Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 2, pp. 793–810
DOI : 10.47974/JIOS-2187

Understanding traceable codes : A review of their functionality and importance

Anu Kathuria
Department of Applied Sciences and Humanities
The Technological Institute of Textile & Sciences
Bhiwani 127021
Haryana
India

Abstract

Traceable Codes and Frameproof Codes are Essential in Secure Communication, Data distribution, and copyright protection. These Combinatorial Codes enable the detection and prevention of malicious activities such as unauthorized redistribution and collusion. This paper reviews the foundational principles, significant developments, and practical applications of these codes. A Comparative Analysis of these codes highlight the Advancements in Construction Methods and identifies challenges and offers future Research directions.

Subject Classification: *12F05, 12F06, 12F15.*

Keywords: *Traceable codes, Frameproof codes, Perfect hash families.*

1. Introduction

The need to conceal information for purposes such as security, privacy, or other reasons is inherent to all living beings and has been addressed through various techniques since ancient times. With the advent of digital technology, the field of information hiding has gained immense importance due to its extensive range of applications, together with protected communication, evidence of possession, authentication, protection against illegal content distribution, customer tracking and information embedding. In the digital realm, three primary techniques dominate: Steganography, Watermarking, and Fingerprinting. Steganography involves concealing data in ways that make the confidential information undetectable, whereas digital watermarking embeds signals into unique content to identify ownership. Fingerprinting, introduced by Wagner[39] in 1983, uniquely marks data to trace the source of illegal copies, especially in digital content distribution. By embedding unique fingerprints for

E-mail: anu_sept24@rediffmail.com

each user using watermarking algorithms, distributors can identify dishonest users in cases of unauthorized redistribution. Even if users attempt to tamper with the Fingerprints, robust watermarking processes ensure their integrity and effectiveness.

2. Background

Preliminaries

In Algebraic Field Theory, there are several key terminologies and axioms that form the foundation of fields. Here we explore some of these Essential terms and Axioms:

Definition 2.1: Algebraic Field [7]: A field F(Vector Space) is a non empty set enabled with two binary operations $+(addition)$ and $\cdot\,(multiplication)$ that satisfy the following Properties ;

(a) Closure Property : For any $l, m \in F$, both $l + m$ *and* $l.m$ belong to F.

(b) Commutative Property : $l + m = m + l,\ l.m = m.l$

(c) Associative Property : $(l + m) + n = l + (m + n), l.(m.n) = (l.m).n$

(d) Distributive Property : $l.(m + n) = l.m + l.n$

Furthermore, identity elements 0 and 1 must exist in F satisfying ;

(e) Existence of Identity: $l + 0 = l$ for all l *in* F.

(f) Existence of Inverse: $l.1 = l$ for all l *in* F.

(g) Existence of Additive Identity : $l + (-l) = 0$ for all l in F.

(h) Existence of Additive Inverse : $l.l^{-1} = 1$; for all l in F.

Examples of Field are ; Q, R and C

Definition 2.1: [7]; "A finite field is a field that contains a finite number of elements, the number of elements in a field is referred to as order of a field. The order of a finite field is q^n for some prime number q *and* a positive integer n. A finite field F *is* also defined as a Galois field and if F is a field of order q^n, then we write $F = GF(q^n)$".

2.1.3 Coding Theory [36]; In this Section,we present fundamental results and definitions central to Coding Theory .

Basic Definitions:

1. **Code:** A set of symbols or sequences (called codewords) designed for encoding information. A code C consists of all possible codewords defined over the

   Set of alphabets. All the codewords of a code are designed using above properties and Generator Matrix.

2. **Hamming Distance:** For two codewords $u, v \in$ C, the Hamming distance $d(u,v)$, between any two codewords is the number of positions where u and v differ. Example : $d(101,111)=1$

3. **Minimum Distance**: The smallest Hamming distance between any two distinct codewords of C is $d_{min.} = \min.(d(u,v))\,; u \neq v$.
4. **Representation of a Code**: A code C can be represented with the following parameters,(n, T, d);
   n: length of codeword
   T: number of codewords
   d: distance between two codewords.

2.1.4 Fingerprinting Technique Introduction[1]

The fingerprinting technique involves embedding unique marks into each copy of digital content, akin to how fingerprints uniquely identify individuals. These marks make each copy distinct, allowing distributors to trace any unauthorized copies back to the user responsible for their illegal distribution. This capability acts as a deterrent, discouraging users from releasing unauthorized copies due to the risk of detection. However, fingerprinting must address the problem of collusion, where two dishonest users may compare their marked copies to identify differences and create a new, untraceable mark. They can then redistribute the content with this new mark without fear of detection. In cases where the same codeword is inadvertently assigned to a third user who did not participate in the conspiracy, they could be wrongly implicated, emphasizing the importance of designing robust fingerprinting systems to prevent such scenarios.

