False negative probabilities in Tardos codes

Des. Codes Cryptogr. (2015) 74:159–182
DOI 10.1007/s10623-013-9856-x

False Negative probabilities in Tardos codes

Antonino Simone · Boris Škorić

Received: 26 November 2012 / Revised: 7 June 2013 / Accepted: 24 June 2013 /
Published online: 11 July 2013

Abstract Forensic watermarking is the application of digital watermarks for the purpose of tracing unauthorized redistribution of content. One of the most powerful types of attack on watermarks is the collusion attack, in which multiple users compare their differently watermarked versions of the same content. Collusion-resistant codes have been developed against these attacks. One of the most famous such codes is the Tardos code. It has the asymptotically optimal property that it can resist c attackers with a code of length proportional to c^2. Determining error rates for the Tardos code and its various extensions and generalizations turns out to be a nontrivial problem. In recent work we developed an approach called the convolution and series expansion (CSE) method to accurately compute false positive accusation probabilities. In this paper we extend the CSE method in order to make it possible to compute a bound on the False *Negative* accusation probabilities.

Keywords Traitor tracing · Tardos code · Collusion · Watermarking

Mathematics Subject Classification 94B60

1 Introduction

1.1 Collusion attacks against forensic watermarking

Fingerprinting provides a means for tracing the (re-)distribution of digital data such as audio/video material. Before distribution of the original content, it is modified by applying an imperceptible fingerprint, which plays the role of a personalized serial number. The fingerprint is imperceptibly embedded using a watermarking algorithm. When an unauthorized

Communicated by M. Paterson.

A. Simone · B. Škorić (✉)
Eindhoven University of Technology, Eindhoven, The Netherlands
e-mail: b.skoric@tue.nl

copy of the content is found, the content vendor wants to determine which users participated in the creation of the unauthorized copy. This is done using a tracing algorithm, which outputs a list of suspicious users. The whole process is variously known as 'forensic watermarking', 'traitor tracing' and 'fingerprinting'.

Reliable tracing of content requires security against attacks that aim to remove the embedded watermark. Collusion attacks, where a group of attackers compare their copies, form a particular threat. Since any differences between the copies have to arise from the watermarks and not the content, such a comparison gives information that can be used to remove the watermark. As a countermeasure, coding theory has produced a number of collusion-resistant codes. The resulting system has two layers [10,23]: The coding layer determines which message to embed and protects against collusion attacks. The watermarking layer hides symbols of the message in segments of the content. The symbols are either binary or from a larger alphabet. The interface between the two layers is usually specified in terms of the *Marking Assumption* [4] together with additional assumptions that are often referred to as a 'model'. The Marking Assumption says that the colluders are able to perform modifications only in those content segments where the colluders received differently marked content. These are called detectable positions. The 'model' specifies the symbol manipulations that the colluders are allowed to perform in the detectable positions. The often used restricted digit model (RDM) or narrow case model [11] only allows them to choose pieces from their copies, i.e. each segment of the unauthorized copy carries exactly one watermark symbol that the coalition has received.

1.2 Tardos codes

Many collusion resistant codes have been proposed. Most notable among the binary codes are the Boneh-Shaw construction [4] and the by now famous Tardos code [28]. The former construction uses a concatenation of an inner code with a random outer code, while the Tardos code is fully randomized. Gabor Tardos' original work in 2003 was followed by a large number of papers giving generalizations, construction improvements, sharper analyses etc. (e.g. [2,6–8,15–17,20,21,29–32]). We briefly mention some of these developments. The number of users is n. The coalition size that should be resisted by the code is denoted as c_0, and ε_1 is the maximum allowed probability of accusing a fixed innocent user. In Tardos' original paper [28] a binary code was given with sufficient length $m = 100c_0^2\lceil \ln \frac{1}{\varepsilon_1} \rceil$, and a proof was given that $m \propto c_0^2$ is asympotically optimal[1] for large coalitions, for arbitrary alphabet size. (Here ε_1 is a function of n and the maximum tolerable overall false accusation probability.) The original construction contained two unfortunate design choices which caused the large constant '100'. First, the False Negative probability ε_2 (not accusing any of the colluders) was coupled to ε_1 as $\varepsilon_2 = \varepsilon_1^{c_0/4}$. This gives $\varepsilon_2 \ll \varepsilon_1$, which is unusual in the context of content distribution; a deterring effect is achieved already at $\varepsilon_2 \approx \frac{1}{2}$, while the overall False Positive probability ($\approx n\varepsilon_1$) has to be very small. In later literature (e.g. [2,31]) the ε_2 and ε_1 were decoupled from each other, yielding an improvement of the code length. Second, the symbols 0 and 1 were originally not treated equally. A score was only computed in segments where the attackers produce a 1. This ignored 50 % of all the available information. A fully symbol-symmetric version of the Tardos code was given in [29], yielding a further improvement of the code length by a factor 4.

