Short collusion-secure fingerprint codes against three pirates

Koji Nuida

Published online: 4 February 2012
© Springer-Verlag 2012

Abstract In this article, we propose a new construction of probabilistic collusion-secure fingerprint codes against up to three pirates and give a theoretical security evaluation. Our pirate tracing algorithm combines a scoring method analogous to Tardos codes (J ACM 55:1–24, 2008) with an extension of parent search techniques of some preceding 2-secure codes. Numerical examples show that our code lengths are significantly shorter than (about 30–40% of) the shortest known $c$-secure codes by Nuida et al. (Des Codes Cryptogr 52:339–362, 2009) with $c = 3$.

Keywords Collusion-secure code · Fingerprint code · 3-secure code · Content protection

1 Introduction

1.1 Background and related works

Recently, digital content distribution services have been widespread by virtue of progress in information technology. Digitization of content distribution has improved convenience for ordinary people. However, the digitization also enables malicious persons to perform more powerful attacks, and the amount of illegal content redistribution is increasing very rapidly. Hence technical countermeasures for such illegal activities are strongly desired. A use of fingerprint code is a possible solution for such problems, which aims at giving traceability of the attacker (pirate) when an illegally redistributed digital content is found, thus letting the potential attackers abandon to perform actual attacks.

In the context of fingerprint codes, each copy of a content is divided into several segments (common to all copies), in each of which a bit of an encoded user ID is embedded by the content provider by using watermarking technique. The embedded encoded ID (fingerprint) provides traceability of an adversarial user (pirate) when an unauthorized copy of the content is distributed. Such a scheme aims at tracing some pirate, without falsely tracing any innocent user, from the fingerprint embedded in the pirated content with an overwhelming probability. It has been noticed that a coalition of pirates can perform certain strong attacks (collusion attacks) to the fingerprint, therefore any effective fingerprint code should be secure against collusion attacks, called collusion-secure codes. In particular, if the code is secure against collusion attacks by up to $c$ pirates, then the code is called $c$-secure [5].

Several constructions of collusion-secure codes have been proposed so far. Among them, the one proposed by Tardos [24] is “asymptotically optimal”, in the sense that the order of his code length with respect to the allowable number $c$ of pirates is theoretically the lowest (which is quadratic in $c$). For improvements of Tardos codes, the constant factor of the asymptotic code length has been reduced by $c$-secure codes given by Nuida et al. [15] to approximately 5.35% of Tardos codes, which is the smallest value so far provable without any additional assumption. There are also other improvements of Tardos codes whose lengths are longer than Nuida’s code [4,21,23] or whose security proofs depend on certain statistical assumptions on the behavior of codewords [21,23]. Moreover, variants of Tardos codes over large alphabets (instead of binary ones as in [15,24]) have been proposed as well [4,21,22]. Some recent works [1,2,8,9] focused on the achievable rates (or “fingerprinting capacity”) of
collusion-secure codes in asymptotic cases, rather than concrete bounds of error probabilities in practical cases.

On the other hand, after the first proposal of Tardos codes, there were proposed several collusion-secure codes [3,6,11,14,16] that restrict the number of pirates to \( c = 2 \) but achieve further short code lengths. Such constructions of short \( c \)-secure codes for a small \( c \) would have not only theoretical but also practical importance; for example, when the users are less anonymous for the content provider (e.g., the case of secret documents distributed in a company), it seems infeasible to make a large coalition confidentially. The aim of this article is to extend such a “compact” construction to the next case \( c = 3 \).

For related works, we notice that there is an earlier work by Schaathun [17, 18] on construction of 3-secure codes (the proposal of 3-secure codes by Sebé and Domingo-Ferrer [20] was earlier than Schaathun’s one, but it was shown later to be insecure by Schaathun [19]). On the other hand, there is another work by Kitagawa et al. [10] on construction of 3-secure codes, in which very short code lengths are proposed but its security is evaluated only by computer experiments for some special attack strategies.

1.2 Our contribution

In this article, we propose a new construction of 3-secure codes and give a theoretical security evaluation. The codeword generation algorithm is just a bit-wise random sampling, which has been used by many preceding constructions as well. The novel point of our construction is in the pirate tracing algorithm, which combines the use of score computation analogous to Tardos codes [24] with an extension of “parent search” technique of some preceding works against two pirates [3,11,16]. Intuitively, the score computation method works well when the parts of fingerprint in the pirated content are not chosen evenly from the codewords of pirates, while the extended “parent search” technique works well when the fingerprint is evenly chosen from the codewords of pirates, therefore their combination is effective.

In comparison under some parameter choices, our code lengths are approximately 1–1.5% of 3-secure codes by Schaathun [17, 18], and approximately 30–40% of \( c \)-secure codes by Nuida et al. [15] for \( c = 3 \). This shows that our code length is even significantly shorter than the shortest known \( c \)-secure codes [15]. See Sect. 3.5 for details of comparison with preceding results.

In fact, Kitagawa et al. [10] claimed that their 3-secure code provides almost the same security level as our code for the case of 100 users and 128-bit length. However, they evaluated the security by only computer experiments for the case of some special attack algorithms (and they studied just one parameter choice as above), while in this article we give a theoretical security evaluation for arbitrary attack algorithms under the standard Marking Assumption (cf., [5]). (One may think that the perfect protection of so-called undetectable positions required by Marking Assumption is not practical. However, this is in fact not a serious problem, as a general conversion technique recently proposed by Nuida [12] can supply robustness against erasure of a bounded number of undetectable bits.)

1.3 Notations

In this article, \( \log \) denotes the natural logarithm. We put \([n] = \{1, 2, \ldots, n\}\) for an integer \( n \). Unless some ambiguity emerges, we often abbreviate a set \( \{i_1, i_2, \ldots, i_k\} \) to \( i_1i_2\cdots i_k \), and when we use this abbreviation, we implicitly assume that \( i_1, i_2, \ldots, i_k \) are all different. Let \( \delta_{a,b} \) denote Kronecker delta, that is, we have \( \delta_{a,b} = 1 \) if \( a = b \) and \( \delta_{a,b} = 0 \) if \( a \neq b \). For a family \( \mathcal{F} \) of sets, let \( \bigcup \mathcal{F} \) and \( \bigcap \mathcal{F} \) denote the union and the intersection, respectively, of all members of \( \mathcal{F} \).

1.4 Organization of the article

In Sect. 2, we give a formal definition of the notion of collusion-secure fingerprint codes. In Sect. 3, we describe our codeword generation algorithm and pirate tracing algorithm, state the main results on the security of our 3-secure codes, and give some numerical examples for comparison to preceding works. Section 4 summarizes the outline of the security proof. Finally, Sect. 5 supplies the details of proofs omitted in Sects. 3 and 4.

2 Collusion-secure fingerprint codes

In this section, we introduce formal definitions for fingerprint codes. Let \( N \) and \( m \) be positive integers, and \( 1 \leq c \leq N \) an integer parameter. Put \( U = [N] \). Fix a symbol “?” different from “0” and “1”. We start with the following definition:

**Definition 1** Given the parameters \( N, m \) and \( c \), we define the following game, which we refer to as **pirate tracing game**. The players of the game is a **provider** and **pirates**, and the game is proceeded as follows:

1. **Provider** generates an \( N \times m \) binary matrix \( W = (w_{i,j})_{i \in [N], j \in [m]} \) and an element \( st \) called **state information**.
2. **Pirates** generate \( U_p \subseteq U, 1 \leq |U_p| \leq c \), without knowing \( W \) and \( st \).
3. **Pirates** receive the codeword \( w_i = (w_{i,1}, \ldots, w_{i,m}) \) for every \( i \in U_p \).
4. **Pirates** generate a word \( y = (y_1, \ldots, y_m) \) on \([0, 1, ?]\) under a certain restriction specified below, and send \( y \) to **provider**.
5. Provider generates $\text{Acc} \subseteq U$ from $y$, $W$, and $\text{st}$, without knowing $U_p$.
6. Then pirates win if $\text{Acc} \cap U_p = \emptyset$ or $\text{Acc} \not\subseteq U_p$, and otherwise provider wins.

We call the word $y$ in Step 4 an attack word and call “?” an erasure symbol. Put $U_1 = U \setminus U_p$. In the definition, $U$ signifies the set of all users, $U_p$ is the coalition of pirates, and $U_1$ is the set of innocent users. The codeword $w_i$ signifies the fingerprint for user $i$, and the word $y$ signifies the fingerprint embedded in the pirated content. The set $\text{Acc}$ consists of the users traced by the provider from the pirated content. The events $\text{Acc} \cap U_p = \emptyset$ and $\text{Acc} \not\subseteq U_p$ specified in Step 6 are referred to as false-negative and false-positive (or false-alarm), respectively. Both of false-negative and false-positive are called tracing error.

Let $\text{Gen}$, $\text{Reg}$, $\rho$, and $\text{Tr}$ denote the algorithms used in Steps 1, 2, 4, and 5, respectively. We call $\text{Gen}$, $\text{Reg}$, $\rho$, and $\text{Tr}$ codeword generation algorithm, registration algorithm, pirate strategy, and tracing algorithm, respectively. We refer to the pair $C = (\text{Gen}, \text{Tr})$ as a fingerprint code, and the following quantity

$$Pr[(W, \text{st}) \leftarrow \text{Gen}(); U_p \leftarrow \text{Reg}();$$

$$y \leftarrow \rho(U_p, (w_i)_{i \in U_p});$$

$$\text{Acc} \leftarrow \text{Tr}(y, W, \text{st}) : \text{Acc} \cap U_p = \emptyset \text{ or } \text{Acc} \not\subseteq U_p$$

(i.e., the overall probability that pirates win) is called an error probability of $C$.

In order to specify the restriction for $y$ mentioned in Step 4, first we present some definitions. For binary words $w^{(1)}, \ldots, w^{(k)}$ of length $m$, we define

$$\mathcal{E}(w^{(1)}, \ldots, w^{(k)}) = \{ y \in \{0, 1\}^m \mid y_j \in \{w^{(1)}_j, \ldots, w^{(k)}_j\} \text{ for every } j \in [m] \}$$

(2)

and call it the envelope of $w^{(1)}, \ldots, w^{(k)}$. On the other hand, we define

$$\tilde{\mathcal{E}}(w^{(1)}, \ldots, w^{(k)}) = \{ y \in \{0, 1, ?\}^m \mid \text{if } w^{(1)}_j = \cdots = w^{(k)}_j \text{ then } y_j = w^{(1)}_j \}$$

(3)

and call it the extended envelope of $w^{(1)}, \ldots, w^{(k)}$. Note that $\tilde{\mathcal{E}}(w^{(1)}, \ldots, w^{(k)}) \cap \{0, 1\}^m = \mathcal{E}(w^{(1)}, \ldots, w^{(k)})$. In this article, we put the following standard assumption called Marking Assumption [5]:

**Definition 2** The Marking Assumption states the following: If $U_p = \{i_1, i_2, \ldots, i_k\}$, then the attack word $y$ belongs to the extended envelope $\tilde{\mathcal{E}}(w_{i_1}, w_{i_2}, \ldots, w_{i_k})$ of codewords for the pirates.

For $j \in [m]$, $j$-th column in codewords is called undetectable if $j$-th bits $w_{i,j}$ of the codewords $w_i$ for pirates $i \in U_p$ coincide with each other; otherwise the column is called detectable. Then the Marking Assumption can be rephrased as follows: For the attack word $y$, for every undetectable column $j$, we have $y_j = w_{i,j}$ for some (or equivalently, all) $i \in U_p$ (while $y_j$ may be freely chosen for detectable columns $j$).