2.1.4.1. Fingerprinting Codes Classification [1]

fingerprinting code of the type (*n, M, q, d*) is defined by the following parameters; Fingerprinting codes are designed for multimedia content protection enabling the identification of users involved in unauthorized redistribution. These codes are categorized into the following types:

1. Frameproof Code (FP)
2. Secure Frameproof Code (SFP)
3. Identifiable Parent Property Code (IPP)
4. Traceable Code (TA)

2.1.4.2. Frameproof Code

The idea of frameproof codes was established by Dan Boneh and James Shaw in 1995. These codes are intended to prevent colluding entities from framing innocent parties in certain applications, such as copyright protection and traitor tracing. The key idea is that no subset of users can produce a suitable codeword that implicates another traitor not in the subset. In their work, Boneh and Shaw suggest a sufficient condition for a code to be frameproof. The formal definition is as follows: “A code D is called **c-frameproof** if, for every set W⊂D of size at most c, the following condition is satisfied: F(W)∩D=W”, where F(W) represents the set of all codewords that could be forged by combining elements of W. Intuitively, this condition ensures that a subset W of colluding codeword

holders cannot produce a forged codeword that matches the codeword of any user outside their group. In other words, if a coalition attempts to produce a new codeword, it will not falsely implicate an innocent user who is not part of the coalition. This property provides traceability while protecting honest users from being framed.

2.1.4.3 Secure Frameproof Code

A secure frameproof code extends the basic properties of frameproof codes by providing additional security against more sophisticated attacks. Specifically, it ensures that even if a coalition of users shares their codewords, they cannot reverse or reconstruct the original content distribution Mechanism.This enhanced notion of security and its groundwork was led by Stinson and Wei in 1998 [15], and later revisited by Boneh and Shaw [13].

Theorem 2.1.4.4 [15]: "*A code D is called totally* $c-$*secure code or secure frameproof then for any* D_1 , $D_2 \subsetneq C$ *with* $|D_1| = c_1$ *and* $|D_2| = c_2$, *holds that* $D_1 \cap D_2 = \emptyset$, $\rightarrow F(D_1) \cap F(D_2) = \emptyset$."

2.1.4.5. Identifiable Parent Property Code

The concept of Identifiable Parent Property (IPP) codes was introduced by Hollman in 1998 [22].IPP is a key property in the design of codes used for applications such as traitor tracing, digital fingerprinting, and secure multimedia distribution.

Formal Definition; A code D is said to satisfy the c-IPP property if, for any coalition W $\subseteq$ D; with |W| $\leq$ c and for any n-tuple x (potentially augumented from codewords in W), there exists at least one codeword in W that can be identified as a source of x. This ensures that the coalition cannot completely obscure their involvement in generating the $n-$tuple.

2.1.4.6 . Traceable (TA) Code

The notion of Traceable (TA) Code was introduced by Chor, Fiat and Naor [8,9] in 1994. It was further investigated by Stinson and Wei in [14, 15 & 16]. For $x, y \in Q^n$; define $I(x, y) = \{i : x_i = y_i\}$representing the set of positions where x *and* y have the same positions.The condition when interpreted in terms of distance is equivalent to $d(x, y) < d(x, z)$, ensuring that x is closer to a codeword in C_i than to any codeword outside C_i .This ensures that if a group of $\leq c$ users collude to produce a new (pirated) codeword x, then the tracing algorithm can identify at least one member of the coalition by checking which user's codeword is closest to x.

3. Literature Survey

To deal with the issue of unauthorized redistribution and user identification in digital content distribution, four distinct types of fingerprinting codes discussed above have been developed and studied extensively in the Literature. These codes provide reliable levels of protection against collusion, framing, and tracing unauthorized users. The foundation work by Boneh and Shaw in 1994

introduces the concept of frameproof codes and further develop the notion of $c-$ secure codes with almost zero error ,i.e. a traitor may be traced from the illegal copy with high probability. Researchers have introduced various Error Correcting Codes to create $c-$frameproof codes and also derived sufficient condition for such Error Correcting Code to be applicable in this construction satisfying as $d > (1-\frac{1}{c})n$, where d is the minimum distance of the code and n is the length of the Code,c defines number of colluders. Furthermore they established the existence of binary $c-$frameproof code with the n number of code words satisfying $n = 2^{\frac{l}{16c}}$, where l is the length of the code and $c\ (>0)$ is an arbitrary integer (number of colluders).This result provides a lower bound on the number of codeword possible in such constructions, ensuring scalability for practical implementations.

The provided excerpt discusses the development and study of IPP codes, particularly with an alphabet size of 2. Hollman initially introduced these codes in [22], and subsequent research by Staddon, Stinson and Wei [24] expanded on them. Additionally, traceability codes, a specific subclass of IPP codes, were analyzed by Chor, Fiat, and Naor in 1994 [8,10].

