An improvement of discrete Tardos fingerprinting codes*

Koji Nuida[1], Satoshi Fujitsu[2], Manabu Hagiwara[13], Takashi Kitagawa[1], Hajime Watanabe[1], Kazuto Ogawa[2], Hideki Imai[14]

[1] Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Akihabara-Daibiru Room 1102, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo, 101-0021, Japan
Tel.: +81-3-5298-4722 Fax: +81-3-5298-4522
k.nuida@aist.go.jp

[2] Science & Technical Research Laboratories, Japan Broadcasting Corporation (NHK), 1-10-11 Kinuta, Setagaya-ku, Tokyo, 157-8510, Japan

[3] Center for Research and Development Initiative, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551, Japan

[4] Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551, Japan

Abstract

It has been known that the code lengths of Tardos's collusion-secure fingerprinting codes are of theoretically minimal order with respect to the number of adversarial users (pirates). However, the code lengths can be further reduced, as some preceding studies on Tardos's codes already revealed. In this article we improve a recent discrete variant of Tardos's codes, and give a security proof of our codes under an assumption weaker than the original assumption (Marking Assumption). Our analysis shows that our codes have significantly shorter lengths than Tardos's codes. For example, in a practical setting, the code lengths of our codes are about 3.01%, 4.28%, and 4.81% of Tardos's codes if the numbers of pirates are 2, 4, and 6, respectively.

1 Introduction

Recent development of computer and network technology has promoted trades of digital contents. This has increased not only convenience for both content servers and users, but also risks of the distributed contents being illegally copied and redistributed. Digital fingerprinting scheme is a solution for such problems, in which the content server embeds some user identification data into each content in advance and detect the redistributor (called a *pirate*) from the data embedded into the redistributed content. The object of this article is *fingerprinting codes* used for encoding the user identification data.

A *collusion attack* by more than one pirates is a typical attack (modification and erasure) to the embedded fingerprint codeword. A fingerprinting code is called *c-secure*, if it is secure against collusion attacks by at most c pirates, namely if it is equipped with a *tracing algorithm* which can output a pirate correctly with an overwhelming probability. The first construction of c-secure

*A part of this work was presented at 17th Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17), Bangalore, India, December 16–20, 2007.

codes for every c was given by Boneh and Shaw [2], where they introduced a certain assumption on the pirates' attack strategies called *Marking Assumption*. Then Tardos [8] proposed c-secure codes (under Marking Assumption) with highly probabilistic codeword generation algorithms. A characteristic of his codes is that by the tracing algorithm, closeness of each user's codeword to the codeword in the redistributed content is quantified as a "score" of each user and then users whose scores exceed a given threshold are output. His work is a milestone in this area because of the fact that code lengths of his c-secure codes are of theoretically minimal order (that is, $O(c^2)$) with respect to c.

After Tardos's work, there have been proposed several improvements of his codes. A direction investigated by Škorić et al. [7] concerns reduction of the code lengths by modifying the scoring function and by sharpening evaluation of error probability of the tracing algorithm. Another direction taken by Blayer and Tassa [1] concerns reduction of the code lengths by improving the parameter choice for Tardos codes. Moreover, a work by Nuida et al. [5, 6] (following Hagiwara et al. [3]) concerns implementation issues of the codes. Namely, they replaced the continuous probability distributions used in Tardos codes with certain finite (hence discrete) probability distributions, and proposed an appropriate way of approximating the scoring function, so that the resulting codes can be implemented by using smaller amount of memory and numbers explicitly representable on computers. In addition, their "discrete Tardos codes" also have shorter lengths than the original.

Our contribution in this article is a further improvement of the discrete Tardos codes in [5, 6], at the following points:

- Modification of the tracing algorithm: In contrast with the previous codes [3, 5, 6, 7, 8], our tracing algorithm outputs *only one* user having the highest score. This results in significant reduction of the error probability.
- Reduction of code lengths: It is deduced from our formula of code lengths that the lengths are reduced to less than or almost equal to $1/20$ of Tardos codes in many practical settings.
- Relaxation of Marking Assumption: Our security proof is given under an assumption weaker than the Marking Assumption, thus it covers more practical cases.

This article is organized as follows. Section 2 summarizes our models and assumptions on fingerprinting codes. In Section 3, we introduce the abovementioned relaxation of Marking Assumption, and describe our codeword generation algorithm and our tracing algorithm. In Section 4, we give our main results regarding the bound of error probabilities and the formula of code lengths of our codes. Section 5 deals with some numerical examples of our codes and their comparison with previous c-secure codes [6, 7, 8]. In Section 6, we investigate an asymptotic behavior of code lengths of our codes. Arguments in these two sections show that the lengths of our codes are significantly short. Finally, Section 7 is devoted to the proofs of our results given in Section 4.

2 Preliminary

2.1 A general model for fingerprinting codes

In this subsection, we give a general model for fingerprinting codes. A specialized model relevant to codes of our proposal will be shown in Section 2.2.

The players in our model are a *content server* (or a *server* in short) and a number (denoted by N) of *users*. The users are classified into two types; adversarial users called *pirates*, and the remaining users called *innocent users*. Let ℓ denote the number of pirates.

Before the codeword generation phase, first the server chooses in a probabilistic manner an auxiliary parameter P used in the remaining phases. This phase may be omitted when such a parameter P is not necessary.

In the codeword generation phase, the server generates a codeword of each user in a probabilistic manner which may depend on the above parameter P. In this article we assume that the codeword $w_i = (w_{i,1}, \dots, w_{i,m})$ of i-th user u_i is a binary sequence of the common length m. Then the server sends each codeword w_i to the corresponding user u_i by a certain way, e.g. by embedding w_i as a digital fingerprint into a digital content and sending it to the user u_i.

When the pirates receive their codewords, they create a new codeword (denoted by y) called a *pirated codeword* by an algorithm referred to as a *pirates' strategy*. It is generally possible that pirates not only modify their codewords but also erase some bits in them. To consider such attacks, we assume that the length of y is also m but y consists of symbols in a larger alphabet $\{0, 1, ?\}$, where '?' signifies an erased bit. The following two assumptions are standard so far in the research area of fingerprinting codes. The former one was first introduced by Boneh and Shaw [2], which is a consequence of a desired property of steganography used by the server. On the other hand, the latter has been implicitly put in most of the preceding works, and it represents a reasonable assumption that codewords of innocent users and the parameter P (if it exists) are kept secret for the pirates.

Definition 2.1 (Marking Assumption)**.** If the bits $w_{i_1,j}, \dots, w_{i_\ell,j}$ in the j-th position of codewords of the pirates $u_{i_1}, \dots, u_{i_\ell}$ $(1 \leq j \leq m)$ all coincide with each other (we call such a position *undetectable*), then the j-th bit y_j of the pirated codeword y also coincides with them.

Definition 2.2 (No Leakage Assumption)**.** The distribution of the pirated codeword y, conditioned on given pirates' codewords, is independent of both innocent users' codewords and the parameter P (if it exists).

Then the pirates distribute the pirated codeword y, e.g. by distributing copies of a pirated content involving a modified fingerprint that coincides with y.

Finally, after the server obtains the pirated codeword y (e.g. by finding a pirated content and extracting the embedded fingerprint), the server performs a *tracing algorithm* to detect the pirates. A tracing algorithm takes the pirated codeword y, the users' codewords and the parameter P (if it exists) as input, and outputs a (possibly empty) set of suspected users. A result of the algorithm is regarded as a *tracing error*, or an *error* in short, unless the list of suspects involves at least one pirate and no innocent user.

A *fingerprinting code* signifies a pair of a codeword generation algorithm (including a choice of parameter P, if it exists) and a tracing algorithm. We say that a fingerprinting code is *c-secure* (*with* ε*-error*) [2], if the probability of tracing error, taken over choices of users' codewords and parameter P (if it exists), does not exceed a negligibly small value ε whenever $\ell \leq c$.

2.2 A model relevant to our codes

Here we give a specialized model based on the one in Section 2.1, which is relevant to our fingerprinting codes proposed in this article. This model also covers Tardos codes [8] and its recent variants such as [3, 5, 6, 7].

In this specialized model, first the server prepares a probability distribution $\mathcal{P}$ with real values in the open interval $(0,1)$, which we refer to as a *bias distribution*. Then the parameter P is a sequence $(p^{(1)}, \dots, p^{(m)})$ of values $p^{(j)} \in (0,1)$ chosen independently according to $\mathcal{P}$. As is explained below, each $p^{(j)}$ signifies the frequency of 1s appearing in j-th positions of users' codewords. We refer to the parameter P as the *bias parameter*.

In the codeword generation phase, the server chooses each bit $w_{i,j}$ in users' codewords independently, with probability

$$Pr(w_{i,j} = 1) = p^{(j)} \text{ and } Pr(w_{i,j} = 0) = 1 - p^{(j)} \enspace .$$

Given a pirated codeword y, the tracing algorithm first calculates a score $S_i^{(j)}$ for j-th bit $w_{i,j}$ of i-th user u_i by a certain real-valued function, and then sums them up as the total score $S_i = \sum_{j=1}^{m} S_i^{(j)}$ of i-th user. Secondly, the algorithm compares the scores with an appropriately selected threshold Z, and picks up every user u_i with $S_i \geq Z$ as a candidate of the output. We let this model include the extreme case "$Z = -\infty$", where no user is exempted from the candidates. Finally, the algorithm selects a part of the candidate users in a certain manner and outputs every user in the selected part.

Example 2.3. In the case of Tardos codes [8], a certain continuous distribution is used as the bias distribution (see [8] for details). By introducing an auxiliary function $\sigma(p) = \sqrt{(1-p)/p}$, the scoring function in [8] is given by $S_i^{(j)} = \sigma(p^{(j)})$ if $(y_j, w_{i,j}) = (1,1)$, $S_i^{(j)} = -\sigma(1 - p^{(j)})$ if $(y_j, w_{i,j}) = (1,0)$, and $S_i^{(j)} = 0$ if $y_j \in \{0, ?\}$. Moreover, the tracing algorithm outputs every user whose score exceeds the threshold Z. In [8], the code length and the threshold are determined by $m = 100c^2 \lceil \log(N/\varepsilon) \rceil$ and $Z = 20c \lceil \log(N/\varepsilon) \rceil$. On the other hand, in a "discrete variant" of Tardos codes proposed by Hagiwara et al. in [3], the bias distribution is a finite (hence discrete) probability distribution with only a small number of possible values. Moreover, in a "symmetrized version" of Tardos codes proposed by Škorić et al. in [7], the scoring function is modified so that $S_i^{(j)} = \sigma(1 - p^{(j)})$ if $y_j \in \{0, ?\}$ and $w_{i,j} = 0$, $S_i^{(j)} = -\sigma(p^{(j)})$ if $y_j \in \{0, ?\}$ and $w_{i,j} = 1$, and $S_i^{(j)}$ is the same as the original otherwise.

