฟ และได้ผลลัพธ์เป็นขอบเขตบนและขอบเขตล่างของรหัสเฟรมพรูฟดังนี้

ทฤษฎีบท 3.1.1 : ให้ C เป็นรหัส $k-FP$ ฐาน q มีความยาว n จะได้ว่า

$$|C| \leq q^{\lceil n(q-1)/\binom{k}{2} \rceil \log_q eq\binom{k}{2}/(q-1)} + k$$

ทฤษฎีบท 3.1.2 : ถ้า $q \leq k+1$ แล้วจะได้ว่าจะมี C ซึ่งเป็นรหัส $k-FP$ ฐาน q มีความยาว n ที่มีจำนวนสมาชิกอย่างน้อย

$$|C| \geq \frac{1}{2^{\frac{k+1}{k}}} \left(\frac{1}{1-(1-\frac{q-1}{k+1})(\frac{q-1}{k+1})k - \frac{q-1}{k+1}(\frac{k}{k+1})k}\right)^{\frac{n}{k}}$$

ในปี 2003 Blackburn [3] ได้สร้างรหัสเฟรมพรูฟ และพิสูจน์ขอบเขตรหัสได้ดังนี้

ทฤษฎีบท 3.1.3 : ให้ C เป็นรหัส $k-FP$ ฐาน q มีความยาว n จะได้ว่า

$$|C| \leq \max\{q^{\lceil n/k \rceil}, r(q^{\lceil n/k \rceil}-1)+(k-r)(q^{\lceil n/k \rceil}-1)\}$$

เมื่อ $r \in \{0,1,...,k-1\}$ เป็นเศษเหลือของ n เมื่อหารด้วย k

ในปี 2001 Staddon และคณะ [16] ได้พิสูจน์ขอบเขตรหัสเฟรมพรูฟได้ดังนี้

ทฤษฎีบท 3.1.4 : ให้ C เป็นรหัส $k-FP$ ฐาน q ที่มีความยาว n จะได้ว่า

$$|C| \leq k(q^{\lceil n/k \rceil}-1)$$

ในปี 2023 Dalai และคณะ [9] ได้ศึกษาขอบเขตรหัสเฟรมพรูฟ ดังนี้

ทฤษฎีบท 3.1.5 : มีรหัส $k-FP$ ฐาน q ที่มีความยาว n แล้ว

$$|C| \leq -k\ln\left(n\frac{k!}{k!-1}\right)/\ln\left(1-(1-\frac{1}{q})^k\right)$$

ปี 2019 Cheng และคณะ [8] ได้ศึกษาขอบเขตรหัสเฟรมพรูฟ ดังนี้

ทฤษฎีบท 3.1.6 : สำหรับทุก ๆ จำนวนเต็ม $q > 48$ ให้ C เป็นรหัส $2-FP$ ฐาน q ที่มีความยาว 4 จะได้ว่า

$$|C| \leq 2q^2-2q+7$$

3.2. ขอบเขตของรหัสซีเคียวเฟรมพรูฟ (Secure Frameproof Codes)

ในปี 2008 Stinson และ Zaverucha [17] ได้ศึกษาขอบเขตรหัสซีเคียวเฟรมพรูฟ และได้ขอบเขตดังนี้

ทฤษฎีบท 3.2.1 : ให้ C เป็นรหัส $k-SFP$ ฐาน q ความยาว $n=2k-1$ จะได้ว่า

$$|C| \leq q + (k-1)(2k-1)(q-1)$$

บทแทรก 3.2.2 : ให้ C เป็นรหัส $k-SFP$ ฐาน q ความยาว n จะได้ว่า

$$|C| \leq (2k^2-3k+2)q^{\lceil \frac{n}{(2k-1)} \rceil} - 2k^2 + 3k - 1$$

ในปี 2001 Staddon และ คณะ [16] ได้ศึกษาขอบเขตรหัสซีเคียวเฟรมพรูฟ และได้ขอบเขตรหัสดังนี้

ทฤษฎีบท 3.2.3 : ให้ C เป็นรหัส $k-SFP$ ฐาน q ที่มีความยาว n จะได้ว่า

$$|C| \leq k(q^{\lceil \frac{n}{k} \rceil} - 1)$$

ในปี 2012 Hajiabolhassan และ Moazami [12] ได้ศึกษาการสร้างรหัสซีเคียวเฟรมพรูฟ และได้ขอบเขตล่างของรหัสซีเคียวเฟรมพรูฟดังนี้

ทฤษฎีบท 3.2.4 : ถ้า $q > 3k$ และ

$$n \geq 2^{2k-1}(1 + \ln(\binom{\lceil \frac{q}{2} \rceil}{k})(\binom{\lfloor \frac{q}{2} \rfloor}{k}))\Pi_{i=0}^{k-1}(1 - \frac{1}{q-2i+1})$$

แล้วจะได้ว่าจะมีรหัส $k-SFP$ ฐาน q ที่มีความยาว n

3.3. ขอบเขตของรหัสระบุต้นกำเนิด (Identifiable Parent Property)

ในปี 2018 Shangguan และคณะ [14] ได้ศึกษาขอบเขตรหัสระบุต้นกำเนิดและรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.3.1 : ให้ C เป็นรหัส $k-IPP$ ฐาน q ที่มีความยาว n กำหนดให้ $v = \lfloor (k/2+1)^2 \rfloor$ และให้ $r \in \{0, 1, ..., v-2\}$ เป็นเศษเหลือของ n เมื่อหารด้วย $v-1$ จะได้ว่า

$$|C| \leq rq^{\lceil n/(v-1) \rceil} + (v-1-r)q^{\lfloor n/(v-1) \rfloor}$$

ในปี 2017 Gu และ Miao [11] ได้ศึกษาขอบเขตรหัสระบุต้นกำเนิด ดังนี้

ทฤษฎีบท 3.3.2 : ให้ C เป็นรหัส $k-IPP$ ฐาน q ที่มีความยาว n โดยที่ $q \geq n \geq k$ จะได้ว่า

$$|C| \leq (\binom{q}{\lceil \frac{n}{\lfloor k^2/4 \rfloor + k} \rceil}) = \mathcal{O}\left(q^{\lceil \frac{n}{\lfloor k^2/4 \rfloor + k} \rceil}\right)$$