These codes present robust security by leveraging the structural properties of IPP codes to trace unauthorized activities. In 2000, Chor, Fiat and Naor [9], show that if a code follows the property of $d > (1-\frac{1}{m^2})n$(where d is the minimum distance and m the number of colluders(traitors) and n is the length of the code),then it is an $m-traceability$ code. For two positive integers t and m ; there exists a $c-$traceabilty scheme with $n = 2^{\frac{t}{8m^4}}$ $d$ecoders, where t is the total number of keys is proved by Chor, Fiat and Naor in [8]. Staddon, Stinson and Wei also [24] suggest that an upper bound on the number of codewords in a $c-$ frameproof code over an alphabet of size $q \geq 2$, the bound is given as $n \leq q^{\frac{l}{c}} + 2c - 2$. Stinson, Trung and Wei[16] establish an upper bound on the number of decoders in a $c-$ traceabilty scheme $n \leq \frac{lc_t}{kc_{t-1}}$. In 2001, Safavi – Naini and Want [41,43] investigated fingerprinting schemes by utilizing constant weight codes derived from certain error-correcting codes.

Recent developments in the study of traceability in fingerprinting systems have highlighted the role of constant-weight codes in establishing lower bounds for authenticity. Fu, Klove and Luo [21] have derived significant conditions to construct equidistant constant weight codes. A notable advancement was made in 2007 when Jin and Blaum[23] introduced a significant contribution by establishing conditions for constructing traceability schemes using linear Maximum Distance Separable (MDS) codes marking a significant contribution in the field of Mathematics.MDS codes, a high class of error-correcting codes, achieve the maximum possible minimum distance for a given code length and dimension. Due to their optimal error-correcting capabilities**,** linear MDS codes are particularly well-suited for applications such as traitor tracing and digital fingerprinting, where both robustness and precision are crucial. In the same work, Jin and Blaum demonstrated that a linear code C is said to be m-traceable

if it satisfies the condition $d > (1 - 1/m^2)n$. An extensive study on all these fingerprinting codes is done by several number of authors. Notably, significant contributions have been made to the development of these codes in [1, 2, 24 & 48] .Their work introduced new constructions and proposed novel classes of codes aimed at enhancing collusion resistance and improving traceability performance. "A new class of 2-IPP Codes [47]contributing to the advancements of fingerprinting code structures was introduced by Sudhir Batra. In 2005, Veerubhotla, Gualti and Pujari [42] proposed a novel construction of Gossip Codes that aimed at developing the shortest possible traceability schemes through the use of $t-$designs.Additionally several authors have employed Perfect Hash Families as a combinatorial tool to construct diverse fingerprinting schemes. In their 2010 work, Blackburn and Etzion [46] explored the application of error-correcting codes with high minimum distance in the construction of traceability codes emphasizing their potential to enhance security against collusion. They investigated the parameters under which this "error-correcting construction" yield efficient traceability codes.These parameters are significant because the error-correcting construction cannot produce *k*-traceability codes of constant rate under certain conditions due to limitations such as the Plotkin bound, which imposes an upper bound on the count of codewords in a code with a given minimum distance.

In the papers[18,19];A hypergraph-based framework is adopted to analyze and construct IPP codes.A hypergraph is a generalization of a graph where edges can connect more than two vertices.Hypergraphs provide a natural way to represent the parent-child relationship in traceability codes and IPP codes ; where a single child (or "descendant") may be traced back to multiple parents.

In Kathuria, Arora, Batra [4, 5] and Kathuria and Batra [6] have derived the Necessary and Sufficient conditions for which an equidistant code can be converted into a 2-traceable code. An unambiguous creation method is anticipated to generate linear MDS $[q+1, 2, q]$ codes over the finite field F_q ;where q is a prime.These codes can also be employed as 2-TA codes for q >2.In [55,56],a few Combinatorial Structures have been discussed using Latin Squares and Proective Planes. The work points out a specific contradiction with a result from Jin and Blaum's[23],2007 paper. In particular, they found that the linear MDS code of length 4 over the field size $q = 5$ and for p=3, negates their earlier result. The paper corrects this by providing the right version of this result, including the proof by using Jacobsthal Matrices and Hadamard Matrices. That paper also discusses an ongoing development of equidistant 2-TA (two-track affine) codes with infinite families. Some of these codes are also identified as high-quality equidistant codes, a subject thoroughly investigated by Sinha et al. [27]. In their work, they analyzed the structure and practical applications of these codes, particularly highlighting their usefulness in improving traceability and resistance to collusion.

In [27], Sinha, Wang and Wu proposed various combinatorial designs that play a crucial role in constructing good equidistant codes. These designs offer

structural properties that guarantee traceability and equidistance, which are essential for the effective functionality of 2-TA codes.

