REPORTS
IN
INFORMATICS

ISSN 0333-3590

Fighting Three Pirates with Scattering Codes

Hans Georg Schaathun

REPORT NO 263 January 2004

Department of Informatics
UNIVERSITY OF BERGEN
Bergen, Norway

This report has URL `http://www.ii.uib.no/publikasjoner/texrap/ps/2004-263.ps`

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at `http://www.ii.uib.no/publikasjoner/texrap/`.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Fighting Three Pirates with Scattering Codes

Hans Georg Schaathun

20th January 2004

Abstract

With a digital fingerprinting scheme a vendor of digital copies of copyrighted material marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates, due to this fingerprint.

A coallition of pirates may be able to produce copies with a false, hybrid fingerprint, but if the fingerprints are taken from a collusion-secure code, then at least one pirate can be traced with probablitity at least $1 - \epsilon$.

Scattering codes were recently introduced by Sebé and Domingo-Ferrer, and used to contstruct a family of codes allegedly collusion-secure against three pirates. In this paper we prove that their codes are insecure against optimal pirate strategies, and we show how to build secure schemes using scattering codes. The new constructions have extremely good rates for reasonable numbers of users.

Keywords

digital fingerprinting, separating code, collusion-secure code, intersecting code

1. Introduction

1.1. Background

The problem of digital fingerprinting was introduced in [16], and have received quite some attention following [2, 3]. A vendor selling digital copies of copyrighted material wants to prevent illegal copying. Digital fingerprinting is supposed to make it possible to trace the guilty user (pirate) when an illegal copy is found. This is done by embedding a secret identification mark, called a fingerprint, in each copy, making every copy unique.

The fingerprint must be embedded in such a way that it does not disturb the information in the data file. It must also be impossible for the user to remove or damage the fingerprint, without damaging the information contents beyond any practical use. In particular, the fingerprint must survive any change of file format (e.g. gif to tiff) and any reasonable compression including lossy compression. This embedding problem is essentially the same as the problem of watermarking.

If a single pirate distributes unauthorised copies, they will carry his fingerprint. If the vendor discovers the illegal copies he can trace them back to the pirate and prosecute him. If several pirates collude, they can to some extent tamper with the fingerprint. When they compare their copies they see some bits (or symbols) which differ and thus must be part of the fingerprint. Identified bits may be changed, and thus the pirates create a hybrid copy with a false fingerprint. A collusion-secure code is a set of fingerprints which enables the vendor to trace pirates even when they collude, given that there are no more than t pirates for some threshold t.

Collusion-secure coding is also employed in traitor tracing [4, 5]. Whereas fingerprinting protects the digital data in themselves, traitor tracing protects broadcast encryption keys. The fingerprinting literature is most often interested in probabilistically collusion-secure coding, where the vendor shall be able to trace a pirate with probability at least $1-\epsilon$ for some small error rate ϵ. In the traitor tracing literature, combinatorially collusion-secure codes is the norm, where the tracing is required to succeed with probaility 1. Still, in principle, there is no reason not to use combinatorial codes for fingerprinting and probabilistic ones for traitor tracing. Other important variants of the problems are dynamic traitor tracing (e.g. [11]) and anonymous fingerprinting [10].

1.2. The fingerprinting problem

We use notation and terminology from coding theory. The set of fingerprints is an $(n, M)_q$ code, which provides for up to M buyers, uses an alphabet of q symbols, and requires n such symbols embedded in the digital file. The Hamming distance between two words $\mathbf{x}$ and $\mathbf{y}$ is denoted $d(\mathbf{x}, \mathbf{y})$.

To understand the fingerprinting problem, we must know what the pirates are allowed to do. This is defined by the Marking Assumption.

Definition 1 (The Marking Assumption)
Let $P \subseteq C$ be the set of fingerprints held by a coallition of pirates. The pirates can produce a copy with a false fingerprint $\mathbf{x}$ for any $\mathbf{x} \in F_C(P)$, where

$$F_C(P) = \{(c_1, \ldots, c_n) : \forall i, \exists (x_1, \ldots, x_n) \in P, x_i = c_i\}.$$

We call $F_C(P)$ the feasible set of P with respect to C.

The Marking Assumption defines the requirements from the embedding of the fingerprint in the digital data. Constructing appropriate embeddings is non-trivial, though it is not theoretically impossible [3]. Alternative assumptions have been proposed, and some overview of this can be found in [1]. Definition 1 defines the socalled narrow-case fingerprinting problem [1], which is the only one we will consider.

A *tracing algorithm* for the code C is any algorithm A which takes a vector $\mathbf{x}$ as input and outputs a set $L \subseteq C$. If $\mathbf{x} \in F_C(P)$ for some pirate coallition P, then A is successful if L is a non-empty subset of P. A code is said to be said to be combinatorially t-secure if it has a tracing algorithm which succeeds with probability 1 when there are at most t pirates. It is said to be t-secure with ϵ-error if A succeeds with probability at least $1 - \epsilon$ when there are at most t pirates.

In most fingerprinting schemes, and in particular in the schemes we consider, the columns are randomly permuted, and the pirates have no information about their ordering. Also the alphabet is randomly permuted for each position. This heavily randomises the false fingerprint, as the pirates cannot make different decisions on a column by column basis.

A group of three pirates can see three different column types, for each user i there is a column Type i where that user is the minority. Thus the pirates can choose a strategy for each of the three column types. We describe a pirate pure strategy as (p_1, p_2, p_3), where p_i is the probability that the pirates choose the majority bit when user i is the minority.

These are not the most general pirate strategies. They could opt to take the majority bit in a certain fraction f_i of the columns of Type i, thus making various bits stochastically dependent. However, if we have sufficiently many columns of each type, then the difference between these two strategies is insignificant.

It is well known that any code with $\delta > 1 - t^{-2}$ is a socalled t-traceability code, which is combinatorially t-secure using closest neighbour decoding. Unfortunately, this large minimum distance is only possible when the alphabet is large. A binary code cannot be combinatorially collusion-secure.

General schemes can be found in [2, 3], with improvements in [12], in [1], and in [9].

Simplex codes were proved to be 2-secure with ϵ-error in [8]. Small simplex codes are very good, and closest neighbour decoding can be used. However, the asymptotic rate of these codes is zero. A similar idea was employed in [13], where an asymptotically good family of $(2, 2)$-separating codes was proven to be 2-secure with ϵ-error, where ϵ tends to zero with increasing code size.

1.3. Report outline

This report features two new results. There is the insecurity of the original scattering code scheme in Chapter 3, and the new construction in Chapter 5. The remaining chapters contain preliminary results which have been published before. Since this is a technical report, we have permitted ourself a more verbose form than what is customary for journal papers.