ปี 2003 Blackburn [4] ได้ศึกษาขอบเขตรหัสระบุต้นกำเนิด ดังนี้

ทฤษฎีบท 3.3.3 : ให้ C เป็นรหัส $k-IPP$ ฐาน q ที่มีความยาว n กำหนดให้ $v = \lfloor (k/2+1)^2 \rfloor$ จะได้ว่า

$$|C| \leq \frac{1}{2}v(v-1)q^{\lceil n/(v-1) \rceil}$$

ปี 2001 Barg และคณะ [1] ได้ศึกษาขอบเขตรหัสระบุต้นกำเนิด ดังนี้

ทฤษฎีบท 3.3.4 : กำหนดให้ $v = \lfloor (k/2+1)^2 \rfloor$ จะมีรหัส C ซึ่งเป็นรหัส $k-IPP$ ฐาน q ที่มีความยาว n ที่มีจำนวนสมาชิกอย่างน้อย

$$|C| \geq \frac{(q-k)!q^v}{(q-k)!q^v - q!(q-k)^{v-k}} q^{\frac{n}{v-1}}$$

3.4. ขอบเขตของรหัสเทรซอะบิลลิที (Traceability)

ในปี 2018 Shangguan และคณะ [14] ได้ศึกษาขอบเขตรหัสระบุต้นกำเนิดและรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.4.1 : ให้ C เป็นรหัส $k-TA$ ฐาน q ที่มีความยาว n จะได้ว่า

$$|C| \leq rq^{\lceil k/9 \rceil}$$

เมื่อค่าคงที่ r เป็นฟังก์ชันที่ขึ้นอยู่กับ n เท่านั้น

ในปี 2023 Chen และ Chen [7] ได้ศึกษาขอบเขตรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.4.2 : ขนาดที่ใหญ่ที่สุดที่เป็นไปได้ของรหัส $2-TA$ ฐาน q ความยาว 3 คือ

$$\lfloor \frac{3(q-1)}{2} \rfloor$$

ทฤษฎีบท 3.4.3 : ขนาดที่ใหญ่ที่สุดที่เป็นไปได้ของรหัส $2-TA$ ฐาน q ความยาว 4 คือ

$$3q$$

เมื่อ $q = 3k$ สำหรับบาง $k \in \mathbb{Z}^+$

ในปี 2010 Blackburn และคณะ [5] ได้ศึกษาขอบเขตรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.4.4 : ให้ k, q เป็นจำนวนเต็มที่ $k \geq 2$ ถ้า

$$k^2 - \lceil k/2 \rceil + 1 \leq q$$

หรือ $k = 2$ และ $q = 3$ แล้วข้อความต่อไปนี้เป็นจริง มีค่าคงที่บวก R (ขึ้นอยู่กับ q และ k) และลำดับ $C_1, C_2, ...$ ของรหัส $k-TA$ ฐาน q ซึ่งมีสมบัติดังนี้ C_n ที่มีความยาว n และ $|C_n| \sim q^{Rn}$ เมื่อ $n \to \infty$

ในปี 2015 Ng และ Owen [13] ได้ศึกษาขอบเขตรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.4.5 : ให้ C เป็นรหัส $k-TA$ ฐาน q ที่มีความยาว n ถ้า $d(C) = 2$ แล้วจะได้ว่า

$$|C| \leq 3q - 2$$

ในปี 2004 Van Trung และ Martirosyan [18] ได้ศึกษาขอบเขตรหัสเทรซอะบิลลิที ดังนี้

ทฤษฎีบท 3.4.6 : ถ้า q เป็นจำนวนเฉพาะยกกำลัง และ $n \leq q+1$ แล้วจะมีรหัส C ซึ่งเป็น $k-TA$ ฐาน q ที่มีความยาว n ที่มีจำนวนสมาชิกอย่างน้อย

$$|C| \geq q^{\lceil n/k^2 \rceil}$$

บทที่ 4

การสร้าง

ในบทนี้จะกล่าวถึงการสร้างของรหัสเฟรมพรูฟปละรหัสเทรซอะบิลลีที ที่มีความยาวไม่เกิน 5 โดยจะเป็นการสร้างที่มีผู้อื่นศึกษาไว้ ตามด้วยการสร้างของผู้ค้นคว้าอิสระ

4.1. **รหัสเฟรมพรูฟ (Frameproof)**

การสร้างต่อไปนี้ นำมาจาก [3] ซึ่งเป็นการสร้างรหัส $3-FP$ ความยาว 5 ซึ่งผู้ศึกษาได้นำมาดัดแปลงเป็นรหัส $2-FP$ ความยาว 4

ขั้นตอนที่ 1 เรานิยามเซต X_1, X_2, X_3, X_4, X_5 ของคำรหัสความยาว 5 บนตัวอักษร $\mathbb{F} \cup \{\infty\}$ ดังนี้

$$X_1 = \{(\infty, a, a, a, a) : a \in \mathbb{Z}_3\}$$

$$X_2 = \{(a, \infty, a, a+1, a+2) : a \in \mathbb{Z}_3\}$$

$$X_3 = \{(a, a, \infty, a+2, a+1) : a \in \mathbb{Z}_3\}$$

$$X_4 = \{(a, a+1, a+2, \infty, a) : a \in \mathbb{Z}_3\}$$

$$X_5 = \{(a, a+2, a+1, a, \infty) : a \in \mathbb{Z}_3\}$$

เห็นได้ชัดเจนว่าแต่ละคู่ของเซต X_i ไม่มีสมาชิกร่วมกัน และแต่ละเซต X_i มีจำนวนสมาชิก 3 ตัว เนื่องจาก a เป็นได้เพียง $0, 1, 2$ นอกจากนี้ สามารถสังเกตได้ว่าทุกสองตำแหน่งของคำรหัสใด ๆ ใน $X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$ จะแตกต่างจากคำรหัสอื่น ดังนั้น ถ้าเราทราบสัญลักษณ์ใน 2 ตำแหน่ง ของคำรหัสใด เราสามารถระบุอีก 3 ตำแหน่งที่เหลือได้ เนื่องจากจะไม่มีตัวที่ซ้ำกันในตำแหน่งดังกล่าวของเซต X

