Designs, Codes and Cryptography (2019) 87:455–462
https://doi.org/10.1007/s10623-018-0551-9

Signature codes for weighted noisy adder channel, multimedia fingerprinting and compressed sensing

Elena Egorova[1] · Marcel Fernandez[2] · Grigory Kabatiansky[1] · Moon Ho Lee[3]

Received: 2 May 2018 / Revised: 29 August 2018 / Accepted: 31 August 2018 /
Published online: 21 September 2018

Abstract
We propose a new approach to construct noise-resistant multimedia fingerprinting codes. Our approach is based on the theory of the signature codes for multiple access channels, mainly, for a weighted noisy adder channel. The corresponding multimedia fingerprinting codes allow to trace the entire coalition of pirates. The codes provide significantly better rate than previously known multimedia fingerprinting schemes. We establish the relationship between multimedia fingerprinting and compressed sensing problems.

Keywords Multimedia fingerprinting · Signature codes for multiple access channels · Compressed sensing

Mathematics Subject Classification 94B60

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

The work of E. Egorova and G. Kabatiansky has been supported by the RFBR Grants 18-07-01427 and 16-01-00716. The work of M. Fernández has been supported by the Spanish Government Grant TEC2015-68734-R and Catalan Government Grant SGR 782.

✉ Elena Egorova
egorovahelene@gmail.com

Marcel Fernandez
marcel@entel.upc.edu

Grigory Kabatiansky
g.kabatyansky@skoltech.ru

Moon Ho Lee
moonho@jbnu.ac.kr

1 Skolkovo Institute of Science and Technology (Skoltech), Moscow, Russia

2 Universitat Politcnica de Catalunya, Barcelona, Spain

3 Division of of Electronics, Chonbuk National University, Jeonju, Republic of Korea

1 Introduction

The problem of data protection against unauthorized copying has given rise to the well established concept of *tracing traitors* [9]; and its three particular cases known as *codes with the identifiable parent property (IPP codes)* [18], *schemes with the identifiable parent property* [11,25] and *collusion secure digital fingerprinting codes* [2,3,26]. The main idea consists in creating such personalized marks (embedded in each copy of the distributed copy) that allow a dealer to reveal the source of a leakage, even in the case of the collusion attacks, i.e., the case when users form a coalition to produce a forged copy based on the copies that they have.

A theoretical model of protection of *continuous* data was proposed in [27] and [22]. The corresponding codes, called *multimedia fingerprinting* codes, became more popular recently, see [6–8,16,19]. First family of multimedia fingerprinting codes with nonvanishing rate, namely with the rate of order t^{-2}, where t is the maximum coalition's size, was constructed in [14]. Some generalization of results from [14] to a noisy case was obtained in [15]. All previous considerations of multimedia fingerprinting codes are based on some discretization, introduced in [27]. In fact, it means that only *hard decoding* algorithms of such codes are investigated. In this paper we consider the output of the corresponding channel without discretization, and we develop *soft decoding* algorithms of multimedia fingerprinting codes. It appeared that the corresponding soft decoding model of multimedia fingerprinting channel is equivalent to a generalization of the binary adder channel introduced in [23], which we call *weighted binary adder channel with partial activity*. We show that the signature codes for such channel is the same as the multimedia fingerprinting codes with soft decoding. We prove that the rate of the best multimedia fingerprinting codes with soft decoding is at least $1/t$ which is much larger than for the hard decoding which rate cannot exceed $O(t^{-2}\log t)$ even for the noiseless case, see [14].