"The effectiveness of a c-traceability code (or IPP code) is largely determined by two key parameters: the number of codewords N (i.e., the size of the code) and the collusion resistance threshold c. Generally, larger values of N and c contribute to higher efficiency and robustness in identifying traitors. In this context, Moreira and Fernandez [26, 31, 32 and 35] have utilized linear codes, particularly Reed–Solomon codes, to construct IPP codes with desirable properties. In [30,33,34,36],they even represent properties of Linear Codes to be traceable Codes .Similarly, Lofvenberg [25], Lindkvist [28], and Lindkvist, Lofvenberg, and Svanstrom [29] explored the use of constant weight codewords for constructing fingerprinting codes of this type. In addition, traceability codes based on combinatorial designs-such as lexicographic codes-have been proposed and analyzed in works like [55,56], further expanding the range of tools available for secure digital content protection."

Here now we characterize the key results of Frameproof Codes in Tabular Form for further Analysis;

Year	Authors	Title	Key Results
2024	Tripathi, Pandey, and Singh [50]	*Boneh-Shaw fingerprint code and Tardos code analysis and optimization in minority collusion attack*	"In this study, the Tardos and Boneh-Shaw fingerprinting codes were compared within the context of collusion attacks. The comparison led to the following conclusions: Boneh-Shaw Codes perform better when minimizing average false positives (FPs) and false negatives (FNs) is a priority, whereas Tardos codes are more efficient when code length is a critical constraint. However, a key limitation of both schemes is their inability to fully eliminate the risk of false positives or false negatives-particularly in the phase of minority collusion attacks"**.**
2000	Stinson,Van Trung, Wei [16]	*Secure Frameproof Codes*	"In this study Stinson ,Van and Wei have explored connections between Frameproof Codes and other Combinatorial Structures like Perfect Hash Families. They have also suggested new constructions and bounds for Frameproof codes".
2003	Blackburn [45]	*Frameproof Codes*	"This study investigates the maximum cardinality n of a c-Frameproof code of length l, with a particular focus on the particular case when q, is large. The paper shows that when $2 \leq l \leq$ c,the maximum

			cardinality is $n = l(q-1)$ and for the specific case of $c = 2$, it demonstrates that n is approximately $tq^{\frac{l}{2}}$, where $t = 1$; when l is odd and $t = 2$ if l is even. Furthermore the paper establishes improved upper bounds on n by applying techniques from extremal set theory (particularly, a generalization of the Erd″os–Ko–Rado theorem).".
2012	Zhang and Chee [49]	***Improved Constructions of Frameproof Codes***	"In this paper, the authors present a recursive construction for c-frameproof codes of length l with respect to the alphabet size q. As an applications of this construction, they establish the existence results for q-ary c-frameproof codes of length $c+2$ and size $\frac{c+2}{c}(q-1)^2+1)$ for all odd q when $c = 2$ and for ll $q \equiv 4(mod6)$ when $c = 3$. Furthermore, they show that $R(c, c+2) = (c+2)/c$, thus it meets the upper bound given by Blackburn and also comes out to be true for all integers c such that $c+1$ is a prime power.".
2024	Liu, and Shangguan[38]	*Near Optimal Constructions of Frameproof Codes*	"Frameproof codes can significantly enhance the security and credibility of digital content. Let $M_{c,l}(q)$ denote the maximum size of a q−ary c−frameproof code with length l .In 2003, Blackburn observed a compelling link between $M_{c,l}(q)$ and the Erdős Matching Conjecture in extremal set theory,and posed the problem of determining the limit $R_{c,l}$=lim q→∞; $M_{c,l}$(q)/q$[\frac{l}{c}]$. By combining several ideas from the probabilistic method, we present a new lower bound for $M_{c,l}$(q) . Together with an upper bound of Blackburn, this completely determines $R_{c,l}$ for all fixed , l , and thereby resolves the above open problem in the full generality. In the same study they also present an improved upper bound for $M_{c,l}$ (q)".

2024	Marco Dalai and Fiore [37]	***Bounds and Algorithms for Frameproof Codes and Related Combinatorial Structures***	"In this paper, the authors demonstrate the existence of q-ary (k, n)-frameproof codes of length t with the following bounds : When q ≤ k , codes of length t = O ($\frac{k2}{q}$ log n) can be constructed using the Lovász Local Lemma, and when $q > k,$ codes of length t =O($\frac{k^2}{log(\frac{q}{k})}$ log(n/k)) can be constructed using the expurgation method. Remarkably, in the practical case when q ≤ k our findings give codes whose length almost matches with the lower bound $\Omega(k^2/q.logk.logn)$ on the length of any q-ary (k,n)-frameproof code and, even more importantly, allow us to derive an algorithm of complexity $O(t.n^2)$ for the construction of such codes".