ตัวอย่าง 4.1.1 : แจกแจงสมาชิกของ X_1, X_2, X_3, X_4, X_5 ได้ดังนี้

$$X_1 = \{(\infty, 0, 0, 0, 0), (\infty, 1, 1, 1, 1), (\infty, 2, 2, 2, 2)\}$$
$$X_2 = \{(0, \infty, 0, 1, 2), (1, \infty, 1, 2, 0), (2, \infty, 2, 0, 1)\}$$
$$X_3 = \{(0, 0, \infty, 2, 1), (1, 1, \infty, 0, 2), (2, 2, \infty, 1, 0)\}$$
$$X_4 = \{(0, 1, 2, \infty, 0), (1, 2, 0, \infty, 1), (2, 0, 1, \infty, 2)\}$$
$$X_5 = \{(0, 2, 1, 0, \infty), (1, 0, 2, 0, \infty), (2, 1, 0, 2, \infty)\}$$

□

ขั้นตอนที่ 2 ต่อไปเราจะนิยามเซต Y_1, Y_2, Y_3, Y_4, Y_5 ให้ m เป็นจำนวนเฉพาะยกกำลัง ที่ $m \geq 4$ ให้ $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ เป็นสมาชิกที่แตกต่างกันใน $\mathbb{F}_m$ กำหนดให้ เซตของ Y_1, Y_2, Y_3, Y_4, Y_5 เป็นคำความยาว 5 เหนือเซตอักษร $\mathbb{F}_m \cup \{\infty\}$

$$Y_1 = \{(\infty, f(\alpha_1), f(\alpha_2), f(\alpha_3), f(\alpha_4)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_2 = \{(f(\alpha_1), \infty, f(\alpha_2), f(\alpha_3), f(\alpha_4)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_3 = \{(f(\alpha_1), f(\alpha_2), \infty, f(\alpha_3), f(\alpha_4)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_4 = \{(f(\alpha_1), f(\alpha_2), f(\alpha_3), \infty, f(\alpha_4)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_5 = \{(f(\alpha_1), f(\alpha_2), f(\alpha_3), f(\alpha_4), \infty) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

□

เห็นได้ชัดว่า เซตของ Y_i ไม่มีสมาชิกร่วมกัน และแต่ละเซตมีจำนวนสมาชิก m^2
นอกจากนั้น ถ้าสมาชิก $x, y \in Y_i$ เหมือนกันในสองตำแหน่งนอกเหนือจาก ตำแหน่งที่ i แล้ว $x = y$
พิสูจน์ สมมติ $x, y \in Y_i$ เหมือนกันในตำแหน่งของ α_j และ α_k โดยที่ x กำหนดโดย $f_1(t) = at + b$ และ y กำหนดโดย $f_2(t) = ct + d$
จะได้ว่า $a\alpha_j + b = c\alpha_j + d$, และ $a\alpha_k + b = c\alpha_k + d$

นำทั้งสองสมการมาลบกัน

$$a\alpha_j + b - a\alpha_k - b = c\alpha_j + d - c\alpha_k - d$$

$$a\alpha_j - a\alpha_k = c\alpha_j - c\alpha_k$$

$$a(\alpha_j - \alpha_k) = c(\alpha_j - \alpha_k)$$

$$a = c$$

นำ $a = c$ ไปแทนในสมการที่ 1

$$a\alpha_j + b = a\alpha_j + d$$

$$b = d$$

ดังนั้น $f_1 = f_2$ ทำให้ $x = y$

ตัวอย่าง 4.1.2 : แจกแจงสมาชิก Y_1, Y_2, Y_3, Y_4, Y_5 เมื่อ $m = 5$ ได้ดังนี้
เราจะได้ว่า $f \in \mathbb{F}_5, \deg f \leq 1$ ทั้งหมดที่เป็นไปได้คือ
$f(x) = 0, 1, 2, 3, 4, x, x+1, ..., 4x+4$
เราเลือก $\alpha_1 = 2, \alpha_2 = 4, \alpha_3 = 1$ และ $\alpha_4 = 3$ ดังนั้น จะได้ว่า $\alpha_i \in \mathbb{F}_m$ แตกต่างกันทั้งหมด

$Y_1 = \{(\infty, 0, , 0, 0), (\infty, 1, 1, 1, 1), ..., (\infty, 3, 0, 2, 4), ..., (\infty, 0, 4, 3, 2), ..., (\infty, 2, 3, 4, 0), ..., (\infty, 4, 2, 0, 3), ...\}$

$Y_2 = \{(0, \infty, 0, 0, 0), (1, \infty, 1, 1, 1), ..., (3, \infty, 0, 2, 4)..., (0, \infty, 4, 3, 2), ..., (2, \infty, 3, 4, 0), ..., (4, \infty, 2, 0, 3), ...\}$

$Y_3 = \{(0, 0, \infty, 0, 0), (1, 1, \infty, 1, 1), ..., (3, 0, \infty, 2, 4)..., (0, 4, \infty, 3, 2), ..., (2, 3, \infty, 4, 0), .., (4, 2, \infty, 0, 3), ...\}$

$Y_4 = \{(0, 0, 0, \infty, 0), (1, 1, 1, \infty, 1), ..., (3, 0, 2, \infty, 4), .., (0, 4, 3, \infty, 2), ..., (2, 3, 4, \infty, 0), ..., (4, 2, 0, \infty, 3), ...\}$

$Y_5 = \{(0, 0, 0, 0, \infty), (1, 1, 1, 1, \infty), ..., (3, 0, 2, 4, \infty), ..., (0, 4, 3, 2, \infty), ..., (2, 3, 4, 0, \infty), ..., (4, 2, 0, 3, \infty), ...\}$

□

ขั้นตอนที่ 3 เรานิยามเซตของคำ C_1, C_2, C_3, C_4, C_5 ที่มีความยาว 5 เหนือเซตอักษร $(\mathbb{F}_3 \times \mathbb{F}_m) \cup \{(\infty, \infty)\}$ ดังนี้