2 Multimedia fingerprinting channel and codes

Following [27] and [22], we consider the multimedia content represented as m-dimensional real-valued vector $\mathbf{x} = (x_1, \ldots, x_m) \in R^m$, called the host signal. To prevent unauthorized redistribution of $\mathbf{x}$ outside of M legal users, the dealer constructs a set of digital fingerprints using a linear modulation scheme that employs n *noise-like* orthonormal signals (vectors) $\mathcal{F} := \{\mathbf{f}_i \in R^m \mid i = 1, \ldots, n,\ n \le m\}$. Note that the set $\mathcal{F}$ is known only to the dealer and the dealer kept them in secret.
The fingerprint $\mathbf{w}_j$ of the j-th user, $j \in \{1, \ldots, M\}$, is defined as follows:

$$\mathbf{w}_j = \sum_{i=1}^{n} h_{ij}\mathbf{f}_i, \tag{1}$$

where $h_{ij} \in \{+1, -1\}$ for antipodal modulation and $h_{ij} \in \{0, 1\}$ for on-off keying type of modulation. In what follows, we consider the case of the on-off keying type of modulation , i.e., $\{0, 1\}$ case. The set $\mathcal{C}$ of all M fingerprints $\{\mathbf{w}_j\}$ will be called a fingerprinting code. For convenience, one can consider the set of n-dimensional binary vectors $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj})$, i.e., vectors consisting of coefficients used for the linear combination of $\mathbf{w}_j$. Such set of vectors forms a binary code C of length n and cardinality M.

The dealer distributes to the j-th user the vector

$$\mathbf{y}_j = \mathbf{x} + \mathbf{w}_j,$$

under assumption that $\sqrt{x_1^2 + \cdots + x_m^2} = \|\mathbf{x}\|_2 \gg \|\mathbf{w}_j\|_2$ that insures that the fingerprinting scheme do not introduce significant changes in the host signal.

A group of malicious users (coalition), called *colluders* or *pirates*, aims to create an unauthorized copy of the content $\mathbf{x}$ such that the dealer cannot trace its origins to any of them. As an analogue of the *Marking Assumption*, introduced in [3] and playing a key role in digital fingerprinting, for multimedia fingerprinting we propose the following notion of *Multimedia Marking Assumption* (M^2 *Assumption*, for short): *members of a pirate coalition cannot manipulate individual signals* $\mathbf{f}_j$, *and their actions are limited to linear attacks only*.

By a linear attack we mean that a pirate coalition $J \subset \{1, \ldots, M\}$ can generate a forged copy $\hat{\mathbf{y}}$ of the host content as a linear combination of their copies $\mathbf{y}_j$ with some coefficients ("weights") λ_j

$$\hat{\mathbf{y}} = \sum_{j \in J} \lambda_j \mathbf{y}_j \tag{2}$$

where $\lambda_j > 0$ for all $j \in J$ and $\sum_{j \in J} \lambda_j = 1$. Hence

$$\hat{\mathbf{y}} = \mathbf{x} + \sum_{j \in J} \lambda_j \mathbf{w}_j, \tag{3}$$

where the coefficients λ_j are chosen by the coalition J and they are unknown to the dealer. Note, that most of the previous papers on multimedia fingerprinting considered even more restricted assumption. Namely, only the averaging attack is considered that means that $\lambda_j = 1/|J|$ for all $j \in J$, see [6,22,27].

Let $< J >$ denote the set of all vectors $\hat{y}$ that coalition J can create according to (2). Then, the property that the dealer can trace the whole coalition by observing $\hat{\mathbf{y}}$, can be formulated in the following way.

Definition 1 A code $\mathcal{C}$ is a *multimedia code with a strong t-IPP property (a strong t-MIPP code)*, if for every $\hat{\mathbf{y}}$ either there is only one coalition J of size at most t such that $\hat{\mathbf{y}} \in < J >$ or there is no t-coalition that can generate $\hat{\mathbf{y}}$.

In order to trace members of J the dealer calculates the vector $\mathbf{S} = \mathbf{S}(J, \{\lambda_j\}) = (s_1, \ldots, s_n)$, where

$$s_k = (\widehat{\mathbf{y}} - \mathbf{x}, \mathbf{f}_k) = \langle \sum_{i=1}^{n} \sum_{j \in J} \lambda_j h_{ij} \mathbf{f}_i, \mathbf{f}_k \rangle = \sum_{j \in J} \lambda_j h_{kj} \tag{4}$$

and $\langle \cdot, \cdot \rangle$ denotes the inner product. Let us form the $n \times M$ binary matrix H which j-th column is vector $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj})$. Then, equivalently,