Now we represent the key papers of Identifiable Parent Property Codes in Tabular Form for Analysis.

Year	Authors	Title	Results
1998	Hollman, Linnartz, Van Lint, Tolhuizen [22]	***On Codes with the Identifiable Parent Property***	"This paper explores families of *fingerprint codewords* with the property that if two users attempt to produce a new copy by combining segments from their respective codewords, the resulting copy can be traced back to at least one of the original users. Furthermore, the authors demonstrate that, for a fixed alphabet size, the maximum number of such distinguishable codewords grows exponentially with the length of the codewords".
2003	Simon R. Blackburn [53]	*An upper bound on the size of a code with the k-identifiable parent property*	"This study investigates an upper bound on the size of a q-ary code of length n that satisfies the *k-identifiable parent property (k-IPP),* a key requirement in Digital Fingerprinting and Traitor Tracing Applications.A key consequence of this bound is that, in many cases where the alphabet size q→∞ with k and n fixed, the optimal rate of

			such codes can be precisely determined.
2008	Boneh and Shaw [12]; Blackburn and Etzion [46]	*Prolific Codes with the Identifiable Parent Property*	"This study defines the concept of a *prolific IPP code*, defined as a code in which every word over the alphabet A of length n(i.e.all possible words) is the descendant of some set of codewords.The paper demonstrates that all linear prolific Identifiable Parent Property (IPP) codes belong to three infinite, structurally 'trivial' families, along with a single known sporadic instance-a ternary code of length four. To date, no prolific IPP codes are known that are not equivalent to these linear constructions. Moreover, the authors establish that for most parameter settings, prolific IPP codes do not exist, leaving only a limited number of unresolved cases. As a secondary contribution, the paper presents new upper bounds on the size of general (not necessarily prolific) IPP codes, thereby improving upon the best-known results in the existing literature.

Here's a comprehensive table detailing the key results of major research papers on Traceable Codes, starting with Chor, Fiat, and Naor's foundational work in 1994;

Year	Authors	Title	Results
1994	Chor, Fiat, and Naor [10]	*Tracing Traitors*	"In this paper, the authors establish different cryptographic schemes designed to trace the origin of data leaks when sensitive or proprietary content is distributed to a large number of recipients. These schemes are particularly crucial in settings such as broadcast and database access systems, where data must remain accessible exclusively to authorized users. Their relevance is especially pronounced in many applications like pay television, where they naturally integrate with and enhance broadcast encryption protocols".

2001	Silverberg, Staddon, Walker [54]	Optimized Traitor Tracing via List Decoding Techniques	"In this study the authors use new powerful techniques for list decoding of error correcting codes to efficiently trace traitors. Because the TA tracing algorithm has a runtime of O(N) in general,where N is the number of users, athough it is inefficient for large populations. They also recommend a few schemes for which the TA algorithm is very fast. The IPP tracing algorithm, though less efficient, can list all coalitions capable of constructing a given pirate. They give the evidence that while using an algebraic structure like field , the ability to trace the traitor with the IPP algorithm implies the ability to trace with the TA algorithm. In the same study they also construct schemes with an algorithm that finds all possible traitor coalitions faster than the IPP algorithm".
2003	Barg, Kabatiansky [3]	Problem Statements and Constructions of Digital Fingerprinting Codes with Efficient Traitor Identification	"The authors investigate a general fingerprinting framework for digital content, wherein coalitions of users may modify or delete portions of their individual copies to produce an unauthorized (pirated) version. Each user is assigned a unique fingerprint - modeled as a codeword from a fingerprinting code of length n and size$M$, corresponding to the total number of users.This study presents constructions of binary fingerprinting codes that are resilient against coalitions of size up to t and demonstrate that the distributor (decoder) can identify at least one member of the colluding group with error probability exponentially small in n specifically, the decoding error is bounded by exp(−Ω(n) even when the number of users satisfies M=exp(Ω(n)).”

2008	Billet and Phan [40]	Efficient Traitor Tracing Using Collusion-Resistant Fingerprinting Codes	"This paper presents a novel traitor tracing scheme that utilizes Tardos' collusion-resistant codes to produce cipher texts of constant size. The scheme also incorporates a black-box tracing algorithm capable of identifying at least one member of a colluding group of pirates, even when they are permitted to decrypt with a non-negligible (potentially high) error rate. Notably, the decoders are constructed to be as compact as possible, with their size being proportional to the length of the underlying Tardos code, thereby maintaining strong security while minimizing resource requirements".
2009	Blackburn, Etzion, and Ng [11]	*Traceability Codes*	"This paper addresses a question posed by Kabatiansky in 2005 concerning the construction and limitations of 2-traceability codes. Let l be a fixed positive integer. The authors demonstrate that,for sufficiently large prime powers q, a Reed–Solomon code can be employed to form q-ary 2-traceability code with length m containing approximately $q^{m}/_{4}$ codewords.Furthermore, they prove the near-optimality of this construction by proving that there exists a constant c, depending only on l so that any 2-traceability code over the same parameters has at most $c.q^{m}/_{4}$ codewords.This result effectively resolves Kabatiansky's open question by establishing tight asymptotic bounds on the maximum size of such codes.
2016	Shangguan [20]	*Good Traceability Codes Do Exist*	"Let F be an alphabet set of size q and n be a positive integer. A t-traceability code is a code $C \subseteq F_n$ which can be used to catch at least one colluder from a collusion of at most t traitors.It has been shown that t-traceability codes do not exist for $q \leq t$. When q >t^2, t-traceability codes with positive code rate can be constructed from error correcting codes with large minimum distance. Therefore, Barg and