We say that a fingerprint code $C$ is collusion-secure if the error probability of $C$ is sufficiently small for any $\text{Reg}$ and $\rho$ under Marking Assumption. More precisely, we say that $C$ is $c$-secure (with $\varepsilon$-error) [5] if the error probability is not higher than a sufficiently small value $\varepsilon$ under Marking Assumption.

### 3 Our 3-secure codes

Here, we propose a codeword generation algorithm $\text{Gen}$ and a tracing algorithm $\text{Tr}$ for 3-secure codes ($c = 3$). The security property will be discussed below.

#### 3.1 Overall structure

The algorithm $\text{Gen}$, with parameter $1/2 \leq p < 1$, is the codeword generation algorithm of Tardos codes [24], but the probability distribution of biases is different: For each (say, $j$-th) column, each user’s bit $w_{i,j}$ is independently chosen by $Pr[w_{i,j} = 1] = p_j$, where $p_j = p$ or $1 - p$ with probability $1/2$ each. Then $\text{Gen}$ outputs $W = (w_{i,j})_{i \in [N], j \in [m]}$ and $\text{st} = (p_j)_{j \in [m]}$.

To describe the algorithm $\text{Tr}$, we introduce some notation. For a binary word $y$ of length $m$ and a collection $W = (w_{i,j})$ of codewords of users, we define

$$\text{Par}(y) = \{i_1i_2i_3 \subseteq U \mid y \in \mathcal{E}(w_{i_1}, w_{i_2}, w_{i_3}) \}$$

(4)

(see Sect. 1.3 for the notation $i_1i_2i_3$). A key property implied by Marking Assumption is that if the attack word $y$ contains no erasure symbols, then $y$ belongs to the envelope of the codewords of pirates and, if furthermore $|U_p| = 3$, the family $\text{Par}(y)$ contains the set of three pirates (here, “Par” stands for “Parents”, which is motivated from the property that if $i_1i_2i_3 \in \text{Par}(y)$, then $y$ can be generated from three words $w_{i_1}, w_{i_2}$ and $w_{i_3}$ according to Marking Assumption).

The overall structure of our tracing algorithm $\text{Tr}$, with words $y$, $w_1, \ldots, w_N$ and state information $\text{st} = (p_j)_{j \in [m]}$ as input, is the following, where $\text{Tr}_1$ and $\text{Tr}_2$ are subroutines defined later:

1. Replace each erasure symbol “?” in $y$ with “0” or “1” independently in the following manner. If $y_j = ?$, then...
it is replaced with “1” with probability \( p_j \), and with “0” with probability \( 1 - p_j \). Let \( y' \) denote the resulting word.

2. Execute the subroutine \( \text{Tr}_1 \), with \( y', w_1, \ldots, w_N \) and \( \text{st} = (p_j)_{j \in [m]} \) as input. If the output of \( \text{Tr}_1 \) is empty, then go to the next step. Otherwise, output the (non-empty) output of \( \text{Tr}_1 \) and halt.

3. Execute the subroutine \( \text{Tr}_2 \), with \( y' \) and \( w_1, \ldots, w_N \) as input. Then output the (possibly empty) output of \( \text{Tr}_2 \) and halt.

Roughly speaking, the first subroutine \( \text{Tr}_1 \) plays a role of coarse filter, which defies “unbalanced” pirate strategies. Namely, if the contribution of a pirate’s codeword to generate the attack word \( y \) is much larger than other pirate’s codeword, then such a pirate will be correctly accused by \( \text{Tr}_1 \) with overwhelming probability; while any innocent user will be unlikely to be falsely accused. Then, after the coarse filtering, the second subroutine \( \text{Tr}_2 \) performs more refined tracing, which is the main part of our tracing algorithm. In fact, this subroutine will fail when the pirate strategy is too unbalanced in the above sense; this is the reason why the auxiliary tracing process \( \text{Tr}_1 \) is introduced before the main part \( \text{Tr}_2 \).

We notice that \( \text{Tr}_1 \) is a kind of so-called single decoders, while \( \text{Tr}_2 \) is a kind of so-called joint decoders. For the case \( p = 1/2 \) of our codeword generation algorithm, it is known that the “minority vote” by three pirates for generating the attack word \( y \) cancels the mutual information between \( y \) and a single codeword, therefore the pirates are likely to escape from the single decoder \( \text{Tr}_1 \). However, even by such a strategy the pirates are unlikely to escape from the joint decoder \( \text{Tr}_2 \), as collections of users rather than individual users are considered there.

In the above algorithm, an arbitrary attack word \( y \), which may contain erasure symbols, is mapped in Step 1 to another word \( y' \) with no erasure symbols, for the purpose of simplifying the subsequent tracing process. As the information on the erasure symbols in \( y \) is missed during this replacement, one may think that the tracing performance can be improved by making use of the missing information on the erasure symbols. However, note that the modified binary attack word \( y' \) generated in Step 1 of the tracing algorithm can be generated as well by some pirate strategy not using erasure symbols. This implies that the highest error probability of the present tracing algorithm can be achieved by a pirate strategy not using erasure symbols; therefore, even if we can improve the performance of the tracing algorithm against pirate strategies using erasure symbols, it does not improve the performance against the best pirate strategy (which will not use erasure symbols). Hence, from the viewpoint of simplicity, we prefer to design the tracing algorithm by ignoring information on the erasure symbols, without any decrease in the tracing performance against the best pirate strategy.

3.2 The first subroutine

We describe the first subroutine \( \text{Tr}_1 \), with binary words \( y', w_1, \ldots, w_N \) and state information \( \text{st} = (p_j)_{j \in [m]} \) as input, as follows:

1. Calculate a threshold parameter \( Z = Z_{y'} \) as specified below.
2. For each \( i \in U \), calculate the score \( S(i) \) of \( i \) by
   \[
   S(i) = \sum_{j \in [m]} \delta_{w_i,j,y'_j} \log \frac{1}{p_j} + \sum_{j \in [m]} \delta_{w_i,j,y'_j} \log \frac{1}{1 - p_j}.
   \]
3. For each \( i \in U \) do the following: Check if \( S(i) \geq Z \), and if it is satisfied, then output \( i \).

Roughly speaking, if some pirates’ codewords contribute to generate the attack word at too many columns than the other pirates’ codewords, then it is very likely that scores of such pirates exceed the threshold and they are correctly accused by Step 3. Hence this process defies “unbalanced” pirate strategies in the above sense.

Note that our scoring function (5) is different from the ones for Tardos codes [24] and its symmetrized version [21] that have been shown to provide significantly good performance. The choice of our scoring function is just due to a technical reason; in our tracing algorithm \( \text{Tr} \) the second subroutine \( \text{Tr}_2 \) is executed only when the scores of all users are lower than the threshold, and the shape of our scoring function makes it easier to theoretically evaluate the error probability of \( \text{Tr}_2 \) conditioned on such lower scores. There is a possibility that the true error probability of our tracing algorithm \( \text{Tr} \) is reduced by applying the conventional scoring functions and another novel evaluation technique enables us to prove a (better) bound of the reduced error probability. Improvements of our result in this way will be a future research topic.

The threshold parameter \( Z = Z_{y'} \) in Step 1 is determined as follows. Let \( A_H \) be the set of column indices \( j \) such that \( (p_j, y'_j) = (p, 1) \) or \( (1 - p, 0) \), that is, the occurrence probability of the bit \( y'_j \in \{0, 1\} \) at \( j \)-th column is \( p \geq 1/2 \), and let \( A_L = [m] \setminus A_H \). Put \( a_H = |A_H| \) and \( a_L = |A_L| \). Choose a parameter \( \varepsilon_0 > 0 \), which is smaller than the desired bound \( \varepsilon \) of error probability. Then choose \( Z = Z_{y'} \) satisfying the
following condition:

\[
\sum_{k_h,k_l} \frac{(a_L)_{k_h,k_l}}{p_L + (k_L - 1)p_L^{k_h} (1-p)^{k_h}} \leq \frac{\epsilon_0}{N},
\]

where the sum runs over all integers \(k_h, k_l \geq 0\) such that \(k_h \log \frac{1}{p} + k_l \log \frac{1}{p} \geq Z\). An example of a concrete choice of \(Z\) satisfying the condition (6) is as follows:

\[
Z_0 = a_H p \log \frac{1}{p} + a_L (1-p) + \frac{1}{2} \left( \log \frac{1}{p} \right)^2 a_H + \frac{1}{2} \left( \log \frac{1}{p} \right)^2 a_L \log \frac{N}{\epsilon_0}
\]

(see Sect. 5.1 for the proof). From now, we suppose that the threshold \(Z\) satisfies the condition (6) and \(Z \leq Z_0\).

Note that when \(p = 1/2\), the score \(S(i)\) of a user \(i\) is equal to \(2 \log 2\) times the number of columns in which the words \(w_i\) and \(y'\) coincide. Hence the calculation of scores can be made easier by using the “normalized” score \(\tilde{S}(i) = S(i)/\log 2\) instead, which is equal to \(m\) minus the Hamming distance of \(w_i\) from \(y'\), together with the “normalized” threshold \(Z_0/\log 2 = m/2 + (m/2) \log (N/\epsilon_0)\).

3.3 The second subroutine

We describe the second subroutine \(T_r\), with binary words \(y'\) and \(w_1, \ldots, w_N\) as input, as follows:

1. Calculate the set \(\text{Par}' = \{ T \in \text{Par}(y') | T \cap T' \neq \emptyset \text{ for every } T' \in \text{Par}(y') \}\). If \(\text{Par}' = \emptyset\), then halt (with empty output).
2. If \(\bigcap \text{Par}' \neq \emptyset\), then output every member of \(\bigcap \text{Par}'\) and halt.
3. Calculate the set \(\mathcal{P} = \{ i i_2 \subseteq U | i i_2 \cap T \neq \emptyset \text{ for every } T \in \text{Par}' \}\). Let \(\mathcal{P}_k\) be the set of all \(i \in U\) such that \(|\{ P \in \mathcal{P} | i \in P \}| = k\).
4. If \(\mathcal{P}_1 \neq \emptyset\), then do the following and halt (otherwise go to the next step): For each \(i \in \bigcup \mathcal{P}\), check if \(ii' \in \mathcal{P}\) for some \(i' \in \mathcal{P}_1\), and if it is satisfied, then output \(i\).
5. If \(|\mathcal{P}| = 7\), then do the following and halt (otherwise go to the next step): For each \(i \in \bigcup \mathcal{P}\), check if \(ii' \in \mathcal{P}\) for some \(i' \in \mathcal{P}_2\), and if it is satisfied, then output \(i\).
6. If \(|\mathcal{P}| = 6\), then output every \(i \in \mathcal{P}_3\) and halt.
7. If \(|\mathcal{P}| = 5\) and \(\text{Par}'' \neq \emptyset\), where \(\text{Par}''\) is defined by

\[
\text{Par}'' = \{ i i_2 i_3 \in \mathcal{P} | i i_2, i_2 i_3, i i_3 \in \mathcal{P} \},
\]

then output every member of \(\mathcal{P}_2 \cap (\bigcup \text{Par}'')\) and halt.
8. If \(|\mathcal{P}| = 5\) and \(\text{Par}'' = \emptyset\), where \(\text{Par}''\) is defined by (8), then do the following and halt (otherwise go to the next step): For each \(i \in \bigcup \mathcal{P}\), check if \(ii' \notin \mathcal{P}\) for some \(i' \in \bigcup \mathcal{P}\), and if it is satisfied, then output \(i\).
9. If \(|\mathcal{P}| = 4\), then do the following and halt (otherwise go to the next step): For each \(i \in \bigcup \mathcal{P}\), check if \(i \notin T\) for every \(T \in \text{Par}'\) such that \(T \subseteq \bigcup \mathcal{P}\), and if it is satisfied, then output \(i\).
10. If \(|\mathcal{P}| = 3\), then output every \(i \in \bigcup \mathcal{P}\) and halt.
11. Output nobody and halt.

