In the Proc. of IEEE ISOC ITW2005 on Coding and Complexity; editor M.J. Dinneen; co-chairs U. Speidel and D. Taylor; pages 183-186

Boneh-Shaw Fingerprinting and Soft Decision Decoding

Hans Georg Schaathun
Department of Informatics
The University of Bergen
Boks 7800
N-5020 Bergen
Norway
Email: georg@ii.uib.no

Marcel Fernandez
Department of Telematics Engineering
The Telecommunications Engineering School
Universitat Politecnica de Catalunya
Spain
Email: marcelf@mat.upc.es

***Abstract*— Collusion-secure codes are used for digital fingerprinting and for traitor tracing. In both cases, the goal is to prevent unauthorised copying of copyrighted material, by tracing at least one guilty user when illegal copies appear. The most well-known collusion-secure code is due to Boneh and Shaw (1995/98). In this paper we improve the decoding algorithm by using soft output from the inner decoder, and we show that this permits using significantly shorter codewords.**

I. Introduction

Copyright piracy and protection against it is a problem receiving tremendous interest, both in research communities and in the daily press. Music and movie industries claim to be losing money by the billions. Different kinds of technology have been proposed in order to protect against illegal copying. Digital fingerprinting is one such method.

Digital fingerprinting was introduced in [7], and given increasing attention following [2]. 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 too much. A human user should not be able to spot any difference between the fingerprinted copy and the original. It must also be impossible for the user to remove or damage the fingerprint, without damaging the information contents beyond any practical use. 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.

As fingerprinting is a forensic technique, used to trace the guilty part when a violation is evidenced, it is less controversial than many techniques for digital rights management, which often restricts legal use and copying of the file as well as the illegal copying.

Collusion-secure coding is also employed in traitor tracing [3]. Whereas fingerprinting protects the digital data in themselves, traitor tracing protects broadcast encryption keys.

The most well-known collusion secure code is the Boneh-Shaw (BS) scheme [2]. An overview of other proposals is found in [5], which also contains a new analysis of the error probability for the BS scheme, showing that the codewords can be made much shorter than initially assumed. In this paper, we make further improvement by using soft output from the inner decoding. The major novelty of this paper is to find a good output parameter from the inner decoding.

II. On collusion-secure codes

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. Let $d(C)$ or just d be the minimum Hamming distance of the code C. The normalised minimum distance is $\delta = d/n$. The rate of the code is $R = (\log M)/n$.

Definition 1 (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.

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

Definition 2 (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 for the embedding of the fingerprint in the digital data. Constructing appropriate embeddings is non-trivial, though it is not theoretically impossible [2]. Alternative assumptions have been proposed, and some overview of this can be found in [1].

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 $\mathbf{x}$ is a false fingerprint produced by some coallition $P \subseteq C$, then A is successful if L is a non-empty subset of P. We say that we have an error of Type I if $L \cap P = \emptyset$ and an error of Type II if $L \backslash P \neq \emptyset$. A Type I error means that we do not find any guilty pirate, wheras Type II means accusing an innocent user. Let ϵ_1 and ϵ_2 denote the probabilites of Type I and Type II errors respectively. Given our juridical system, Type II is clearly a graver error than Type I, so we might accept ϵ_1 higher than we can accept ϵ_2.

An (n, M) code is 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 the probability of error (of either type) is at most ϵ when there are at most t pirates.

Our challenge is to find codes with the best possible parameters. The number of users M and the the threshold t should be as large as possible. The length n and the error probability ϵ should be as small as possible. Evidently, these are conflicting goals. Typically, we will fix M, t, and ϵ and do our best to minimise n.

III. Code and decoding

The Boneh-Shaw code is a concatenated code. The inner code will be called BS-RS (Boneh-Shaw replication scheme); it is a binary $(r(M-1), M)$ code which is (M, ϵ)-secure. The code book has $M-1$ distinct columns replicated r times. A set of identical columns will be called a type. Every column has the form $(1 \ldots 10 \ldots 0)$, such that the i-th $(1 \leq i \leq M)$ user has zeroes in the first $i-1$ types and a one in the rest.

Theorem 1 (Boneh and Shaw) *The BS-RS with replication factor* r *is* M*-secure with* ϵ*-error whenever* $r = 2M^2 \log(2M/\epsilon)$.

A hybrid fingerprint is characterised by the number F_i of ones for each column type i. Let $F_0 = 0$ and $F_q = r$ by convention (as if there were a column type 0 with all zeroes, and a type q with all ones). The F_i are stochastic variables with distributions depending on the pirate strategy. If user i be innocent, the pirates cannot distinguish between column types i and $i-1$, and consequently $F_i \sim F_{i-1}$. The decoding algorithm of Boneh-Shaw scheme used a hard decision. If $|F_i - F_{i-1}|$ was sufficiently large, then user i was assumed to be guilty.