[1] The proportionality $m \propto c_0^2$ was already noted in the context of spread-spectrum watermarking by Kilian et al. [14]. They showed that, if the watermarks have a component-wise normal distribution, $\Omega(\sqrt{m/ln\, n})$ differently marked copies are required to erase any mark with non-negligible probability.

Yet another improvement was achieved in [21]. The code construction consists of two probabilistic steps. First, a bias parameter is generated for each segment. In Tardos' original construction the probability density function (pdf) for the bias is continuous, suitable for any coalition size. In [21] a class of discrete bias distributions was given that performs better against finite coalition sizes.

The above mentioned work all followed the 'simple decoder' approach, i.e. a score is computed for each user independently; if the score exceeds a certain threshold, the user is considered suspicious. In contrast, one can also use a 'joint decoder' which looks at sets of users [5,18].

Amiri and Tardos [1] proposed a capacity-achieving joint decoder in the case of a binary alphabet. (Capacity refers to the information-theoretic treatment [3,13,19,27] of the collusion attack as a communication channel with malicious noise.) However, the construction is rather impractical, requiring computations for an exponential number of candidate coalitions. Even if more practical joint decoders are found, the simple decoder will serve as a first step in their operation. Thus, there is considerable interest in the simple decoder approach.

In [29] the binary Tardos code was generalized to arbitrary alphabet size q. For the Restricted Digit Model it was demonstrated that the transition to a larger alphabet has advantages beyond the mere fact that a q-ary symbol carries $\log_2 q$ bits of information: the sufficient code length decreases by a factor larger than $\log_2 q$. (In other words, the fingerprinting rate of the code is improved.)

1.3 Exact computation of the error rates of Tardos codes

The so-called 'Gaussian approximation' or 'Gaussian assumption', introduced in [31], has been a useful tool in the analysis of Tardos codes. The assumption is that the pdf of a user's accusation score has a normal distribution. When this is the case, the statistical analysis of the code's performance can be drastically simplified; the performance is almost completely determined by a single parameter, namely the average score $\tilde{\mu}$ of the coalition.

The Gaussian assumption is motivated by the Central Limit Theorem (CLT): A user accusation consists of a sum of per-segment contributions, which are independent and identically distributed (i.i.d.). When many of these get added together, the result is close to normal-distributed, i.e. the pdf is very close to a Gaussian in a certain region around the average, and deviates in the tails. The longer the code becomes (i.e. the larger the coalition size c_0), the wider this central region. In [31] and [29] theoretical results were provided arguing that the central region is sufficiently wide to allow for application of the Gaussian approximation for realistic parameter choices. However, these arguments are not very precise.

In [24–26] an in-depth analytical and numerical investigation of the Gaussian approximation was given in the RDM case. The approach is based on the convolution rule for characteristic functions, and on a way to express the false accusation probability as a power series expansion in the small parameter $1/\sqrt{m}$. This was dubbed the 'CSE method' (Convolution and Series Expansion). The advantage of the CSE method over simulations and other methods is that it yields reliable results also when the error probability of the code is very small. For instance, if the error rate is around 10^{-10}, then a number of simulations of order at least 10^{10} is required to measure this rate; in contrast, the computational effort in the CSE method does not depend on the error rate. The work of [24,25] showed, for various parameter settings and attack strategies, how the false positive probability has a transition from Gaussian behavior in the central region to worse-than-Gaussian power-law behavior outside the center. In [26] an overview was given of False Positive (FP) error

rates for the main known attack strategies in the RDM, for a large part of the parameter space.