$C_i = \{((x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5) : (x_1, x_2, x_3, x_4, x_5) \in X_i$ และ $(y_1, y_2, y_3, y_4, y_5) \in Y_i\}$

สำหรับทุก $i \in \{1, 2, 3, 4, 5\}$

ตัวอย่าง 4.1.3 : ให้ $a \in \mathbb{Z}_3$ โดยที่ $a = \{0, 1, 2\}$ และให้ $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$
โดยกำหนดให้ $\alpha_1 = 2, \alpha_2 = 4, \alpha_3 = 1$ และ $\alpha_4 = 3$ แจกแจงสมาชิกของ C_2 ได้ดังนี้

$C_2 = \{\big((0,0),(\infty,\infty),(0,0),(1,0),(2,0)\big),...,\big((1,0),(\infty,\infty),(1,0),(2,0),(0,0)\big),...,$
$\big((2,0),(\infty,\infty),(2,0),(0,0),(1,0)\big),...,\big((0,0),(\infty,\infty),(0,4),(1,3),(2,2)\big),...,$
$\big((0,2),(\infty,\infty),(0,3),(1,4),(2,0)\big),...,\big((0,4),(\infty,\infty),(0,2),(1,0),(2,3)\big),...,$
$\big((0,1),(\infty,\infty),(0,1),(1,1),(2,1)\big),...,\big((1,1),(\infty,\infty),(1,1),(2,1),(0,1)\big),...,$
$\big((2,1),(\infty,\infty),(2,1),(0,1),(1,1)\big),...,\big((1,0),(\infty,\infty),(0,3),(1,4),(2,0)\big),...,$
$\big((1,2),(\infty,\infty),(1,3),(2,4),(0,0)\big),...,\big((1,4),(\infty,\infty),(1,2),(2,0),(0,3)\big),...,$
$\big((2,0),(\infty,\infty),(2,0),(0,0),(1,0)\big),...,\big((2,1),(\infty,\infty),(2,1),(0,1),(1,1)\big),...,$
$\big((2,3),(\infty,\infty),(2,0),(0,2),(1,4)\big),...,\big((2,0),(\infty,\infty),(2,4),(0,3),(1,2)\big),...,$
$\big((2,2),(\infty,\infty),(2,3),(0,4),(1,0)\big),...,\big((2,4),(\infty,\infty),(2,2),(0,0),(1,3)\big),...\}$ □

การสร้าง 4.1.4 : ให้ $q = 3m+1$ เมื่อ m เป็นจำนวนเฉพาะยกกำลัง และ $m \geq 4$ ให้เซต C_1, C_2, C_3, C_4, C_5 ของคำรหัสความยาว 5 เหนือเซตอักษร $F = (\mathbb{F}_3 \times \mathbb{F}_m) \cup \{\infty, \infty\}$ กำหนดดังส่วนต้นของหัวข้อนี้จะได้ว่า C ซึ่งกำหนดโดย

$$C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$$

จะเป็นรหัส $3 - FP$ ความยาว 5 และ $|C| = \frac{5}{3}q^2 - \frac{10}{3}q + \frac{5}{3}$

พิสูจน์ จากตำแหน่งของ (∞, ∞) จะได้ว่า แต่ละคู่ของเซต C_i ไม่มีสมาชิกร่วมกัน
และ $|C_i| = 3m^2 = \frac{1}{3}(q^2 - 2q + 1)$
ดังนั้น เหลือเพียง จะแสดงว่า C เป็น $3 - FP$
สำหรับคำรหัส $x \in C$ กำหนดให้ $\pi_1(x)$ เป็นคำใน $X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$
โดยการแทนที่แต่ละตำแหน่ง $(a, b) \in F$ ของ x ด้วย $a \in \mathbb{F}_3 \cup \{\infty\}$
สังเกตว่า $\pi_1(x) \in X_i$ ถ้า $x \in C_i$
ในทำนองเดียวกัน กำหนด $\pi_2(x)$ เป็นคำใน $Y_1 \cup Y_2 \cup Y_3 \cup Y_4 \cup Y_5$
โดยการแทนที่แต่ละตำแหน่ง $(a, b) \in F$ ของ x ด้วย $b \in \mathbb{F}_m \cup \{\infty\}$
สมมติ $x \in C$ และ $P \subseteq C$ และ $x \in \mathrm{desc}(P)$ เราต้องแสดงให้เห็นว่า $x \in P$
ให้ $x \in C_j$ สำหรับบาง $j \in \{1, 2, 3, 4, 5\}$
ดังนั้น ตำแหน่งที่ j ของ x เป็น (∞, ∞) และ $\pi_1(x) \in X_j$
เนื่องจาก $|P| \leq 3$ จะมี $y \in P$ ที่ตรงกันกับ x มากกว่าหรือเท่ากับ 2 ตำแหน่งในตำแหน่งอื่น ๆ นอกจากตำแหน่งที่ j

จะแสดงว่า $x = y$
เนื่องจาก x และ y มีสัญลักษณ์ตรงกันมากกว่าหรือเท่ากับ 2 ตำแหน่ง
$\pi_1(x)$ และ $\pi_1(y)$ ก็เช่นเดียวกัน
ดังนั้น $\pi_1(y) = \pi_1(x)$ เราจะได้ว่า $\pi_1(y) \in X_j$ และ $y \in C_j$
นอกจากนี้ x และ y จะมีอย่างน้อย 2 ตำแหน่งที่ตรงกันนอกเหนือจากตำแหน่งที่ j
$\pi_2(x)$ และ $\pi_2(y)$ ก็เช่นเดียวกัน
ดังนั้น $\pi_2(x) = \pi_2(y)$
เนื่องจาก $\pi_1(x) = \pi_1(y)$ และ $\pi_2(x) = \pi_2(y)$ เราจะได้ $x = y \in P$ ตามต้องการ □

หมายเหตุ 4.1.5 : เงื่อนไขที่ $m \geq 4$ ในการสร้าง สามารถทำให้เบาลงจนถึงแค่ $m \geq 3$ ถ้าเรากำหนด $\alpha_4 = \infty$ ในนิยามของการสร้างเซต Y_i