Our idea is to return soft information. The output is a vector $\mathbf{v} = (v_1, \ldots, v_q)$, given as

$$v_j = \frac{F_j - F_{j-1}}{r}. \tag{1}$$

Observe that all the v_j sum to 1 and $v_j \in [-1, 1]$ for all j. Furthermore, if the pirates cannot see symbol j, then $E(v_j) = 0$.

The alert reader may think that the definition v_j is a strange choice, and indeed it is. Soft-decision decoding is based on the idea that the larger v_j is, the more likely it is that j is correct decoding. However, when j is incorrect, v_j is expected to be close to zero, and both high and low values of v_j indicates that j is likely to be correct. The advantage of the present definition is that the distribution is nice and easy to work with in the error analysis. We tried to use the absolute value of v_j instead, but then the analysis became too complicated to complete. Our definition might not be optimal, but it does work well.

As outer codes, Boneh and Shaw suggested random q-ary code which would be decoded using closest neighbour decoding. We will study two schemes: Boneh-Shaw inner codes with random outer codes, and Boneh-Shaw inner codes with outer codes with large distance (Algebraic Geometry or Reed-Solomon codes). Both schemes use soft-decision list decoding as described below.

After inner decoding of all the blocks, we form the $q \times n$ reliability matrix $R = [r_{i,j}]$ where the i-th row is the vector $\mathbf{v}$ from inner decoding of the i-th block. The outer decoding algorithm takes the $q \times n$ reliability matrix R as input and returns all codewords $\mathbf{c} = (c_1, \ldots, c_n)$ that satisfy

$$W(\mathbf{c}) = \sum_{i=1}^{n} r_{i,c_i} \geq \Delta n. \tag{2}$$

It is important that the terms r_{i,c_i} of the sum are stochastically independent. Furthermore, r_{i,c_i} is bounded in the interval $[-1, 1]$ and has a fairly simple distribution. This will allow us to use the well-known Chernoff bound in the error analysis.

IV. Error analysis

In this section, we shall bound the error probability for concatenated codes with Boneh-Shaw inner codes and soft decision decoding as defined in the previous section. The principle of the analysis follows [5], and the results are phrased in terms of the relative entropy defined as follows:

$$D(\sigma||p) = \sigma \log \frac{\sigma}{p} + (1-\sigma) \log \frac{1-\sigma}{1-p}. \tag{3}$$

Theorem 2 (Probability of failure) *Using the concatenated code with a BS-RS inner code and soft input list decoding with threshold* $\Delta < 1/t$ *for the outer code, the probability of failing to accuse any guilty user is given as*

$$\epsilon_I \leq 2^{-nE}, \text{ where } E = D\left(\frac{1+\Delta}{2} \Big|\Big| \frac{t+1}{2t}\right). \tag{4}$$

This bound is independent of the choice of outer code.

Proof: The probability ϵ_{I} that the decoding algorithm outputs no guilty user, is bounded as

$$\epsilon_{\mathrm{I}} \leq P\left(\frac{1}{t}\sum_{i=1}^{n}\sum_{\mathbf{c}\in P} r_{i,c_i} \leq \Delta n\right) = P\left(\sum_{i=1}^{n} Y_i \leq \Delta n\right).$$

where

$$Y_i = \sum_{\mathbf{c}\in P}\frac{r_{i,c_i}}{t} = \frac{1}{t}\sum_{\mathbf{c}\in P}\frac{F_{c_i} - F_{c_i-1}}{r}.$$

Obviously

$$\sum_{\gamma\in Q}\frac{F_\gamma - F_{\gamma-1}}{r} = 1,$$

and $E(F_\gamma - F_{\gamma-1}) = 0$ when γ is not seen by the pirates. Hence we get $E(Y_i) = 1/t$. Observe that $-1 \leq Y_i \leq 1$. In order to get a stochastic variable in the range $[0,1]$, we set $X_i = (1+Y_i)/2$. Thus

$$E(X_i) = \bar{x} = \frac{t+1}{2t},$$

and we get

$$\epsilon_{\mathrm{I}} \leq P\left(\sum_{i=1}^{n} X_i \leq \frac{1+\Delta}{2}n\right).$$

If $1/t > \Delta$, the Chernoff bound is applicable, proving the theorem. ■

Theorem 3 (False accusations for random codes) *Concatenating a $(r(q-1), q)$ BS-RS code with a random outer code using soft input list decoding with threshold $\Delta > 1/q$ for the outer code, the probability of accusing an innocent user is*

$$\epsilon_{\mathrm{II}} \leq 2^{(R_O \log q - E)n}, \text{ where } E = D\left(\frac{1+\Delta}{2}\Big|\Big|\frac{q+1}{2q}\right). \quad (5)$$