Chapter 2 presents the scattering codes with the error analysis. The presentation is slightly simplified compared to [15], but nothing is really new. Chapter 4 defines intersecting and separating codes and presents a way to construct them. These results have been assembled from various articles.

2. Scattering codes (SC)

The scattering code $SC(r,t)$ is a probabilistic encoding of a single bit. Each bit value is encoded as one out of t possible words, chosen uniformly at random. The code has $2t+1$ distinct columns replicated r times. We divide the columns in three zones. Zone A has r identical columns where a word has one if and only if it encodes one. Zone B has t distinct columns of weight one replicated r times, and all words encoding zero are zero. Zone C is similar, with t distinct columns of weight 1, and words encoding one are zero.

The scattering codes were designed [15] in order to fight three pirates. It is used as an inner code for concatenation to reveal the most frequent bit value among the pirates, regardless of the pirate strategy. E.g. if the pirates see two ones and a zero, then inner decoding outputs one with probability $1-\epsilon$. The following decoding algorithm is simplified from [15], but does give the same output.

Algorithm 1 (Descattering)
*The decoding algorithm for scattering codes (*descattering*) uses the first applicable rule in the following list. One block is one set of r identical columns.*

1. *If there are at least two blocks of Zone B with at least one one-bit, then decode as 1.*
2. *If there are at least two blocks of Zone C with at least one one-bit, then decode as 0.*
3. *If there are more ones than zeroes in Zone A, then decode as 1.*
4. *If there are more zeroes than ones in Zone A, then decode as 0.*
5. *With the same number of zeroes and ones in Zone A, decode as unreadable.*

Encodes	Zone A	Zone B	Zone C
	1111	1111 0000 0000	0000 0000 0000
1	1111	0000 1111 0000	0000 0000 0000
	1111	0000 0000 1111	0000 0000 0000
	0000	0000 0000 0000	1111 0000 0000
0	0000	0000 0000 0000	0000 1111 0000
	0000	0000 0000 0000	0000 0000 1111

Table 2.1.: The scattering code $SC(4,3)$.

A r bits	B_1 r bits	B_2 r bits	X_1 $(t-2)r$ bits	C r bits	X_2 $(t-1)r$ bits
$1\dots1$	$1\dots1$	$0\dots0$	$0\dots0$	$0\dots0$	$0\dots0$
$1\dots1$	$0\dots0$	$1\dots1$	$0\dots0$	$0\dots0$	$0\dots0$
$0\dots0$	$0\dots0$	$0\dots0$	$0\dots0$	$1\dots1$	$0\dots0$

Table 2.2.: Three pirate codewords.

Clearly, if P is three words encoding the same bit value, then Zone A and either Zone B or Zone C are not detectable, and consequently any $\mathbf{x} \in F(P)$ is always decoded correctly.

We are going to determine the probability of correct decoding of $\mathbf{x} \in F(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ where the pirate words $\mathbf{b}_i$ encode two distinct bits. Due to the symmetries in the scattering code, we can assume without loss of generality, that $\mathbf{b}_1$ and $\mathbf{b}_2$ encode 1 while $\mathbf{b}_3$ encodes 0.

Theorem 1
The probability of correctly decoding one bit produced by three scattering codewords encoding two different bits is

$$r(p) = 1 - \frac{1+(t-1)(2p^r - p^{2r})}{t} \sum_{i=0}^{\lfloor r/2 \rfloor} \binom{r}{i} p^i (1-p)^{r-i},$$

when the pirates pick the majority bit with probability p in each column type.

This is only a special case of the following lemma which we prove specifically.

Lemma 1
Suppose the pirates pick the majority bit with probability p_i whereever user i is the minority. Then the probability of decoding to the majority bit in a block where user i has the minority bit is

$$r_i = 1 - \frac{1+(t-1)(\sum_{j\neq i} p_j^r - \prod_{j\neq i} p^r)}{t} \sum_{j=0}^{\lfloor r/2 \rfloor} \binom{r}{j} p_i^j (1-p_i)^{r-j}.$$

Proof: We consider first the case where $\mathbf{b}_1 \neq \mathbf{b}_2$. Suppose the pirate codewords are as depicted in Table 2.2. There are four blocks concerning us, A, B_1, B_2, and C. Let $x1$ denote the event that there are only ones in Block x, and $x0$ the event that there are only zeroes. Let A^+ denote the event that there are more ones than zeroes in Block A. Likewise we have Event A^- if there are more zeroes than ones in Block A. Obviously, two events are correlated if and only if they concern the same block.

Let R_i denote the event that decoding rule no. i applies, and let M denote the event of decoding error. We have that

$$
\begin{aligned}
R_1 &= \neg B_1 0 \wedge \neg B_2 0, \\
R_2 &= \emptyset, \\
R_3 &= A^+ \wedge (B_1 0 \vee B_2 0), \\
R_4 &= A^- \wedge (B_1 0 \vee B_2 0), \\
R_5 &= \neg A^+ \wedge \neg A^- \wedge (B_1 0 \vee B_2 0).
\end{aligned}
$$

If correct decoding is 1, we get the event of not decoding to 1 to be

$$M = R_4 \vee R_5 = (\neg A^+) \wedge (B_1 0 \vee B_2 0).$$

We have the following basic probabilities,

$$
\begin{aligned}
P(B_i 0) &= p_i^r, \quad i = 1, 2, \\
P(\neg A^+) &= b_C\left(\lfloor r/2 \rfloor ; r, 1 - p_3\right).
\end{aligned}
$$

Due to symmetry, the probability of erroneous decoding is independent of which bit is correct, and we get

$$P(M) = b_C\left(\lfloor r/2 \rfloor ; r, p_3\right)(p_1^r + p_2^r - p_1^r p_2^r),$$

If $\mathbf{b}_1 = \mathbf{b}_2$, we have only three detectable blocks. There is only one detectable block, say B_1, in Zone B, where both $\mathbf{b}_1$ and $\mathbf{b}_2$ are one. This implies that $B_2 0$ is always true, and consequently $R_4 \vee R_5 = \neg A^+$.

For each bit, one of the t codewords is chosen uniformly at random. Hence $P(\mathbf{b}_1 = \mathbf{b}_2) = 1/t$, and we get the following total probability.

$$P(M) = b_C\left(\lfloor r/2 \rfloor ; r, p_3\right) \frac{(t-1)(p_1^r + p_2^r - p_1^r p_2^r) + 1}{t},$$

which is equivalent to the formula in the theorem. Note that $P(M)$ increases in p_1 and p_2, whereas it decreases in p_3. □

Define $p^*(r,t) := \min_p r(p)$, which is the worst-case probabilty of successful descattering as majoroity choice. In Table 2.3, we calculate this number for some choices of r and t.