Until now the CSE method has not been applied to accusation probabilities of *guilty* users.

1.4 Contributions and outline

In this paper we adapt the CSE method so that it can be used to compute accusation probabilities of *guilty* users in the q-ary Tardos fingerprinting scheme with the simple decoder of [29]. We present a number of consistency checks which demonstrate that the method (and our implementation) works, and we give ROC curves combining data on guilty *and* innocent user accusation probabilities.

The outline is as follows. In Sect. 2 we introduce notation, briefly summarize the q-ary Tardos scheme, and give a number of lemmas necessary for computing expectation values. In Sect. 3 we derive the probability density function for the guilty user score function in a single content segment. We study the tails and the first two moments of the distribution, and then compute the Fourier transform. Section 4 first details the adaptations necessary to make the CSE method work for guilty user scores. Then numerical results are presented.

2 Preliminaries

2.1 General notation

Vectors are denoted in boldface. Sets will be (mostly) written in calligraphic font. For a scalar x and a vector $\boldsymbol{p}$, the notation $\boldsymbol{p}^x$ stands for $\prod_\alpha p_\alpha^x$. For vectors $\boldsymbol{p}, \boldsymbol{x}$, the notation $\boldsymbol{p}^{\boldsymbol{x}}$ means $\prod_\alpha p_\alpha^{x_\alpha}$.

Definition 1 (*Generalized Beta function*) Let $\boldsymbol{v}$ be an n-component vector. The Beta function is defined as

$$B(\boldsymbol{v}) := \frac{\prod_{a=1}^n \Gamma(v_a)}{\Gamma(\sum_{b=1}^n v_b)}. \tag{1}$$

For parameters $v_1, \cdots, v_n > 0$ the Beta function has the following Dirichlet integral representation:

$$B(\boldsymbol{v}) = \int_0^1 \mathrm{d}^n\boldsymbol{x}\ \delta\left(1 - \textstyle\sum_{a=1}^n x_a\right) \prod_{b=1}^n x_b^{-1+v_b}. \tag{2}$$

2.2 The q-ary Tardos scheme

We briefly summarize the most important aspects of the Tardos scheme. The number of symbols in a codeword is m. The number of users is n. The alphabet is $\mathcal{Q}$, with size q. $X_{ji} \in \mathcal{Q}$ stands for the i'th symbol in the codeword of user j. The whole matrix of codewords is denoted as X.

2.2.1 Two-step code generation

m bias vectors $\boldsymbol{p}^{(i)} \in [0,1]^q$ are independently drawn according to a Dirichlet distribution F, with

$$F(\boldsymbol{p}) = \delta(1 - \textstyle\sum_{\beta\in\mathcal{Q}} p_\beta) \cdot \dfrac{1}{B(\kappa \mathbf{1}_q)} \prod_{\alpha\in\mathcal{Q}} p_\alpha^{-1+\kappa}. \tag{3}$$

Here $\mathbf{1}_q$ stands for the vector $(1,\ldots,1)$ of length q. All elements X_{ji} are drawn independently according to $\Pr[X_{ji} = \alpha|\boldsymbol{p}^{(i)}] = p_\alpha^{(i)}$. The κ is a positive constant called the concentration parameter. If one uses the simple decoder as described below in Eqs. (6,7), it is a good choice [29] to set κ slightly larger than $1/q$. It was shown [12] that the asymptotic ($c \to \infty$) fingerprinting capacity is achieved with $\kappa = 1/2$.