In this and the next paragraphs, we give some explanation of the construction of the algorithm. The first insight is that, given a “binarized” attack word \(y'\) under Marking Assumption, the triple of pirates (when there are precisely three pirates) belongs to the set \(\text{Par}(y')\), while any triple of innocent users is very unlikely to be a member of \(\text{Par}(y')\) (as shown in later sections). Therefore, the triple of pirates will be a member of the set \(\text{Par}'\) with overwhelming probability, which gives a condition to significantly refine the candidates of pirates. This process is represented as Steps 1 and 2.

When the algorithm did not halt until Step 2, next we intend to determine a pirate by investigating the detailed “structure” of the set \(\text{Par}'\). Roughly speaking, it will be shown in later sections that \(\text{Par}'\) is very unlikely to involve certain “symmetric” structures (see “Type III error” and “Type IV error” in Sect. 4), and the resulting asymmetry of \(\text{Par}'\) gives us a key to determine a pirate. Such possible asymmetric structures of \(\text{Par}'\) can even be classified into a few dozens of patterns in a certain manner, but it is space-consuming to enumerate them and specify an appropriate output for each pattern in a case-by-case manner. (Some examples of the possibilities of \(\text{Par}'\) are given in Fig. 1, where 1, 2, 3 are the pirates, \(i_2\) are innocent users and the members of \(\text{Par}'\) are denoted by triangles.) Moreover, it also takes non-negligible computing cost to determine, from given data of \(\text{Par}'\), to which of the enumerated patterns the present \(\text{Par}'\) belongs. Instead, we prefer to give a somewhat artificial but explicit algorithm (Steps 3–11) to determine a suitable output directly from the set \(\text{Par}'\), which is much less space-consuming than the complete enumeration.

Here, we give a brief discussion on computational complexity of the algorithm \(T_r\), in particular, of calculation of the set \(\text{Par}'\) from \(\text{Par}(y')\). We consider the case \(p = 1/2\) for simplicity. The computational complexity depends mainly on the size of the set \(\text{Par}(y')\), which is of order \(\Theta(N^3)\) in the worst case. Nevertheless, it can be significantly reduced in average case. First, as we have mentioned above, it holds with overwhelming probability that every member of \(\text{Par}(y')\) has non-empty intersection with the set of the three pirates. The number of members of \(\text{Par}(y')\) that consists of two pirates and one innocent user is at most \(3(N-3)\). On the other hand, for each pirate \(i \in U_p\), we may assume that the words \(w_i\) and \(y'\) differ at \(m - Z_0/\log 2 = m/2 - \sqrt{(m/2)} \log (N/\epsilon_0)\) more columns, as otherwise the tracing algorithm \(T_r\)
should have halted at the first part Tr₁ by outputting i. As the codewords of innocent users are chosen independently and uniformly at random from all m-bit binary words, it follows that for two distinct innocent users i₁ and i₂, we have \( i₁i₂ ∈ \text{Par}(y') \) with probability at most \((3/4)^m - Z₀/\log 2\), therefore the expected number of members of \( \text{Par}(y') \) that consist of one pirate and two innocent users is at most \(3(N-3)3/4^m - Z₀/\log 2\). This number is not too large in practical cases, as m should not be too small in order to keep the security [see (12) below]. This argument suggests that the calculation of \( \text{Par}' \) from \( \text{Par}(y') \) is less dominant than calculation of \( \text{Par}(y') \) itself, the latter seeming to require \( \Omega(N^3) \) computational complexity in a naive manner.

3.4 The security

For the security of the proposed fingerprint code, first we present the following result, which will be proven in Sect. 4:

**Theorem 1** By the above choice of \( ε₀ \) and \( Z \), if the number of pirates is three, then the error probability of the proposed fingerprint code is lower than

\[
ε₀ + \binom{N-3}{3} f₁(p)^m + 3(N-3)(N-4)f₂(p)^m + (N-3)(1-p)^{-3\sqrt{(m/2)\log(N/ε₀)}} f₃(p)^m.
\]

\[ f₁(p) = 1 - 3p^2 + 10p^3 - 15p^4 + 12p^5 - 4p^6. \]
\[ f₂(p) = p^2(1-p)^2(\sqrt{p} + \sqrt{1-p}) + 1 - p - p^2 + 4p^3 - 2p^4, \]
\[ f₃(p) = p^{4-3p}(p^2 - 3p + 3) + (1-p)^{3p+1} × (p^2 + p + 1). \]

Some numerical analysis suggests that the choice \( p = 1/2 \) would be optimal (or at least pretty good) to decrease the bound of error probabilities specified in Theorem 1. In fact, an elementary analysis shows that the second term \( (N-3)f₁(p)^m \) in the sum, which seems dominant (cf., Theorem 2 below), takes the minimum over \( p ∈ [1/2, 1] \) at \( p = 1/2 \). Hence, we use \( p = 1/2 \) in the following argument. Now, it is shown that the error probability against less than three pirates also has the same bound under a condition (12) below (which seems trivial in practical situations), therefore we have the following (which will be proven in Sect. 4):

**Theorem 2** By using the value \( p = 1/2 \), the proposed fingerprint code is 3-secure with error probability lower than

\[
eₐ + \binom{N-3}{3} \left( \frac{7}{8} \right)^m + 3(N-3)(N-4) \left( \frac{10 + \sqrt{2}}{16} \right)^m + (N-3)8^{(m/2)\log(N/ε₀)} \left( \frac{7\sqrt{2}}{16} \right)^m \]

provided

\[ m ≥ 8 \log \frac{N}{ε₀} \left( 1 + \frac{1}{16\log(N/ε₀)} \right)^2 . \]

Here, we give a remark on a relation between false-negative and false-positive in the tracing algorithm. It will be shown in Sect. 4 and later sections that, in the bounds (9) and (11) of error probabilities, the first term \( ε₀ \) corresponds to false-negative, while the second term corresponds to false-negative (the other terms are relevant to both of false-positive and false-negative). As the second term would be dominant (unless \( ε₀ \) is set to be too large), the probability of false-negative would be dominant among the whole error probability. This means that if some application requires the probability of false-positive to be very low while it allows the probability of false-negative to be relatively high, it is expected that the code length can be reduced further in such a situation. This relation between false-negative and false-positive seems practically desirable, as usually false-positive is regarded as being more crucial than false-negative.

3.5 Comparison of code lengths with other codes

Table 1 shows comparison of our code lengths (numerically calculated by using Theorem 2) with 3-secure codes
secure codes by Nuida et al. for mainly studied from asymptotic viewpoints and given much longer code lengths than the codes in [15], and even significantly shorter than the codes in [18], and almost all significantly shorter than the codes in [15].

In order to perform comparisons with the latter codes, here we show some asymptotic properties of our codes. First, for the rate of our proposed codes, we have the following result, which will be proven in Sect. 5.8:

**Theorem 3** We use the value \( p = 1/2 \). Then, for any positive number \( R \) such that

\[
R < R_0 = 1 - \frac{\log 7}{3 \log 2} \approx 0.064215 \ldots
\]

the error probability of our proposed 3-secure code with code length \( m \) and user number \( N = \lfloor 2^m R \rfloor \) approaches to 0 exponentially in \( m \), where the parameter \( \epsilon_0 \) is set to be \( \epsilon_0 = \exp(-\alpha m) \) with positive constant \( \alpha \) satisfying

\[
\alpha < \frac{2}{9(\log 2)^2} \left( R_0 \log 2 + \log \left( \frac{7\sqrt{2}}{16} \right) \right)^2 - R_0 \log 2
\]

\[
\approx 0.043250 \ldots
\]
By the theorem, the achievable rate of our 3-secure code is at least $R_0$. Regarding preceding results on the achievable rates of 3-secure codes, the rate of c-secure codes by Barg, Blakley and Kabatiansky [2] in the case $c = 3$, which is shown in Corollary 5.2 of [2], is at most $R(s)^c / c^3 = R(s)^c / 27$, where $R(s)^c$ denotes (as in [2]) the maximum achievable rate of $(c, c)$-separating codes. In particular, this rate cannot be higher than $1/27 \approx 0.037037 \ldots$, therefore the rate of our code is significantly higher than that in [2]. On the other hand, the c-secure codes by Amiri and Tardos [1] have, in the case $c = 3$, achievable rate 0.0975 (as shown in Table 1 of [1]), which is much higher than our codes. However, their tracing algorithm would require much more computational time than our algorithm and therefore be not practical, as it seems that their algorithm needs to solve certain convex optimization problem associated with each triple of users. Moreover, it is claimed in Fig. 2(a) of [9] by Huang and Moulin (which is a full version of [8]) that their c-secure codes in the case $c = 3$ have achievable rate higher than (or at least the same as) our rate. However, their argument restricts the pirate strategies to some “symmetric” ones, therefore it is not yet guaranteed that their codes have sufficiently low error probabilities in practical cases against arbitrary pirate strategies under Marking Assumption. It is a future research topic to construct 3-secure codes that are provably secure with concrete bounds of error probabilities, have efficient tracing algorithms, and have achievable rates close to the latter two results.

Secondly, for the asymptotic behavior of our code lengths, we have the following result, which will be proven in Sect. 5.9:

**Theorem 4** We use the value $p = 1/2$, and put $\epsilon_0 = N \exp(-3\min /40)$. If $0 < \epsilon \leq 1/3$, then the code length $m$ of our 3-secure code with error probability $\epsilon$ is shorter than or equal to $m = \lceil 9K \log(N/\epsilon) \rceil$, where

$$K = \frac{1}{9R_0 \log 2} \approx 2.4963 \ldots$$  

(16)

[see (14) for the definition of $R_0$].

This result shows that the ratio $m / (c^2 \log(N/\epsilon))$, which has been used in the literature to compare the code lengths in asymptotic cases, is approximately 2.50 for our 3-secure codes. This value is significantly smaller than the theoretically proven asymptotic ratios in [21] (i.e., $\pi^2 / 2 \approx 4.93$) and in [23] (i.e., $2\pi^2 \approx 19.7$), and the ratio shown in Fig. 1 of [4] (i.e., over 25 for $c = 3$). Our ratio is also significantly smaller than the asymptotic ratio $\pi^2 / 2 \approx 4.93$ in [21] under an experimentally verified assumption on approximation based on Central Limit Theorem. This suggests that our code length is much shorter than the 3-secure codes in [4, 21, 23].

### 4 Security proof

In this section, we present an outline of the proof of Theorems 1 and 2. Omitted details of the proof will be supplied in Sect. 5.