			Kabatiansky asked in 2004 that whether there exist t-traceability codes with positive code rate for t+1 ≤ $q \leq \ t^2$. in short they constructed explicit traceability codes with optimal asymptotic parameters**.** They also proved the existence of efficient codes with good rates".
2017	Shang guan, Ma, and Ge[44]	*New Upper Upper Bounds for Parent-Identifying Codes and Traceability Codes*	"They Derived new upper bounds for **parent-identifying and traceability codes**. They have also improved previous known results of Blackburn, Alon and Stav. By using some complicated combinatorial counting arguments, they prove this bound for t = 3. This was the first non-trivial upper bound in the literature for traceability codes with strength three till now".
2020	Zhandry [51]	*New Techniques for Traitor Tracing: Size* $N^{\frac{1}{3}}$ *and More from Pairings*	"Existing schemes and results available in literature have $O(sqrt(N)$parameters, where N is the number of users.This result has been standard since 2006. The authors in this paper demonstrate that the $O(sqrt(N)$limitation is not inherent. They construct a scheme with $O(N^{\frac{1}{3}})$ challenging long-held assumptions about the constraints of pairing-based approaches. This work introduces new techniques for traitor tracing, achieving the first significant parameter size improvements in over a decade for pairing-based methods."
2021	Zhandry [52]	*WhiteBox Traitor Tracing*	"The authors propose new white box tracing schemes designed to ensure *consistency* (accuracy in identifying traitors) and/or *privacy* (preserving certain confidential attributes). These schemes leverage a variety of cryptographic tools, including Public Key Encryption, Non-Interactive Zero-Knowledge Proofs and Indistinguishability Obfuscation . The work emphasizes a general framework for white box tracing, potentially expanding applicability beyond specific decoder designs."
2023	Rodriguez-Lois, and Perez-Gonzalez [17]	Robust Traitor Tracing in Black-and White-Box	"In this paper, they propose a black-and-white-box watermarking method for DNN classifiers that opens the door to collusion-resistant traitor tracing in

		Neural Network Watermarking via Tardos Codes	black-box, exploiting the properties of Tardos codes, and making it possible to identify the source of the leak before access to the model is granted. While experimental results show that the method can successfully identify traitors, even when further attacks have been performed, they also discuss its limitations and open problems for traitor tracing in black-box “

4. Conclusion

This review paper has explored the development and applications of traceable codes, highlighting their significance in secure communications, supply chain management, and data integrity. The evolution of traceable codes reflects the growing demand for robust and efficient systems capable of tracking and verifying data across various domains. While significant advancements have been made in algorithmic design, error correction, and scalability, critical gaps remain in areas such as resistance to emerging security threats and integration with advanced technologies like blockchain and quantum computing. Future research should focus on addressing these challenges by exploring adaptive algorithms, enhancing interoperability, and leveraging artificial intelligence to optimize code performance.

References

[1] A Barg, R Blakley and G Kabatiansky, “Digital Fingerprinting Codes: Problem Statements, Construction, identification of Traitors” *IEEE Transactions on Information Theory*, vol. 49. no. 4, pp. 852-865 (April 03).

[2] A. Barg and G. Kabatiansky, “A class of IPP Codes with efficient identification” *J. Complexity,* vol. 20, no. 23, pp. 35-39 (April 04).

[3] A. Barg, G. Cohen, S. Encheva, G. Kabatiansky and G. Zemor “A Hypergraph Approach to the Identifying Parent Property: The Case of Multiple Parents” *SIAM Journal of Discrete Mathematics* (SIAM J. Discrete Math.), vol. 14, pp. 423-431 (2001).

[4] Anu Kathuria, S.K. Arora, and Sudhir Batra, “On traceability property of equidistant codes” *Journal of Discrete Mathematics,* vol. 340, pp. 713-721 (2017).

[5] Anu Kathuria, Sudhir Batra and S.K. Arora “A class of 2-FP Codes” *Journal of Information and Optimization Sciences*, Taylor and Francis, vol. 38, no. 8, pp.1311-1324 (December 2017) .