2.2.2 Attack

The coalition is a subset of the set of all users. We denote the coalition as $\mathcal{C}$, with size c. The i'th segment of the attacked content contains a symbol $y_i \in \mathcal{Q}$. We define vectors $\boldsymbol{\sigma}^{(i)} \in \{0,\ldots,c\}^q$ as

$$\sigma_\alpha^{(i)} = |\{j \in \mathcal{C} : X_{ji} = \alpha\}| \tag{4}$$

satisfying $\sum_{\alpha\in\mathcal{Q}} \sigma_\alpha^{(i)} = c$. In words: $\sigma_\alpha^{(i)}$ counts how many colluders have received symbol α in segment i. For fixed q and c, we define the set of possible $\boldsymbol{\sigma}$ values as $\mathcal{S}_{qc} = \left\{\boldsymbol{\sigma} \in \{0,\ldots,c\}^q \,|\, \sum_{\alpha\in\mathcal{Q}} \sigma_\alpha = c\right\}$.

The attack strategy may be nondeterministic. As usual, it is assumed that this strategy is segment-symmetric (the same in all segments), symbol-symmetric (invariant under permutation of the alphabet) and attacker-symmetric (invariant under permutation of the attackers). The strategy is expressed as probabilities $\theta_{y|\boldsymbol{\sigma}}$ that apply independently for each segment. Omitting the column index,

$$\Pr[y|\boldsymbol{\sigma}] = \theta_{y|\boldsymbol{\sigma}}. \tag{5}$$

Some often studied strategies are listed below.

Strategy	Abbrev.	Description	$\theta_{y\|\boldsymbol{\sigma}}$
Minority voting	MinV	Select symbol that occurs least often	
Majority voting	MajV	Select symbol that occurs most often	
Interleaving	Int	Select random attacker's symbol	σ_y/c
$\tilde{\mu}$-minimizing	$\tilde{\mu}$-min	Select $\sigma_y > 0$ that minimizes $\tilde{\mu}$ (see below)	
Random symbol	RS	Choose uniformly from received symbols	$\frac{[\sigma_y>0]}{\lvert\{\alpha\in\mathcal{Q}:\sigma_\alpha>0\}\rvert}$

2.2.3 Accusation

The watermark detector sees the symbols y_i. For each user j, a score S_j is computed,

$$S_j = \textstyle\sum_{i=1}^m S_j^{(i)} \qquad \text{where} \qquad S_j^{(i)} = g_{[X_{ji}==y_i]}(p_{y_i}^{(i)}), \tag{6}$$

where the expression $[X_{ji} == y_i]$ evaluates to 1 if $X_{ji} = y_i$ and to 0 otherwise, and the functions g_0 and g_1 are defined as

$$g_1(p) = \sqrt{(1-p)/p}; \qquad g_0(p) = -\sqrt{p/(1-p)}. \tag{7}$$

The total score of the coalition is $S_{\mathcal{C}} = \sum_{j\in\mathcal{C}} S_j$. The choice (7) is the unique choice that, for innocent users, yields zero average accusation and variance equal to 1 independent of $\boldsymbol{p}$,

$$pg_1(p) + (1-p)g_0(p) = 0 \quad ; \quad p[g_1(p)]^2 + (1-p)[g_0(p)]^2 = 1. \tag{8}$$

This has been shown to have optimal properties for $q = 2$ [8,31]. Its unique properties (8) also hold for $q \geq 3$; that is the main motivation for using (7). A user j is 'accused' if his score S_j exceeds a threshold Z, i.e. if $S_j > Z$. The list of accused users is denoted as $\mathcal{L}$. The False Positive and False Negative error probability are defined as $P_{\text{FP}} = \Pr[\mathcal{L} \setminus \mathcal{C} \neq \emptyset]$ and $P_{\text{FN}} = \Pr[\mathcal{L} \cap \mathcal{C} = \emptyset]$.

The parameter $\tilde{\mu}$ is defined as $\frac{1}{m}\mathbb{E}[S]$, where $\mathbb{E}$ stands for the expectation value over all random variables. The $\tilde{\mu}$ depends on q, κ, the collusion strategy, and weakly on c. In the limit of large c it converges to a finite value, and the code length scales as $m \propto c^2/\tilde{\mu}^2$.

2.3 Expectation values

We will need to compute expectation values over several of the random variables mentioned above. To this end we list a number of lemmas, most of which are from the literature.