$$\mathbf{S} = \mathbf{S}(\mathbf{\Lambda}) = \sum_{j \in J} \lambda_j \mathbf{h}_j = H \mathbf{\Lambda}^T, \tag{5}$$

where $\mathbf{\Lambda} = (\lambda_1, \ldots, \lambda_M)$ with $\lambda_j = 0$ for $j \notin J$. This equation looks like the syndrome equation of coding theory where $\mathbf{S}(\mathbf{\Lambda})$ plays the role of a syndrome and $\mathbf{\Lambda}$ plays the role of an error vector, but for fingerprinting purposes we need to know only the coalition set J, i.e. to know only the *support* of the vector $\mathbf{S}(\mathbf{\Lambda})$. This similarity will lead us later to a new way of constructing good matrices H.

2.1 Discrete model for multimedia fingerprinting and multiple access channels

Nevertheless the Eq. (5) is a bit far from the traditional syndrome equation since all elements of (5) are considered over the field $\mathbf{R}$ of real numbers. It was suggested in [22,27] to consider the following discretization, when the dealer knows only whether $s_k = 0$, or $s_k = 1$, or that $0 < s_k < 1$, but does not know the value of s_k in the last case. Note, that $s_k = 0$ means that $h_{kj} = 0$ for all $j \in J$, $s_k = 1$ means that $h_{kj} = 1$ for all $j \in J$ and finally $0 < s_k < 1$ means that

$$\{\cup_{j\in J} h_{kj}\} = \{0, 1\}. \tag{6}$$

Hence, it means that within the frame of this discrete fingerprinting model the dealer knows for every k that either *no one* coalition member has a given noise-like signal $\mathbf{f}_k$ in their fingerprints $\mathbf{w}_j$, or *all* coalition member have $\mathbf{f}_k$ in their fingerprints $\mathbf{w}_j$, or some members have and some not. Hence, each coalition J with chosen weights λ_j corresponds to the following *uniquely defined* ternary output vector $D(\mathbf{S}(J))$, which we call *discrete signature* of J, where D is the following mapping of the segment $[0, 1]$ to the set $\{0, 1, *\}$ with $D(0) = 0$, $D(1) = 1$ and $D(x) = *$ for $0 < x < 1$. The aim of the dealer is to construct such multimedia fingerprinting code that has the following property: *for any two different coalitions J, I of size at most t their signatures are distinct, i.e., $D(S(J)) \neq D(S(I))$.*

In fact, the considered problem is equivalent to one of constructing signature codes for an A-channel—a special class of multiple access channels. Recall the definition of A-channel, i.e., the q-frequencies multiple access channel without intensity information, see [5].

Definition 2 The *A-channel* is a multiple-access noiseless channel with M independent users and q-ary input alphabet Q. The output of the A-channel is a binary sequence of length q whose i-th position is zero if no users transmit the i-th symbol of the alphabet Q, and one otherwise. In other words, the outputs of the A-channel are $2^q - 1$ nonempty subsets of $\{0, 1, \ldots, q - 1\}$.

The above considered discrete fingerprinting model corresponds to $q = 2$; the number of time-slots equals to the number of noise-like signals, i.e., equals to n, and the dealer observes ternary output of this A-channel. Hence, the dealer's goal is to construct a t-signature code for the binary A-channel. Recall that a code $C = \{c_1, \ldots, c_M\}$ called a t-signature code for a given multiple access channel if for any two different sets of codevectors, each of the cardinality at most t, the corresponding outputs of the multiple access channel are distinct.

It turned out that the so called separating codes [10,24] can be used as signature codes for the A-channel. Recall the definition of *separating codes*.

Definition 3 A q-ary code C is called (t_1, t_2)-separating if for any two non intersecting sets U and W of codewords, such that $|U| \leq t_1$ and $|W| \leq t_2$, there is a coordinate $j = j(U, W)$ which separates them, i.e.

$$U_j \cap W_j = \emptyset \tag{7}$$

Separating codes have a long history being introduced half a century ago, see [10,24] for good overviews. Particular cases of $(1, t)$ and (t, t)-separating codes were rediscovered in [3] under the names of frameproof and secure frameproof codes, correspondingly.