[6] Anu Kathuria and Sudhir Batra "On Algebraic Conditions of Equidistant Codes" *International Journal of Science and Research Archive*", vol.8(02), pg. 575-588 (April 2023).

[7] L.R. Virmani, "The Theory of Error Correcting Codes", Chapman and Hall, CRC Press

[8] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", in Advances in Cryptology – CRYPTO, 94 (Lecture Notes in Computer Science) Berlin, Germany, Springer Verlag, vol. 839, pp. 257-270 (1994).

[9] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 893-910 (May 2000)

[10] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", in Advances in Cryptology – CRYPTO, 94 (Lecture Notes in Computer Science) Berlin, Heidelberg, Springer NewYork, vol. 839, pp. 480- 491 (1994).

[11] Blackburn, Tuvi Etzion and Siaw – Ng. "Traceability Codes–*Journal of Combinatorial Theory*, https://doi.org/10.1016/j.jcta.2010.02.009

[12] D. Boneh and J. Shaw, "Collusion –Secure fingerprinting for Digital Data", *IEEE Transactions on Information Theory*, vol. 44, pp. 1897-1905 (1998).

[13] D. Boneh and J. Shaw, "Collusion –Secure fingerprinting for Digital Data", In Advances in Cryptology – CRYPTO '95, (Lecture Notes in Computer Science), vol. 963, pp. 453-465, New York (1995).

[14] D.R. Stinson, "Combinatorial Designs : Construction and Analysis", Springer –Verlag, New York Berlin, Heidelberg (2003).

[15] D.R.Stinson and R. Wei "Combinatorial Properties and Constructions of traceability schemes and frameproof codes", *SIAM Journal of Discrete Mathematics,* vol.2, pp.41-53 (1998).

[16] D.R. Stinson, Van Trung and R.Wei "Secure frameproof Codes, Key Distribution Patterns, Group Testing Algorithms and related Structures", *Journal of Statistical Planning Inference*, vol. 86(2), pp. 595-617 (2000).

[17] E.Rodriguez-Lois and Perez-Gonzalez, "Towards Traitor Tracing in Black-and-White-BoxDNN Watermarking with Tardos-based Codes, https://doi.org/10.1109/WIFS58808.2023.10374879

[18] Gerard Cohen and Encheva Sylvia "Frameproof Codes against coalition of pirates" *Theoretical Computer Science*, vol. 273, no. 2, pp.295-304 (February 2002).

[19] Gerard Cohen and Encheva Sylvia, "Some new p-array two secure frameproof codes" *Applied Mathematics Letters*, 14; pp.177-182 (2001).

[20] Ge, Shangguan, "Good Traceability Codes do exist" "https://doi.org/10.48550/arXiv.1601.04810

[21] Fang-Wei Fu, Torleiv Klove and Yuan Luo "On Equidistant Constant Weight Codes" *Discrete Applied Mathematics*, 128, pg. 157-164 (2003).

[22] H.D.L. Hollman, Jack H. Van Lint and Jean-Paul Linnartz "On codes with the identifiable Parent Property" *Journal of Combinatorial Theory, Series* A-82, pp. 121-133 (1998).

[23] Hongxia Jin and Mario Blaum, "Combinatorial Properties of Traceability Codes using Error Correcting Codes" *IEEE Transactions on Information Theory*, vol. 53, no. 2 (February 2007).

[24] J.N. Staddon, D.R. Stinson and R. Wei, "Combinatorial Properties of Frameproof and Traceable Codes" *IEEE Transactions on Information Theory*, vol.47, pp. 1042-1049 (2001).

[25] J. Lofvenberg, "Binary Fingerprinting Codes" *Designs Codes and Cryptography,* vol. 36, pp. 69-81 (July 05).

[26] J. Moreira, M. Fernandez and M.Soriano "Properties and Evaluation of Fingerprinting Codes", PHD. Thesis (2007)

[27] K.Sinha, Z. Wang and D.Wu "Good Equidistant Codes constructed from Combinatorial Designs", *Discrete Mathematics*, vol. 308, pp. 4205-4211 (2008).

[28] T. Lindkvist, "Fingerprinting of Digital Documents" Dissertation 706, Linkoping University, Sweden (2001).

[29] T. Lindkvist and J. Lofvenberg, and M. Svanstrom, "A class of traceability Codes" *IEEE Transactions on Information Theory*, vol. 48, 7, pp. 2094-2096 (2002).