Now we give a remark on comparison between tracing algorithms of the following two types. An algorithm of the first type outputs every user with the score exceeding a threshold Z (e.g. Tardos codes). On the other hand, an algorithm in the second type does not use a threshold (in other words, it is in the extreme case $Z = -\infty$) and outputs just one of the users with the highest score. Then we have the following result:

Proposition 2.4. *If all the remaining attributes are in common, the error probability of a fingerprinting code with a tracing algorithm of second type is not more than the error probability of a code with a tracing algorithm of first type.*

Proof. In the case that a tracing algorithm of the second type results in an error, an innocent user has the highest score, therefore we have either an innocent user's score exceeds a given threshold or no pirate's score exceeds the same threshold. Thus the corresponding tracing algorithm of the first type also results in an error in this case. Hence the proposition follows. □

3 Our proposal

This section summarizes our proposal; a relaxed version of Marking Assumption, a codeword generation algorithm, and an improved tracing algorithm. An appropriate choice of the code lengths together with a security proof of our codes will be given in later sections.

3.1 A relaxation of Marking Assumption

An issue of the Marking Assumption (Definition 2.1) is that fingerprint embedding schemes assuring this assumption strictly seem difficult to realize. From this viewpoint, we put the following relaxed version of Marking Assumption:

Definition 3.1 (δ-Marking Assumption)**.** The number of undetectable positions (see Definition 2.1 for terminology) in which y differs from the pirates' codewords is not more than $m\delta$, where m is the code length and $\delta \geq 0$ is a fixed parameter.

When $\delta = 0$, this assumption coincides with the Marking Assumption.

3.2 Our codeword generation algorithm

The following description of our codeword generation process is based on the model in Section 2.2. Thus it now suffices to determine the bias distribution. Here we introduce the following bias distribution $\mathcal{P}^{\mathrm{GL}} = \mathcal{P}_c^{\mathrm{GL}}$ for each c:

Definition 3.2. Let $L_k(t) = (\frac{d}{dt})^k (t^2-1)^k / (k!\, 2^k)$ be the k-th Legendre polynomial, and put $\widetilde{L}_k(t) = L_k(2t-1)$. Then we define $\mathcal{P}_{2k-1}^{\mathrm{GL}} = \mathcal{P}_{2k}^{\mathrm{GL}}$ to be the finite probability distribution whose values are the k zeroes of $\widetilde{L}_k$, with each value p taken with probability $C\big(p(1-p)\big)^{-3/2} \widetilde{L}_k{}'(p)^{-2}$, where C is the normalized constant making the sum of the probabilities equal to 1.

These bias distributions $\mathcal{P}_c^{\mathrm{GL}}$ were first introduced by a discrete variant [5, 6] of Tardos codes. In [5, 6], $\mathcal{P}_c^{\mathrm{GL}}$ are called "Gauss-Legendre distributions" due to their deep relation to the Gauss-Legendre quadrature in numerical approximation theory. It is shown in [5, 6] that $\mathcal{P}_c^{\mathrm{GL}}$ minimizes, among the bias distributions with certain desirable property, the memory amount required to record the bias parameter P, and that the code lengths are also reduced by using $\mathcal{P}_c^{\mathrm{GL}}$ instead of the continuous bias distributions for Tardos codes. This is the main reason of adopting the distributions $\mathcal{P}_c^{\mathrm{GL}}$ as our bias distributions.

We should note that the values and the corresponding emerging probabilities of $\mathcal{P}_c^{\mathrm{GL}}$ are not rational, therefore we need some approximation to implement these distributions on computer. Effects of such approximations will also be considered in our security proof. In this article, we assume the following condition on the bias distribution $\mathcal{P}$ approximating $\mathcal{P}_c^{\mathrm{GL}}$:

Definition 3.3. We say that a bias distribution $\mathcal{P}$ is *symmetric*, if $\mathcal{P}$ takes the values p and $1-p$ with the same probability for any $0 < p < 1$.

Note that the original $\mathcal{P}_c^{\mathrm{GL}}$ are also symmetric in this sense.

3.3 Our tracing algorithm

Our tracing algorithm is also defined along the model in Section 2.2. For the scoring rule, we put

$$\sigma(p) = \sqrt{(1-p)/p}$$

and define the bitwise scores $S_i^{(j)}$ by

$$S_i^{(j)} = \begin{cases} \sigma(p^{(j)}) & \text{if } y_j = 1 \text{ and } w_{i,j} = 1 \ , \\ -\sigma(1-p^{(j)}) & \text{if } y_j = 1 \text{ and } w_{i,j} = 0 \ , \\ -\sigma(p^{(j)}) & \text{if } y_j \in \{0, ?\} \text{ and } w_{i,j} = 1 \ , \\ \sigma(1-p^{(j)}) & \text{if } y_j \in \{0, ?\} \text{ and } w_{i,j} = 0 \ . \end{cases} \tag{1}$$

Note that this scoring rule was used in a preceding work [7] to reduce the code lengths of Tardos codes.

Then, instead of comparing users' scores with a threshold, our tracing algorithm simply outputs one of the users with the highest score. This modification is in fact an improvement, due to Proposition 2.4. Note that the way of choosing just one user from the users with the highest score may be arbitrarily designed, since our security proof covers any possible way for this choice.

Note that scores determined by the above rule are in general not explicitly representable on computer, therefore we also need some approximations of these values. For this purpose, we enumerate the values of the symmetric (in the sense of Definition 3.3) bias distribution $\mathcal{P}$ (which is either the distribution $\mathcal{P}_c^{\mathrm{GL}}$ itself or its approximation) in increasing order as $p_0, p_1, \dots, p_k$, and fix an approximated value U_i of each $\sigma(p_i)$. Now by the symmetry property of $\mathcal{P}$, we have $1 - p_i = p_{k-i}$, therefore the value U_{k-i} (denoted by U_i' for simplicity) is an approximated value of $\sigma(1-p_i)$. In this setting, we modify the above scoring rule (1) for bitwise scores as follows:

$$S_i^{(j)} = \begin{cases} U_\nu & \text{if } y_j = 1 \text{ and } w_{i,j} = 1 \ , \\ -U_\nu' & \text{if } y_j = 1 \text{ and } w_{i,j} = 0 \ , \\ -U_\nu & \text{if } y_j \in \{0, ?\} \text{ and } w_{i,j} = 1 \ , \\ U_\nu' & \text{if } y_j \in \{0, ?\} \text{ and } w_{i,j} = 0 \ , \end{cases} \quad \text{where } p^{(j)} = p_\nu \ . \tag{2}$$

Our security proof also consider the effects of this approximation.

4 Code lengths and error probabilities of our codes

For our codes proposed in Section 3, in this section we give a bound of tracing error probabilities and a formula of code lengths (Theorem 4.2), which show that our codes are c-secure. Proofs of the results will be provided in Section 7.

First, we present some notations and terminology. Let $\mathcal{P}$ be a symmetric bias distribution (see Definition 3.3), which is either the distribution $\mathcal{P}_c^{\mathrm{GL}}$ in Definition 3.2 or its approximation. Let $p_0, p_1, \dots, p_k$, U_i, and U_i' be as defined in the last paragraph of Section 3.3. Put

$$\eta = \sigma(p_0) \ .$$

Let

$$\delta' = \max_{0 \le i \le k} |\sigma(p_i) - U_i| = \max_{0 \le i \le k} |\sigma(1-p_i) - U_i'| \ ,$$

i.e. the bound of approximation errors of the bitwise scores. Then we define the *tolerance rate* Δ of our code by

$$\Delta = \delta' + 2\eta\delta \ ,$$

where the value δ is that appearing in δ-Marking Assumption (Definition 3.1). For each $1 \le \ell \le c$ and $0 \le x \le \ell$, put

$$\begin{aligned} R_{\ell,x} &= \max\{0, E\big[p^x(1-p)^{\ell-x}\big(x\sigma(p) - (\ell-x)\sigma(1-p)\big)\big]\} \ , \\ \mathcal{R}_\ell &= \ell E\Big[(1-p)^{\ell-1/2}p^{1/2}\Big] - \sum_{x=1}^{\ell-1}\binom{\ell}{x} R_{\ell,x} \ , \end{aligned}$$

where the expectation values $E[\cdot]$ are taken over the values p of $\mathcal{P}$. Then fix a value $\mathcal{R}$ such that $2c\Delta \le \mathcal{R} \le \mathcal{R}_\ell$ for all $1 \le \ell \le c$. Moreover, define the following functions

$$\begin{aligned} B_1(t) &= \frac{e^{t\eta} + \eta^2 e^{-t/\eta}}{\eta^2+1} \ , \ B_{2,\ell}(t) = 1 + \frac{e^{t\ell\eta} - 1 - t\ell\eta}{\ell\eta^2} - 2t\mathcal{R} \ , \\ \Phi(t) &= t(1 - \log t) \ , \end{aligned}$$

where log denotes the natural logarithm, and put

$$T_\ell = B_1(\beta\ell)B_{2,\ell}(\beta)e^{2\beta\ell\Delta} \text{ for each } 1 \le \ell \le c \ ,$$

where $\beta > 0$ is an appropriately chosen parameter (see below). These functions have the following properties, from which it follows that the values T_ℓ are positive and bounded below from zero. The proofs will be given in Section 7.

Lemma 4.1. *1. For $t > 0$, $B_1(t)$ is an increasing function and $B_1(t) > 1$.*

2. For each $1 \le l \le c$, the function $B_{2,\ell}(t)$ $(t > 0)$ takes the minimum value at $t = (\ell\eta)^{-1}\log(1 + 2\mathcal{R}\eta)$, and $B_{2,\ell}(t) > 1/2$.

Now our bound of error probabilities and our formula of code lengths are summarized as follows. The proofs will be given in Section 7. Moreover, some numerical examples concerning this result will be provided in Section 5.

Theorem 4.2. *Let $0 < \varepsilon < 1$, and choose $\beta > 0$ so that $N{T_c}^m < 1$. Let ℓ be the number of pirates. We put δ-Marking Assumption (Definition 3.1) and No Leakage Assumption (Definition 2.2).*

1. *If $\ell \leq c$, $T_c \leq T_0$ and $N{T_0}^m < 1$, then the tracing error probability of our code, using the scoring rule (2) instead of (1), is not more than $\Phi(N{T_0}^m)$. Hence our code is c-secure with ε-error if $\Phi(N{T_0}^m) \leq \varepsilon$.*

2. *Let $a > 1$ such that $\varepsilon \leq ae^{1-a}$ (e.g. $a = 10/9$ for $\varepsilon \leq 0.99$). Then our code is c-secure with ε-error if the code length satisfies that*

$$m \geq -\frac{1}{\log T_c}\left(\log\frac{N}{\varepsilon} + \log\frac{a}{a-1} + \log\log\frac{a}{\varepsilon}\right) \tag{3}$$

(note that $T_c < 1$ by our assumption, therefore $-(\log T_c)^{-1} = |\log T_c|^{-1}$).

This result implies that, for the sake of reducing code lengths, the parameter β should be chosen so that the value T_c becomes as small as possible (note that the function $\Phi(t)$ is increasing for $0 < t < 1$). Since it seems very difficult to determine the optimal value β_{optimal} of the parameter β for a general case, here we instead give (by a heuristic approach) a simple formula β_{formula} of nearly optimal values of β. The definition of β_{formula} is

$$\beta_{\text{formula}} = \frac{1}{\eta^2 j_1}\log\left(1 + \frac{2\eta}{c}(\mathcal{R} - \eta j_1 \Delta)\right) \quad , \tag{4}$$

where

$$j_1 = 2.40482\cdots \tag{5}$$

denotes the smallest positive zero of the 0th-order Bessel function $J_0(t) = \sum_{i=0}^{\infty}(-1)^i(t/2)^{2i}/(i!)^2$ of the first kind. The examples in Section 5 suggest that the formula (4) is "pretty good", though it is not optimal.