Proof: Let $\mathbf{c} \notin P$ be an innocent user. The probability of accusing $\mathbf{c}$ is

$$\pi(\mathbf{c}) = P\left(\sum_{i=1}^{n} r_{i,c_i} \geq \Delta n\right).$$

Clearly $E(r_{i,c_i}) = 1/q$. Like in the last section, we make a stochastic variable in the $[0,1]$ range,

$$X_i = \frac{1+r_{i,c_i}}{2},$$
$$E(X_i) = \frac{q+1}{2q},$$

and

$$\pi(\mathbf{c}) = P\left(\sum_{i=1}^{n} X_i \geq \frac{1+\Delta}{2}n\right).$$

Multiplying by the number of innocent users gives the theorem. ■

Theorem 4 (Asymptotic codes) *For any $q > t$, there is an asymptotic class of (t,ϵ)-secure codes with $\epsilon \to 0$ and rate given by*

$$R_t \approx \frac{D\left(\frac{t+1}{2t}||\frac{q+1}{2q}\right)}{q-1},$$

using Boneh-Shaw inner codes and random outer codes.

Proof: For asymptotic codes, $\epsilon_{\mathrm{I}} \to 0$ if $\Delta < 1/t$, so we can take $\Delta \approx 1/t$. Likewise, $\epsilon_{\mathrm{II}} \to 0$ if $\Delta > 1/q$ and

$$R_O < \frac{D\left(\frac{t+1}{2t}||\frac{q+1}{2q}\right)}{\log q}.$$

Since $R_I = \log q/(q-1)$, we get the theorem. ■

Theorem 5 (False accusations for AG codes) *Concatenating a $(r(q-1), q)$ BS-RS code with a $(n, 2^{R_O n}, \delta n)$ outer code using soft input list decoding with threshold Δ for the outer code, the probability of accusing an innocent user is*

$$\epsilon_{\mathrm{II}} \leq 2^{(R_O \log q - [1-t(1-\delta)]D(\sigma||1/2))n}, \quad (6)$$

where

$$\sigma = \frac{1}{2} + \frac{\Delta - t(1-\delta)}{2(1-t(1-\delta))}, \quad (7)$$

provided $\Delta > t(1-\delta)$.

Proof: We bound the probability $\pi(\mathbf{c})$ of accusing $\mathbf{c}$ when $\mathbf{c}$ is innocent, i.e.

$$\pi(\mathbf{c}) \leq P\left(\sum_{i=1}^{n} r_{i,c_i} \geq \Delta n\right).$$

An innocent user $\mathbf{c}$ can match a given pirate in at most $(1-\delta)n$ positions. Thus there are at most $t(1-\delta)n$ positions where $\mathbf{c}$ matches some pirate. For the purpose of a worst case analysis, we assume that $r_{i,c_i} = 1$ whenever c_i matches a pirate. There are at least $N = [1-t(1-\delta)]n$ positions $i_1, \ldots, i_N$, where $r_{i,j} = v_j$ is given by (1) with $F_j \sim F_{j-1}$. Thus we get

$$\pi(\mathbf{c}) \leq P\left(\sum_{j=1}^{N} r_{i_j,c_{i_j}} \geq \tau N\right),$$
$$N = [1-t(1-\delta)]n,$$
$$\tau = \frac{\Delta - t(1-\delta)}{1-t(1-\delta)}.$$

Clearly, τ increases in δ as well as in Δ.

When $F_j \sim F_{j-1}$, we have $E(F_j - F_{j-1}) = 0$. Setting $Y_j = (1 + r_{i_j,c_{i_j}})/2$, we get $E(Y_j) = 1/2$ and

$$\pi(\mathbf{c}) \leq P\left(\sum_{j=1}^{N} Y_j \geq \frac{1+\tau}{2}N\right),$$

The result follows. ■

		Hard dec. [5]	Random codes	Reed-Solomon
$\log M$	t	n	n	n
10	10	306 548 964	1 441 600	23 046 144
20	20	$6.44 \cdot 10^9$	13 000 000	260 840 448
20	100	$5.10 \cdot 10^{12}$	1 642 612 000	3 298 531 737 600
30	30	$4.09 \cdot 10^{10}$	48 412 000	8 589 672 448
30	150	$1.38 \cdot 10^{23}$	6 102 770 000	1 991 730 298 880

TABLE I

COMPARISON OF FINITE CONSTRUCTIONS OF THE TWO NEW SCHEMES AND THE ORIGINAL BONEH-SHAW CODE WITH IMPROVED ERROR ANALYSIS. THE ERROR RATE IS $\epsilon \leq 10^{-10}$.