It is easy to check that any binary $(1, t)$-separating code is a t-signature code for binary A-channel [14]. On the other hand, any t-signature code for binary A-channel is $(1, t - 1)$-separating codes (in fact, this is Lemma 4.6 of [6]). Then, based on known results about the rate of best $(1, t)$ separating codes [10,24], it was proved in [14] that for the rate $R_t = n^{-1} \log_2 M$

of the best (largest) multimedia fingerprinting codes capable to find the entire pirate coalition (under the considered discretization) the following bounds are valid for large t

$$t^{-2} \le R_t \le t^{-2} \log t \tag{8}$$

In the next section we will show that the usage of full information provided by the Eqs. (4)–(5) allows to significantly increase the rate of the best multimedia codes with strong t-IPP property.

3 Codes for noiseless weighted adder channel

Let's consider $\mathbf{S}(\mathbf{\Lambda})$ as the output of *continuous* multimedia fingerprinting channel which is in fact a modification of well known adder channel. We call this channel as *weighted binary adder channel* (WbAC, for short). Indeed, Eqs. (4)–(5) with $\lambda_j \equiv 1$ describes the output of the adder channel with binary input in the case of t active users among M. In the general case, λ_j play the role of weights. Hence, multimedia fingerprinting codes capable to trace the whole coalition of size t are in fact the same as t-signature codes for the weighted adder channel, and the number of users M equals to the cardinality of the corresponding signature code. Note that an intermediate case of the weighted adder channel $\lambda_j > 0$ was firstly considered in [23], where weights λ_j were called gains.

So, the dealer observes the output of WbAC, with unknown weights λ_j and unknown set J of active users of WbAC, i.e., the set of traitors. The dealer's goal is to find the set J, what corresponds to zero-error coding for multiple-access channel (MAC) with *partial activity*, i.e. when not all possible users of MAC are active, but not more than t of them. Consider the set of n-dimensional binary vectors $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj}) \in \mathbf{R}^n$ as a binary multimedia fingerprinting code of cardinality M. Such code is capable to find any set of t or less traitors iff for any subsets $J, J' \subset \{1, \ldots, M\}$ such that $|J| \le t,\ |J'| \le t$ the following equality

$$\sum_{j \in J} \lambda_j \mathbf{h}_j = \sum_{j \in J'} \lambda'_j \mathbf{h}_j \tag{9}$$

implies that $J = J'$.

Denote by $A(n, t)$ the maximal possible cardinality of a binary t-signature code of length n for WbAC, i.e., the maximal cardinality of a set of binary vectors in n-dimensional Euclidean space for which the condition (9) holds.

Theorem 1

$$A(n, t) \ge 2^{\lfloor n/t \rfloor} \tag{10}$$

Proof Consider more stronger property than (9), namely, that additionally $\lambda_j = \lambda'_j$ for all j. This property is equivalent to the linear independence (over real numbers) of any $2t$ vectors $\mathbf{h}_j$. In order to construct such a set let us consider the binary Goppa code of length 2^m with $r \le tm$ redundancy symbols which corrects t errors. Then all 2^m columns of a parity-check matrix of this code forms the desired binary t-signature code of length r for WbAC. Indeed, any $2t$ columns are linear independent over the field of residues by module 2, and hence they are linear independent over the field of rational numbers and also over the real numbers since in all cases dependency means that the determinant of the corresponding $t \times t$ minor equals to 0. □

This theorem shows that in the case of absence of quantization, i.e., soft decision, the rate of the best multimedia fingerprinting code is at least $1/t$ whereas for hard decoding the rate of any multimedia fingerprinting code is at most $O(t^{-2}\log t)$ [14].

Remark Denote by $A^*(n,t)$ the maximal cardinality of a set of binary vectors in $\mathbf{R}^n$ such that any its $2t$ vectors are linearly independent in $\mathbf{R}^n$. In Theorem 1 we proved that $A^*(n,t) \geq 2^{\lfloor n/t \rfloor}$. It is not clear if this result is even weakly optimal, i.e., $n^{-1}\log_2 A^*(n,t) = t^{-1}(1 + o(1))$?