The asymptotic behavior of the code lengths of our codes will be investigated in Section 6.

5 Numerical examples

This section is devoted to numerical examples of our c-secure codes, where c varies as $c = 2$, 3, 4, 6, and 8, and to comparison of our codes with previously proposed c-secure codes [5, 6, 7, 8].

5.1 Approximations of bias distributions and scoring functions

The former part of Table 1 shows an approximation $\mathcal{P}$ of the bias distribution $\mathcal{P}_c^{\text{GL}}$ for each c, where columns entitled 'p' and 'q' denote, respectively, the values of $\mathcal{P}$ and the emerging probabilities of the corresponding values. Note that these distributions $\mathcal{P}$ are symmetric in the sense of Definition 3.3. Moreover, approximations U_i of values of the function σ are given in the latter part of Table 1. Now the bound δ' of the approximation error is $\delta' = 0$ for $c \leq 2$, and $\delta' = 10^{-5}$ for $c \geq 3$. Table 2 shows approximations of the values of $\mathcal{R}$ and η.

Table 1: Approximations of the bias distributions $\mathcal{P}_c^{\mathrm{GL}}$ and bitwise scores

c	p	q	c	p	q
$1,2$	0.50000	1.00000	$7,8$	0.06943	0.24833
$3,4$	0.21132	0.50000		0.33001	0.25167
	0.78868	0.50000		0.66999	0.25167
$5,6$	0.11270	0.33201		0.93057	0.24833
	0.50000	0.33598			
	0.88730	0.33201			

c	U_0	U_1	U_2	U_3
2	1			
4	1.93187	0.51763		
6	2.80590	1	0.35639	
8	3.66101	1.42485	0.70182	0.27314

Table 2: Auxiliary values for our examples

c	2	3	4	6	8
$\mathcal{R}$	0.50000	0.40823	0.40823	0.37796	0.36291
η	1.00000	1.93188	1.93188	2.80591	3.66102

5.2 Calculation of code lengths

Table 3 shows the code lengths of our codes under δ-Marking Assumption (Definition 3.1). Here we set the tolerance late $\Delta = \delta' + 2\eta\delta$ to 0.01; namely, our codes are still c-secure even if $m\delta \approx m/(200\eta)$ bits in undetectable positions are flipped or erased. In the table, we consider the following three cases:

- Case 1: $N = 100c$ and $\varepsilon = 10^{-11}$,
- Case 2: $N = 10^9$ and $\varepsilon = 10^{-6}$,
- Case 3: $N = 10^6$ and $\varepsilon = 10^{-3}$.

In this example, we calculate the code lengths by using the first part of Theorem 4.2 and a numerical calculation, instead of a slightly looser formula (3) in the second part of Theorem 4.2. The code length shown in the first row for each c in Table 3 is calculated by using the optimal value β_{optimal} determined by a numerical search. On the other hand, the code length in the second row for each c in Table 3 is derived by using the formula (4) instead of β_{optimal}. This table shows that the code lengths derived from (4) are not very apart from the ones derived from β_{optimal}, namely the formula (4) is a good approximation of β_{optimal}.

A similar table (Table 4) is also given for the case under the Marking Assumption instead of the δ-Marking Assumption (or equivalently, Table 4 deals with the case that $\delta = 0$). Again, the code lengths derived from the parameters in (4) are not very apart from the ones derived from β_{optimal}.

5.3 Comparison of our code lengths with other codes

Tables 3 and 4 also show the code lengths $100c^2\lceil\log(N/\varepsilon)\rceil$ of Tardos codes [8] for the same settings (except that the lengths of Tardos codes for the cases in Table 3

Table 3: Length comparison under δ-Marking Assumption (where $\Delta = 0.01$) Values in parentheses are code lengths calculated by using β_{formula} instead of β_{optimal}.

c		Case 1	Case 2	Case 3	Case 4	β_{optimal}
2	Ours	**403** (404)	**444** (444)	**273** (274)		0.16921
	Tardos	12400	14000	8400		
	%	**3.25**	**3.17**	**3.25**	**2.97**	
3	Ours	**1514** (1630)	**1646** (1771)	**1014** (1091)		0.057404
	Tardos	28800	31500	18900		
	%	**5.26**	**5.23**	**5.37**	**4.89**	
4	Ours	**2671** (2672)	**2879** (2880)	**1774** (1775)		0.034093
	Tardos	51200	56000	33600		
	%	**5.22**	**5.14**	**5.28**	**4.81**	
6	Ours	**7738** (7743)	**8244** (8249)	**5079** (5082)		0.013798
	Tardos	115200	126000	75600		
	%	**6.72**	**6.54**	**6.72**	**6.13**	
8	Ours	**16920** (16934)	**17879** (17894)	**11015** (11024)		0.0071633
	Tardos	211200	224000	134400		
	%	**8.01**	**7.98**	**8.20**	**7.47**	

Table 4: Length comparison under Marking Assumption (here $\Delta = \delta'$) Values in parentheses are code lengths calculated by using β_{formula} instead of β_{optimal}.

c		Case 1	Case 2	Case 3	Case 4	β_{optimal}
2	Ours	**373** (374)	**410** (411)	**253** (253)		0.17549
	Tardos	12400	14000	8400		
	%	**3.01**	**2.93**	**3.01**	**2.74**	
3	Ours	**1309** (1390)	**1423** (1511)	**877** (931)		0.061345
	Tardos	28800	31500	18900		
	%	**4.55**	**4.52**	**4.64**	**4.23**	
4	Ours	**2190** (2190)	**2360** (2360)	**1454** (1454)		0.037405
	Tardos	51200	56000	33600		
	%	**4.28**	**4.21**	**4.33**	**3.95**	
6	Ours	**5546** (5547)	**5909** (5909)	**3640** (3641)		0.016111
	Tardos	115200	126000	75600		
	%	**4.81**	**4.69**	**4.81**	**4.39**	
8	Ours	**10469** (10469)	**11062** (11062)	**6815** (6816)		0.0089586
	Tardos	211200	224000	134400		
	%	**4.96**	**4.94**	**5.07**	**4.62**	

are derived under Marking Assumption instead of δ-Marking Assumption), and the percentages of our code lengths relative to those of Tardos codes. Moreover, we also give (as "Case 4") the percentages in the limit case $N/\varepsilon \to \infty$ (i.e. $N \to \infty$ or $\varepsilon \to 0$). For the limit case, we use the formula (3) for code lengths of our codes, therefore the percentage $m/\bigl(c^2\lceil\log(N/\varepsilon)\rceil\bigr)$ converges to $-\bigl(c^2\log T_c\bigr)^{-1} = \bigl(c^2|\log T_c|\bigr)^{-1}$ when $N/\varepsilon \to \infty$. These two tables show that our codes have much shorter code lengths than Tardos codes. Moreover, our code lengths are also significantly shorter than a preceding improvement [5, 6] of Tardos codes. In fact, numerical examples in [5, 6] show that the code lengths in [5, 6] are more than 30% of those of Tardos codes for $c \leq 8$.

On the other hand, it is proved in [7] that the code lengths of Tardos codes (under Marking Assumption) can be reduced to $\pi^2/2\% \approx 4.93\%$ of the original by using the symmetrized scoring rule (1), *provided we put a certain statistical assumption on distributions of innocent users' scores* (see [7] for details). It is worth noticing that, despite the *unconditional* security of our codes (that is, our security proof holds without such a statistical assumption), our code lengths shown in Tables 3 and 4 are almost the same as, or even shorter than, the lengths given in [7] (i.e. 4.93% of Tardos codes) for many cases. Moreover, the *unconditionally* c-secure code lengths given in [7] are $\pi^2\% \approx 9.87\%$ of lengths of Tardos codes, and our code lengths are shorter than their code lengths for every case shown in the two tables.

6 Asymptotic behavior of our code lengths

In this section, we investigate an asymptotic behavior of code lengths m of our c-secure codes in the limit case $c \to \infty$. More precisely, we show that $m \sim Kc^2\log(N/\varepsilon)$ for some $K < \infty$ when $c \to \infty$, and determine the constant factor K (Theorem 6.3). Note that the factor K is 100 for Tardos codes.

6.1 The results

In our analysis, we use the following asymptotic properties of the bias distributions $\mathcal{P}_c^{\mathrm{GL}}$, which are proved in [5]:

Lemma 6.1 ([5]). *If $\mathcal{P} = \mathcal{P}_c^{\mathrm{GL}}$, then $\mathcal{R} = \min_{1\leq\ell\leq c}\mathcal{R}_\ell \to 1/\pi$ and $\eta/c \to 1/j_1$ when $c \to \infty$, where j_1 is as defined in (5).*

Following Lemma 6.1, we choose an approximation $\mathcal{P}$ of $\mathcal{P}_c^{\mathrm{GL}}$ for each c such that $\mathcal{R} \to 1/\pi$, $\eta/c \to 1/j_1$ and $c\Delta \to \Delta_0$ when $c \to \infty$, where $0 \leq \Delta_0 < \infty$. (Although the values $\mathcal{R}$, η and Δ depend on c, we omit subscripts 'c' in the notations for simplicity.) In particular, $\eta \to \infty$ when $c \to \infty$. Note that $\Delta_0 \leq (2\pi)^{-1}$ by our assumption $2c\Delta \leq \mathcal{R}$ for each c (see Section 4).

We use the formula (3) for code lengths and the formula (4) for the parameter β. Now we have $N/\varepsilon \to \infty$ when $c \to \infty$, since $\varepsilon \leq 1$ and $N \geq c$. Thus by (3), the ratio $m/\bigl(c^2\log(N/\varepsilon)\bigr)$ converges (when $c \to \infty$) to the same value as the limit of $-1/\bigl(c^2\log T_c\bigr)$, whenever the latter converges. Since

$$c^2\log T_c = c^2\log B_1(\beta c) + c^2\log B_{2,c}(\beta) + 2\beta c^3\Delta \ ,$$

it suffices to calculate the limit of each term in the right-hand side. Now put

$$A = 1 + \frac{2\eta}{c}(\mathcal{R} - \eta j_1 \Delta) \text{ and } A_0 = 1 + \frac{2}{j_1}\left(\frac{1}{\pi} - \Delta_0\right) \quad ,$$

therefore $A \to A_0 > 1$ when $c \to \infty$. Then for the third term, we have

$$2\beta c^3 \Delta = \frac{c^2}{\eta^2} \cdot \frac{2c\Delta}{j_1} \log A \to 2 j_1 \Delta_0 \log A_0 \text{ when } c \to \infty \quad .$$

In the remaining argument, we use the following lemma, which will be proved in Section 6.2:

Lemma 6.2. *Let $f(c)$ and $g(c)$ be real-valued functions.*

1. *If $c^2(f(c) - 1) \to a \in \mathbb{R}$ when $c \to \infty$, then $c^2 \log f(c) \to a$ when $c \to \infty$.*
2. *If $f(c) \to a$ and $g(c) \to 0$ when $c \to \infty$, $0 < a < \infty$, and $g(c) \neq 0$ for all sufficiently large c, then $(f(c)^{g(c)} - 1)/g(c) \to \log a$ when $c \to \infty$.*