Problem 2.1 *In [15], the worst case success probability is given as* 0.68 *for* $SC(3,4)$. *Is this a misprint?*

r	t	length	p
1	2	5	0.4557
1	3	7	0.5286
1	4	9	0.5556
1	7	15	0.5843
3	3	21	0.6667
3	4	27	0.75
3	5	33	0.8
5	10	105	0.9
31	100	6231	0.99

Table 2.3.: Worst case probability p of correct majority decoding for scattering codes SC(r,t) for certain parameters.

3. Concatenated fingerprinting codes

Concatenation is a standard technique from coding, and it has proven extremely useful in fingerprinting.

Definition 2 (Concatenation)
Let C_1 be a $(n_1, Q)_q$ and let C_2 be an $(n_2, M)_Q$ code. Then the concatenated code $C_1 \circ C_2$ is the $(n_1 n_2, M)_q$ code obtained by taking the words of C_2 and mapping every symbol on a word from C_1.

Each set of n_1 symbols corresponding to one word of the inner code will be called a block.

Sebé and Domingo-Ferrer suggested a scheme with scattering inner codes and simplex codes as outer codes. The tracing algorithm first descatters each inner code block to obtain a vector **x**, and then decodes the outer code using closest neighbour to return the codeword $\mathbf{b} \in C$ minimising $d(\mathbf{b}, \mathbf{x})$.

The pirates choose a strategy $\mathbf{p} = (p_1, p_2, p_3)$ with respect to the concatenated code. After descattering there is a probability r_i of majority choice in column of the outer code of Type i. Thus we effectively get a pirate strategy (r_1, r_2, r_3) with respect to the outer code, given by Lemma 1.

Theorem 2
A fingerprinting scheme with scattering inner codes and simplex codes with any decoding algorithm for the outer code has error rate at least $1/4$ if the pirates use an optimal strategy.

Proof: We propose that the pirates choose a pure strategy (p_1, p_2, p_3) uniformly at random from $(1,1,1)$, $(1,0,0)$, $(0,1,0)$, and $(0,0,1)$. Observe that for these four strategies we get $(r_1, r_2, r_3) = (p_1, p_2, p_3)$. Consider four codewords $\mathbf{a}_1, \ldots, \mathbf{a}_4$ where $\mathbf{a}_4 = \mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3$. Any coallition of three out of these four codewords will produce the same four false fingerprints with our proposed strategy. Hence when one of these false fingerprints is detected, there are four users which are equally likely to be guilty, and one of them is innocent. ☐

By the same proof, we also get the following more general corollary.

Corollary 1
Any binary, linear code which is 3-secure with ϵ-error has $\epsilon \geq 1/4$.

4. Intersection and separation

4.1. Intersecting Codes

We say that a binary code C is t-wise intersecting if any t linearly independent codewords have at least one position where they are all 1. The number of such positions is the intersection weight of the t-tuple, and the intersection weights $(\varrho_3, \bar{\varrho}_3)$ of C are the lower and upper bounds of intersections weights of any such t-tuple from the code.

Lemma 2
Let C be a binary code. Consider t linearly independent codewords. The number N of positions where these words intersect is bounded as

$$d_1 - m_1(1 - 2^{1-t}) \leq N \leq m_1 - d_1(1 - 2^{1-t}).$$

Proof: Let $P = \{\mathbf{x}_1, \ldots, \mathbf{x}_t\}$ be t linearly independent codewords. The following formula holds [6],

$$2^{t-1} \left| \bigcap_{\mathbf{x} \in P} \chi(\mathbf{x}) \right| = \sum_{S \subseteq P} (-1)^{|S|} w\Big(\sum_{\mathbf{x} \in S} \mathbf{x} \Big). \tag{4.1}$$

Each term on the right hand side is the weight of a codeword. There are 2^{t-1} weights with positive sign, and $2^{t-1} - 1$ with negative sign. Since each weight is bounded by d_1 and m_1, the lemma follows. □

The duals of BCH codes often have high intersection weights [14, 6]. Particularly for the simplex codes, and for the duals of BCH(2) and BCH(3), the exact values of m_1 and d_1 are known. The $[2^k - 1, k]$ simplex code has $\varrho_i = 2^{k-i}$ when $0 < i \leq k$. For the duals of BCH(2) we have

$$\varrho_2 = 2^{m-2} - 3 \cdot 2^{\lfloor m/2 \rfloor - 1}, \quad \bar{\varrho}_2 = 2^{m-2} + 3 \cdot 2^{\lfloor m/2 \rfloor - 1},$$
$$\varrho_3 = 2^{m-3} - 7 \cdot 2^{\lfloor m/2 \rfloor - 2}, \quad \bar{\varrho}_3 = 2^{m-3} + 7 \cdot 2^{\lfloor m/2 \rfloor - 2},$$

and for duals of BCH(3) we get

$$\varrho_2 = 2^{m-2} - 3 \cdot 2^{\lceil m/2 \rceil - 1}, \quad \bar{\varrho}_2 = 2^{m-2} + 3 \cdot 2^{\lceil m/2 \rceil - 1},$$
$$\varrho_3 = 2^{m-3} - 7 \cdot 2^{\lceil m/2 \rceil - 2}, \quad \bar{\varrho}_3 = 2^{m-3} + 7 \cdot 2^{\lceil m/2 \rceil - 2}.$$

In Table 4.1, we present some BCH-duals which we will use in the sequel. Due to the floor and ceiling expressions in the weight formulæ, BCH(2) works best for

e	m	$[n,k]$	(d_1,m_1)	$(\ell_2,\bar{\ell}_2)$	$(\ell_3,\bar{\ell}_3)$
2	7	$[127,14]$	$(56,72)$	$(20,44)$	$(2,30)$
2	9	$[511,18]$	$(240,272)$	$(104,152)$	$(36,92)$
2	11	$[2047,22]$	$(992,1056)$	$(464,560)$	$(200,312)$
2	13	$[2^{13}-1,26]$	$(4032,4160)$	$(1952,2144)$	$(912,1136)$
2	15	$[2^{15}-1,30]$	$(16256,16512)$	$(8000,8384)$	$(3872,4320)$
3	8	$[256,24]$	$(112,144)$	$(40,88)$	$(4,60)$
3	10	$[1023,30]$	$(480,544)$	$(208,304)$	$(72,184)$
3	12	$[4095,36]$	$(1984,2112)$	$(928,1120)$	$(400,624)$
3	14	$[2^{13}-1,42]$	$(8064,8320)$	$(3904,4288)$	$(1824,2272)$

Table 4.1.: Some instances of $\mathrm{BCH}^{\perp}(e)$.

even m and BCH(3) best for odd m. The minimum values of m required for a t-wise intersecting code can be found in [14]. We need ℓ_3 relatively large, so we need m somewhat larger than the minimum values.