ต่อไปจะสร้างรหัส $2 - FP$ ความยาว 4 โดยดัดแปลงจากการสร้างข้างต้น สิ่งสำคัญคือสองตำแหน่งใด ๆ ของสมาชิกใน $\bigcup X_i$ ต้องแตกต่างกัน
และสองตำแหน่งใด ๆ ของสมาชิกใน Y_i เดียวกัน ต้องแตกต่างกัน
ขั้นแรก สร้างเซตของ X_i โดยที่ $i = \{1, 2, 3, 4\}$

$$X_1 = \{(\infty, a, a, a : a \in \mathbb{Z}_2)\}$$
$$X_2 = \{(a, \infty, a, a + 1 : a \in \mathbb{Z}_2)\}$$
$$X_3 = \{(a, a + 1, \infty, a : a \in \mathbb{Z}_2)\}$$
$$X_4 = \{(a, a, a + 1, \infty : a \in \mathbb{Z}_2)\}$$

เห็นได้ชัดเจนว่าแต่ละคู่ของเซต X_i ไม่มีสมาชิกร่วมกัน และแต่ละเซต X_i มีจำนวนสมาชิก 2 ตัว เนื่องจาก a เป็นได้เพียง $0, 1$ นอกจากนี้ สามารถสังเกตได้ว่าทุกสองตำแหน่งของคำรหัสใด ๆ ใน $X_1 \cup X_2 \cup X_3 \cup X_4$ จะแตกต่างจากคำรหัสอื่น ดังนั้น ถ้าเราทราบสัญลักษณ์ใน 2 ตำแหน่ง ของคำรหัสใด เราสามารถระบุอีก 2 ตำแหน่งที่เหลือได้ เนื่องจากจะไม่มีตัวที่ซ้ำกันในตำแหน่งดังกล่าวของเซต X

ตัวอย่าง 4.1.6 : แจกแจงสมาชิกของ X_i โดยที่ $i = 1, 2, 3, 4$ ได้ดังนี้
$X_1 = \{(\infty, 0, 0, 0), (\infty, 1, 1, 1)\}$
$X_2 = \{(0, \infty, 0, 0), (1, \infty, 1, 0)\}$
$X_3 = \{(0, 1, \infty, 0), (1, 0, \infty, 1)\}$
$X_4 = \{(0, 0, 1, \infty), (1, 1, 0, \infty)\}$ □

ขั้นที่สอง สร้างเซตของ Y_i

ให้ α_1, α_2 และ α_3 เป็นสมาชิกที่แตกต่างกันของ $\mathbb{F}_m$ ซึ่ง $m \geq 3$

$$Y_1 = \{(\infty, f(\alpha_1), f(\alpha_2), f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

$$Y_2 = \{(f(\alpha_1), \infty, f(\alpha_2), f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

$$Y_3 = \{(f(\alpha_1), f(\alpha_2), \infty, f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

$$Y_4 = \{(f(\alpha_1), f(\alpha_2), f(\alpha_3), \infty) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

ตัวอย่าง 4.1.7 : แจกแจงสมาชิกของ Y_i โดยที่ $i = 1, 2, 3, 4$ เมื่อ $m = 3$ ได้ดังนี้

$Y_1 = \{(\infty, 0, 0, 0), (\infty, 1, 1, 1), (\infty, 2, 2, 2), (\infty, 2, 3, 1), (\infty, 0, 1, 2), (\infty, 1, 1, 0),$

$(\infty, 1, 0, 2), (\infty, 2, 1, 0), (\infty, 0, 2, 1)\}$

$Y_2 = \{(0, \infty, 0, 0), (1, \infty, 1, 1), (2, \infty, 2, 2), (2, \infty, 3, 1), (0, \infty, 1, 2), (1, \infty, 1, 0)$

$(1, \infty, 0, 2), (2, \infty, 1, 0), (0, \infty, 2, 1)\}$

$Y_3 = \{(0, 0, \infty, , 0), (1, 1, \infty, 1), (2, 2, \infty, 2), (, 2, 3, \infty, 1), (0, 1, \infty, 2), (1, 1, \infty, 0)$

$(1, 0, \infty, 2), (2, 1, \infty, 0), (0, 2, \infty, 1), \}$

$Y_4 = \{(0, 0, 0, \infty,), (1, 1, 1, \infty,), (2, 2, 2, \infty,)(2, 3, 1, \infty,), (0, 1, 2, \infty,), (1, 1, 0, \infty,),$

$(1, 0, 2, \infty,), (2, 1, 0, \infty,), (0, 2, 1, \infty,)\}$ □

ขั้นที่สาม สร้าง $C_i = X_i \times Y_i$ จาก X_i, Y_i ข้างต้น ดังนี้

$$C_i = \{((x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) : (x_1, x_2, x_3, x_4) \in X_i \text{ และ } (y_1, y_2, y_3, y_4) \in Y_i\}$$

ตัวอย่าง 4.1.8 : จงสร้าง C_1 จากเซต X_i, Y_i ข้างต้น

$C_1 = \big\{\big((\infty, \infty), (0, 0), (0, 0), (0, 0)\big), \big((\infty, \infty), (0, 1), (0, 1), (0, 1)\big), \big((\infty, \infty), (0, 2), (0, 2), (0, 2)\big),$

$\big((\infty, \infty), (0, 2), (0, 3), (0, 1)\big), \big((\infty, \infty), (0, 0), (0, 1), (0, 2)\big), \big((\infty, \infty), (0, 1), (0, 1), (0, 0)\big),$

$\big((\infty, \infty), (0, 1), (0, 0), (0, 2)\big), \big((\infty, \infty), (0, 2), (0, 1), (0, 0)\big), \big((\infty, \infty), (0, 0), (0, 2), (0, 1)\big),$

$\big((\infty, \infty), (1, 0), (1, 0), (1, 0)\big), \big((\infty, \infty), (1, 1), (1, 1), (1, 1)\big), \big((\infty, \infty), (1, 2), (1, 2), (1, 2)\big),$