Owing to the first part of Lemma 6.2, it now suffices to determine the limit of the values $c^2(B_1(\beta c) - 1)$ and $c^2(B_{2,c}(\beta) - 1)$. First, we have

$$c^2(B_1(\beta c) - 1) = \frac{c^2}{\eta^2} \cdot \frac{\eta^2}{\eta^2 + 1}\left(A^{c/(\eta j_1)} - 1 - \frac{c}{\eta j_1} \cdot \frac{A^{-c/(\eta^3 j_1)} - 1}{-c/(\eta^3 j_1)}\right) \quad .$$

Since $A \to A_0 > 1$ when $c \to \infty$, the second part of Lemma 6.2 implies that

$$\lim_{c\to\infty} c^2(B_1(\beta c) - 1) = {j_1}^2 \cdot 1 \cdot ({A_0}^0 - 1 - 1 \cdot \log A_0) = {j_1}^2(A_0 - 1 - \log A_0)$$

(recall that $\eta \to \infty$ when $c \to \infty$). On the other hand, we have

$$c^2(B_{2,c}(\beta) - 1) = \frac{c}{\eta} \cdot \frac{1}{\eta}\left(A^{c/(\eta j_1)} - 1 - \frac{c}{\eta j_1} \log A\right) - \frac{c^2}{\eta^2} \cdot \frac{2\mathcal{R}}{j_1} \log A \quad .$$

Since $A^{c/(\eta j_1)} - 1 - (\eta j_1)^{-1} c \log A$ is bounded when $c \to \infty$, we have

$$\lim_{c\to\infty} c^2(B_{2,c}(\beta) - 1) = 0 - {j_1}^2 \cdot \frac{2/\pi}{j_1} \log A_0 = -\frac{2j_1}{\pi} \log A_0 \quad .$$

Hence by the first part of Lemma 6.2, we have

$$\begin{aligned} \lim_{c\to\infty} c^2 \log T_c &= {j_1}^2(A_0 - 1 - \log A_0) - \frac{2j_1}{\pi} \log A_0 + 2j_1 \Delta_0 \log A_0 \\ &= -{j_1}^2(A_0 \log A_0 - A_0 + 1) \ , \end{aligned}$$

therefore $\lim_{c\to\infty} m/\big(c^2 \log(N/\varepsilon)\big) = {j_1}^{-2}(A_0 \log A_0 - A_0 + 1)^{-1}$. The right-hand side is a decreasing function of $A_0 > 1$, therefore an increasing function of $\Delta_0 \geq 0$. Hence it is optimal for decreasing the value to set $\Delta_0 = 0$.

Summarizing, we have the following result (assuming Lemma 6.2):

Theorem 6.3. *In this setting, by putting $A_0 = 1 + 2/(j_1 \pi)$ where j_1 is as defined in (5), the asymptotic behavior of lengths m of our codes is given by*

$$m \sim K c^2 \log(N/\varepsilon) \text{ where } K = \frac{1}{{j_1}^2(A_0 \log A_0 - A_0 + 1)} \approx 5.35310\cdots \quad .$$

As a comparison with other codes, the constant factor K is $K = 100$ for Tardos codes [8], $K \approx 20.6021$ for codes in [5], $K \approx 20$ for codes in [1], and $K \approx 9.87$ for codes in [7]. Theorem 6.3 shows that our asymptotic code lengths are significantly shorter than those for the above codes. Note also that $K \approx 4.93$ for codes in [7] under a certain statistical assumption (cf. Section 5.3), and that our asymptotic ratios are close to that value though our security proof does not require such an additional assumption.

6.2 Proof of Lemma 6.2

Here we give a proof of Lemma 6.2 to complete the proof of Theorem 6.3.

of Lemma 6.2. For the first part of Lemma 6.2, note that $f(c) \to 1$ when $c \to \infty$ since $c^2(f(c) - 1)$ is bounded. First, if the set $f^{-1}(1) = \{c \mid f(c) = 1\}$ is bounded, then we have $c^2 \log f(c) = c^2(f(c) - 1) \cdot (f(c) - 1)^{-1} \log f(c)$ for all sufficiently large c, and $\lim_{c\to\infty}(f(c)-1)^{-1} \log f(c) = \lim_{x\to 1}(x-1)^{-1} \log x = 1$ by L'Hôpital's Rule, therefore our claim follows. Secondly, if the set $f^{-1}(1)$ is not bounded, then a must be 0, since there is an infinite sequence $c_1, c_2, \dots$ diverging to ∞ such that $f(c_i) = 1$ for all i. Now we define another function $\overline{f}(c)$ by $\overline{f}(c) = f(c)$ if $f(c) \neq 1$ and $\overline{f}(c) = e^{c^{-3}}$ if $f(c) = 1$. This function satisfies that $\overline{f}(c) \neq 1$ for any c and $c^2(\overline{f}(c) - 1) \to 0$ when $c \to \infty$, since $c^2(e^{c^{-3}} - 1) = (e^{c^{-3}} - 1)/c^{-2} \to 0$ when $c \to \infty$ by L'Hôpital's Rule. Thus $c^2 \log \overline{f}(c) \to 0$ when $c \to \infty$ by the above argument, while we have $c^2 \log f(c) = 0$ if $f(c) = 1$. Hence we have $c^2 \log f(c) \to 0$ when $c \to \infty$, therefore our claim follows.

From now, we prove the second part of Lemma 6.2. First note that, if $f(c)$ is constantly equal to a, then we have

$$\lim_{c\to\infty}(f(c)^{g(c)} - 1)/g(c) = \lim_{x\to 0}(a^x - 1)/x = \log a$$

by L'Hôpital's Rule. Now for a general case, for any $0 < \lambda < a$, we have $0 < a - \lambda < f(c) < a + \lambda$ for all sufficiently large c since $f(c) \to a$ when $c \to \infty$. This implies that

$$\frac{(a-\lambda)^{g(c)} - 1}{g(c)} < \frac{f(c)^{g(c)} - 1}{g(c)} < \frac{(a+\lambda)^{g(c)} - 1}{g(c)} \tag{6}$$

for any sufficiently large c. By the above argument, the left-hand side and the right-hand side of (6) converge to $\log(a - \lambda)$ and $\log(a + \lambda)$, respectively, when $c \to \infty$. Thus

$$\log(a - \lambda) \le \liminf_{c\to\infty} \frac{f(c)^{g(c)} - 1}{g(c)} \le \limsup_{c\to\infty} \frac{f(c)^{g(c)} - 1}{g(c)} \le \log(a + \lambda) \ . \tag{7}$$

By taking the limit $\lambda \to 0$, both the left-hand side and the right-hand side converge to $\log a$, therefore the middle two terms are both equal to $\log a$. This means that $(f(c)^{g(c)} - 1)/g(c)$ also converges to $\log a$.

Hence the proof of Lemma 6.2 is concluded. □

7 Proofs of results in Section 4

In this section, we give the proofs of our results in Section 4. First, in Section 7.1 we prove Lemma 4.1. Secondly, in order to prove Theorem 4.2, we present in Section 7.2 a key lemma for the proof, and we show in Section 7.3 some properties of distributions of the users' scores. Section 7.4 is the body of the proof of Theorem 4.2. Finally, in Section 7.5, we give a proof of the key lemma presented in Section 7.2.

7.1 Proof of Lemma 4.1

In this subsection, we prove Lemma 4.1. The first part of Lemma 4.1 can be proved by an easy analysis. Namely, we have $B_1'(t) = \eta(e^{t\eta} - e^{-t/\eta})/(\eta^2+1) > 0$ for $t > 0$ since $\eta > 0$, therefore $B_1(t)$ is increasing for $t > 0$, and $B_1(t) > B_1(0) = 1$ for $t > 0$.

From now, we prove the second part of Lemma 4.1. The first claim, namely $B_{2,\ell}(t)$ takes the minimum value for $t > 0$ at $t = t_0 = (\ell\eta)^{-1}\log(1 + 2\mathcal{R}\eta)$, is proved by a straightforward analysis. For the remaining claim, it suffices to show that $B_{2,\ell}(t_0) > 1/2$. We have

$$B_{2,\ell}(t_0) = 1 + \frac{4\mathcal{R}^2}{\ell} f(s) \text{ , where } f(t) = \frac{t - (1+t)\log(1+t)}{t^2} \text{ and } s = 2\mathcal{R}\eta \ .$$

Now we use the following two lemmas:

Lemma 7.1. *We have $f(t) > -1/2$ for $t > 0$.*

Proof. First, by putting $g(t) = (t+2)\log(t+1) - 2t$, a direct calculation implies that $f'(t) = g(t)t^{-3}$. Now we have $g'(t) = \log(t+1) + (t+1)^{-1} - 1$ and $g''(t) = (t+1)^{-1} - (t+1)^{-2} > 0$ for $t > 0$, therefore $g'(t) > g'(0) = 0$ for $t > 0$ and $g(t) > g(0) = 0$ for $t > 0$. Thus $f(t)$ is increasing for $t > 0$. Moreover, we have $\lim_{t\to 0} f(t) = -1/2$ by applying L'Hôpital's Rule twice. Hence the claim follows. □

Lemma 7.2. *We have $\mathcal{R} \leq 1/2$.*

Proof. Recall our assumption given in Section 4 that $2c\Delta \leq \mathcal{R} \leq \mathcal{R}_{\ell'}$ for all $1 \leq \ell' \leq c$. In particular, $\mathcal{R} \leq \mathcal{R}_1 = E\big[(1-p)^{1/2}p^{1/2}\big]$. Now the claim follows from the fact that $\sqrt{(1-p)p} \leq 1/2$ for any $0 < p < 1$. □

By these two lemmas, we have $B_{2,\ell}(t_0) > 1 + (1/\ell)\cdot(-1/2) \geq 1/2$ (note that $2\mathcal{R}\eta > 0$). Hence the proof of Lemma 4.1 is concluded.

7.2 A key lemma

In this subsection, we present the following inequality regarding two random variables, which will be a key ingredient of our proof of Theorem 4.2:

Lemma 7.3. *Let g_1 and g_2 be two real-valued random variables on the same probability space, and $G(x) = Pr(g_2 \leq x)$ ($x \in \mathbb{R}$) the distribution function of g_2. Suppose that we are given a weakly decreasing function $\varphi : \mathbb{R} \to \mathbb{R}_{\geq 0}$ (where $\mathbb{R}_{\geq 0}$ denotes the set of nonnegative real numbers) and a right-continuous, weakly increasing function $F : \mathbb{R} \to \mathbb{R}_{\geq 0}$ satisfying the following conditions:*

1. *we have $G(x) \leq F(x)$ for all $x \in \mathbb{R}$, and $\lim_{x\to-\infty} F(x) = 0$,*

2. for any finite closed interval $I \subset \mathbb{R}$ and any $\varepsilon' > 0$, there exists a $\kappa > 0$ such that $Pr(g_1 \geq x_1 \mid x_1 \leq g_2 < x_2) \leq \varphi(x_1) + \varepsilon'$ whenever $x_1, x_2 \in I$, $0 < x_2 - x_1 < \kappa$ and $Pr(x_1 \leq g_2 < x_2) > 0$.

Then $Pr(g_1 \geq g_2) \leq \int_{\mathbb{R}} \varphi \, dF$, where the integral in the right-hand side is the Lebesgue-Stieltjes integral (see e.g. [4]) with respect to the function F.

The proof of this lemma will be given in Section 7.5.

7.3 Lemmas on distributions of users' scores

In this subsection, we give two lemmas concerning distributions of the scores of users in our codes, which will be used in our proof of Theorem 4.2. These lemmas and their proofs presented below are based on the ones for similar properties given in [3, 6, 8].