First, we present some properties of the threshold parameter $Z = Z_l$, which will be proven in Sect. 5.1:

**Proposition 1** If $Z$ satisfies the condition (6), then the conditional probability that $S(l) \geq Z$ for some $l \in U_1$, conditioned on the choice of $y$, is not higher than $(N - 1)\epsilon_0 / N$.

**Proposition 2** The value $Z = Z_0$ in (7) satisfies the condition (6).

To prove Theorem 1, we consider the case that the number of pirates $|U_p|$ is three. By symmetry, we may assume that $U_p = \{1, 2, 3\}$. Put $T_p = 123$, therefore we have $T_p \in \text{Par}(y')$ by Marking Assumption. Now, we consider the following four kinds of events:

1. Type I error: $S(l) \geq Z$ for some innocent user $l \in U_1$.
2. Type II error: $T \cap T_p = \emptyset$ for some $T \in \text{Par}(y')$.
3. Type III error: There are $T_1, T_2 \in \text{Par}(y')$ such that $\emptyset \neq T_1 \cap T_2 \subseteq U_1$, $|T_1 \cap T_p| = 1$ and $|T_2 \cap T_p| = 1$.
4. Type IV error: $S(i) < Z$ for every $i = 1, 2, 3$, and there is an innocent user $l$ such that $12l \in \text{Par}(y')$, $13l \in \text{Par}(y')$ and $23l \in \text{Par}(y')$.

Then, we have the following property, which will be proven in Sect. 5.2:

**Proposition 3** If $|U_p| = 3$, then the probability of Type II error is not higher than $(N - 3)^3 f_1(p)^m$.

**Proposition 4** If $|U_p| = 3$, then the probability of Type III error is not higher than $3(N - 3)^2(N - 4)^2 f_2(p)^m$.

**Proposition 5** If $|U_p| = 3$ and the threshold $Z$ is chosen so that the condition (6) holds and $Z \leq Z_0$, then the probability of Type IV error is lower than 

$$(N - 3)(1 - p)^{-3} \sqrt{(m/2) \log(N/\epsilon_0)} f_3(p)^m.$$  

(17)

Note that Type I error mainly corresponds to false-positive, while Type II error causes false-negative only. Type III and Type IV errors are relevant to both false-positive and
false-negative. As the probability of Type II error seems dominant among the four kinds of errors (unless $\varepsilon_0$ is too large), it follows that the whole error probability would mainly consist of that of false-negative.

To prove Theorem 2, we set $p = 1/2$. Then the bound of error probability given by Theorem 1 is specialized to the value specified in Theorem 2. Hence our remaining task is to evaluate the error probabilities for the case that the number of pirates is one or two.

First, we consider the case that there are exactly two pirates, say, $1, 2 \in U$. The key property is the following, which will be proven in Sect. 5.6:

**Proposition 6** In this situation, if the condition (12) is satisfied, then the probability that $S(1) < Z$ and $S(2) < Z$ is lower than $\varepsilon_0/N$.

By this proposition, when the condition (12) is satisfied, at least one of the two pirates is output in Step 3 of the tracing algorithm with probability not lower than $1 - \varepsilon_0/N$. On the other hand, by Proposition 1, some innocent user is output in Step 3 with probability not higher than $(N - 1)\varepsilon_0/N$. Hence in Step 3, at least one pirate and no innocent users are output with probability not lower than $1 - \varepsilon_0$. This implies that the error probability is bounded by $\varepsilon_0$ in this case.

Secondly, we consider the case that there is exactly one pirate, say, $1 \in U$. Then, we have the following property, which will be proven in Sect. 5.7:

**Proposition 7** In this situation, if $m \geq 2\log(N/\varepsilon_0)$, then the score $S(1)$ of the pirate is always higher than or equal to $Z$.

By this proposition, when the condition (12) is satisfied, the pirate is always output in Step 3 of the tracing algorithm. Hence by the same argument as the previous paragraph, the error probability is bounded by $\varepsilon_0$ in this case as well. Summarizing, the proof of Theorem 2 is concluded.

## 5 Proofs of the propositions

### 5.1 Proof of Proposition 1

First, we prove the claim 1 of Proposition 1. For each $l \in U_1$ and $\sigma \in \{H, L\}$, let $K_\sigma = \{j \in A_\sigma \mid w_{l,j} = y'_j\}$. Then, we have $S(l) = |K_H| \log(1/p) + |K_L| \log(1/(1 - p))$. Now note that the choice of $y'$ is independent of $w_l$. This implies that we have $Pr[w_{l,j} = y'_j \mid y'] = p$ for each $j \in A_H$, and we have $Pr[w_{l,j} = y'_j \mid y'] = 1 - p$ for each $j \in A_L$. Hence the conditional probability that $|K_H| = k_H$ and $|K_L| = k_L$, conditioned on this $y'$, is $\binom{n}{k_H} \binom{m - n}{k_L} (1 - p)^k_H p^{m - k_H} (1 - p)^k_L (1 - p)^{m - k_H}$. This implies that $Pr[S(l) \geq Z \mid y']$ is equal to the left-hand side of (6), therefore the claim 1 holds as there exist at most $N - 1$ innocent users $l$.

Secondly, to prove the claim 2 of Proposition 1, we use the following Hoeffding’s Inequality:

**Theorem 5** ([7], Theorem 2) Let $X_1, X_2, \ldots, X_n$ be independent random variables such that $a_i \leq X_i \leq b_i$ for each $i$. Let $\bar{X}$ be the average value of $X_1, \ldots, X_n$. Then for $t > 0$, we have

$$Pr[|\bar{X} - E[\bar{X}]| \geq t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right).$$

As mentioned above, the left-hand side of (6) is equal to $Pr[S(l) \geq Z \mid y']$, where $l$ is any specified innocent user. Now for each $j \in [m]$, let $X_j$ be a random variable such that

$$Pr[X_j = \log(1/p)] = p \quad \text{if } j \in A_H,$$

$$Pr[X_j = 0] = 1 - p \quad \text{if } j \in A_L.$$idents and $S(l) = m\bar{X}$. Now by a direct calculation, we have $E[S(l) \mid y'] = m E[\bar{X} \mid y'] = \mu$ where $\mu = a_H p \log(1/p) + a_L (1 - p) \log(1/(1 - p))$. Moreover, we have $0 \leq X_j \leq \log(1/p)$ if $j \in A_H$, and we have $0 \leq X_j \leq \log(1/(1 - p))$ if $j \in A_L$. Hence Theorem 5 implies that

$$Pr[S(l) \geq mt \mid y'] \leq \exp\left(-\frac{2m^2t^2}{a_H \log(1/p)^2 + a_L \log(1/(1 - p))^2}\right)$$

for $t > 0$. Now by setting $t = \eta/m$ where

$$\eta = \sqrt{\frac{1}{2} \left(\left(\log \frac{1}{p}\right)^2 a_H + \left(\log \frac{1}{1 - p}\right)^2 a_L\right) \log \frac{N}{\varepsilon_0}},$$

the right-hand side of (20) is equal to $\varepsilon_0/N$. On the other hand, for the left-hand side of (20), we have

$$Pr[S(l) - \mu \geq mt \mid y'] = Pr[S(l) \geq \mu + \eta \mid y'],$$

while the value of $Z = Z_0$ in (7) is equal to $\mu + \eta$. Hence the condition (6) is satisfied, concluding the proof of Proposition 1.

### 5.2 Proof of Proposition 2

To prove Proposition 2, suppose that it is not the case of Type I-IV errors. We show that tracing error does not occur in this case. Recall that $T_P = 123 \in Par(y')$. By the absence of Type I error, it holds that either some pirate and no innocent users are output in Step 3 of $\mathcal{Tr}$, or $S(t) < Z$ for every $t \in U$ and nobody is output in Step 3. It suffices to consider the latter case. We have $T_P \in Par'$ by the absence of Type II error. Hence every $T \in Par'$ intersects $T_P$, and
\( \bigcap \Par' \subseteq T_P. \) By virtue of Step 2, it suffices to consider the case that \( \bigcap \Par' = \emptyset. \) Now, there are the following two cases: (A) we have \( |T \cap T_P| = 1 \) for some \( T \in \Par; \) (B) we have \( |T \cap T_P| = 2 \) for every \( T \in \Par \setminus \{T_P\}. \)

### 5.2.1 Case (A)

Let \( T_1 \in \Par' \) and \( |T_1 \cap T_P| = 1. \) By symmetry, we may assume that \( T_1 \cap T_P = \{1\}. \) By the fact \( \bigcap \Par' = \emptyset, \) there is a \( T_2 \in \Par' \) such that \( 1 \not\in T_2. \) We may assume by symmetry that \( 2 \not\in T_2, \) as \( T_2 \cap T_P \neq \emptyset. \) We have \( T_1 \cap T_2 = \emptyset \) as \( T_1 \in \Par', \) therefore the absence of Type III error implies that \( 3 \in T_2. \) Put \( T_2 = 23I \) with \( I \in U_1, \) and \( T_1 = 1I' \) with \( I' \in U_1. \) Now, if we calculate the set \( \Par' \) by using \( \{T_P, T_1, T_2\} \) instead of \( \Par', \) then the result is

\[
\{12, 13, 11, 2I, 2I', 3I, 3I'\}. \tag{23}
\]

In general, the actual set \( \Par \) is included in the set (23). Now, we present two properties. First, we show that 12, 13 \( \in \Par. \) Indeed, if \( 12 \not\in \Par, \) then we have \( 12 \cap T = \emptyset \) for some \( t \in \Par'. \) Now, we have \( 3 \in T \) and \( T_1 \cap T = \emptyset \) as \( T \in \Par', \) therefore \( T_1 \) and \( T \) contradict the absence of Type III error. Hence we have 12 \( \in \Par, \) and 13 \( \in \Par \) by symmetry. Secondly, we show that no innocent users are output in Step 4. Indeed, if an \( I' \in U_1 \) is output in Step 4, then the possibility of \( \Par \) mentioned above implies that \( I'' \in \{1, I'\} \) and we have \( i \in \Par_1 \) and \( iI'' \in \Par \) for some \( i \in 123. \) This is impossible, as 12, 13 \( \in \Par. \) Hence this claim holds, therefore it suffices to consider the case that nobody is output in Step 4, namely \( \Par_1 = \emptyset. \)

By these properties, we have either 2I', 3I' \( \in \Par \) or 2I', 3I' \( \not\in \Par \) (otherwise \( I' \in \Par_1, \) a contradiction). Similarly, we have \( \Par \cap \{2I', 3I'\} \neq \emptyset \) and \( \Par \cap \{3I', 3I'\} \neq \emptyset. \) First, we consider the case that 2I', 3I' \( \in \Par \). As \( \Par_1 = \emptyset, \) it does not hold that \( |\Par \cap \{11, 2I', 3I'| \neq 1. \) If \( 1I, 2I, 3I \in \Par, \) then \( |\Par| = 7, \Par_2 = \{I\}, \) and 2 and 3 are output in Step 5. If \( |\Par \cap \{11, 2I, 3I\}| = 2, \) then \( |\Par| = 6, \Par_2 = \{1I' \subseteq U_1\} \) and a pirate is correctly output in Step 6. Finally, if 1I, 2I, 3I \( \not\in \Par, \) then \( |\Par| = 4 \) and \( \Par = \{12, 13, 2I', 3I'\}. \) Now, \( I' \) is not output in Step 9, as 123 \( \in \Par'. \) Moreover, if none of 1, 2, and 3 is output in Step 9, then it should hold that 12I', 13I', 23I' \( \in \Par', \) contradicting the absence of Type IV error. Hence a pirate is correctly output in Step 9, concluding the proof in the case 2I', 3I' \( \in \Par. \)

Secondly, we suppose that 2I', 3I' \( \not\in \Par, \) therefore 2I, 3I \( \in \Par. \) There are two possibilities \( \Par = \{12, 13, 2I, 3I\} \) and \( \Par = \{12, 13, 11, 2I, 3I\}. \) The former case is the same as the previous paragraph. In the latter case, we have \( |\Par| = 5, \Par'' \subseteq \{12I, 13I\} \) and \( \Par_2 = 23. \) Hence 2 or 3 is correctly output in Step 7 when \( \Par'' \neq \emptyset. \) On the other hand, when \( \Par'' = \emptyset, \) 2 and 3 are correctly output in Step 8. Hence the proof in the case 2I', 3I' \( \not\in \Par \) [therefore in the case (A)] is concluded.