4.2. Separating Codes

Let $T,U \subseteq C$ be two disjoint sets of codewords. We say that $T = \{\mathbf{a}_1,\dots,\mathbf{a}_t\}$ and $U = \{\mathbf{b}_1,\dots,\mathbf{b}_u\}$ are separated on a position i if any word of T is different from any word of U on this position. The number of such positions is the separating weight and denoted $\theta(\mathbf{a}_1,\dots,\mathbf{a}_t;\mathbf{b}_1,\dots,\mathbf{b}_u)$. We say that C is (t,u)-separating if $\theta(\mathbf{a}_1,\dots,\mathbf{a}_t;\mathbf{b}_1,\dots,\mathbf{b}_u) > 0$ for any $t+u$ distinct codewords $\mathbf{a}_i$ and $\mathbf{b}_j$. Separating codes can be constructed from intersecting codes [7]. The following lemmata give the special cases needed in this paper.

Lemma 3
Let C be a code with 3-wise intersection weight $(\ell_3,\bar{\ell}_3)$, and consider four distinct codewords $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$, and $\mathbf{c}$. We have

$$\begin{aligned} \theta(\mathbf{c};\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3) &= 0, \quad \text{if } \mathbf{c} = \mathbf{a}_1+\mathbf{a}_2+\mathbf{a}_3, \\ \ell_3 \le \theta(\mathbf{c};\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3) &\le \bar{\ell}_3, \quad \text{otherwise}. \end{aligned}$$

Proof: If $\mathbf{c} = \mathbf{a}_1+\mathbf{a}_2+\mathbf{a}_3$, then, in every bit position where all the $\mathbf{a}_i$ are equal, $\mathbf{c}$ will have the same value and thus it cannot be separated from the $\mathbf{a}_i$.

If $\mathbf{c}$ is not the sum of the $\mathbf{a}_i$, then $\mathbf{c}+\mathbf{a}_i$ are three linearly independent words for $i = 1,2,3$. Hence

$$\theta(\mathbf{c};\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3) = \theta(\mathbf{0};\mathbf{a}_1+\mathbf{c},\mathbf{a}_2+\mathbf{c},\mathbf{a}_3+\mathbf{c}),$$

which is bounded by the intersection weights. □

Lemma 4
Let C be a code with 3-wise intersection weight $(\varrho_3, \bar{\varrho}_3)$, and consider four distinct codewords $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$. We have

$$\begin{aligned} \theta_{2,1} \le \theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{b}_1, \mathbf{b}_2) \le \bar{\theta}_{2,1}, &\quad \textit{if } \mathbf{a}_1 + \mathbf{a}_2 = \mathbf{b}_1 + \mathbf{b}_2, \\ \varrho_3 \le \theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{b}_1, \mathbf{b}_2) \le \bar{\varrho}_3, &\quad \textit{otherwise}. \end{aligned}$$

Proof: Consider first the case when the four words sum to zero. Viewing the words as rows of a matrix, all the columns have even weight. Hence $\mathbf{b}_1$ is separated from $\{\mathbf{a}_1, \mathbf{a}_2\}$ if and only if $\mathbf{b}_2$ is. Consequently

$$\theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{b}_1, \mathbf{b}_2) = \theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{b}_1),$$

which is bounded as given.

If the four words have non-zero sum, then $\mathbf{a}'_1 = \mathbf{a}_1 - \mathbf{b}_2$, $\mathbf{a}'_2 = \mathbf{a}_2 - \mathbf{b}_2$, and $\mathbf{b} = \mathbf{b}_1 - \mathbf{b}_2$ are linearly independent, and the separating weight to be bounded is

$$\theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{b}_1, \mathbf{b}_2) = \theta(\mathbf{a}'_1, \mathbf{a}'_2; \mathbf{b}, \mathbf{0}), \tag{4.2}$$

which is equal to the number of positions where $\mathbf{a}'_1$, $\mathbf{a}'_2$, and $\mathbf{b} - \mathbf{a}'_1$ intersect. Since these three words are also linearly independent, we get the bounds. ☐

Lemma 5
Given an $[n, 2k]$ code, there is a non-linear $(n, 2^k)$ subcode where any four non-zero codewords are linearly independent.

Proof: Let C' be the $[2^k - 1, 2^k - 1 - 2r, 5]$ BCH code. The columns of the parity check matrix of C' make a set Γ' of $2^k - 1$ vectors from $\mathsf{GF}(2)^{2k}$, such that no four of them are linearly independent. Now there is an isomorphism $\phi : \mathsf{GF}(2)^{2k} \to C$, so let $\Gamma = \phi(\Gamma') \cup \{\mathbf{0}\}$. ☐

From the lemmata, we can deduce the following proposition.

Proposition 1
If there is an $[n, 2k]$ code C with 3-wise intersection weights $(\varrho_3, \bar{\varrho}_3)$, then there is a non-linear $(n, 2^k)$ code $\Gamma \subseteq C$ with minimum and maximum $(2, 2)$- and $(3, 1)$-separating weights in the interval $[\varrho_3, \bar{\varrho}_3]$.

5. Separating codes against three pirates

We propose a new scheme of concatenated fingerprinting codes, where the inner code is $\mathrm{SC}(r, t)$. Tracing consists of descattering and closest neighbour decoding just like in the scheme by Sebé and Domingo-Ferrer.

The outer code C_O must be both $(2, 2)$- and $(3, 1)$-separating, with relatively large separating weights. Let ℓ_3 and $\bar{\ell}_3$ be integers such that for any four codewords $\mathbf{a}_1, \ldots, \mathbf{a}_4 \in C_O$, we have

$$\begin{aligned} \ell_3 &\leq \theta(\mathbf{a}_1; \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4) \leq \bar{\ell}_3, \\ \ell_3 &\leq \theta(\mathbf{a}_1, \mathbf{a}_2; \mathbf{a}_3, \mathbf{a}_4) \leq \bar{\ell}_3. \end{aligned}$$

If C_O is constructed as a non-linear subcode of a 3-wise intersecting code, then $(\ell_3, \bar{\ell}_3)$ are the intersection weights.

Consider an arbitrary pirate coallition $P = \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\} \subseteq C_O$. The pirates use a strategy (p_1, p_2, p_3) with respect to the concatenated codes. Due to the scattering inner code, this corresponds to a strategy (r_1, r_2, r_3) with respect to C_O. We name the pirates such that $p_3 \leq p_2 \leq p_1$, that is such that $\mathbf{a}_3$ is statistically closest to $\mathbf{x}$.

Let $\mathbf{c} \in C \backslash P$ be some innocent user, and let B be a matrix with rows $\mathbf{a}_3$, $\mathbf{a}_2$, $\mathbf{a}_1$, and $\mathbf{c}$, in this order. We write $\pi(\mathbf{c})$ for the probability that $\mathbf{c}$ is returned by the tracing algorithm. The error probability for the fingerprinting scheme will be bounded as

$$\epsilon \leq \sum_{\mathbf{c} \notin P} \pi(\mathbf{c}) \leq M \cdot \alpha,$$

where α is any upper bound on $\pi(\mathbf{c})$.