4 Codes for noisy weighted adder channel and the compressed sensing problem

In almost all previous works on multimedia fingerprinting codes it was assumed that the dealer observes the forged copy $\hat{\mathbf{y}}$ *without noise*. Moreover, we have to note that the problem of noise in multiple-access channels was also almost ignored probably because of the following old remark in [5] "A more sophisticated model taking such errors into account could easily be developed. One method would be to use a noisy channel in cascade with our noiseless channel. It is our contention, however, that although the details are different, the basic ideas are the same in the noisy and noiseless cases."
This simplified assumption of considering noiseless channel is not realistic since there are at least two sources of noise: a measurement noise, and a malicious noise, produced by pirates. Therefore we assume that the dealer observes the following vector $\widehat{\mathbf{z}}$ as a result of a coalition forgery

$$\widehat{\mathbf{z}} = \mathbf{x} + \sum_{j\in J} \lambda_j \mathbf{w}_j + \varepsilon, \tag{11}$$

where $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_m) \in R^m$ is an error vector and let for simplicity ε_i be i.i.d.random variables. Similarly to (4) and (5) the dealer evaluates

$$s_k(\varepsilon, \mathbf{\Lambda}) = (\widehat{\mathbf{z}} - \mathbf{x}, \mathbf{f}_k)$$

and the following vector

$$\mathbf{S}(\varepsilon, \mathbf{\Lambda}) = (s_1(\varepsilon, \mathbf{\Lambda}), \ldots, s_n(\varepsilon, \mathbf{\Lambda})) = \sum_{j\in J} \lambda_j \mathbf{h}_j + \mathbf{e} = H\mathbf{\Lambda}^T + \mathbf{e}, \tag{12}$$

where $\mathbf{e} = (e_1, \ldots, e_n)$ and $e_k = \langle \varepsilon, \mathbf{f}_k \rangle$. Based on the known value of the vector $\mathbf{S}(\varepsilon, \mathbf{\Lambda})$, which plays the role the syndrome for error-correcting codes, the dealer tries to trace the whole coalition, which produced this forgery, or at least one of its members, which we call "weak" multimedia fingerprinting codes and what can be considered as an analogue to the problem considered in [1,12] for the case of disjunctive channel. The entire problem is very similar to the compressed sensing problem, see [4,13], but with the following three differences:

1. for "weak" multimedia fingerprinting code it is sufficient to find at least one $j \in J$ for sure;
2. for "strong" multimedia fingerprinting we need to find only the "error" set J, and solution of compressed sending problem means to find J and the corresponding values λ_j;
3. vectors $\mathbf{h}_j$ are *binary*.

The last difference seems to us the most important.

Consider slightly other statement of the problem, more in the spirit of coding theory, namely, that the number of errors is limited, i.e., $wt(\mathbf{e}) \leq T$. A solution of this problem was

given in [21], see also [20]. If to omit details (which can be found in [21]) then in order to correct T syndrom's errors one should "add" $T\log(t\log M)$ redundant symbols what gives the total redundancy

$$n = t\log_2 M + T\log_2\log_2 M + T\log_2 t$$

It is easy to check that for $T - const$ it keeps the same order of rate, namely

$$R = t^{-1}(1 + o(1))$$

Note that a similar technique was used in [17].