### 5.2.2 Case (B)

As \( \bigcap \Par' = \emptyset, \) there are \( 1I, 2I, 3I \in U_1 \) such that \( 12I, 13I, 23I \in \Par'. \) By the absence of Type IV error, it does not hold that \( 1I = 2I = 3I. \) By symmetry, we may assume that \( 1I \neq 2I. \) Then by calculating the set \( \Par \) by using \( \{123, 12I, 13I, 23I\} \) instead of \( \Par', \) it follows that the actual \( \Par \) satisfies \( \Par \subseteq \{12, 13, 23, 1I, 2I, 3I\} \), while 12, 13, 23 \( \in \Par \) by the assumption of the case (B). If \( \Par = \{12, 13, 23\} \), then 1 and 2 are output in Step 10. Therefore, it suffices to consider the case that \( \{12, 13, 23\} \not\subseteq \Par. \)

If \( 1I \neq 1I \neq 1I, \) then we have \( 1I \neq 1I \neq 1I \) and a pirate is correctly output in Step 4. Hence it suffices to consider the remaining case. By symmetry, we may assume that \( 1I \neq 1I \neq 1I \). If \( 2I \in \Par, \) then we have \( 1I \in \Par_1 \subseteq 1I \) and 2 is correctly output in Step 4. From now, we assume that \( 2I \neq 1I. \) If \( 1I \neq 2I \) or \( 3I \neq 2I, \) then we have \( \Par = \{1I\} \) as \( \{12, 13, 23\} \subseteq \Par, \) therefore 1 or 3 is correctly output in Step 4. On the other hand, if \( 1I, 1I \notin \Par, \) then we have \( \Par = \{12, 13, 23, 1I, 3I\}, \) while \( 1I \notin \Par \) by the absence of Type IV error (note that \( 1I, 2I \in \Par' \)), therefore \( \Par'' = \{123, 2I \} \) and 2 is correctly output in Step 7. Hence the proof in the case (B), therefore the proof of Proposition 2, is concluded.

### 5.3 Proof of Proposition 3

To prove Proposition 3, let \( l_1, l_2, l_3 \) be three distinct innocent users. Given \( y' \) and \( st = (p_j)_j, \) we introduce the following notation for \( j \in [m]: \)

\[
\xi_j^H = \begin{cases} 
1 & \text{if } p_j = p, \\
0 & \text{if } p_j = 1 - p,
\end{cases} \quad \xi_j^L = 1 - \xi_j^H. \tag{24}
\]

Note that the sets \( A_\sigma \) for \( \sigma \in \{H, L\} \) defined in Sect. 3 satisfy that \( A_\sigma = \{j \mid y'_j = \xi_j^\sigma\}. \) We write \( A_\sigma = (y'_j, st) \) and \( a_\sigma = |A_\sigma| = a_\sigma(y'_j, st) \) when we emphasize the dependency on \( y'_j \) and \( st. \) Then, as the bits of codewords are independently chosen, we have

\[
Pr[l_1l_2l_3 \in \Par(y') \mid y'_j, st] = (1 - p^3)^{a_H}(1 - (1 - p)^3)^{a_L} , \tag{25}
\]

therefore

\[
Pr[l_1l_2l_3 \in \Par(y')] = \sum_{y'_j, st} Pr[y'_j, st](1 - p^3)^{a_H(y'_j, st)} \times (1 - (1 - p)^3)^{a_L(y'_j, st)} . \tag{26}
\]

Now, we present the following key lemma, which will be proven later:

**Lemma 1** Among the possible pirate strategies \( p, \) the maximum value of the right-hand side of (26) is attained by the majority vote attack, namely the attack word \( y \) for codewords
proof of Lemma 1} Fix the codewords $w_1, w_2, w_3$ of the three pirates $1, 2, 3 \in U$. Let $w_p$ denote the collection of those three codewords. Let $j_0 \in [m]$ be the index of a detectable column. By symmetry, we may assume without loss of generality that $w_{1,j_0} = w_{2,j_0} = 0$ and $w_{3,j_0} = 1$. Now let $y^0$ be an arbitrary attack word such that $y^0_{j_0} = 0$, and let $y^1$ and $y^2$ be the attack words obtained from $y^0$ by changing the $j_0$-th component to 1 and to 0, respectively. We show that if the pirate strategy $\rho$ for the input $w_p$ is modified so that it outputs $y^0$ instead of $y^1$ and $y^2$, then the right-hand side of (26) will not decrease. As $w_p, j_0$ and $y^0$ are arbitrarily chosen, the claim of Lemma 1 then follows.

Let $y^0$ be an $m$-bit word such that $y^0_j = y^0_j$ for any $j \in [m]$ with $y^0_j \neq \overline{y^0_j}$, therefore $y^0$ is obtained from $y_0$ in Step 1 in the tracing algorithm with positive probability. Let $y^1$ be the $m$-bit word obtained from $y^0$ by changing the $j_0$-th column to 1. Moreover, let $s^0 = (p_{j_0})$, be any state information such that $p_{j_0} = 1 - p$, and let $s^1$ be the state information obtained from $s^0$ by changing the $j_0$-th component to $p$.

In this case, by independence of the columns, we have $Pr[w_p | s^0] = \alpha p^2(1 - p)$ and $Pr[w_p | s^1] = \alpha p(1 - p)^2$ for a common $\alpha > 0$. As $Pr[s^0] = Pr[s^1] > 0$ and $Pr[w_p] > 0$, Bayes Theorem implies that $Pr[s^0 | w_p] = \alpha' p^2(1 - p)$ and $Pr[s^1 | w_p] = \alpha' p(1 - p)^2$ for a common $\alpha' > 0$, therefore

$$Pr[s^0 | w_p, (s^0 \text{ or } s^1)] = \frac{\alpha' p^2(1 - p)}{\alpha' p^2(1 - p) + \alpha' p(1 - p)^2} = p$$

(28)

and $Pr[s^1 | w_p, (s^0 \text{ or } s^1)] = 1 - p$. Now there is a common $\beta > 0$ such that, for each $x \in \{0, 1\}$,

$$Pr[y^0 | s^0, y^0] = Pr[y^1 | s^1, y^1] = \beta,$$

$$Pr[y^0 | s^0, y^1] = Pr[y^1 | s^1, y^0] = 0,$$

$$Pr[y^0 | s^0, y^2] = Pr[y^1 | s^1, y^0] = \beta p,$$

$$Pr[y^0 | s^1, y^0] = Pr[y^0 | s^0, y^0] = \beta(1 - p).$$

As the choice of the attack word $y$ for given $w_p$ is independent of $s$, and the choice of the word $y'$ will be independent of $w_p$ once the attack word $y$ is determined, it follows that

$$Pr[y^x, s^{x'} | w_p, (s^0 \text{ or } s^1), y^{x''}] = Pr[s^{x'} | w_p, (s^0 \text{ or } s^1)] Pr[y^x | s^0, s^1, y^{x''}]$$

(30)

for $x, x' \in \{0, 1\}$ and $x'' \in \{0, 1, \}$. By these relations, we have

$$Pr[(y^0, s^0) \text{ or } (y^1, s^1)] | w_p, (s^0 \text{ or } s^1), y^0] = p \cdot \beta + (1 - p) \cdot 0 = p \beta,$$

$$Pr[(y^1, s^0) \text{ or } (y^0, s^1)] | w_p, (s^0 \text{ or } s^1), y^0] = 1 - p \beta,$$

$$Pr[(y^0, s^0) \text{ or } (y^1, s^1)] | w_p, (s^0 \text{ or } s^1), y^1] = p \cdot 0 + (1 - p) \cdot \beta = (1 - p) \beta,$$

$$Pr[(y^1, s^0) \text{ or } (y^0, s^1)] | w_p, (s^0 \text{ or } s^1), y^1] = 1 - (1 - p) \beta,$$

$$Pr[(y^0, s^0) \text{ or } (y^1, s^1)] | w_p, (s^0 \text{ or } s^1), y^2] = p \cdot \beta p + (1 - p) \cdot \beta p = p \beta,$$

$$Pr[(y^1, s^0) \text{ or } (y^0, s^1)] | w_p, (s^0 \text{ or } s^1), y^2] = 1 - p \beta.$$

Now note that $p \geq 1/2$, therefore we have $1 - p^3 \leq 1 - (1 - p)^3$ and $p \beta \geq (1 - p) \beta$. Note also that $a_H(y^0, s^0) = a_H(y^1, s^1) = a_H(y^0, s^1) + 1 = a_H(y^1, s^0) + 1$. This implies that, in the case $s \in \{s^0, s^1\}$, if the pirate strategy $\rho$ for the input $w_p$ is modified in such a way that it outputs $y^0$ instead of $y^1$ and $y^2$, then the right-hand side of (26) will not decrease. As this property is in fact independent of the choice of $s^0$ and $s^1$, the claim in the proof follows, concluding the proof of Lemma 1.

\[ \square \]
5.4 Proof of Proposition 4

To prove Proposition 4, we fix an innocent user \( l_0 \in U_1 \) and consider the probability that there are \( T_1, T_2 \in \text{Par}(y') \) such that \( l_0 \in T_1 \cap T_2 \subseteq U_1, T_1 \cap T_2 = \{l_1\} \) and \( T_2 \cap T_2 = \{l_2\} \); or equivalently, there are innocent users \( l_1, l_2 \in U_1 \setminus \{l_0\} \) such that \( 1 l_0 l_1, 2 l_2 \in \text{Par}(y') \). We introduce some notations. Given \( y', w_1, w_2, w_{l_0}, \) and \( \text{st} = (p_j)_j \), we define, for \( \alpha, \beta, \gamma, \delta \in \{H, L\}, \)

\[
\begin{align*}
& a_{\alpha\beta\gamma\delta} = |\{j \in [m] \mid y'_j = \xi^\alpha_j\}, \\
& w_{1,j} = \xi^\beta_j, w_{2,j} = \xi^\gamma_j, w_{l_0,j} = \xi^\delta_j | \quad (32)
\end{align*}
\]

[see (24) for the notations]. Moreover, by using \( "*" \) as a wild-card, we extend naturally the definition of \( a_{\alpha\beta\gamma\delta} \) to the case \( \alpha, \beta, \gamma, \delta \in \{H, L, \ast\} \). For example, we have \( a_{\alpha\beta\gamma\delta} = a_{\alpha H\beta\delta} + a_{\alpha L\beta\delta} + a_{\alpha L\gamma\delta} + a_{\alpha L\lambda\delta} \). Note that \( a_{\alpha\beta\gamma\delta} (x \in \{H, L\}) \) is equal to the value \( a_x \) in Sect. 3.