Define $D = d(\mathbf{x}, \mathbf{a}_3) - d(\mathbf{x}, \mathbf{c})$. Clearly we get that $\pi(\mathbf{c}) \leq P(D \geq 0)$. The matrix B has essentially eight types of columns. In Table 5.1 we present the column types, and their contribution to the two distances and the difference D per column.

Let N_1, N_2, and N_3 be the number of columns of Types 2B, 3B, and 4A respectively. Observe that $\ell_3 \leq N_i \leq \bar{\ell}_3$. The columns of Types 1A, 2A, 3A, and 4B make no contribution to D. Type 1B gives a fixed contribution of at most $-\ell_3$. The contributions from each of the types 2B, 3B, and 4A are as follows:

$$\begin{aligned} &N_1 - 2Y_1, \quad \text{where } Y_1 \sim \mathcal{B}(N_1; p_1), \\ &N_2 - 2Y_2, \quad \text{where } Y_2 \sim \mathcal{B}(N_2; p_2), \\ &N_3 - 2Y_3, \quad \text{where } Y_3 \sim \mathcal{B}(N_3; 1 - p_3), \end{aligned}$$

Column type	Majority choice			Minority choice		
	$d(\mathbf{x},\mathbf{a}_3)$	$d(\mathbf{c},\mathbf{x})$	D	$d(\mathbf{x},\mathbf{a}_3)$	$d(\mathbf{c},\mathbf{x})$	D
1A: (1111), (0000)	0	0	0	0	0	0
1B: (1110), (0001)	0	1	−1	0	1	−1
2A: (1101), (0010)	0	0	0	1	1	0
2B: (1100), (0011)	0	0	0	1	1	0
3A: (1011), (0100)	1	0	1	0	1	−1
3B: (1010), (0101)	0	1	−1	1	0	1
4A: (0111), (1000)	0	1	−1	1	0	1
4B: (0110), (1001)	0	0	0	1	1	0

Table 5.1.: Distance contributions from a single column.

where $\mathcal{B}(n;p)$ denotes the binomial distribution with n trials and probability p. Write

$$Y = Y_1 + Y_2 + Y_3,$$
$$N = N_1 + N_2 + N_3.$$

Hence $D \leq N - 2Y - \ell_3$, and it follows that

$$\pi(\mathbf{c}) \leq \max_{p_1,p_2,p_3} P(Y \leq (N - \ell_3)/2).$$

Lemma 6
If the pirates choose a strategy (p_1, p_2, p_3) where $p_1 \geq p_2 \geq p_3$ minimising $P(Y \leq (N - \ell_3)/2)$, then $p_2 = p_3$ (and consequently $r_2 = r_3$).

Proof: The higher r_3 is, the more often columns of Type 4A make a positive contribution, and the lower r_2 and r_1 are, the more often columns of Types 2B and 3B make a positive contribution. Therefore the pirates will seek to maximise r_3 and minimise r_2 and r_1. We know that r_3 is growing in p_3, whereas r_2 and r_1 decrease in p_3. Hence the pirates will maximise p_3, and since we have assumed that $p_3 \leq p_2$, this implies $p_3 = p_2$. □

Define

$$m = E(Y) = r_1 N_1 + r_2 N_2 + (1 - r_3) N_3,$$

and

$$\varepsilon = 1 - \frac{N - \ell_3}{2m}.$$

Lemma 7
For any optimal pirate strategy (p_1, p_2, p_3), if $\bar{\ell}_3 \leq 2\ell_3$ and $p^*(r,t) \geq 1/2$, we get $0 \leq \varepsilon \leq 1$.

Proof: That $\varepsilon \le 1$ follows from $N \ge \ell_3$. Recall that $p_2 = p_3$, and thus $r_2 = r_3$ for any optimal pirate strategy by Lemma 6. That $\varepsilon \ge 0$, is equivalent to

$$L := N_1(1/2 - r_1) + N_2(1/2 - r_2) + N_3(r_2 - 1/2) - \ell_3/2 \le 0.$$

We prove that this holds when L is maximised. We have

$$\begin{aligned} L &\le N_1(1/2 - r_1) + (1/2 - r_2)(N_3 - N_2) - \ell_3/2 \\ &\le N_1(1/2 - r_1) + |1/2 - r_2| \cdot \ell_3 - \ell_3/2 \le N_1(1/2 - r_1). \end{aligned}$$

If $r_1 \ge 1/2$, then this is clearly negative. Now observe that r_1 is decreasing in p_2 and p_3, and increasing in p_1, and since $p_3 \le p_2 \le p_1$, r_1 is minimised when $p_1 = p_2 = p_3$. It follows that $r_1 \ge p^*(r, t) \ge 1/2$. □

For the error bound, we will use the following well-known theorem.

Theorem 3 (Chernoff)
Let $X_1, \ldots, X_t$ be independent stochastic variables taking the values 0 and 1, and let X be their sum. Write $m = E(X)$. Then for any $0 < \epsilon < 1$, we have

$$P\left(\sum_{i=1}^{t} X_i \le (1-\epsilon)m\right) \le e^{-\epsilon^2 m/2}.$$

Lemma 8
The probability of accusing an innocent user **c** *is bounded as*

$$\pi(\mathbf{c}) \le A := e^{-E}, \text{ where } E = \frac{1}{2}\left(1 - \frac{N - \ell_3}{2m}\right)^2 m.$$

Proof: We have $\pi(\mathbf{c}) \le P(Y \le (1-\varepsilon)m)$, where $0 \le \varepsilon \le 1$ by Lemma 7. Thus the lemma follows from Theorem 3. □

The worst case is when A is maximised, which happens when E is minimised.

Lemma 9
If E is minimised, r is odd, and $\ell_3 \le N_i \le 2\ell_3$ for $i = 1, 2, 3$, then we can assume either $p_1 = 1$ or $p_1 = p_2$.