Our first lemma concerns the scores of innocent users:

Lemma 7.4. *Let u_i be an innocent user, and $z \in \mathbb{R}$. Then for any fixed bias parameter P, any pirated codeword y, and any $\alpha > 0$, the score S_i of u_i calculated by the rule (1) satisfies*

$$\begin{aligned} Pr(S_i \geq z \mid P, y) &= Pr(e^{\alpha S_i} \geq e^{\alpha z} \mid P, y) \\ &\leq E\big[e^{\alpha S_i} \mid P, y\big]\, e^{-\alpha z} \leq B_1(\alpha)^m e^{-\alpha z} \ , \end{aligned}$$

where the conditional probabilities and the conditional expectation are taken over choices of the codeword w_i of the user u_i.

Proof. The first equality in the statement is obvious, while the former of the two inequalities is derived from Markov's Inequality. For the latter of the two inequalities, since each bit in w_i is chosen independently of each other, we have $E\big[e^{\alpha S_i} \mid P, y\big] = \prod_{j=1}^{m} E\Big[e^{\alpha S_i^{(j)}} \mid P, y\Big]$. Now we define a function $f(t)$ for $0 < t < 1$ by $f(t) = te^{\alpha\sqrt{(1-t)/t}} + (1-t)e^{-\alpha\sqrt{t/(1-t)}}$. Note that $E\Big[e^{\alpha S_i^{(j)}} \mid P, y\Big]$ is equal to $f(p^{(j)})$ if $y_j = 1$ and to $f(1 - p^{(j)})$ if $y_j \in \{0, ?\}$. By putting $\lambda = \alpha/\sqrt{t(1-t)}$, a straightforward calculation shows that

$$f'(t) = \frac{e^{-\alpha\sqrt{t/(1-t)}}}{2}\big((2-\lambda)e^{\lambda} - 2 - \lambda\big)$$

(note that $\sqrt{(1-t)/t} = \lambda/\alpha - \sqrt{t/(1-t)}$), while an elementary analysis implies that $(2-\lambda)e^{\lambda} - 2 - \lambda < 0$ for any $\lambda > 0$. Thus $f'(t) < 0$ for $0 < t < 1$, therefore $f(p^{(j)}) \leq f(p_0)$ and $f(1 - p^{(j)}) \leq f(p_0)$ since $p^{(j)} \geq p_0$ and $1 - p^{(j)} \geq p_0$ by the assumption that $\mathcal{P}$ is symmetric (see Definition 3.3). Finally, we have $f(p_0) = B_1(\alpha)$ by the choice of η. Hence the claim follows. $\square$

On the other hand, our second lemma concerns the scores of the pirates:

Lemma 7.5. *Fix an arbitrary pirates' strategy satisfying Marking Assumption. Let S_i denote the score of a pirate u_i calculated by the rule (1). Let S_{pmax} denote the maximum of the S_i among the ℓ pirates u_i, and S_{psum} denote the sum of the ℓ scores S_i. Then for any $z \in \mathbb{R}$ and any $\alpha > 0$, we have*

$$\begin{aligned} Pr(S_{\mathrm{pmax}} \leq z) \leq Pr(S_{\mathrm{psum}} \leq \ell z) &= Pr(e^{-\alpha S_{\mathrm{psum}}} \geq e^{-\alpha \ell z}) \\ &\leq E\big[e^{-\alpha S_{\mathrm{psum}}}\big]\, e^{\alpha \ell z} \leq B_{2,\ell}(\alpha)^m e^{\alpha \ell z} \ , \end{aligned}$$

where the probabilities and the expectation are taken over choices of the bias parameter P, the pirates' codewords w_i, and the pirated codeword y.

Proof. The claim except the last inequality $E\left[e^{-\alpha S_{\mathrm{psum}}}\right] e^{\alpha \ell z} \leq B_{2,\ell}(\alpha)^m e^{\alpha \ell z}$ follows from Markov's Inequality and easy arguments. In order to prove the above inequality, we investigate the value $E\left[e^{-\alpha S_{\mathrm{psum}}}\right]$. In this proof, we assume for simplicity that $u_1, \dots, u_\ell$ are the ℓ pirates.

By No Leakage Assumption (Definition 2.2), the fixed (probabilistic) pirates' strategy satisfies that $Pr(y \mid w, P) = Pr(y \mid w)$ for any bias parameter P, any collection $w = (w_i)_i$ of the pirates' codewords, and any pirated codeword y. Thus we have $Pr(P, w, y) = Pr(P) Pr(w \mid P) Pr(y \mid w)$, therefore

$$E\left[e^{-\alpha S_{\mathrm{psum}}}\right] = \sum_w \sum_y E_{(P)}\left[e^{-\alpha S_{\mathrm{psum}}} Pr(w \mid P)\right] Pr(y \mid w) \ , \tag{8}$$

where $E_{(P)}[\cdot]$ denotes the expectation value taken over choices of P.

Put $x_j = \#\{i \in \{1, \dots, \ell\} \mid w_{i,j} = 1\}$ for each $1 \leq j \leq m$. Then, since each $w_{i,j}$ depends solely on $p^{(j)}$ and is chosen independently of each other, we have

$$\begin{aligned} e^{-\alpha S_{\mathrm{psum}}} Pr(w \mid P) &= e^{-\alpha \sum_{j=1}^m \sum_{i=1}^\ell S_i^{(j)}} \prod_{j=1}^m \prod_{i=1}^\ell Pr(w_{i,j} \mid p^{(j)}) \\ &= \prod_j \left(e^{-\alpha \sum_i S_i^{(j)}} (p^{(j)})^{x_j} (1 - p^{(j)})^{\ell - x_j}\right) \ . \end{aligned}$$

Since the j-th term of the product in the right-hand side depends on $p^{(j)}$ but not on $p^{(j')}$ for other j', and each $p^{(j)}$ is chosen independently according to the same bias distribution $\mathcal{P}$, we have (for any w and y)

$$E_{(P)}\left[e^{-\alpha S_{\mathrm{psum}}} Pr(w \mid P)\right] = \prod_{j=1}^m E_{(p^{(j)})}\left[e^{-\alpha \sum_i S_i^{(j)}} (p^{(j)})^{x_j} (1 - p^{(j)})^{\ell - x_j}\right] \ ,$$

where $E_{(p^{(j)})}[\cdot]$ denotes the expectation value taken over the values $p^{(j)}$ of $\mathcal{P}$. Now note that $\sum_i S_i^{(j)} = \mathcal{L}_{x_j, p^{(j)}}$ if $y_j = 1$ and $\sum_i S_i^{(j)} = -\mathcal{L}_{x_j, p^{(j)}}$ if $y_j \in \{0, ?\}$, where $\mathcal{L}_{x,p} = x\sigma(p) - (\ell - x)\sigma(1 - p)$. Then we have

$$E_{(P)}\left[e^{-\alpha S_{\mathrm{psum}}} Pr(w \mid P)\right] \leq \prod_{j=1}^m \max{}^*\{N_{0,x_j}, N_{1,x_j}\} \ ,$$

where

$$N_{0,x} = E_{(p)}\left[e^{\alpha \mathcal{L}_{x,p}} p^x (1 - p)^{\ell - x}\right] \ , \ N_{1,x} = E_{(p)}\left[e^{-\alpha \mathcal{L}_{x,p}} p^x (1 - p)^{\ell - x}\right]$$

and $\max^*$ takes the first term N_{0,x_j} if $x_j = 0$, the second term N_{1,x_j} if $x_j = \ell$, and the maximum of N_{0,x_j} and N_{1,x_j} if $1 \leq x_j \leq \ell - 1$ (this definition of $\max^*$ reflects the Marking Assumption; i.e. y_j must be 0 if $x_j = 0$, and 1 if $x_j = \ell$). This bound does not depend on y, and both N_{0,x_j} and N_{1,x_j} depend solely on

x_j. Thus by substituting it into (8) we have

$$\begin{aligned} E\big[e^{-\alpha S_{\mathrm{psum}}}\big] &\leq \sum_{w} \prod_{j=1}^{m} \max{}^{*}\{N_{0,x_j}, N_{1,x_j}\} \\ &= \sum_{x_1,\dots,x_m} \prod_{j=1}^{m} \binom{\ell}{x_j} \prod_{j=1}^{m} \max{}^{*}\{N_{0,x_j}, N_{1,x_j}\} \\ &= \prod_{j=1}^{m} \sum_{x_j=0}^{\ell} \binom{\ell}{x_j} \max{}^{*}\{N_{0,x_j}, N_{1,x_j}\} = \left(\sum_{x=0}^{\ell} \binom{\ell}{x} M_x \right)^{m} \quad , \end{aligned}$$

where $M_0 = N_{0,0}$, $M_\ell = N_{1,\ell}$ and $M_x = \max\{N_{0,x}, N_{1,x}\}$ for $1 \leq x \leq \ell - 1$.

Since $|\mathcal{L}_{x,p}| \leq \ell\eta$ for any value p of $\mathcal{P}$ and any $0 \leq x \leq \ell$, an elementary analysis shows that $e^{\pm\alpha\mathcal{L}_{x,p}} \leq 1 \pm \alpha\mathcal{L}_{x,p} + r(\alpha\ell\eta)\alpha^2{\mathcal{L}_{x,p}}^2$, respectively, where $r(t) = (e^t - 1 - t)/t^2$ (note that this $r(t)$ is an increasing function, where we put $r(0) = \lim_{t\to 0} r(t) = 1/2$). Thus we have

$$\begin{aligned} M_x \leq E_{(p)}\big[p^x(1-p)^{\ell-x}\big] &- \alpha E_{(p)}\big[p^x(1-p)^{\ell-x}\mathcal{L}_{x,p}\big] \\ &+ r(\alpha\ell\eta)\alpha^2 E_{(p)}\big[p^x(1-p)^{\ell-x}{\mathcal{L}_{x,p}}^2\big] + 2\alpha R_{\ell,x} \end{aligned}$$

for $1 \leq x \leq \ell - 1$ (see Section 4 for the definition of $R_{\ell,x}$), while

$$\begin{aligned} M_0 \leq E_{(p)}\big[p^0(1-p)^{\ell-0}\big] &+ \alpha E_{(p)}\big[p^0(1-p)^{\ell-0}\mathcal{L}_{0,p}\big] \\ &+ r(\alpha\ell\eta)\alpha^2 E_{(p)}\big[p^0(1-p)^{\ell-0}{\mathcal{L}_{0,p}}^2\big] \end{aligned}$$

and

$$\begin{aligned} M_\ell \leq E_{(p)}\big[p^\ell(1-p)^{\ell-\ell}\big] &- \alpha E_{(p)}\big[p^\ell(1-p)^{\ell-\ell}\mathcal{L}_{\ell,p}\big] \\ &+ r(\alpha\ell\eta)\alpha^2 E_{(p)}\big[p^\ell(1-p)^{\ell-\ell}{\mathcal{L}_{\ell,p}}^2\big] \quad . \end{aligned}$$