$\big((\infty, \infty), (1, 2), (1, 3), (1, 1)\big), \big((\infty, \infty), (1, 0), (1, 1), (1, 2)\big), \big((\infty, \infty), (1, 1), (1, 1), (1, 0)\big),$

$\big((\infty, \infty), (1, 2), (1, 1), (1, 0)\big), \big((\infty, \infty), (1, 0), (1, 2), (1, 1)\big)\big\}$ □

หมายเหตุ 4.1.9 : ทั้งนี้ทั้งนั้น Chee และ Zhang [6] ได้ขยายแนวคิดนี้ไปสู่การสร้าง รหัส $k - FP$ ฐาน q ความยาว $k + 2$ สำหรับค่า k ใด ๆ โดยใช้อาร์เรย์เชิงตั้งฉาก (Orthogonal array)

4.2. **รหัสเทรซอะบิลลิที (Traceability)**

รหัสเทรซอะบิลลิที ถูกสร้างขึ้นครั้งแรกโดย Chor และ Naor [10] ภายใต้แบบแผนการแพร่สัญญาณออกอากาศที่เรากล่าวถึงในบทที่ 2 โดยมีวัตถุประสงค์เพื่อให้สามารถติดตามหนึ่งในผู้ใช้ร่วมกันสร้างชุดกุญแจดัดแปลงได้

ต่อไปนี้จะเป็นตัวอย่างรหัส $2-TA$ ที่มีความยาว 3 โดย Chor และ Naor [5]

<u>การสร้าง 4.2.1</u> : ให้ $q = 2r + 1$ เมื่อ r เป็นจำนวนเต็มบวก และ $A = \{0, 1, ...2r\}$ กำหนด $C = C_1 \cup C_2 \cup C_3$ เมื่อ

$$C_1 = \{(0, i, i) : 1 \leq i \leq r\}$$

$$C_2 = \{(i, 0, r + i) : 1 \leq i \leq r\}$$

$$C_3 = \{(r + i, r + i, 0) : 1 \leq i \leq r\}$$

พิสูจน์ ก่อนอื่นสังเกตได้ว่า เมื่อพิจารณาทีละตำแหน่งทั้งสามเซตย่อยไม่มีการใช้สัญลักษณ์ร่วมกัน
ให้ $x, y \in C$ และให้ $P = \{x, y\}$ โดยที่ P เป็นต้นกำเนิดของรหัส

ให้ $a \in \text{desc}(P)$ จะแสดงว่า มี $t \in P$ ที่ $d_H(a, t) \leq 1$
สมมติให้ $d_H(a, x) \geq 2$ และ $d_H(a, y) \geq 2$
นั่นคือ a และ x ตรงกันอย่างมาก 1 ตำแหน่ง
a และ y ตรงกันอย่างมาก 1 ตำแหน่ง
เพราะฉะนั้น $a \notin \text{desc}(P)$ ทำให้เกิดข้อขัดแย้งที่ $a \in \text{desc}(P)$
ดังนั้นมี $t \in P$ ที่ $d_H(a, t) \leq 1$ โดยไม่เสียนัยทั่วไป สมมติให้ $t = x$

ต่อไปจะแสดงว่า $d(a, z) \geq 2$ สำหรับทุก $z \in C - P$
<u>กรณีที่ 1</u> x, z มาจากคนละเซต C_i
จากการนิยามจะได้ว่า z ต่างจาก x ในทุกตำแหน่ง
ดังนั้น z ต่างจาก a อย่างน้อย 2 ตำแหน่งที่ a ตรงกับ z
ดังนั้น $d(a, z) \geq 2$
<u>กรณีที่ 2</u> x, z อยู่ในเซต C_i เดียวกัน
กรณีที่ 2.1 a และ x ตรงกันในตำแหน่งที่ไม่เป็น 0 ทั้ง 2 ตำแหน่ง
จากนิยาม จะได้ว่า z ต่างจาก x ในตำแหน่งที่ไม่เป็น 0
ดังนั้น z ต่างจาก a ใน 2 ตำแหน่งดังกล่าว
กรณีที่ 2.2 a และ x ตรงกันในตำแหน่งที่ 0 และอีกตำแหน่งใดตำแหน่งหนึ่งที่ไม่เป็น 0

จากการนิยาม จะได้ว่า z ต่างจาก x ในตำแหน่งที่ไม่เป็น 0
ดังนั้น a ต่างจาก z ในตำแหน่งดังกล่าว
นอกจากนี้ ตำแหน่งที่เหลือของ z จะไม่เป็น 0
เพราะคำรหัสมี 0 ได้เพียงตำแหน่งเดียว จึงไม่ตรงกับ a และ y
ดังนั้น $d_H(a,z) \geq 2$
เพราะฉะนั้น $d_H(a,z) \geq 2$
ดังนั้น C เป็น รหัส $2-TA$ คำฐาน q ความยาว 3 โดยมี $3r = \frac{3}{2}(q-1)$ คำรหัส

ทฤษฎีบท 4.2.2 : [5] ให้ C เป็นรหัสแก้ไขข้อผิดพลาด ฐาน q ที่มีความยาว n ถ้า

$$d(C) > n - \lceil n/k^2 \rceil$$

แล้ว C เป็นรหัส $k-TA$

ตัวอย่างต่อไปนี้จะแสดงการสร้างรหัส TA โดยใช้รหัสแก้ไขข้อผิดพลาด

ตัวอย่าง 4.2.3 : ให้ $C = \{(0,1,2,3,1,2),(0,2,3,1,2,1),(1,0,1,2,3,3),(2,3,0,0,2,0)\}$
จะได้ว่า C เป็นรหัส $2-TA$ ฐาน 4 ความยาว 6
พิสูจน์ $d((0,1,2,3,1,2),(0,2,3,1,2,1)) = 5$
$d((0,1,2,3,1,2),(1,0,1,2,3,3)) = 6$
$d((0,1,2,3,1,2),(2,3,0,0,2,0)) = 6$
$d((0,2,3,1,2,1),(1,0,1,2,3,3)) = 6$
$d((0,2,3,1,2,1),(2,3,0,0,2,0)) = 5$
$d((1,0,1,2,3,3),(2,3,0,0,2,0)) = 6$
ดังนั้น $d(C) = 5$
ตรวจสอบ จากทฤษฎีบท