Proof: By differentiation, we have for $j = 1, 2$ that

$$\begin{aligned} \frac{\partial E}{\partial r_j} &= \left(1 - \frac{N - \ell_3}{2m}\right) \cdot m \cdot \frac{\partial}{\partial r_j}\left(1 - \frac{N - \ell_3}{2m}\right) + \frac{1}{2}\left(1 - \frac{N - \ell_3}{2m}\right)^2 \frac{\partial m}{\partial r_j} \\ &= \left[\left(1 - \frac{N - \ell_3}{2m}\right) \cdot m \cdot \frac{N - \ell_3}{2m^2} + \frac{1}{2}\left(1 - \frac{N - \ell_3}{2m}\right)^2\right] \frac{\partial m}{\partial r_j}. \\ &= \frac{1}{2} \cdot \left(1 - \frac{N - \ell_3}{2m}\right) \cdot \left(1 + \frac{N - \ell_3}{2m}\right) \cdot N_j \\ &= C_0 \cdot N_j, \end{aligned}$$

where

$$C_0 = \frac{1}{2}\left(1 - \left(\frac{N - \ell_3}{2m}\right)^2\right),$$

is independent of j. Similarly, we have

$$\frac{\partial E}{\partial r_3} = -C_0 \cdot N_3.$$

By Lemma 7, we get $C_0 > 0$. Differentiating with respect to p_j, we have

$$\frac{\partial E}{\partial p_j} = C_0 \cdot \left(N_1 \frac{\partial r_1}{\partial p_j} + N_2 \frac{\partial r_2}{\partial p_j} - N_3 \frac{\partial r_3}{\partial p_j}\right). \tag{5.1}$$

By Lemma 6, we have $r_2 \equiv r_3$, and thus we get

$$\frac{\partial E}{\partial p_1} = C_0 \cdot \left(N_1 \frac{\partial r_1}{\partial p_1} + (N_2 - N_3)\frac{\partial r_2}{\partial p_1}\right) = C_0 \cdot u,$$

where

$$u := N_1 \frac{\partial r_1}{\partial p_1} + (N_2 - N_3)\frac{\partial r_2}{\partial p_1}.$$

We have

$$\begin{aligned} u =& - N_1 \frac{(t-1)(2p_2^r - p_2^{2r}) + 1}{t} \cdot \frac{db_C(\lfloor r/2 \rfloor; r, p_1)}{dp_1} \\ & - (N_2 - N_3)\frac{(t-1)rp_1^{r-1}(1-p_2^r)}{t} b_C(\lfloor r/2 \rfloor; r, p_2) \\ =& N_1 \frac{(t-1)(2p_2^r - p_2^{2r}) + 1}{t} \cdot r \cdot b(\lfloor r/2 \rfloor; r-1, p_1) \\ & - (N_2 - N_3)\frac{(t-1)rp_1^{r-1}(1-p_2^r)}{t} b_C(\lfloor r/2 \rfloor; r, p_2), \end{aligned}$$

by using Lemma 12. Writing $u' = ut/r$, we get that

$$\begin{aligned} u' =& N_1[(t-1)(2p_2^r - p_2^{2r}) + 1] \cdot b(\lfloor r/2 \rfloor; r-1, p_1) \\ & - (N_2 - N_3)(t-1)p_1^{r-1}(1-p_2^r) b_C(\lfloor r/2 \rfloor; r, p_2) \end{aligned}$$

We use the assumption that r be odd, to get

$$\begin{aligned} u' =& N_1[(t-1)(2p_2^r - p_2^{2r}) + 1] \cdot \binom{r-1}{\frac{r-1}{2}} p_1^{\frac{r-1}{2}} (1-p_1)^{\frac{r-1}{2}} \\ & - (N_2 - N_3)(t-1)p_1^{r-1}(1-p_2^r) b_C(\lfloor r/2 \rfloor; r, p_2) \end{aligned}$$

Recall that $\partial E/\partial p_1$ and u' have the same sign. If $u' = 0$, then either $p_1 = 0$ or

$$\left(\frac{1-p_1}{p_1}\right)^{\frac{r-1}{2}} = \frac{(N_2 - N_3)(t-1)(1-p_2^r)b_C(\lfloor r/2 \rfloor; r, p_2)}{N_1[(t-1)(2p_2^r - p_2^{2r}) + 1] \cdot \binom{r-1}{\frac{r-1}{2}}}. \tag{5.2}$$

If $N_3 > N_2$, then this equation has no solution on $[0,1]$ and $u' > 0$ for all p_1. In this case E is minimised when $p_1 = p_2$. If $N_3 \leq N_2$ and $r > 1$, given p_2, there is a unique value p_1^* of $p_1 \in [0,1]$ solving (5.2). If $p_1 > p_1^*$, we get $u' < 0$, and if $0 < p_1 < p_1^*$, then $u' > 0$. It follows that if p_1 solves $u' = 0$, then E is maximised. If E is minimised, then either $p_1 = 1$ or $p_1 = p_2$. In the case where $r = 1$, the left hand side of (5.2) is 1, so the equation either has no solution or every $p_1 \in [0,1]$ is a solution and minimises E. □

Lemma 10
If E is minimised and $p_1 = 1$, then either $p_2 = p_3 = 0$, $p_2 = p_3 = 1$, or $N_2 = N_3$. In the latter case, any value of $p_2 = p_3$ minimises E.

Proof: We know that $p_2 = p_3$, so write $r_2 = r_3 = r_0$, where

$$r_0 = 1 - b_C(\lfloor r/2 \rfloor; r, p_2).$$

Also note that $r_1 = 1$ whenever $p_1 = 1$. From (5.1), we get

$$\frac{\partial E}{\partial p_2} = C_0 \cdot (N_2 - N_3) \cdot r \cdot b(\lfloor r/2 \rfloor; r-1, p_2).$$

If $N_2 = N_3$, this is zero, making E constant. It is negative for $N_3 > N_2$ and positive for $N_2 > N_3$. Hence, if $N_3 \neq N_2$ and E is minimised, then $p_2 = p_3$ must be either maximised or minimised. □

Observe that if (p_1, p_2, p_3) is either $(1,0,0)$ or $(1,1,1)$, then $(r_1, r_2, r_3) = (p_1, p_2, p_3)$. We can also see that for any N_1, E has the same evalution for $(p_1, p_2, p_3) = (1,1,1)$, $N_2 = a$, and $N_3 = b$, as it has for $(p_1, p_2, p_3) = (1,0,0)$, $N_2 = b$, and $N_3 = a$. It follows that the minimum value of E with $p_1 = p_2 = p_3$ is not larger than the minimum value of E under strategy $(1,0,0)$.

Lemma 11
If $p_1 = p_2 = p_3$, (r,t) are such that $p^*(r,t) \geq 1/2$, and $\lambda = \bar{\varrho}_3/\varrho_3 \leq 2$, then

$$E \geq \frac{\left(1 + 2(2p^*(r,t) - 1)v_{1,2}^* - (2p^*(r,t) - 1)\lambda\right)^2}{8(2v_{1,2}^* p^*(r,t) + (1 - p^*(r,t))\lambda))}\varrho_3,$$

where

$$v_{1,2} = \begin{cases} \lambda, & \text{if } p = 1/2 \text{ or } v_{1,2}^* \geq \lambda, \\ 1, & \text{if } v_{1,2}^* \leq 1, \\ v_{1,2}^*, & \text{otherwise,} \end{cases}$$

and

$$v_{1,2}^* = \frac{p + (5p - 2p^2 - 2)\lambda}{2(2p^2 - p)}.$$

Proof: We write

$$v_{1,2} = \frac{N_1 + N_2}{2\ell_3}, \quad v_3 = \frac{N_3}{\ell_3}$$

We have $1 \leq v_{1,2}, v_3 \leq \lambda$. The proof is made through three claims, conserning the worst-case values of respectively p, v_3, and $v_{1,2}$.