Expectation over $\boldsymbol{p}$: Let $r(\boldsymbol{p})$ be an arbitrary function. Then the expectation over $\boldsymbol{p}$ is defined as

$$\mathbb{E}_{\boldsymbol{p}}[r(\boldsymbol{p})] := \int_0^1 \mathrm{d}^q\boldsymbol{p}\ F(\boldsymbol{p}) r(\boldsymbol{p}). \tag{9}$$

The following lemma is helpful when one component of $\boldsymbol{p}$ has a special status, for instance p_y, with y the symbol chosen by the attackers. The rest of $\boldsymbol{p}$ is denoted as $\boldsymbol{p}_{\setminus y}$.

Lemma 1 (Marginals of the Dirichlet distribution) *Let r be any function of $\boldsymbol{p}$. The expectation value $\mathbb{E}_{\boldsymbol{p}}$ can be split into two parts as*

$$\mathbb{E}_{\boldsymbol{p}}[r(\boldsymbol{p})] = \mathbb{E}_{p_y}\left[\mathbb{E}_{\boldsymbol{p}_{\setminus y}|p_y}[r(\boldsymbol{p})]\right], \tag{10}$$

with

$$\mathbb{E}_{p_y}[\cdots] = \frac{1}{B(\kappa, \kappa[q-1])} \int_0^1 \mathrm{d}p_y\ p_y^{-1+\kappa}(1-p_y)^{-1+\kappa[q-1]}[\cdots] \tag{11}$$

$$\mathbb{E}_{\boldsymbol{p}_{\setminus y}|p_y}[r(\boldsymbol{p})] = \frac{1}{B(\kappa\mathbf{1}_{q-1})} \int_0^1 \mathrm{d}^{q-1}\boldsymbol{t}\,\delta(1 - \sum_{\beta\in\mathcal{Q}\setminus\{y\}} t_\beta)\ \boldsymbol{t}^{-1+\kappa} r(\boldsymbol{p})\big|_{\boldsymbol{p}_{\setminus y}=(1-p_y)\boldsymbol{t}}. \tag{12}$$

Proof See Appendix. □

Expectation over $\boldsymbol{\sigma}|\boldsymbol{p}$: Let $r(\boldsymbol{\sigma})$ be an arbitrary function. Then

$$\mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}}[r(\boldsymbol{\sigma})] := \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}} \binom{c}{\boldsymbol{\sigma}} \boldsymbol{p}^{\boldsymbol{\sigma}} r(\boldsymbol{\sigma}). \tag{13}$$

Expectation over $y|\boldsymbol{\sigma}$: Let $r(y)$ be an arbitrary function. Then

$$\mathbb{E}_{y|\boldsymbol{\sigma}}[r(y)] := \sum_{y\in\mathcal{Q}} \theta_{y|\boldsymbol{\sigma}} r(y). \tag{14}$$

Expectation over $y|\boldsymbol{p}$: We introduce the notation $T_{y|\boldsymbol{p}}$ to denote the following sum,

$$T_{y|\boldsymbol{p}} = \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}} \binom{c}{\boldsymbol{\sigma}} \boldsymbol{p}^{\boldsymbol{\sigma}} \theta_{y|\boldsymbol{\sigma}}, \tag{15}$$

where the condition $\sum_\alpha p_\alpha = 1$ is *not* enforced. This will allow us to write several important expressions compactly in terms of partial derivatives of T. The notation $\tau_{y|\boldsymbol{p}}$ is defined as $T_{y|\boldsymbol{p}}$ where we *do* enforce the 'on-shell' condition $\sum_\alpha p_\alpha = 1$. It represents the conditional probability that y occurs given $\boldsymbol{p}$.

$$\mathbb{E}_{y|\boldsymbol{p}}[r(y)] = \sum_{y\in\mathcal{Q}} \tau_{y|\boldsymbol{p}} r(y). \tag{16}$$

Lemma 2 *(*See Lemma 6 in *[25]) For $d > 0$, $v > 0$, the following holds*

$$\int_0^\infty \mathrm{d}u \, \frac{u^{2d-1}}{(1+u^2)^{d+v}} = \frac{1}{2} B(d, v). \tag{17}$$