Note that $\sum_{x=0}^{\ell}\binom{\ell}{x}p^x(1-p)^{\ell-x} = 1$, $\sum_{x=0}^{\ell}\binom{\ell}{x}p^x(1-p)^{\ell-x}\mathcal{L}_{x,p} = 0$, and $\sum_{x=0}^{\ell}\binom{\ell}{x}p^x(1-p)^{\ell-x}{\mathcal{L}_{x,p}}^2 = \ell$. Then we have

$$\begin{aligned} \sum_{x=0}^{\ell}\binom{\ell}{x} M_x &\leq 1 + 2\alpha E_{(p)}\big[p^0(1-p)^{\ell-0}\mathcal{L}_{0,p}\big] + r(\alpha\ell\eta)\alpha^2\ell + 2\alpha\sum_{x=1}^{\ell-1} R_{\ell,x} \\ &= 1 - 2\alpha\ell E_{(p)}\Big[p^{1/2}(1-p)^{\ell-1/2}\Big] + r(\alpha\ell\eta)\alpha^2\ell + 2\alpha\sum_{x=1}^{\ell-1} R_{\ell,x} \\ &= 1 + r(\alpha\ell\eta)\alpha^2\ell - 2\alpha\mathcal{R}_\ell \leq B_{2,\ell}(\alpha) \quad . \end{aligned}$$

Thus we have $E\big[e^{-\alpha S_{\mathrm{psum}}}\big] \leq B_{2,\ell}(\alpha)^m$, therefore the claim follows. □

7.4 Proof of Theorem 4.2

In this subsection, we give a proof of Theorem 4.2 assuming Lemma 7.3. Let ρ be an arbitrary pirates' strategy satisfying δ-Marking Assumption, and let y denote a pirated codeword generated by ρ. Then we define another pirates' strategy ρ', whose output is denoted by y', in the following manner: The j-th bit y'_j is equal to j-th bit of the codeword of any pirate if the j-th position is undetectable, and $y'_j = y_j$ otherwise. Note that this ρ' satisfies Marking Assumption, and y and y' differ in at most $m\delta$ positions owing to δ-Marking Assumption on ρ.

In this proof, let S_i denote the score of a user u_i determined by y and the scoring rule (2), and let S'_i denote the score of u_i determined by y' and the rule (1). Let S_{imax} and S'_{imax} denote the maximum of S_i and of S'_i, respectively, among the innocent users u_i. We define S_{pmax} and S'_{pmax} similarly for the pirates instead of innocent users. Then the error probability of our code with the pirates' strategy ρ is not more than the probability $Pr(S_{\mathrm{pmax}} \leq S_{\mathrm{imax}})$ regardless of the way of choosing the output user from the users with the highest score. Now note that

$$|S_i^{(j)} - S_i'^{(j)}| \leq \begin{cases} \delta' + \eta & \text{if } y_j \neq y'_j \ , \\ \delta' & \text{if } y_j = y'_j \ , \end{cases}$$

therefore $|S_i - S'_i| \leq m\delta' + m\delta\eta = m\Delta$. Thus we have

$$Pr(S_{\mathrm{pmax}} \leq S_{\mathrm{imax}}) \leq Pr(S'_{\mathrm{pmax}} \leq S'_{\mathrm{imax}} + 2m\Delta) \ .$$

Put $g_1 = S'_{\mathrm{imax}} + 2m\Delta$ and $g_2 = S'_{\mathrm{pmax}}$, both of which are random variables on the same probability space. Let $G(x) = Pr(g_2 \leq x)$ be the distribution function of g_2, therefore $G(x) \leq 1$. Now given a parameter $\beta > 0$, define a function $F(x)$ by

$$F(x) = \begin{cases} B_{2,\ell}(\beta)^m e^{\beta\ell x} & \text{if } x \leq Z_2 \ , \\ 1 & \text{if } x \geq Z_2 \ , \end{cases}$$

where

$$Z_2 = -\frac{m}{\beta\ell} \log B_{2,\ell}(\beta)$$

(note that $B_{2,\ell}(\beta) \geq 1/2$ by Lemma 4.1). Then $F(x)$ is a continuous, weakly increasing function such that $\lim_{x\to-\infty} F(x) = 0$, and we have $G(x) \leq F(x)$ by Lemma 7.5. Namely, the first condition in Lemma 7.3 is now satisfied.

On the other hand, define another function $\varphi(x)$ by

$$\varphi(x) = \begin{cases} NB_1(\beta\ell)^m e^{-\beta\ell x + 2\beta\ell m\Delta} & \text{if } x \geq Z_1 \ , \\ 1 & \text{if } x \leq Z_1 \ , \end{cases}$$

where β is the given positive parameter and

$$Z_1 = \frac{\log N + m \log B_1(\beta\ell)}{\beta\ell} + 2m\Delta$$

(note that $B_1(\beta\ell) > 1$ by Lemma 4.1). Then $\varphi(x)$ is a weakly decreasing function and $\varphi(x) > 0$, and we have $Pr(g_1 \geq x \mid P, y') \leq \varphi(x)$ for any bias parameter P and any pirated codeword y' by Lemma 7.4 (where we put $\alpha = \beta\ell$). Now we give the following lemma:

Lemma 7.6. *The second condition in Lemma 7.3 is satisfied.*

Proof. It suffices to show that, for any finite closed interval $I \subset \mathbb{R}$, we have $Pr(g_1 \geq x_1 \mid x_1 \leq g_2 < x_2) \leq \varphi(x_1)$ whenever $x_1, x_2 \in I$, $x_1 < x_2$ and $Pr(x_1 \leq g_2 < x_2) > 0$. Let w^{p} and w^{i} denote the collections of codewords of the pirates and of the innocent users, respectively. Then for any P, w^{p}, w^{i} and y', we have $Pr(y' \mid P, w^{\mathrm{i}}, w^{\mathrm{p}}) = Pr(y' \mid P, w^{\mathrm{p}})$ by No Leakage Assumption (Definition 2.2), and $Pr(w^{\mathrm{i}} \mid P, w^{\mathrm{p}}) = Pr(w^{\mathrm{i}} \mid P)$ since users' codewords are chosen independently with each other. This implies that

$$\begin{aligned}
& Pr(g_1 \geq x_1,\ x_1 \leq g_2 < x_2) \\
= & \sum_{P, w^{\mathrm{p}}, w^{\mathrm{i}}, y';\ g_1 \geq x_1,\ x_1 \leq g_2 < x_2} Pr(P, w^{\mathrm{p}}, w^{\mathrm{i}}, y') \\
= & \sum_{P, w^{\mathrm{p}}, w^{\mathrm{i}}, y';\ g_1 \geq x_1,\ x_1 \leq g_2 < x_2} Pr(P) Pr(w^{\mathrm{p}} \mid P) Pr(w^{\mathrm{i}} \mid P) Pr(y' \mid P, w^{\mathrm{p}}) \\
= & \sum_{P, w^{\mathrm{p}}, y';\ x_1 \leq g_2 < x_2} Pr(P) Pr(w^{\mathrm{p}} \mid P) Pr(y' \mid P, w^{\mathrm{p}}) \sum_{w^{\mathrm{i}};\ g_1 \geq x_1} Pr(w^{\mathrm{i}} \mid P) \\
= & \sum_{P, w^{\mathrm{p}}, y';\ x_1 \leq g_2 < x_2} Pr(P, w^{\mathrm{p}}, y') \cdot Pr(g_1 \geq x_1 \mid P, y') \\
\leq & \sum_{P, w^{\mathrm{p}}, y';\ x_1 \leq g_2 < x_2} Pr(P, w^{\mathrm{p}}, y') \varphi(x_1) = \varphi(x_1) Pr(x_1 \leq g_2 < x_2)
\end{aligned}$$

(recall that $Pr(g_1 \geq x_1 \mid P, y') \leq \varphi(x_1)$ by the argument before Lemma 7.6). Thus we have $Pr(g_1 \geq x_1 \mid x_1 \leq g_2 < x_2) \leq \varphi(x_1)$. Hence the claim holds. □

By Lemma 7.6, the conditions in Lemma 7.3 are satisfied. Therefore Lemma 7.3 implies that $Pr(g_2 \leq g_1) \leq \int_{\mathbb{R}} \varphi \, dF$, where the right-hand side is the Lebesgue-Stieltjes integral (see e.g. [4]). Now note that $Z_1 \leq Z_2$ if and only if $N T_\ell{}^m \leq 1$. Thus in the case that $N T_\ell{}^m \leq 1$, we have

$$\int_{\mathbb{R}} \varphi \, dF = \int_{(-\infty, Z_1]} dF + \int_{(Z_1, Z_2]} \varphi \, dF + \int_{(Z_2, \infty)} \varphi \, dF \enspace .$$

Since F is differentiable on the interval $(-\infty, Z_2]$, F is constant on (Z_2, ∞), and $\lim_{x \to -\infty} F(x) = 0$, it follows from properties of Lebesgue-Stieltjes integral that

$$\begin{aligned}
\int_{\mathbb{R}} \varphi \, dF &= \int_{-\infty}^{Z_1} F'(x) \, dx + \int_{Z_1}^{Z_2} \varphi(x) F'(x) \, dx + 0 \\
&= F(Z_1) + \int_{Z_1}^{Z_2} \beta \ell N T_\ell{}^m \, dx \\
&= N T_\ell{}^m + \beta \ell N T_\ell{}^m (Z_2 - Z_1) = \Phi(N T_\ell{}^m) \enspace .
\end{aligned}$$

Summarizing, the error probability of our codes (under δ-Marking Assumption and the scoring rule (2)) is not more than $\Phi(N T_\ell{}^m)$ if the number of pirates is ℓ and $N T_\ell{}^m \leq 1$.

Now note that $T_\ell \leq T_c$ for any $1 \leq \ell \leq c$ (since each of $B_1(\beta\ell)$, $B_{2,\ell}(\beta)$ and $e^{2\beta\ell\Delta}$ is increasing as ℓ is getting larger) and $\Phi(t)$ is an increasing function for $0 < t \leq 1$. Thus if $T_c \leq T_0$ and $N T_0{}^m < 1$, then whenever the number of the pirates is $\ell \leq c$, we have $N T_\ell{}^m \leq N T_0{}^m < 1$ and the error probability is not more than $\Phi(N T_0{}^m)$. Hence the first part of Theorem 4.2 is proved.

From now, we prove the second part of Theorem 4.2. For a given $0 < \varepsilon < 1$, we introduce a function $\Phi_\varepsilon(t) = \Phi(t) - \varepsilon$, which is increasing, continuous and concave up for $0 < t < 1$. Since $\lim_{t\to+0} \Phi_\varepsilon(t) = -\varepsilon < 0$ and $\lim_{t\to 1-0} \Phi_\varepsilon(t) = 1 - \varepsilon > 0$, there exists a unique $0 < t_0 < 1$ such that $\Phi_\varepsilon(t_0) = 0$. Now if $a > 1$ and $\varepsilon \le ae^{1-a}$, then we have

$$\Phi_\varepsilon(\varepsilon/a) = \frac{\varepsilon}{a}\left(1 - \log\frac{\varepsilon}{a}\right) - \varepsilon \ge \frac{\varepsilon}{a} \cdot a - \varepsilon \ge 0 \ ,$$

therefore $t_0 \le \varepsilon/a < 1$. Moreover, put

$$t_1 = \frac{\varepsilon}{a} - \frac{\Phi_\varepsilon(\varepsilon/a)}{\Phi'_\varepsilon(\varepsilon/a)} = \frac{a-1}{a}\frac{\varepsilon}{\log(a/\varepsilon)} > 0 \ ,$$

which is the x-intercept of the tangent line of the curve $y = \Phi_\varepsilon(x)$ in the x-y plane at $x = \varepsilon/a$. Since $\varepsilon/a \ge t_0$, and $\Phi_\varepsilon(t)$ is increasing and concave up, we have $t_1 \le t_0$, therefore $\Phi_\varepsilon(t_1) \le 0$. Thus we have $\Phi(NT_c{}^m) \le \Phi(t_1) \le \varepsilon$ whenever $NT_c{}^m \le t_1$, or equivalently, whenever the inequality (3) is satisfied. Hence the proof of Theorem 4.2 (assuming Lemma 7.3) is concluded.