Claim 1. *In the worst case we have $p = p^*(r,t)$.*

For $r_1 = r_2 = r_3 = p$, Lemma 8 gives

$$E = \frac{1}{2}\left(1 - \frac{2v_{1,2} + v_3 - 1}{2(2pv_{1,2} + (1-p)v_3)}\right)^2 (2pv_{1,2} + (1-p)v_3)\ell_3. \tag{5.3}$$

If $\bar{\ell}_3 \leq 2\ell_3$, then this expression is clearly increasing in p, and thus minimised for $p = p^*(r,t)$.

Claim 2. *In the worst case we have $v_3 = \lambda$.*

Differentiating with respect to v_3, we get

$$\begin{aligned}
\frac{\partial E}{\partial v_3} &= \frac{1}{2}\left(1 - \frac{N - \ell_3}{2m}\right)^2 (1-p)\ell_3 + m\left(1 - \frac{N - \ell_3}{2m}\right)\left(\frac{-\ell_3}{2m} + \frac{N - \ell_3}{2m^2}(1-p)\ell_3\right) \\
&= \frac{\ell_3^2}{2m}\left(1 - \frac{N - \ell_3}{2m}\right) \cdot F_3,
\end{aligned}$$

where

$$\begin{aligned}
F_3 &= \left(\frac{m}{\ell_3} - \frac{N - \ell_3}{2\ell_3}\right)(1-p) - \frac{m}{\ell_3} + \frac{N - \ell_3}{\ell_3}(1-p) \\
&= \left(\frac{m}{\ell_3} + \frac{N - \ell_3}{2\ell_3}\right)(1-p) - \frac{m}{\ell_3} = -\frac{m}{\ell_3}p + \frac{N}{2\ell_3}(1-p) - \frac{1-p}{2} \\
&= -2v_{1,2}p^2 - v_3(1-p)p + v_{1,2}(1-p) + v_3\frac{1-p}{2} - \frac{1-p}{2} \\
&= (-2p^2 + 1 - p)v_{1,2} + (p^2 - p + (1-p)/2)v_3 - (1-p)/2. \\
&\leq -4p^2 + 2 - 2p + 2p^2 - 2p + 1 - p - (1-p)/2 \\
&= -2p^2 + 3 - 5p - (1-p)/2 \leq -1/2 + 3 - 5/2 - (1-p)/2 = -(1-p)/2 < 0.
\end{aligned}$$

Thus E decreases in v_3 and is minimised for $v_3 = \lambda$.

Question 3. The worst case value of $v_{1,2}$.

By differentiating E as given in Lemma 8 with respect to $v_{1,2}$, we have

$$
\begin{aligned}
\frac{\partial E}{\partial v_{1,2}} &= \frac{1}{2}\left(1-\frac{N-\ell_3}{2m}\right)^2 (2p\ell_3) + m\left(1-\frac{N-\ell_3}{2m}\right)\frac{\partial}{\partial v_{1,2}}\frac{\ell_3-N}{2m} \\
&= \left(1-\frac{N-\ell_3}{2m}\right)^2 p\ell_3 + m\left(1-\frac{N-\ell_3}{2m}\right)\left(\frac{-2\ell_3}{2m}+\frac{N-\ell_3}{2m^2}(2p\ell_3)\right) \\
&= \left(1-\frac{N-\ell_3}{2m}\right)^2 p\ell_3 + \frac{\ell_3}{m}\left(1-\frac{N-\ell_3}{2m}\right)(-m+(N-\ell_3)p) \\
&= \left(1-\frac{N-\ell_3}{2m}\right)\cdot\frac{\ell_3^2}{m}\cdot F_{1,2},
\end{aligned}
$$

where

$$
\begin{aligned}
F_{1,2} &= \left(\frac{m}{\ell_3}-\frac{N-\ell_3}{2\ell_3}\right)p - \frac{m}{\ell_3} + \frac{N-\ell_3}{\ell_3}p \\
&= \left(\frac{m}{\ell_3}+\frac{N-\ell_3}{2\ell_3}\right)p - \frac{m}{\ell_3} \\
&= (2p^2+p-2p)v_{1,2} + ((1-p)p+p/2-(1-p))v_3 - p/2 \\
&= (2p^2-p)v_{1,2} + (5p/2-p^2-1))\lambda - p/2.
\end{aligned}
$$

For $p = 1/2$, this is clearly negative, which makes $v_{1,2} = \lambda$ the worst case value. If $p > 1/2$, $F_{1,2} < 0$ for small values of $v_{1,2}$ and positive for big values. Hence in the worst case, we have $F_{1,2} = 0$, or

$$
v_{1,2} = \frac{p+(5p-2p^2-2)\lambda}{2(2p^2-p)}.
$$

If this is outside the permissible bounds $[1,\lambda]$, $v_{1,2}$ clearly takes one of the end values in the worst case. Substituting into (5.3) gives the lemma. □

The following theorem is an immediate consequence of the lemma.

Theorem 4
Let C_O be a code with $(2,2)$- and $(3,1)$-separating weights in the interval $[\ell_3,\bar{\ell}_3]$, where $\lambda = \bar{\ell}_3/\ell_3 \leq 2$, and concatenate it with $SC(r,t)$. Suppose r is odd and $p^*(r,t) \geq 1/2$. Then the concatenated code is 3-secure with ϵ-error where

$$
\epsilon \leq M \cdot e^{-a\cdot\ell_3},
$$

and

$$
a = \frac{\left(1+2(2p^*(r,t)-1)v_{1,2}^* - (2p^*(r,t)-1)\lambda\right)^2}{8(2v_{1,2}^* p^*(r,t) + (1-p^*(r,t))\lambda))}.
$$

$BCH^{\perp}$ (e,m)	C_O (n,M)	SC(1,4) $p=0.5556$	SC(3,3) $p=0.6667$	SC(3,4) $p=0.75$
$(2,13)$	$(2^{13}-1,2^{13})$	$0.63\cdot 10^{-29}$	$0.37\cdot 10^{-40}$	$0.12\cdot 10^{-47}$
$(2,15)$	$(2^{15}-1,2^{15})$	$0.32\cdot 10^{-148}$	$0.74\cdot 10^{-202}$	$0.58\cdot 10^{-241}$
$(3,12)$	$(4095,2^{18})$	$0.13\cdot 10^{-6}$	$0.10\cdot 10^{-9}$	$0.21\cdot 10^{-11}$
$(3,14)$	$(2^{14}-1,2^{21})$	$0.12\cdot 10^{-59}$	$0.43\cdot 10^{-82}$	$0.44\cdot 10^{-97}$
$(5,16)$	$(2^{16}-1,2^{40})$	$0.94\cdot 10^{-173}$	$0.39\cdot 10^{-222}$	$0.30\cdot 10^{-249}$

Table 5.2.: Upper bounds on ϵ for some dual BCH codes.