Now for an innocent user \( l_1 \neq l_0 \), we have

\[
Pr[l_0 l_1 \in \text{Par}(y') \mid y', w_1, w_2, w_{l_0}, \text{st}] = p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}} .
\]

(33)

Therefore, we have

\[
Pr[l_0 l_1 \in \text{Par}(y') \text{ for some } l_1 \in U_1 \mid y', w_1, w_2, w_{l_0}, \text{st}] \leq (N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}}
\]

as there are \( N - 4 \) choices of \( l_1 \). Similarly, we have

\[
Pr[2 l_2 \in \text{Par}(y') \text{ for some } l_2 \in U_1 \mid y', w_1, w_2, w_{l_0}, \text{st}] \leq (N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}} .
\]

(35)

Hence the probability that \( 1 l_0 l_1, 2 l_2 \in \text{Par}(y') \) for some \( l_1, l_2 \in U_1 \), conditioned on the given \( y', w_1, w_2, w_{l_0}, \) and \( \text{st} \), is lower than the minimum of the two values \((N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}} \) and \((N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}} \), which is not higher than

\[
\sqrt{(N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}}} \cdot \sqrt{(N - 4) p^{a_{HL\ast}} (1 - p)^{a_{LH\ast}}} .
\]

(36)

Now given \( y', w_1, w_2, \) and \( \text{st} \), the probability that \( w_{l_0} \) attains the given values of \( a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast} \), \( a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast} \), denoted here by \( \eta \) is the product of the following six values

\[
\begin{align*}
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast} - a_{HL\ast}} .
\end{align*}
\]

(37)

(38)

(39)

(40)

(41)

(42)

By the above results, it follows that

\[
Pr[l_0 l_1, 2 l_2 \in \text{Par}(y') \text{ for some } l_1, l_2 \in U_1 \mid y', w_1, w_2, \text{st}] \leq \sum \left( \eta (N - 4) \sqrt{p^{2a_{HL\ast} + a_{HL\ast} + a_{HL\ast}}} \right) ,
\]

where the sum runs over the possible values of \( a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast}, a_{HL\ast} \). Now by the above definition of \( \eta \), the summand in the right-hand side is the product of \( N - 4 \) and the following six values

\[
\begin{align*}
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}}, \\
& (a_{HL\ast})(1 - p)^{a_{HL\ast}} p^{a_{HL\ast}} .
\end{align*}
\]

(43)

(44)

(45)

(46)

(47)

(48)

(49)

Then by the binomial theorem, the sum is equal to

\[
(N - 4) (p(2 - p)^{a_{HL\ast} + (p + (1 - p) \sqrt{p})^{a_{HL\ast} + a_{HL\ast}}} \cdot (1 - p + p \sqrt{1 - p})^{a_{HL\ast} + a_{HL\ast}} \cdot ((1 - p)(1 + p))^{a_{HL\ast}} .
\]

(50)

Given \( y', \text{st}, w_1, w_2, \) and \( w_3, \) we define, for \( \alpha, \beta, \gamma, \delta \in \{H, L\}, \)

\[
b_{\alpha\beta\gamma\delta} = |\{j \in [m] \mid y'_j = \xi^\alpha_j, w_{1,j} = \xi^\beta_j, w_{2,j} = \xi^\gamma_j, w_{3,j} = \xi^\delta_j | .
\]

(51)
Then by Marking Assumption, (50) is equal to
\[ (N - 4)(2p - p^2)^{b_{HLLL}} \]
\[ \cdot \left( p + (1 - p)\sqrt{p} \right)^{b_{HLLL} + b_{HLLL} + b_{LLLH} + b_{LHHL}} \]
\[ \cdot \left( 1 - p + p\sqrt{1 - p} \right)^{b_{HLLL} + b_{HLLL} + b_{LLLH} + b_{LHHL}} \]
\[ \cdot \left( 1 - p^2 \right)^{b_{LHHL}} \]
\[ = (N - 4)(2p - p^2)^{b_{HLLL}} (1 - p^2)^{b_{LHHL}} \]
\[ \cdot \left( p + (1 - p)\sqrt{p} \right)^{b_{HLLL} + b_{HLLL} + b_{LLLH} + b_{LHHL}} \]
\[ \cdot \left( 1 - p + p\sqrt{1 - p} \right)^{b_{HLLL} + b_{HLLL} + b_{LLLH} + b_{LHHL}} \]
\[ \cdot \left( 1 - p^2 \right)^{b_{LHHL}} . \] (52)

By writing the right-hand side of (52) as \( \eta' \), it follows that
\[ \Pr[1|l_0l_1, 2l_0l_2 \in \text{Par}(y') \text{ for some } l_1, l_2 \in U_1 \]
\[ | w_1, w_2, w_3] \leq \sum_{y', st} \Pr[y', st | w_1, w_2, w_3] \eta' . \] (53)

Now, we present the following key lemma, which will be proven later:

**Lemma 2** Among the possible pirate strategies \( \rho \), the maximum value of the right-hand side of (53) is attained by majority vote attack \( \rho_{\text{maj}} \) (cf., Lemma 1).

By (53), we have
\[ \Pr[1|l_0l_1, 2l_0l_2 \in \text{Par}(y') \text{ for some } l_1, l_2 \in U_1 \]
\[ \leq \sum_{w_1, w_2, w_3} \Pr[w_1, w_2, w_3] \sum_{y', st} \Pr[y', st | w_1, w_2, w_3] \eta' \]
\[ = \sum_{y', st, w_1, w_2, w_3} \Pr[y', st, w_1, w_2, w_3] \eta' . \] (54)

By virtue of Lemma 2, the maximum value of the right-hand side is attained by majority vote attack \( \rho_{\text{maj}} \). Now for \( \rho = \rho_{\text{maj}} \), the word \( y' \) is uniquely determined by \( w_1, w_2, \) and \( w_3 \), and we have \( b_{HLLL} = b_{LHHL} = b_{LHHL} = b_{HHLL} = b_{HHLL} = b_{HLLL} = b_{LHHL} = b_{LHLL} = b_{HHLL} = b_{HHLL} = b_{HLLL} = b_{LHHL} = b_{LHLL} = b_{HHLL} = b_{HHLL} = 0 \), \( b_{HLLL} = d_{HLLL} \), \( b_{LHHL} = d_{LHHL} \), and \( b_{LHLL} = d_{LHLL} \), where, for \( \alpha, \beta, \gamma \in \{ H, L \}, \)
\[ d_{\alpha\beta\gamma} = | \{ j \in [m] | w_{1,j} = \xi^\alpha_j, w_{2,j} = \xi^\beta_j, w_{3,j} = \xi^\gamma_j \} | . \] (55)

This implies that
\[ \eta' = (N - 4) (p + (1 - p)\sqrt{p})^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot \left( 1 - p + p\sqrt{1 - p} \right)^{d_{HLLL} + d_{HLLL}} . \] (56)

Put \( d_{\text{other}} = m - d_{HLLL} - d_{LHHL} - d_{LHHL} - d_{HLLL} \). Now given \( st \), the probability that \( w_1, w_2 \) and \( w_3 \) attain the given values of \( d_{HLLL}, d_{LHHL}, d_{LHHL} \) and \( d_{HLLL} \) is
\[ \left( \frac{m}{N} \right)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p(1 - p)^2)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p^2(1 - p))^{d_{HLLL} + d_{HLLL} (1 - 2p(1 - p))^{d_{other}}} \] (57)

which is independent of \( st \). This implies that
\[ \sum_{y', st, w_1, w_2, w_3} \Pr[y', st, w_1, w_2, w_3] \eta' \]
\[ = \sum_{y', st} \left( \frac{m}{N} \right)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p(1 - p)^2)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p^2(1 - p)(1 - p + \sqrt{p}))^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (1 - 2p(1 - p))^{d_{other}} \] (58)

(where the sum runs over the possible values of \( d_{HLLL}, d_{LHHL}, d_{LHLL} \), and \( d_{HLLL} \))
\[ = \sum_{d_{HLLL}, d_{LHHL}, d_{LHLL}} \left( \frac{m}{N} \right)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p(1 - p)^2)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (p^2(1 - p)(1 - p + \sqrt{p}))^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (1 - 2p(1 - p))^{d_{other}} \] (59)

(where the sum runs over the possible values of \( d_{HLLL} = d_{HLLL} + d_{HLLL} \) and \( d_{HLLL} = d_{LHHL} + d_{LHLL} \))
\[ = (N - 4) \left( p(1 - p)^{\sqrt{p}} + \sqrt{p} \right)^{d_{HLLL} + d_{HLLL}} \]
\[ \cdot (1 - 2p(1 - p))^{d_{other}} \] (60)

By the above argument, the value \( \Pr[1|l_0l_1, 2l_0l_2 \in \text{Par}(y') \text{ for some } l_1, l_2 \in U_1] \) for a general \( \rho \) is also bounded by the above value. Hence Proposition 4 follows, by considering the number of choices of the pair 1, 2 and the innocent user \( l_0 \).

To complete the proof of Proposition 4, we give a proof of Lemma 2.

**Proof of Lemma 2** First, note that \( 1/2 \leq p < 1 \), therefore \( 0 < 2p - p^2 < 1, 0 < 1 - p^2 < 1 \) and \( 0 < 1 - p + p\sqrt{1 - p} \leq 0 + (1 - p)\sqrt{p} < 1 \). Now by the definition (52) of \( \eta' \), for each \( j \in [m] \) such that \( w_{1,j} = w_{2,j} \neq w_{3,j} \), the value of \( \eta' \) is increased by setting the \( j \)-th bit of the attack word \( y \) to be \( w_{1,j} \) instead of \( w_{3,j} \) or \( w_{2,j} \) (which makes the values of \( b_{HLLL} \) and \( b_{LHHL} \) smaller).

We consider the case that \( w_{1,j} = w_{3,j} \neq w_{2,j} \). If \( w_{1,j} = \xi^H_j \), then the contribution of the \( j \)-th column to the value \( \eta' \) is \( p(1 - p)\sqrt{p} \) when \( y_j = w_{1,j} \) and \( 1 - p + p\sqrt{1 - p} \) when
$y_j' = w_{2,j}$. On the other hand, if $w_{1,j} = \xi_j^L$, then the contribution of the $j$-th column to the value $\nu_j$ is $1 - p + p \sqrt{1 - p}$ when $y_j' = w_{1,j}$ and $p + (1 - p) \sqrt{p}$ when $y_j' = w_{2,j}$. Recall the relation $1 - p + p \sqrt{1 - p} \leq p + (1 - p) \sqrt{p}$. Now the same argument as Lemma 1 implies that $Pr[w_{1,j} = \xi_j^H] = p \geq 1 - p = Pr[w_{1,j} = \xi_j^L]$ in this case. This implies that the value of the right-hand side of (53) is not decreased by setting $y_j'$ to be $w_{1,j}$ instead of $w_{2,j}$ (the detail of the proof is similar to the proof of Lemma 1). Similarly, in the case that $w_{1,j} \neq w_{2,j} = w_{3,j}$, the value of the right-hand side of (53) is not decreased by setting $y_j'$ to be $w_{2,j}$ instead of $w_{1,j}$.