$$d(C) > 6 - \lceil 4/2^2 \rceil = 4$$

□

บทที่ 5

สรุปผลการศึกษา

การค้นคว้าอิสระนี้ได้ศึกษานิยามและขอบเขตของรหัสลายนิ้วมือดิจิทัล 4 ชนิด คือ รหัสเฟรมพรูฟ รหัสซีเคียวเฟรมพรูฟ รหัสระบุต้นกำเนิด และรหัสเทรซอะบิลลีที พบว่ารหัสทั้ง 4 ชนิดมีความสัมพันธ์กันดังนี้ รหัสเทรซอะบิลลิทีเป็นรหัสระบุต้นกำเนิด รหัสระบุต้นกำเนิดเป็นรหัสซีเคียวเฟรมพรูฟ และรหัสซีเคียวเฟรมพรูฟเป็นรหัสเฟรมพรูฟ

นอกจากนี้เรายังได้ศึกษาการสร้างรหัส 3-FP ความยาว 5 และได้ดัดแปลงเป็นการสร้างรหัส 2-FP ความยาว 4 ที่มีทั้งสิ้น 16 คำรหัส และศึกษาการสร้างรหัสเทรซอะบิลลิทีโดยใช้รหัสแก้ไขข้อผิดพลาดและได้สร้างรหัส $2-TA$ ฐาน 4 ความยาว 6 ที่มีทั้งสิ้น 4 คำรหัส

บรรณานุกรม

[1] Alexander Barg, Gerard Cohen, Sylvia Encheva, Gregory Kabatiansky, and Gillés Zémor, *A hypergraph approach to the identifying parent property: the case of multiple parents*, SIAM Journal on Discrete Mathematics **14** (2001), no. 3, 423–431.

[2] Simon R Blackburn, *Combinatorial schemes for protecting digital content*, Surveys in combinatorics **307** (2003), 43–78.

[3] _____ , *Frameproof codes*, SIAM Journal on Discrete Mathematics **16** (2003), no. 3, 499–510.

[4] _____ , *An upper bound on the size of a code with the k-identifiable parent property*, Journal of Combinatorial Theory, Series A **102** (2003), no. 1, 179–185.

[5] Simon R Blackburn, Tuvi Etzion, and Siaw-Lynn Ng, *Traceability codes*, Journal of Combinatorial Theory, Series A **117** (2010), no. 8, 1049–1057.

[6] Yeow Meng Chee and Xiande Zhang, *Improved constructions of frameproof codes*, IEEE transactions on information theory **58** (2012), no. 8, 5449–5453.

[7] Hong-Bin Chen and Geng-Yu Chen, *Optimal 2-traceability codes of length 4*, Theoretical Computer Science **954** (2023), 113800.

[8] Minquan Cheng, Jing Jiang, and Qiang Wang, *Improved bounds on 2-frameproof codes with length 4*, Designs, Codes and Cryptography **87** (2019), 97–106.

[9] Marco Dalai, Stefano Della Fiore, Adele A Rescigno, and Ugo Vaccaro, *Bounds and algorithms for frameproof codes and related combinatorial structures*, arXiv preprint arXiv:2303.07211 (2023).

[10] Yvo G Desmedt, *Advances in cryptology—crypto'94: 14th annual international cryptology conference, santa barbara, california, usa, august 21–25, 1994. proceedings*, vol. 839, Springer, 2008.

[11] Yujie Gu and Ying Miao, *Bounds on traceability schemes*, IEEE Transactions on Information Theory **64** (2017), no. 5, 3450–3460.

[12] Hossein Hajiabolhassan and Farokhlagha Moazami, *Secure frameproof codes through biclique covers*, Discrete Mathematics & Theoretical Computer Science **14** (2012), no. Graph Theory.

[13] Siaw-Lynn Ng and S Owen, *A note on an upper bound of traceability codes.*, Australas. J Comb. **62** (2015), 140–146.

[14] Chong Shangguan, Jingxue Ma, and Gennian Ge, *New upper bounds for parent-identifying codes and traceability codes*, Designs, Codes and Cryptography **86** (2018), 1727–1737.

[15] Chong Shangguan, Xin Wang, Gennian Ge, and Ying Miao, *New bounds for frameproof codes*, IEEE Transactions on Information Theory **63** (2017), no. 11, 7247–7252.

[16] Jessica N Staddon, Douglas R Stinson, and Ruizhong Wei, *Combinatorial properties of frameproof and traceability codes*, IEEE transactions on information theory **47** (2001), no. 3, 1042–1049.

[17] Douglas R Stinson and Gregory M Zaverucha, *Some improved bounds for secure frameproof codes and related separating hash families*, IEEE Transactions on Information Theory **54** (2008), no. 6, 2508–2514.

[18] Tran Van Trung and Sosina Martirosyan, *On a class of traceability codes*, Designs, Codes and Cryptography **31** (2004), 125–132.

Digital Fingerprints Codes: Property and Construction

Miss Natthanan Jaisom
Asst. Prof. Dr.Penying Rochanakul
Department of Mathematics, Faculty of Science, Chiang Mai University

Abstract

In this independent study, we are interested in properties and constructions of digital fingerprint codes, which can be used against digital piracy. We study 4 types of codes, namely frameproof codes, secureframeproof codes, parent identifying codes and traceability codes, including properties and relations between them. Moreover, we do literature review on bounds of codes and creates a 2-FP code of length 4 of the largest size possible. In addition, we construct traceability codes from error-correction codes.

1. Introduction

Nowadays, it is important to prevent digital piracy. But it can be difficult. Especially since the internet digital data such as music, movies, documents, e-books, or software can be easily copied and distributed which causes the illegal distribution of information or what is called **Piracy of copyright** is widespread. We can use hardware techniques that prevent copying of intellectual property to help prevent copyright infringement. However, these techniques may reduce the convenience of authorized users from doing legitimate things, such as making copies of CDs or DVDs. or the use of copyrighted material for research and education under fair use laws. Therefore, we are interested in techniques that inject some form of uniqueness into each piece of digital data. This makes it possible to collect evidence so that it can be traced to the group of owners of the original files. Although each copy of digital data can be altered and illegal redistributors of copies are prosecuted, These techniques are commonly known as **Digital Fingerprint** In this independent study we are interested in the properties of organized mathematics. The technique behind this technique is called **fingerprint code**.