	Random codes		AG codes		Old record
t	q	Rate	q	Rate	Rate
2	5	0.0180	9^2	$6.79 \cdot 10^{-4}$	0.0688 [5]
3	8	0.00466	19^2	$6.14 \cdot 10^{-5}$	0.000638 [1]
4	11	0.00187	32^2	$1.10 \cdot 10^{-5}$	
5	14	0.000930	49^2	$2.89 \cdot 10^{-6}$	

TABLE II

ASYMPTOTIC RATES FOR SOME CONSTRUCTIONS WITH BONEH-SHAW INNER CODE AND SOFT DECISSION DECODING.

Theorem 6 (Asymptotic codes) *For any $q > t$, there is an asymptotic class Boneh-Shaw codes with AG outer codes which are (t, ϵ)-secure with $\epsilon \to 0$ and rate given by*

$$R_t = \frac{R_O \log q}{q-1}, \tag{8}$$

where R_O solves

$$R_O = \frac{1 - t\left(R_O + \frac{1}{\sqrt{q}-1}\right)}{\log q} D\left(\frac{1+\alpha}{2} || \frac{1}{2}\right), \tag{9}$$

$$\alpha = \frac{1 - t^2\left(R_O + \frac{1}{\sqrt{q}-1}\right)}{t - t^2\left(R_O + \frac{1}{\sqrt{q}-1}\right)} > 0. \tag{10}$$

Proof: For asymptotic codes, $\epsilon_{\mathrm{I}} \to 0$ if $\Delta < 1/t$, so we can take $\Delta \approx 1/t$. Likewise, $\epsilon_{\mathrm{II}} \to 0$ if both $\Delta > t(1-\delta)$ and

$$R_O < \frac{1 - t(1-\delta)}{\log q} D(\sigma || 1/2).$$

Using AG codes with

$$R = 1 - \delta - \frac{1}{\sqrt{q}-1},$$

where q is an even prime power, we can get codes with R_O solving (9). The inner rate is $\log q/(q-1)$, thus giving the theorem. ∎

The number of pirates t, is a property of the resulting codes, whereas q is a control parameter chosen so as to maximise R_t. We have computed some asymptotic rates in Table II, by choosing q by trial and error, and solving (9) by fix point iteration.

Interestingly, both the bounds on ϵ_{I} and ϵ_{II} are independent of r, and hence we are going to choose $r = 1$ to minimise the length. In Table I, we compare lengths for the different variants. A similar comparison of asymptotic rates appears in Table II.

V. ON COMPLEXITY, CONCLUSIONS, OPEN PROBLEMS

The contribution of these paper is to show how the Boneh-Shaw fingerprinting scheme can be significantly improved by passing soft information from the inner to the outer decoder. The only existing scheme with comparable or better information rate is the Tardos scheme, which may unfortunately be subject to adverse selection (see [5]).

The decoding complexity is $O(M \log M)$ using random codes and linear search. This complexity is typical for collusion-secure codes, and the Tardos scheme also has this complexity. The only known schemes with better complexity are those using Guruswami-Sudan (GS) decoding for the outer code, such as [1]. Using outer codes with large distance, we may be able to get complexity $O(\log M)$, by Kötter-Vardy (KV) decoding [4], which is a soft-input variant of GS decoding. However, some adaptions will be required to make our codes work with KV decoding.

The best known lower bound on the length is $n = \Omega(t^2 \log(M/\epsilon))$ [6], this bound is also reached by the Tardos scheme [6] with a slight relaxation of the security definition. Our scheme with random codes has $n = \Theta(t^4 \log t)$, and with AG codes it becomes $n = \Omega(t^6 \log t)$, so improvements may be possible.

Another important open question is to adapt the scheme for KV decoding, which requires non-negative entries in the reliability matrix and a certain form for the threshold (linear in $||R||\sqrt{n}$). If the reliability matrix and the threshold can be adapted to be compatible with KV decoding, we would get a fingerprinting scheme with the best known decoding complexity and the best known information rate for this complexity.

REFERENCES

[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. *IEEE Trans. Inform. Theory*, 44(5):1897–1905, 1998. Presented in part at CRYPTO'95.

[3] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Trans. Inform. Theory*, 46(3):893–910, May 2000. Presented in part at CRYPTO'94.

[4] Ralf Koetter and Alexander Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 49(11):2809–2825, 2003.

[5] Hans Georg Schaathun. Binary collusion-secure codes: Comparison and improvements. Technical Report 275, Dept. of Informatics, University of Bergen, 2004. Also available at `http://www.ii.uib.no/~georg/sci/inf/coding/public/`.

[6] G. Tardos. Optimal probabilistic fingerprint codes. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, 2003. `http://www.renyi.hu/~tardos/fingerprint.ps`.

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