7.5 Proof of Lemma 7.3

Finally, to complete the proof of Theorem 4.2, we give a proof of Lemma 7.3. First, we recall the following well-known facts used in our proof:

Proposition 7.7. *If φ is a weakly decreasing function on a finite interval in $\mathbb{R}$, then the number of points of discontinuities of φ is either finite or countably infinite.*

Theorem 7.8. *Let (Ω, μ) be a measurable space, $\{\varphi_i\}_{i=1}^\infty$ a sequence of measurable functions on Ω, and φ a function on Ω such that $\lim_{n\to\infty} \varphi_n = \varphi$.*

1. **(Bounded Convergence Theorem)** *If $\mu(\Omega) < \infty$ and there is a constant $M > 0$ such that $|\varphi_n(\omega)| < M$ for any n and any $\omega \in \Omega$, then φ and each φ_n are μ-integrable and $\lim_{n\to\infty} \int_\Omega \varphi_n \, d\mu = \int_\Omega \varphi \, d\mu$.*
2. **(Monotone Convergence Theorem)** *If $0 \le \varphi_n(\omega) \le \varphi_{n+1}(\omega)$ for any n and any $\omega \in \Omega$, then $\lim_{n\to\infty} \int_\Omega \varphi_n \, d\mu = \int_\Omega \varphi \, d\mu$ (this includes the case that both terms are ∞).*

Our proof of Lemma 7.3 is done by showing the following two properties:

1. $Pr(g_1 \ge g_2) \le \int_\mathbb{R} \varphi \, dG$,
2. $\int_\mathbb{R} \varphi \, dG \le \int_\mathbb{R} \varphi \, dF$.

7.5.1 Proof of the first property

We show that $Pr(g_1 \ge g_2) \le \int_\mathbb{R} \varphi \, dG$. We denote the common underlying probability space for g_1 and g_2 by Ω, and denote the values of g_1 and of g_2 at $\omega \in \Omega$ by $g_1(\omega)$ and by $g_2(\omega)$, respectively. First, we have

$$Pr(g_1 \ge g_2) = 1 - Pr(g_1 < g_2) = 1 - \lim_{n\to\infty} Pr(g_1 < g_2, \ -n \le g_2 < n) \ . \quad (9)$$

Since φ is weakly decreasing, Proposition 7.7 implies that the set A_n of the points of discontinuities of φ in the interval $[-n, n)$ is either finite or countably infinite. Enumerate the elements of A_n as $a_1^{(n)}$, $a_2^{(n)}$, and so on. Then for each integer $k \geq 1$, we define finite sets $D_k^{(n)}$ by

$$D_k^{(n)} = \{-n + i/2^k \mid 0 \leq i \leq n2^{k+1}\} \cup \{a_i^{(n)} \mid 1 \leq i \leq k\}$$

and enumerate the points in $D_k^{(n)}$ in increasing order as $d_{k,0}^{(n)} < d_{k,1}^{(n)} < \cdots < d_{k,\ell_{n,k}}^{(n)}$. Now we have the following properties:

$$D_k^{(n)} \subset D_{k+1}^{(n)} \ , \ d_{k,0}^{(n)} = -n \text{ and } d_{k,\ell_{n,k}}^{(n)} = n \text{ for any } k \ ; \tag{10}$$

$$\text{for each } k, \text{ we have } d_{k,i}^{(n)} - d_{k,i-1}^{(n)} \leq 2^{-k} \text{ for every } i \ . \tag{11}$$

Now we use the following lemma:

Lemma 7.9. *In this setting, for any n we have*

$$\begin{aligned} &\{\omega \in \Omega \mid g_1(\omega) < g_2(\omega), \ -n \leq g_2(\omega) < n\} \\ = &\lim_{k \to \infty} \bigsqcup_{i=1}^{\ell_{n,k}} \{\omega \in \Omega \mid g_1(\omega) < d_{k,i-1}^{(n)} \leq g_2(\omega) < d_{k,i}^{(n)}\} \ , \end{aligned}$$

where the symbol '$\sqcup$' in the right-hand side means the disjoint union.

Proof. Since each summand in the right-hand side is disjoint with each other and is contained in the left-hand side by (10), our remaining task is to show that any element ω in the left-hand side is included in the right-hand side. Choose $M > 0$ such that $2^{-M} < g_2(\omega) - g_1(\omega)$. Then for any $k \geq M$, it follows from (11) that $D_k^{(n)}$ intersects with the interval $(g_1(\omega), g_2(\omega)]$, thus there exists an index i such that $g_1(\omega) < d_{k,i-1}^{(n)} \leq g_2(\omega) < d_{k,i}^{(n)}$. This means that ω belongs to the set in the right-hand side. Hence the claim holds. $\square$

By Lemma 7.9, the right-hand side of (9) is equal to

$$\begin{aligned} &1 - \lim_{n \to \infty} \lim_{k \to \infty} \sum_{i=1}^{\ell_{n,k}} Pr(g_1 < d_{k,i-1}^{(n)} \leq g_2 < d_{k,i}^{(n)}) \\ &= 1 - \lim_{n \to \infty} \lim_{k \to \infty} \sum_{i=1}^{\ell_{n,k}} \Big(Pr(d_{k,i-1}^{(n)} \leq g_2 < d_{k,i}^{(n)}) \\ &\qquad - Pr(d_{k,i-1}^{(n)} \leq g_2 < d_{k,i}^{(n)}, \ g_1 \geq d_{k,i-1}^{(n)}) \Big) \ . \end{aligned} \tag{12}$$

For an interval $I = [-n, n]$ and any $\varepsilon' > 0$, take a $\kappa > 0$ as in the second condition in the statement of Lemma 7.3. Then by (10) and (11), for any sufficiently large k, we have $d_{k,i-1}^{(n)}, d_{k,i}^{(n)} \in I$ and $d_{k,i}^{(n)} - d_{k,i-1}^{(n)} < \kappa$ for every i, therefore the second condition in Lemma 7.3 implies that

$$Pr(d_{k,i-1}^{(n)} \leq g_2 < d_{k,i}^{(n)}, \ g_1 \geq d_{k,i-1}^{(n)}) \leq (\varphi(d_{k,i-1}^{(n)}) + \varepsilon') Pr(d_{k,i-1}^{n} \leq g_2 < d_{k,i}^{(n)})$$

for every i. Thus the right-hand side of (12) is less than or equal to

$$
\begin{aligned}
1-(1-\varepsilon')\lim_{n\to\infty}\lim_{k\to\infty}\sum_{i=1}^{\ell_{n,k}} Pr(d_{k,i-1}^{(n)} \le g_2 < d_{k,i}^{(n)}) \\
+\lim_{n\to\infty}\lim_{k\to\infty}\sum_{i=1}^{\ell_{n,k}} \varphi(d_{k,i-1}^{(n)}) Pr(d_{k,i-1}^{(n)} \le g_2 < d_{k,i}^{(n)}) \ .
\end{aligned} \tag{13}
$$

By (10), the second term in (13) is equal to

$$(1-\varepsilon')\lim_{n\to\infty}\lim_{k\to\infty} Pr(-n \le g_2 < n) = (1-\varepsilon')\lim_{n\to\infty} Pr(-n \le g_2 < n) = 1-\varepsilon' \ .$$

Thus the right-hand side of (12) is less than or equal to

$$\varepsilon' + \lim_{n\to\infty}\lim_{k\to\infty}\sum_{i=1}^{\ell_{n,k}} \varphi(d_{k,i-1}^{(n)}) \Pr(d_{k,i-1}^{(n)} \le g_2 < d_{k,i}^{(n)}) \ . \tag{14}$$

Since $\varepsilon' > 0$ is arbitrary, taking the limit $\varepsilon' \to 0$ implies that the right-hand side of (12) is less than or equal to

$$\lim_{n\to\infty}\lim_{k\to\infty}\sum_{i=1}^{\ell_{n,k}} \varphi(d_{k,i-1}^{(n)}) Pr(d_{k,i-1}^{(n)} \le g_2 < d_{k,i}^{(n)}) \ . \tag{15}$$

Moreover, if μ_G denotes the measure on $\mathbb{R}$ induced by the function G (thus $\mu_G((a,b]) = G(b) - G(a)$), then $Pr(d_{k,i-1}^{(n)} \le g_2 < d_{k,i}^{(n)})$ is equal to

$$
\begin{aligned}
& \lim_{t\to+0} Pr(d_{k,i-1}^{(n)} - t < g_2 \le d_{k,i}^{(n)} - t) \\
= \ & \lim_{t\to+0} \mu_G\big((d_{k,i-1}^{(n)} - t, d_{k,i}^{(n)} - t]\big) \\
= \ & \mu_G\big(\lim_{t\to+0}(d_{k,i-1}^{(n)} - t, d_{k,i}^{(n)} - t]\big) = \mu_G\big([d_{k,i-1}^{(n)}, d_{k,i}^{(n)})\big) \ .
\end{aligned}
$$

Now define $\varphi_{n,k} = \sum_{i=1}^{\ell_{n,k}} \varphi(d_{k,i-1}^{(n)})\chi_{[d_{k,i-1}^{(n)}, d_{k,i}^{(n)})}$ for $k \ge 1$ (where χ_A denotes the characteristic function of a set A), which is a nonnegative, μ_G-measurable function on $\mathbb{R}$. Then by the above argument, the right-hand side of (15) is equal to

$$\lim_{n\to\infty}\lim_{k\to\infty}\sum_{i=1}^{\ell_{n,k}} \varphi(d_{k,i-1}^{(n)})\mu_G\big([d_{k,i-1}^{(n)}, d_{k,i}^{(n)})\big) = \lim_{n\to\infty}\lim_{k\to\infty}\int_{\mathbb{R}} \varphi_{n,k}\, d\mu_G \ . \tag{16}$$

Now we use the following lemma:

Lemma 7.10. *In this setting, we have* $\lim_{k\to\infty}\varphi_{n,k} = \varphi\chi_{[-n,n)}$.

Proof. Since both functions $\varphi_{n,k}$ and $\varphi\chi_{[-n,n)}$ take the value 0 outside the interval $[-n,n)$, it suffices to show that $\lim_{k\to\infty}\varphi_{n,k}(x) = \varphi(x)$ for any $-n \le x < n$. First, if $-n \le x < n$ and $x \in A_n$, then $x \in D_k^{(n)}$ for any sufficiently large k by the definition of $D_k^{(n)}$, therefore $\varphi_{n,k}(x) = \varphi(x)$ for any sufficiently large k by the definition of $\varphi_{n,k}$ (note that $x \neq n = d^{(n)}_{k,\ell_{n,k}}$ by (10)). Thus the claim holds in this case.