2. Scope of study

1. Study about digital fingerprint codes.
2. Study frameproof code
3. Study the secure frameproof code
4. Study the identifiable parent property code.
5. Study the traceability code.
6. Study the relationship between the 4 types of digital fingerprint codes.
7. Creating constructions of digital fingerprint codes

3. Definition

Let q and n be positive integers a *q-ary alphabet* is set of q different element, called *symbols*

A *code* over A of length n is not empty subset C of A^n.
A *word* of length n over an alphabet A is a sequence $(x_1, x_2, ..., x_n)$ where $x_i \in A$ for each i

Let $x, y \in A^n$ be words of lenth n. The *Hamming distance* between x, y
denoted $d_H(x, y)$ is the number of position in which x and y are different .

$$d_H(x, y) = |\{i \in [n] : x_i \neq y_i\}|$$

Let C be a code the minimum *distance* of C denoted by $d(C)$, is $d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}$
For $X \subseteq A^n$, the set *decendants* of X, denoted desc(X) is subset of A^n such that:

$$\text{desc}(X) = \{d \in A^n : \forall i \in [n], \exists x \in X \;\; d_i = x_i\}$$

Let k be a positive integer. For a code C define the *k-descendant code* of C,
denoted $\text{desc}_k(C)$, as follows

$$\text{desc}_k(C) = \bigcup_{\substack{X \subseteq C \\ |X| \leq k}} \text{desc}(X)$$

4. Definition of Fingerprint codes

Let C be a $q-$ary code of length n and let k be a positive integer
(i) C has $k - frameproof$ property or is $k-$FP if for all $X \subseteq C$ such that $|X| \leq k$

$$\text{desc}(X) \cap C \subseteq X$$

.
(ii) C has $k - secure\ frameproof$ property or is $k-$SFP
if for all $X_1, X_2 \subseteq C$ of $|X_1|, |X_2| \leq k$ if $\text{desc}(X_1) \cap \text{desc}(X_2) = \emptyset then \text{X}_1 \cap X_2 = \emptyset$
(iii) C has $k - identifiable\ parent\ property$ or is $k-$IPP if for all $x \in \text{desc}_k(C)$ then

$$\bigcap_{\substack{X \subseteq C : |X| \leq k \\ x \in \text{desc}(X)}} X \neq \emptyset$$

.
(iv) C has $k - traceability$ property or is $k-$TA if for all $X \subseteq C$ such that $|X| \leq k$
and for all $x \in \text{desc}(X)$ such that $z \in C$ if $d_H(x, z) = \min_{y \in C} d_H(x, y)$ then $z \in X$.

5. Construction of 2-FP length 4

Construction of set X_i

$$X_1 = \{(\infty, a, a, a : a \in \mathbb{Z}_2)\}$$
$$X_2 = \{(a, \infty, a, a + 1 : a \in \mathbb{Z}_2)\}$$
$$X_3 = \{(a, a + 1, \infty, a : a \in \mathbb{Z}_2)\}$$
$$X_4 = \{(a, a, a + 1, \infty : a \in \mathbb{Z}_2)\}$$

Construction of set Y_i

$$Y_1 = \{(\infty, f(\alpha_1), f(\alpha_2), f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_2 = \{(f(\alpha_1), \infty, f(\alpha_2), f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_3 = \{(f(\alpha_1), f(\alpha_2), \infty, f(\alpha_3)) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$
$$Y_4 = \{(f(\alpha_1), f(\alpha_2), f(\alpha_3), \infty) : f \in \mathbb{F}_m[x], \deg f \leq 1\}$$

Construction of set C_i

$$C_i = \{((x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5)) : (x_1, x_2, x_3, x_4, x_5) \in X_i \text{ and } (y_1, y_2, y_3, y_4, y_5) \in Y_i\}$$

Then $C = c_1 \cup c_2 \cup c_3 \cup c_4 \cup c_5$ is a $q-$ary 2-FP code of size $2(q-1)^2$.

6. Theorem and Construction the 2-TA code from the theorem

Let C be a q-ary error-correcting code of length n. If

$$d(C) > n - \lceil n/k^2 \rceil$$

then C is $k - TA$ code
Example Let $C = \{(0, 1, 2, 3, 1, 2), (0, 2, 3, 1, 2, 1), (1, 0, 1, 2, 3, 3), (2, 3, 0, 0, 2, 0)\}$
Then C is a 4-ary $2 - TA$ code of length 6. Since $d(C) = 5$, we have

$$d(C) > 6 - \lceil 4/2^2 \rceil = 4.$$

Conclusion

This independent research studied the definition and scope of 4 types of digital fingerprint codes: frame proof code, secure frame proof code, identifiable parent property code and traceability Code It was found that the four types of codes were related as follows. The traceability code is an identifiable parent property code, The identifiable parent property code is the Secure Frameproof Code and the Secure Frameproof code is the Frameproof code. Moreover, We also studied created of a 3-FP code of length 5 and modified it to created a 2-FP code length 4 with a total of 16 codewords, and studied the created of traceability codes using error-correction codes and created the code $2 - TA$ 4-ary length 6 with total 4 codewords.

Refererence

[1]Blackburn, Simon R., Tuvi Etzion, and Siaw-Lynn Ng. "Traceability codes." Journal of Combinatorial Theory, Series A 117.8 (2010): 1049-1057.

[2]Blackburn, Simon R. "Frameproof codes." SIAM Journal on Discrete Mathematics 16.3 (2003): 499-510.

[3]Chee, Yeow Meng, and Xiande Zhang. "Improved constructions of frameproof codes." IEEE transactions on information theory 58.8 (2012): 5449-5453.

[4]Shangguan, Chong, Jingxue Ma, and Gennian Ge. "New upper bounds for parent-identifying codes and traceability codes." Designs, Codes and Cryptography 86 (2018): 1727-1737.