Summarizing, the value of the right-hand side of (53) is not decreased by setting $y_j'$ to be the majority of $w_{1,j}, w_{2,j}$, and $w_{3,j}$, instead of the minority of them. Hence the maximum value of the right-hand side of (53) is attained by the majority vote attack, concluding the proof of Lemma 2. □

5.5 Proof of Proposition 5

To prove Proposition 5, we fix an innocent user $l$ and suppose that $S(i) < Z$ for every $i \in 123$. Given $y', w_1, w_2, w_3,$ and $st$, we define, for $\alpha, \beta, \gamma, \delta \in \{H, L\}$,

$$a_{\alpha r y'3} = |\{j \in [m] \mid y'_j = \xi_j^\alpha, w_{1,j} = \xi_j^\beta, w_{2,j} = \xi_j^\gamma, w_{3,j} = \xi_j^\delta\}|.$$  

(61)

Then, we have

$$Pr[12l, 13l, 23l \in Par(y') \mid y', w_1, w_2, w_3, st] = p^{a_HLHH + a_HHLH + a_HLLL} (1 - p)^{a_HLHH + a_HHLH + a_HLLL}.$$  

(62)

Let $a_L$ and $a_H$ be as defined in Sect. 3. For $x \in \{L, H\}$, let $a^x_L$ and $a^x_H$ be the number of indices $j \in [m]$ of undetectable and detectable columns, respectively, such that $y_j' = \xi_j^x$. Note that $a_H = a_H^H + a_H^L$, while we have $a_H^H = a_{HLLL}$ and $a_H^L = a_{LLLL}$ by Marking Assumption. Now, we have

$$S(1) + S(2) + S(3) = 3(a_{HLLL} + 2(a_{HLHH} + a_{HLHL} + a_{LHHH}) + a_{HHHL} + a_{HHLH} + a_{HLLL}) \log \frac{1}{p} + 3(a_{LLLL} + 2(a_{LHHH} + a_{LHLH} + a_{LLLL}) + a_{LHHH} + a_{LHLH} + a_{LLLL}) \log \frac{1}{1 - p}$$

$$a_H^H \log \frac{1}{p} + a_L^H \log \frac{1}{1 - p} + 2 \left( a_H \log \frac{1}{p} + a_L \log \frac{1}{1 - p} \right)$$

$$= 3 \left( a_{HLLL} + 2(a_{HLHH} + a_{HLHL} + a_{LHHH}) + a_{HHHL} + a_{HHLH} + a_{HLLL} \right) \log \frac{1}{p}$$

$$+ 3 \left( a_{LLLL} + 2(a_{LHHH} + a_{LHLH} + a_{LLLL}) + a_{LHHH} + a_{LHLH} + a_{LLLL} \right) \log \frac{1}{1 - p}$$

$$= a_H^H \log \frac{1}{p} + a_L^H \log \frac{1}{1 - p} + 2 \left( a_H \log \frac{1}{p} + a_L \log \frac{1}{1 - p} \right)$$

$$- (a_{HLLH} + a_{HLHL} + a_{LHHH}) \log \frac{1}{p}$$

$$- (a_{LHHH} + a_{LHLH} + a_{LLLL}) \log \frac{1}{1 - p}.$$

(63)

therefore

$$\left( a_{HLLH} + a_{HLHL} + a_{LHHH} \right) \log \frac{1}{p}$$

$$+ \left( a_{LHHH} + a_{LHLH} + a_{LLLL} \right) \log \frac{1}{1 - p}$$

$$= 2 \left( a_H \log \frac{1}{p} + a_L \log \frac{1}{1 - p} \right) + a_H^L \log \frac{1}{p}$$

$$+ a_L^H \log \frac{1}{1 - p} - S(1) - S(2) - S(3)$$

$$> 2 \left( a_H \log \frac{1}{p} + a_L \log \frac{1}{1 - p} \right) + a_H^L \log \frac{1}{p}$$

$$+ a_L^H \log \frac{1}{1 - p} - 3Z_0$$

(64)

where we used the assumptions that $S(i) < Z$ for every $i \in 123$ and $Z \leq Z_0$. By using the relation $a_L = m - a_H$ and the definition (7) of $Z_0$, the right-hand side of the above inequality is equal to

$$(3p - 1)m \log \frac{1}{1 - p}$$

$$+ a_H \left( 2 - 3p \right) \log \frac{1}{p} + (1 - 3p) \log \frac{1}{1 - p} \right)$$

$$+ a_H^L \log \frac{1}{p} + a_L \log \frac{1}{1 - p}$$

$$- \left( \left( \log \frac{1}{p} \right)^2 a_H + \left( \log \frac{1}{1 - p} \right)^2 a_L \right) \log \frac{N}{\varepsilon_0}$$

$$= (3p - 1)m \log \frac{1}{1 - p} + a_L^H \log \frac{1}{1 - p}$$

$$+ a_L^H \left( 2 - 3p \right) \log \frac{1}{p} + (1 - 3p) \log \frac{1}{1 - p} \right)$$

$$+ a_L^H \log \frac{1}{p} + a_L \log \frac{1}{1 - p}$$

$$- \left( \left( \log \frac{1}{1 - p} \right)^2 - \left( \log \frac{1}{p} \right)^2 \right) a_H \log \frac{N}{\varepsilon_0} \right)^{1/2}$$

(65)

(where we used the relation $a_H = a_H^H + a_H^L$)

$$\geq (3p - 1)m \log \frac{1}{1 - p}$$

$$+ a_L^H \left( 2 - 3p \right) \log \frac{1}{p} + (1 - 3p) \log \frac{1}{1 - p} \right).$$
Lemma 3

Among the possible pirate strategies $\rho$, the maximum value of the right-hand side of (68) is attained by majority vote attack $\rho_{maj}$ (cf., Lemma 1).

By (68), we have

$$Pr[12l, 13l, 23l \in Par(y') | y', w_1, w_2, w_3]$$

$$< \sum_{y',st} Pr[y', st | w_1, w_2, w_3]$$

$$\leq \sum_{y',st} Pr[y', st | w_1, w_2, w_3] \eta .$$

Now we present the following key lemma, which will be proven later:

**Lemma 3** Among the possible pirate strategies $\rho$, the maximum value of the right-hand side of (68) is attained by majority vote attack $\rho_{maj}$ (cf., Lemma 1).

By (68), we have

$$Pr[12l, 13l, 23l \in Par(y')]$$

$$< \sum_{y',st} Pr[y', st | w_1, w_2, w_3] Pr[y', st | w_1, w_2, w_3] \eta$$

$$= \sum_{y',st} Pr[y', st | w_1, w_2, w_3] \eta .$$

By virtue of Lemma 3, the maximum value of the right-hand side is attained by majority vote attack $\rho_{maj}$. Now for $\rho = \rho_{maj}$ and given $st$, the probability that $w_1, w_2, w_3$ and $y'$ attain the given values of $a_{H}^d$, $a_{L}^d$, and $a_{H}^u$ is

$$\left( \begin{array}{c} m \\ a_{H}^u, a_{L}^u, a_{H}^d, a_{L}^d \end{array} \right) (p^{3}y_{H}^u (1 - p)^{3}y_{L}^u$$

$$(3p^{2}(1 - p))y_{H}^u (3p(1 - p)^{2})y_{L}^u$$

which is independent of $st$, where we put $a_{L}^d = m - a_{H}^d - a_{L}^u - a_{H}^u$. Hence we have

$$\sum_{y',st} Pr[y', st | w_1, w_2, w_3]$$

$$= \sum_{a_{H}^u, a_{L}^u, a_{H}^d, a_{L}^d} \left( \begin{array}{c} m \\ a_{H}^u, a_{L}^u, a_{H}^d, a_{L}^d \end{array} \right) (p^{3}y_{H}^u (1 - p)^{3}y_{L}^u$$

$$(3p^{2}(1 - p))y_{H}^u (3p(1 - p)^{2})y_{L}^u$$

By the above argument, the value $Pr[12l, 13l, 23l \in Par(y')]$ for a general $\rho$ is also bounded by the above value. Hence Proposition 5 follows, as there exist $N - 3$ choices of the innocent user $l$.

To complete the proof of Proposition 5, we give a proof of Lemma 3.

**Proof of Lemma 3** First note that, by Marking Assumption, the terms in $\eta$ other than $(p^{2}\cdot 3p(1 - p)^{1-3}p)\eta^i$ are independent of the choice of $y'$ for given $w_1, w_2, w_3$. An elementary analysis shows that $p^{2}\cdot 3p(1 - p)^{1-3}p$ is an increasing function of $p \in [1/2, 1]$, therefore $p^{2}\cdot 3p(1 - p)^{1-3}p \geq (1/2)^{2-3/2}/(1/2)^{1-3/2} = 1$. Hence the value of $\eta$ will be increased by making the value of $a_{H}^d$ as large as possible. By the same argument as Lemma 1, under the condition that the $j$-th column is detectable, the probabilities that the majority among $w_{1,j}, w_{2,j},$ and $w_{3,j}$ is $\xi_{j}^H$ and $\xi_{j}^L$ are $p$ and $1 - p$, respectively. In other words, the probabilities that $\xi_{j}^H$ is the majority and the minority among $w_{1,j}, w_{2,j},$ and $w_{3,j}$ are $p$ and $1 - p$, respectively. As $p \geq 1 - p$, it follows that the value of the right-hand side of (68) will not decrease by setting the $j$-th bit of $y'$ to be the majority of $w_{1,j}, w_{2,j},$ and $w_{3,j}$ instead of the minority of them (the detail of the proof is similar to the proof of Lemma 1). Hence the maximum value of the right-hand side of (68) is attained by the majority vote attack, concluding the proof of Lemma 3. □
5.6 Proof of Proposition 6

First, we introduce some notations. Given the codewords \(w_1\) and \(w_2\) of the two pirates 1 and 2, let \(a_u\) and \(a_d\) denote the numbers of undetectable and detectable columns, respectively. Then by Marking Assumption and the choice \(p = 1/2\), we have \(S(1) + S(2) = (2a_u + a_d) \log 2\) regardless of the pirate strategy \(\rho\). This implies that, if \(S(1) < Z\) and \(S(2) < Z\), then we have

\[
(2a_u + a_d) \log 2 < 2Z \leq 2Z_0
= m \log 2 + \sqrt{2m \log \frac{N}{\varepsilon_0} \log 2}.
\] (73)

By the relation \(a_u + a_d = m\), this implies that \(2m - a_d < m + \sqrt{2m \log (N/\varepsilon_0)}\), or equivalently \(a_d - m/2 > m/2 - \sqrt{2m \log (N/\varepsilon_0)}\). Now for each \(j \in [m]\), the probability that the \(j\)-th column becomes detectable is \(1/2\), therefore, the expected value of \(a_d\) is \(m/2\). Then, Hoeffding’s Inequality (Theorem 5) implies that

\[
Pr[S(1) < Z \text{ and } S(2) < Z] \\
\leq Pr[a_d - m/2 > m/2 - \sqrt{2m \log (N/\varepsilon_0)}] \\
\leq \exp \left(-\frac{-2m^2 \left(\frac{m/2 - \sqrt{2m \log (N/\varepsilon_0)}}{m}\right)^2}{m}\right) \\
= \exp \left(-\frac{-m^2 \left(\sqrt{m} - \sqrt{8 \log (N/\varepsilon_0)}\right)^2}{2}\right)
\] (74)

provided \(m/2 - \sqrt{2m \log (N/\varepsilon_0)} > 0\). The last condition is equivalent to that \(m > 8 \log (N/\varepsilon_0)\) which is satisfied under the condition (12). Now put \(m = 8\alpha \log (N/\varepsilon_0)\) with \(\alpha > 1\). Then under the condition (12), we have

\[
m^2 \left(\sqrt{m} - \sqrt{8 \log (N/\varepsilon_0)}\right)^2 \\
= \frac{m^2}{2} \left(\sqrt{\alpha} \cdot \sqrt{8 \log \frac{N}{\varepsilon_0}} - \sqrt{8 \log \frac{N}{\varepsilon_0}}\right)^2 \\
= 4m^2 \left(\sqrt{\alpha} - 1\right)^2 \log \frac{N}{\varepsilon_0} \\
> 16^2 \left(\log \frac{N}{\varepsilon_0}\right)^3 \left(1 + \frac{1}{16 \log (N/\varepsilon_0)} - 1\right)^2 \\
= \log \frac{N}{\varepsilon_0},
\] (75)

therefore the right-hand side of (74) is smaller than \(\varepsilon_0/N\). Hence the proof of Proposition 6 is concluded.