On the other hand, assume that $-n \leq x < n$ and $x \notin A_n$. Take an arbitrary $\lambda > 0$. Then by the choice of x, there is a $\kappa_\lambda > 0$ such that $|\varphi(x') - \varphi(x)| < \lambda$ whenever $-n \leq x' < n$ and $|x' - x| < \kappa_\lambda$. Now by an argument similar to the proof of Lemma 7.9, it follows from (11) that for any sufficiently large k, we have $d^{(n)}_{k,i-1} \leq x < d^{(n)}_{k,i}$ and $x - d^{(n)}_{k,i-1} < d^{(n)}_{k,i} - d^{(n)}_{k,i-1} < \kappa_\lambda$ for some i, therefore $\varphi_{n,k}(x) = \varphi(d^{(n)}_{k,i-1})$ and $|\varphi_{n,k}(x) - \varphi(x)| = |\varphi(d^{(n)}_{k,i-1}) - \varphi(x)| < \lambda$ for this i by the above argument. This means that $\lim_{k\to\infty} \varphi_{n,k}(x) = \varphi(x)$. Hence the claim holds. $\square$

Note that $\mu_G(\mathbb{R}) = 1$, and $\varphi_{n,k} \leq \varphi(-n)$ since $d^{(n)}_{k,0} = -n$ and φ is weakly decreasing. Thus $\lim_{k\to\infty} \int_{\mathbb{R}} \varphi_{n,k}\, d\mu_G = \int_{\mathbb{R}} \varphi\chi_{[-n,n)}\, d\mu_G$ by Lemma 7.10 and Bounded Convergence Theorem (Theorem 7.8). Moreover, since φ is nonnegative, we have $\lim_{n\to\infty} \int_{\mathbb{R}} \varphi\chi_{[-n,n)}\, d\mu_G = \int_{\mathbb{R}} \varphi\, d\mu_G$ by Monotone Convergence Theorem (Theorem 7.8). Thus the right-hand side of (16) is equal to $\int_{\mathbb{R}} \varphi\, d\mu_G = \int_{\mathbb{R}} \varphi\, dG$.

Summarizing, we have $Pr(g_1 \geq g_2) \leq \int_{\mathbb{R}} \varphi\, dG$, as desired.

7.5.2 Proof of the second property

From now, we show that $\int_{\mathbb{R}} \varphi\, dG \leq \int_{\mathbb{R}} \varphi\, dF$, which concludes the proof of Lemma 7.3. First, we introduce some notations. We define

$$\mathbb{R}' = \mathbb{R} \cup \{a_- \mid a \in \mathbb{R}\} \cup \{-\infty, \infty_-\}$$

and extend the order $<$ on $\mathbb{R}$ to $\mathbb{R}'$ by $-\infty < a_- < a < b_- < \infty_-$ for every $a, b \in \mathbb{R}$ such that $a < b$. Put

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\} \text{ for any } a, b \in \mathbb{R}'$$

(for example, we have $(a_-, b_-] = [a, b)$ in the usual notation for $a, b \in \mathbb{R}$). Moreover, for each $H \in \{F, G\}$, write $H(a_-) = \lim_{b\to a-0} H(b)$ for any $a \in \mathbb{R}$, $H(-\infty) = \lim_{b\to-\infty} H(b)$, and $H(\infty_-) = \lim_{b\to\infty} H(b)$. Then for any $a, b \in \mathbb{R}$ such that $a \leq b$, we have $\mu_H((a_-, b_-]) = H(b_-) - H(a_-)$ since $(a_-, b_-] = \lim_{t\to+0} (a - t, b - t]$ (note that $\mu_H((a, b]) = H(b) - H(a)$ by the definition of μ_H). By similar arguments, it follows that

$$\mu_H((a, b]) = H(b) - H(a) \text{ for any } a, b \in \mathbb{R}' \text{ such that } a \leq b\ , \qquad (17)$$

where we put $H(b) - H(a) = 0$ in the case that $a = b$ (even if $H(a) = \pm\infty$).

For any $n \geq 1$, define $I_{n,i} = \{x \in \mathbb{R} \mid i2^{-n} \leq \varphi(x) < (i+1)2^{-n}\}$ for each $1 \leq i \leq 4^n - 1$, and $I_{n,4^n} = \{x \in \mathbb{R} \mid \varphi(x) \geq 2^n\}$. Then, since φ is weakly decreasing, each $I_{n,i}$ is a (possibly empty or infinite) interval in $\mathbb{R}$. Moreover, for each n, there exist $\alpha_{n,i} \in \mathbb{R}'$ (for $1 \leq i \leq 4^n + 1$) such that $-\infty = \alpha_{n,4^n+1} \leq \alpha_{n,4^n} \leq \cdots \leq \alpha_{n,2} \leq \alpha_{n,1}$ and $I_{n,i} = (\alpha_{n,i+1}, \alpha_{n,i}]$ for each $1 \leq i \leq 4^n$. We have $\mu_H(I_{n,i}) = H(\alpha_{n,i}) - H(\alpha_{n,i+1})$ for each $H \in \{F, G\}$ by (17). Now put $\psi_n = \sum_{i=1}^{4^n} i2^{-n}\chi_{I_{n,i}}$, which is a nonnegative, μ_F-measurable and μ_G-measurable simple function on $\mathbb{R}$. Then for each $H \in \{F, G\}$, the integral

$\int_{\mathbb{R}} \psi_n \, d\mu_H$ is equal to

$$\begin{aligned}
& \sum_{i=1}^{4^n} i2^{-n} \mu_H(I_{n,i}) \\
= & \sum_{i=1}^{4^n-1} i2^{-n}(H(\alpha_{n,i}) - H(\alpha_{n,i+1})) + 2^n(H(\alpha_{n,4^n}) - H(-\infty)) \\
= & \sum_{i=1}^{4^n} H(\alpha_{n,i}) \left(\frac{i}{2^n} - \frac{i-1}{2^n} \right) - 2^n H(-\infty) = \sum_{i=1}^{4^n} \frac{H(\alpha_{n,i})}{2^n} - 2^n H(-\infty)
\end{aligned}$$

(this equality holds even if $H(\alpha_{n,i}) = \infty$ for an index i, in which case all the terms are ∞). By the first condition in Lemma 7.3, we have $G(\alpha_{n,i}) \leq F(\alpha_{n,i})$ for every i, and $G(-\infty) = F(-\infty) = 0$. Thus we have

$$\int_{\mathbb{R}} \psi_n \, d\mu_G = \sum_{i=1}^{4^n} \frac{G(\alpha_{n,i})}{2^n} \leq \sum_{i=1}^{4^n} \frac{F(\alpha_{n,i})}{2^n} = \int_{\mathbb{R}} \psi_n \, d\mu_F \ .$$

To conclude the proof, we need the following lemma:

Lemma 7.11. *We have $\psi_n \leq \psi_{n+1}$ for any n, and $\lim_{n\to\infty} \psi_n = \varphi$.*

Proof. First we show that $\psi_n(x) \leq \psi_{n+1}(x)$ for any $x \in \mathbb{R}$. Since $\psi_n(x) \leq 2^n$ by definition, it suffices to consider the case that $\psi_{n+1}(x) < 2^n$, namely $x \notin \bigcup_{i=2^{2n+1}}^{4^{n+1}} I_{n+1,i}$. Now if $2 \leq i \leq 2^{2n+1} - 1$ and $x \in I_{n+1,i}$, then we have $x \in I_{n,\lfloor i/2 \rfloor}$ and $\psi_n(x) = \lfloor i/2 \rfloor 2^{-n} \leq i2^{-n-1} = \psi_{n+1}(x)$. On the other hand, if $x \notin \bigcup_{i=2}^{2^{2n+1}-1} I_{n+1,i}$, then we have $\varphi(x) < 2^{-n}$, therefore $\psi_n(x) = 0 \leq \psi_{n+1}(x)$. Hence we have $\psi_n \leq \psi_{n+1}$.

Secondly, we show that $\lim_{n\to\infty} \psi_n(x) = \varphi(x)$ for any $x \in \mathbb{R}$. By definition of ψ_n, we have $0 \leq \varphi(x) - \psi_n(x) < 2^{-n}$ whenever $\varphi(x) < 2^n$. Now for any $x \in \mathbb{R}$ and any $\lambda > 0$, we have $\varphi(x) < 2^n$ and $2^{-n} < \lambda$ for all sufficiently large n, therefore $|\varphi(x) - \psi_n(x)| < \lambda$ for all these n. This means that $\psi_n(x)$ converges to $\varphi(x)$ when $n \to \infty$. Hence the claim holds. $\square$

This lemma and Monotone Convergence Theorem (Theorem 7.8) imply that

$$\begin{aligned}
\int_{\mathbb{R}} \varphi \, dG = \int_{\mathbb{R}} \varphi \, d\mu_G &= \lim_{n\to\infty} \int_{\mathbb{R}} \psi_n \, d\mu_G \\
&\leq \lim_{n\to\infty} \int_{\mathbb{R}} \psi_n \, d\mu_F = \int_{\mathbb{R}} \varphi \, d\mu_F = \int_{\mathbb{R}} \varphi \, dF \ .
\end{aligned}$$

Hence the proof of Lemma 7.3 is concluded.

8 Conclusion

In this article, we proposed a construction of c-secure fingerprinting codes for every c, which improves recent discrete variants [3, 5, 6] of Tardos's c-secure codes [8]. Our security proof was given under an assumption weaker than the usual Marking Assumption. The ratio of the code length divided by the value $c^2 \log(N/\varepsilon)$, where N is the number of the users and ε is the error probability, converges to approximately 5.35 when c goes to infinity, and the ratio is further smaller in some cases for $c \leq 8$. Thus we have shown that the lengths of our codes are significantly shorter than the lengths of c-secure codes in [3, 5, 6, 8], and also shorter than the lengths of c-secure codes recently proposed by [7] in the case without the statistical assumption introduced in [7].

Acknowledgements

This study has been sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contract, New-generation Information Security R&D Program. This study has also been supported by 2007 Research Grants of the Science and Technology Foundation of Japan (JSTF).

References

[1] Blayer, O., Tassa, T.: Improved versions of Tardos' fingerprinting scheme. Des. Codes Cryptogr. **48**, 79–103 (2008).

[2] Boneh, D., Shaw, J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inform. Theory **44**(5), 1897–1905 (1998).

[3] Hagiwara, M., Hanaoka, G., Imai, H.: A short random fingerprinting code against a small number of pirates. In: Proceedings of 16th Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-16), LNCS 3857, pp. 193–202 (2006).

[4] Carter, M., van Brunt, B.: The Lebesgue-Stieltjes Integral: A Practical Introduction. Springer-Verlag, Berlin (2000).

[5] Nuida, K., Hagiwara, M., Watanabe, H., Imai, H.: Optimization of Memory Usage in Tardos's Fingerprinting Codes. Preprint at arXiv repository, `http://www.arxiv.org/abs/cs/0610036` (2006).

[6] Nuida, K., Hagiwara, M., Watanabe, H., Imai, H.: Optimization of Tardos's fingerprinting codes in a viewpoint of memory amount. In: Proceedings of 9th Information Hiding (IH 2007), LNCS 4567, pp. 279–293 (2007).

[7] Škorić, B., Katzenbeisser, S., Celik, M.U.: Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. Des. Codes Cryptogr. **46**, 137–166 (2008).

[8] Tardos, G.: Optimal probabilistic fingerprint codes. In: Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC), pp. 116–125 (2003).