$BCH^{\perp}(e,m)$	$SC(r,t)$	SC length	(n,M)	$\epsilon \leq$
$(2,13)$	$(1,3)$	7	$(57\,337,2^{13})$	10^{-25}
$(2,15)$	$(1,3)$	7	$(229\,369,2^{15})$	10^{-75}
$(3,12)$	$(3,4)$	27	$(110\,565,2^{18})$	10^{-11}
$*(3,12)$	$(1,3)$	7	$(57\,330,2^{18})$	10^{-16}
$(3,14)$	$(1,3)$	7	$(114\,681,2^{21})$	10^{-53}
$(5,16)$	$(1,3)$	7	$(458\,745,2^{40})$	10^{-148}

Table 5.3.: Some codes with $\epsilon \leq 10^{-10}$. For the outer code marked $*$, each column in the outer code is replicated twice, essentially doubling ℓ_3 and n.

Observe that larger ℓ_3 improves the error rate. By replicating the columns $r \geq 2$ times in the outer code, we can easily obtain codes with vastly better error rate and only twice the length. In Table 5.3, we can see how this gives shorter length and better error rate than using a larger scattering code. Also observe that λ should be made as small as possible, and $p^*(r,t)$ as big as possible in order to minimise the error rate.

In Table 5.2, we show the parameters of some separating codes, and in Table 5.3 some of the best concatenated codes. A previous record code was a $(329\,008,16\,000)$ code with error rate 10^{-10} from [9]. We observe that several of our codes beat this code in all parameters.

We can also note that Table 5.3 is easily extrapolated. Increasing m by two will roughly increase the length by a factor of four, and increase the size by a factor of 2^e. The error rate drops exponentially. For bigger codes it is better to increase e than m, even though the bounds on $(\ell_3,\bar{\ell}_3)$ are less accurate for these codes. The tables include one example with $BCH^{\perp}(5)$.

A. Auxiliary lemmata

Lemma 12
Let $b_C(x;r,p) = P(X \leq x)$ for $X \sim \mathcal{B}(r,p)$. Then we have

$$\frac{db_C(x;r,p)}{dp} = -r\binom{r-1}{x}p^x(1-p)^{r-x-1} = -r \cdot b(x;r-1,p).$$

Proof:

$$\begin{aligned}
\frac{db_C(x;r,p)}{dp} &= \frac{d}{dp}\sum_{i=0}^{x}\binom{r}{x}p^i(1-p)^{r-i} \\
&= \sum_{i=0}^{x}\binom{r}{i}(ip^{i-1}(1-p)^{r-i} - (r-i)p^i(1-p)^{r-i-1}) \\
&= \sum_{i=0}^{x-1}\binom{r}{i+1}(i+1)p^i(1-p)^{r-1-i} - \sum_{i=0}^{x}\binom{r}{i}(r-i)p^i(1-p)^{r-i-1} \\
&= -\binom{r}{x}(r-x)p^x(1-p)^{r-x-1} \\
&+ \sum_{i=0}^{x-1}\left(\binom{r}{i+1}(i+1) - \binom{r}{i}(r-i)\right)p^i(1-p)^{r-i-1} \\
&= -\binom{r}{x}(r-x)p^x(1-p)^{r-x-1} \\
&+ \sum_{i=0}^{x-1}\left(\binom{r}{i+1}(i+1) - \binom{r}{i}(r-i)\right)p^i(1-p)^{r-i-1} \\
&= -\binom{r}{x}(r-x)p^x(1-p)^{r-x-1} \\
&= -r\binom{r-1}{x}p^x(1-p)^{r-x-1}
\end{aligned}$$

$\square$

Bibliography

[1] A. Barg, G. R. Blakley, and G. A. Kabatiansky. Digital fingerprinting codes: Problem statements, constructions, identification of traitors. *IEEE Trans. Inform. Theory*, 49(4):852–865, April 2003.

[2] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. In *Advances in Cryptology - CRYPTO'95*, volume 963 of *Springer Lecture Notes in Computer Science*, pages 452–465, 1995.

[3] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inform. Theory*, 44(5):1897–1905, 1998. Presented in part at CRYPTO'95.

[4] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Advances in Cryptology - CRYPTO '94*, volume 839 of *Springer Lecture Notes in Computer Science*, pages 257–270. Springer-Verlag, 1994.

[5] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Trans. Inform. Theory*, 46(3):893–910, May 2000.

[6] Gérard Cohen and Gilles Zémor. Intersecting codes and independent families. *IEEE Trans. Inform. Theory*, 40:1872–1881, 1994.

[7] Gérard D. Cohen, Sylvia B. Encheva, Simon Litsyn, and Hans Georg Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 128(1):75–83, 2003.

[8] J Herrera-Joancomarti and Josep Domingo-Ferrer. Short collusion-secure fingerprints based on dual binary Hamming codes. *Electronics Letters*, 36:1697–1699, September 2000.

[9] Tri Van Le, Mike Burmester, and Jiangyi Hu. Short c-secure fingerprinting codes. In *Proceedings of the 6th Information Security Conference*, October 2003. Available at `http://websrv.cs.fsu.edu/~burmeste/`.

[10] Birgit Pfitzmann and Michael Waidner. Anonymous fingerprinting. In *Advances in cryptology—EUROCRYPT '97*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 88–102. Springer, Berlin, 1997.

[11] Reihaneh Safavi-Naini and Yejing Wang. Sequential traitor tracing. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 316–332. Springer, Berlin, 2000.

[12] Hans Georg Schaathun. The Boneh-Shaw fingerprinting scheme is better than we thought. Technical Report 256, Department of Informatics, University of

Bergen, 2003. Also available at `http://www.ii.uib.no/~georg/sci/inf/coding/public/`.

[13] Hans Georg Schaathun. Fighting two pirates. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of *Springer Lecture Notes in Computer Science*, pages 71–78. Springer-Verlag, May 2003.

[14] Hans Georg Schaathun and Tor Helleseth. Separating and intersecting properties of BCH and Kasami codes. Springer Lecture Notes in Computer Science. Springer-Verlag, December 2003. To be presented at IMA'03, Cirencester, Dec. 2003.

[15] Francesc Sebé and Josep Domingo-Ferrer. Short 3-secure fingerprinting codes for copyright protection. In *ACISP 2002*, volume 2384 of *Springer Lecture Notes in Computer Science*, pages 316–327. Springer-Verlag, 2002.

[16] Neal R. Wagner. Fingerprinting. In *Proceedings of the 1983 Symposium on Security and Privacy*, 1983.