5.7 Proof of Proposition 7

Let \(1 \in U\) be the unique pirate. Then by Marking Assumption and the choice \(p = 1/2\), we have \(\gamma = w_1\) and \(S(1) = m \log 2\), while \(Z \leq Z_0 = (m/2) \log 2 + \sqrt{(m/2) \log (N/\varepsilon_0)} \log 2\). Now by the assumption \(m \geq 2 \log (N/\varepsilon_0)\), we have

\[
\frac{S(1) - Z_0}{\log 2} = \frac{m}{2} - \sqrt{\frac{m}{2} \log \frac{N}{\varepsilon_0}} \\
= \sqrt{\frac{m}{2} \left(\frac{m}{2} - \sqrt{\log \frac{N}{\varepsilon_0}}\right)} > 0,
\] (76)

therefore \(S(1) \geq Z_0 \geq Z\). Hence the proof of Proposition 7 is concluded.

5.8 Proof of Theorem 3

First, by the choice of parameters, we have \(\log (N/\varepsilon_0) = \log N + \alpha m \sim (R \log 2 + \alpha) m\) when \(m \to \infty\) and \(0 < R \log 2 + \alpha < 1/10\), therefore the condition (12) in Theorem 2 is satisfied for any sufficiently large \(m\). Now it suffices to show that, when \(m \to \infty\), the latter three of the four terms in (11) approach to 0 exponentially. The second term is smaller than \(N^3 (7/8)m^6/6\), and we have

\[
\log \left(\frac{N^3}{\left(\frac{7}{8}\right)^m}\right) = 3 \log N + m \log \frac{7}{8} \\
\sim (3R \log 2 + \log 7 - 3 \log 2)m
\] (77)

when \(m \to \infty\), and \(3R \log 2 + \log 7 - 3 \log 2 < 0\) by the condition for \(R\). Hence the second term approaches exponentially to 0. Similarly, the third term is smaller than \(3N^2((10 + \sqrt{2})/16)^m\) and we have \(\log (N^2((10 + \sqrt{2})/16)^m)/m \sim 2R \log 2 + \log ((10 + \sqrt{2})/16) < 0\) when \(m \to \infty\), therefore the third term also approaches exponentially to 0. Moreover, the natural logarithm of the fourth term is smaller than

\[
\log N + 3 \sqrt{\frac{m}{2} \log \frac{N}{\varepsilon_0} \log 2 + m \log \frac{7\sqrt{2}}{16}}
\] (78)

and this value is asymptotically equal to

\[
mR \log 2 + 3 \sqrt{\frac{m}{2} (mR \log 2 + \alpha m) \log 2 + m \log \frac{7\sqrt{2}}{16}} \\
= \left(\frac{R \log 2 + R \alpha}{2} \log 2 + 2 \log \frac{7\sqrt{2}}{16}\right)m
\] (79)

Now note that if we regard the second term in (15) as a function \(f(R_0)\) of \(R_0\), then the function \(f(x)\) is monotonically decreasing for \(x \leq 1 - \log 7/(3 \log 2)\), therefore we have
while we have \( R \log 2 + \alpha < (R \log 2 + \log(7\sqrt{2}/16))^2 / 3 \log 2 \),

\[
\frac{R \log 2 + \alpha}{2} < \left( \frac{R \log 2 + \log(7\sqrt{2}/16)}{3 \log 2} \right)^2, \tag{80}
\]

where we put \( \beta = (10 + \sqrt{2})/16 \) for simplicity. As \( 9K \log \beta < -2, N \geq 1 \) and \( 0 < \varepsilon \leq 1/3 \), the right-hand side of the above equality is not larger than \( 3^{9K \log \beta + 2 \varepsilon} \). Moreover, by the choice of \( \varepsilon_0 \), the fourth term in (11) is equal to

\[
(N - 3)^{\sqrt{(m/21) - (5m/40)}} \left( \frac{7\sqrt{2}}{16} \right)^m.
\]

As \( 8\sqrt{15}/207\sqrt{12}/16 < \exp(-3/40) \), the right-hand side of the above equality is not larger than \( \varepsilon_0 \), therefore the above argument implies that the fourth term in (11) is not larger than \( 3^{1 - 27K/40} \varepsilon \).

Summarizing, the error probability is lower than

\[
\left( 2 \cdot 3^{1 - 27K/40} + 1/54 + 3^{9K \log \beta + 2 \varepsilon} \right) \varepsilon. \tag{88}
\]

A numerical calculation shows that this value is smaller than \( \varepsilon \). Hence the proof of Theorem 4 is concluded.

### 6 Conclusion

In this article, we proposed a new construction of probabilistic 3-secure codes and presented a theoretical evaluation of their error probabilities. A characteristic of our tracing algorithm is to make use of both score comparison and search of the triples of “parents” for a given pirated fingerprint word. Some numerical examples showed that code lengths of our proposed codes are significantly shorter than the previous provably secure 3-secure codes.

**Acknowledgments** A preliminary version of this article was presented at The 12th Information Hiding (IH 2010), Calgary, Canada, June 28–30, 2010 [13]. The author would like to express his deep gratitude to Dr. Teddy Furon, who gave several invaluable comments and suggestions as the shepherd of the author’s article in the conference. Also, the author would like to thank the anonymous referees at both the conference and this journal for their precious and detailed comments.

### References

1. Amiri, E., Tardos, G.: High rate fingerprinting codes and the fingerprinting capacity. In: Proceedings of SODA 2009, pp. 336–345. ACM (2009)
2. Barg, A., Blakley, G.R., Kabatiansky, G.A.: Digital fingerprinting codes: problem statements, constructions, identification of traitors. IEEE Trans. Inf. Theory 49, 852–865 (2003)
3. Blakley, G.R., Kabatiansky, G.A.: Random coding technique for digital fingerprinting codes. In: Proceedings of IEEE ISIT 2004, p. 202. IEEE, Los Alamitos (2004)
4. Blayer, O., Tassa, T.: Improved versions of Tardos’ fingerprinting scheme. Des. Codes Cryptogr. 48, 79–103 (2008)
5. Boneh, D., Shaw, J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inf. Theory 44, 1897–1905 (1998)
6. Cotrina-Navau, J., Fernandez, M., Soriano, M.: A family of collusion 2-secure codes. In: Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S., Pérez-González, F. (eds.) IH 2005. LNCS, vol. 3727, pp. 387–397. Springer, Heidelberg (2005)
7. Hoeffding, W.: Probability inequalities for sums of bounded random variables. J. Am. Stat. Assoc. 58, 13–30 (1963)
8. Huang, Y.-W., Moulin, P.: Maximin optimality of the arcsine fingerprinting distribution and the interleaving attack for large coalitions. In: Proceedings of IEEE WIFS 2010. IEEE, Los Alamitos (2010)
9. Huang, Y.-W., Moulin, P.: On the saddle-point solution and the large-coalition asymptotics of fingerprinting games. e-Print arXiv (cs.IT) 1011.1261v2. http://arXiv.org/abs/1011.1261v2 (2011)
10. Kitagawa, T., Hagiwara, M., Nuida, K., Watanabe, H., Imai, H.: A group testing based deterministic tracing algorithm for a short random fingerprint code. In: Proceedings of ISITA 2008, pp. 706–710 (2008)
11. Nuida, K.: An improvement of short 2-secure fingerprint codes strongly avoiding false-positive. In: Katzenbeisser, S., Sadeghi, A.-R. (eds.) IH 2009. LNCS, vol. 5806, pp. 161–175. Springer, Heidelberg (2009)
12. Nuida, K.: Making collusion-secure codes (more) robust against bit erasure. IACR Cryptology ePrint Archive 2009/549. http://eprint.iacr.org/2009/549 (2009)
13. Nuida, K.: Short collusion-secure fingerprint codes against three pirates. In: Böhme, R., Fong, P.W.L., Safari-Naini, R. (eds.) IH 2010. LNCS, vol. 6387, pp. 86–102. Springer, Heidelberg (2010)
14. Nuida, K., Fujitsu, S., Hagiwara, M., Imai, H., Kitagawa, T., Ogawa, K., Watanabe, H.: An efficient 2-secure and short random fingerprint code and its security evaluation. IEICE Trans. Fundam. E92-A, 197–206 (2009)
15. Nuida, K., Fujitsu, S., Hagiwara, M., Kitagawa, T., Watanabe, H., Ogawa, K., Imai, H.: An improvement of discrete Tardos fingerprinting codes. Des. Codes Cryptogr. 52, 339–362 (2009)
16. Nuida, K., Hagiwara, M., Kitagawa, T., Watanabe, H., Ogawa, K., Fujitsu, S., Imai, H.: A tracing algorithm for short 2-secure probabilistic fingerprinting codes strongly protecting innocent users. In: Proceedings of IEEE CCNC 2007, pp. 1068–1072. IEEE, Los Alamitos (2007)
17. Schaathun, H.G.: Fighting three pirates with scattering codes. In: Proceedings of IEEE ISIT 2004. IEEE, Los Alamitos (2004)
18. Schaathun, H.G.: Fighting three pirates with scattering codes. Reports in informatics 263, Department of Informatics, University of Bergen. http://www.ii.uib.no/publikasjoner/textrap/pdf/2004-263.pdf (2004)
19. Schaathun, H.G.: On the assumption of equal contributions in fingerprinting. IEEE Trans. Inf. Forensics Secur. 3, 569–572 (2008)
20. Sébé, F., Domingo-Ferrer, J.: Short 3-secure fingerprinting codes for copyright protection. In: Batten, L., Seberry, J. (eds.) ACISP 2002. LNCS, vol. 2384, pp. 316–327. Springer, Heidelberg (2002)
21. Škorić, B., Katzenbeisser, S., Celik, M.U.: Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. Des. Codes Cryptogr. 46, 137–166 (2008)
22. Škorić, B., Katzenbeisser, S., Schaathun, H.G., Celik, M.U.: Tardos fingerprinting codes in the combined digit model. In: Proceedings of IEEE WIFS 2009. IEEE, Los Alamitos (2009)
23. Škorić, B., Vladimirrova, T.U., Celik, M.U., Talstra, J.C.: Tardos fingerprinting is better than we thought. IEEE Trans. Inf. Theory 54, 3663–3676 (2008)
24. Tardos, G.: Optimal probabilistic fingerprint codes. J. ACM 55, 1–24 (2008)