References

1. Alon N., Asodi V.: Tracing many users with almost no rate penalty. IEEE Trans. Inf. Theory **53**(1), 437–439 (2007).
2. Barg A., Blakley G.R., Kabatiansky G.: Digital fingerprinting codes: problems statements, constructions, identification of traitors. IEEE Trans. Inf. Theory **49**(4), 852–865 (2003).
3. Boneh D., Shaw J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inf. Theory **44**(5), 1897–1905 (1998).
4. Candes E.J., Tao T.: Near-optimal signal recovery from random projections: universal encoding strategies? IEEE Trans. Inf. Theory **52**(4), 5406–5425 (2006).
5. Chang S.C., Wolf J.K.: On the T-user M-frequency noiseless multiple-access channel with and without intensity information. IEEE Trans. Inf. Theory **27**(1), 41–48 (1981).
6. Cheng M., Miao Y.: On anti-collusion codes and detection algrithms for multimedia fingerprinting. IEEE Trans. Inf. Theory **57**(7), 4843–4851 (2011).
7. Cheng M., Ji L., Miao Y.: Separable codes. IEEE Trans. Inf. Theory **58**(3), 1791–1803 (2012).
8. Cheng M., Fu H.-L., Jiang J., Lo Y.-H., Miao Y.: New bounds on 2-separable codes of length 2. Des. Codes Cryptogr. **74**(3), 31–40 (2015).
9. Chor B., Fiat A., Naor M.: Tracing traitors. In: Desmedt Y.G. (ed.) Advances in Cryptology–Crypto'94, LNCS, vol. 839, pp. 480–491. Springer, New York (1994).
10. Cohen G.D., Schaathun H.G.: Asymptotic overview on separating codes. Tech. Report 248, Department of Informatics, University of Bergen, Bergen, Norway (2003).
11. Collins M.J.: Upper bounds for parent-identifying set systems. Des. Codes Cryptogr. **51**(2), 167–173 (2009).
12. Csros M., Ruszinko M.: Single-user tracing and disjointly superimposed codes. IEEE Trans. Inf. Theory **51**(4), 1606–1611 (2005).
13. Donoho D.L.: Compressed sensing. IEEE Trans. Inf. Theory **52**(4), 1289–1306 (2006).
14. Egorova E., Fernandez M., Kabatiansky G., Lee M.H.: Signature codes for A-channel and collusion-secure multimedia fingerprinting codes. In: Proceedings 2016 IEEE International Symposium on Information Theory, Barcelona, pp. 3043–3047 (2016).
15. Egorova E., Fernandez M., Kabatiansky G.: Multimedia fingerprinting codes resistant against colluders and noise. In: Proceedings of 8th IEEE International Workshop on Information Forensic and Security, Abu Dhabi, pp. 1–5 (2016).
16. Gao F., Ge G.: New bounds on separable codes for multimedia fingerprinting. IEEE Trans. Inf. Theory **60**, 5257–5262 (2014).
17. Gritsenko V., Kabatiansky G., Lebedev V., Maevskiy A.: Signature codes for noisy multiple access adder channel. Des. Codes Cryptogr. **82**(1), 293–299 (2017).
18. Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.: On codes with the identifiable parent property. J. Comb. Theory Ser. A **82**(2), 121–133 (1998).
19. Jiang J., Cheng M., Miao Y.: Strongly separable codes. Des. Codes Cryptogr. **79**(2), 303–318 (2016).
20. Kabatiansky G., Vladuts S., Tavernier C.: On the doubly sparse compressed sensing problem. In: Proceedings of IMAAC 2015, LNCS, vol. 9496, pp. 1–6 (2015).
21. Kabatiansky G., Lomakov V., Vladuts S.: On codes correcting errors in channel and syndrom. Probl. Inf. Transm. **51**(2), 50–57 (2015).
22. Liu K.J.R., Trappe W., Wang Z.J., Wu M., Zhao H.: Multimedia Fingerprinting Forensics for Traitor Tracing, vol. 4. Hindawi Publishing Corporation, Cairo (2005).

23. Mathys P.: A class of codes for a T active users out of N multiple-access communvation system. IEEE Trans. Inf. Theory **36**(6), 1206–1219 (1990).
24. Sagalovich Yu.L: Separating systems. Probl. Inf. Transm. **30**(2), 105–123 (1994).
25. Stinson D.R., Wei R.: Combinatorial properties and constructions of traceability schemes and frameproof codes. SIAM J. Discret. Math. **11**(1), 41–53 (1998).
26. Tardos G.: Optimal probabilistic fingerprint codes. In: Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA, ACM, pp. 116–125 (2003).
27. Trappe W., Wu M., Wang Z.J., Liu K.J.R.: Anti-collusion fingerprinting for multimedia. IEEE Trans. Signal Process. **51**, 1069–1087 (2003).