[30] M. Fernandez and M. Soriano "Fingerprinting concatenated codes with efficient identification "Proc. ISC 02, Springer Publishing, Heidelberg, New York, pp. 459-470 (2002)

[31] M. Fernandez and M. Soriano, "Algorithm to decode Identifiable Parent Property Codes "Electronic Letters, 6th June, vol. 38, no. 12 (2002)

[32] M. Fernandez and M. Soriano," On the IPP property of Reed Solomon Codes "in Emerging Challenges for Security, Privacy and Trust, *Advances in Information and Communication Technology* vol. 297, Springer Boston, pp.87-97 2009.

[33] M. Fernandez and M. Soriano "A new class of IPP Codes for Fingerprinting Schemes "Springer –Verlag Berlin Heidelberg, pp. 398-409 (2005).

[34] M. Fernandez and Josep Cotrina "Equidistant Binary Fingerprinting Codes : Existence and Identification Algorithms", Proc. Springer – Verlag, Berlin Heidelberg, pp. 527-536 (2005).

[35] M. Fernandez and Josep Cotrina "A note about the Traceability of Linear Codes", Springer – Verlag Berlin, Heidelberg, pp. 308-409 (2005).

[36] F. J. Mac Williams and N. J. A. Sloane, "The Theory of Error Correcting Codes" Bell Laboratories, Murray Hills, NJO 7974, USA (1978).

[37] Marco Dalai and Stefano Della Fiore "Bounds and Algorithms for Frameproof Codes And related Combinatorial Structures" *IEEE Transactions on Information Theory*, 713-721 (2023)

[38] Miao Liu and Ching Shangguan "Near Optimal Constructions of frameproof codes" *IEEE International Symposium on Information Theory (*2024), https://doi.org/10.1109/ISIT57864.2024.10619230.

[39] N.Wagner, "Fingerprinting Techniques "in Proceedings 1983, *IEEE Symposium on Security and Privacy*, pp.18-22 (April 1983).

[40] Olivier Billet and Duong Phan "Efficient Traitor Tracing from Collusion Secure Codes, Springer Nature, Information Theoretic Securitry (2008)".

[41] R. Safavi –Naini and Yeing Want "New Results on Frameproof Codes and Traceability Schemes" Proc. Wollongong, pp. 3029-3033 (2001).

[42] R.S.Veerubhotla, V.P.Gualti and A. K.Pujari "Gossip Codes for Fingerprinting :Construction, Erasure and Pirate Tracing" *Journal of Universal Computer Science*, vol. 11, no. 1 pp.122-149 (2005)

[43] R. Safavi-Naini and Y. Wang, "Collusion Secure q-ary Fingerprinting for perceptual content "Proceedings SPDRM 01, Springer Publishing, Heidelberg/NewYork, pp. 57-75 (2002).

[44] Chong Shangguan, Jingxue Ma and Gennian Ge "New Upper Upper Bounds for Parent-Identifying Codes and Traceability Codes" Des. Codes Cryptogr. DOI 10.1007/s10623-017-0420-y

[45] Simon R. Blackburn, "Frameproof Codes" *SIAM Journal of Discrete Mathematics*" vol. 16, no. 3, pp. 499-510.

[46] Simon R. Blackburn and Tuvi Etzion "Prolific Codes with the Identifiable Parent Property Codes" *SIAM Journal of Discrete Mathematics* (2007).

[47] Sudhir Batra "A new class of 2-IPP Codes" *Journal of Informatics and Mathematical Sciences,* vol. 5 no. 2, pp.65-76 (2013).

[48] T. Van, Trung and S. Maritosyan, "On a class of Traceability Codes" *Design, Codes and Cryptography,* vol. 31, no. 2, pp.125-132 (2004).

[49] Xiande Zhang and Yeow Mang Chee, "Improved constructions of frameproof codes" https://doi.org/10.48550/arXiv.1206.5863

[50] Alok Tripathi, Rajiv Pandey and Amarjeet Singh "Boneh-Shaw fingerprint code and Tardos code analysis and optimization in minority collusion attack." https://doi.org/10.1016/j.measen.2024.101173

[51] Zhandry, "New Techniques for Traitor Tracing: Size $N^{(1/3)}$ and More from Pairings (2020) "https://ia.cr/2020/954

[52] Zhandry, "WhiteBox Traitor Tracing" (2021) https://eprint.iacr.org/2021/891.

[53] Simon Blackburn,"An upper bound on the size of a code with the k-identifiable parent property"; https://ia.cr/2002/101

[54] Silverberg, Staddon and Walker," Efficient Traitor Tracing Algorithms using List Decoding". https://ia.cr/2001/016

[55] Anu Kathuria, "Traceable Codes Constructed from Certain Combinatorial Designs", *Journal of Discrete Mathematics and Cryptography,* vol. 27, issue 8, pp.2473-2482 (2024).

[56] Anu Kathuria, "Optimizing Traceable Codes Through Latin Squares and Projective Planes" *Journal of Discrete Mathematics and Cryptography,* https ://doi/10.4974/JDMSC-2301

Received July, 2025