Lemma 3 *(*See Lemma 3 in *[25]) The overall probability distribution for one component of $\boldsymbol{\sigma}$ is*

$$\mathbb{P}_1(b) := \Pr[\sigma_\alpha = b] = \binom{c}{b} \frac{B(\kappa + b, \kappa[q-1] + c - b)}{B(\kappa, \kappa[q-1])} \quad \textit{for any fixed } \alpha \in \mathcal{Q}. \tag{18}$$

Corollary 1 *(*See Corollary 1 in *[25]) Let $\boldsymbol{\sigma}_{\setminus\alpha}$ denote the vector $\boldsymbol{\sigma}$ without the component σ_α. The probability distribution of $\boldsymbol{\sigma}_{\setminus\alpha}$ conditioned on σ_α is given by*

$$\mathbb{P}_{q-1}(\boldsymbol{x}|b) := \Pr[\boldsymbol{\sigma}_{\setminus\alpha} = \boldsymbol{x} | \sigma_\alpha = b] = \binom{c-b}{\boldsymbol{x}} \frac{B(\kappa \mathbf{1}_{q-1} + \boldsymbol{x})}{B(\kappa \mathbf{1}_{q-1})} \quad \textit{for any fixed } \alpha \in \mathcal{Q}. \tag{19}$$

Definition 2 Let $\alpha \in \mathcal{Q}$, $b \in \{0, \ldots, c\}$, $\boldsymbol{x} \in \{0, \ldots, c\}^{q-1}$ and $\boldsymbol{\sigma} \in \mathcal{S}_{qc}$ such that $\sigma_\alpha = b$ and $\boldsymbol{\sigma}_{\setminus\alpha} = \boldsymbol{x}$. We define

$$\Psi_b(\boldsymbol{x}) = \theta_{\alpha|\boldsymbol{\sigma}} \text{ for the above given form of } \boldsymbol{\sigma}. \tag{20}$$

Due to the Marking Assumption we have that $\Psi_c(\mathbf{0}) = 1$ and $\Psi_0(\boldsymbol{x}) = 0$.

Definition 3 Let $b \in \{1, \ldots, c\}$. Consider a segment for which it is given that there exists at least one symbol $\alpha \in \mathcal{Q}$ satisfying $\sigma_\alpha = b$, and pick one such symbol. We define K_b as the probability that the attackers output this particular symbol.

$$K_b = \mathbb{E}_{\boldsymbol{x}|b} \Psi_b(\boldsymbol{x}) = \sum_{\boldsymbol{x}} \mathbb{P}_{q-1}(\boldsymbol{x}|b) \Psi_b(\boldsymbol{x}). \tag{21}$$

Lemma 4 *(*See Lemma 4 in *[25]) The numbers K_b satisfy*

$$q \sum_{b=1}^{c} K_b \mathbb{P}_1(b) = 1. \tag{22}$$

Lemma 5 *(*See Theorem 2 in *[25]) The expected coalition score in a single segment is*

$$\tilde{\mu} \;=\; \mathbb{E}[S_{\mathcal{C}}^{(i)}] = q \sum_{b=1}^{c} \mathbb{P}_1(b) K_b W(b) \left\{ \frac{1}{2} - \kappa + \frac{b}{c}(\kappa q - 1) \right\}, \tag{23}$$

$$\textit{with } W(b) := c \frac{\Gamma(b + \kappa - \frac{1}{2})}{\Gamma(b+\kappa)} \frac{\Gamma(c - b + \kappa[q-1] - \frac{1}{2})}{\Gamma(c - b + \kappa[q-1])}. \tag{24}$$

3 Properties of the guilty-user score in a single segment

In this section we study the properties of the single-segment score $S_j^{(i)}$ for a guilty user $j \in \mathcal{C}$. In Sect. 3.1 we derive the probability density function (pdf) ψ for $S_j^{(i)}$, and we investigate the first two moments, as well as the tails of the distribution. In Sect. 3.2 we compute the Fourier transform (characteristic function) of ψ and investigate its main properties, such as its power series expansion. The Fourier transform is then used in Sect. 4 to implement the CSE method.

3.1 Distribution of the guilty-user score

Throughout this section we will use the shorthand notation u for $S_j^{(i)}$. We derive the distribution function $\psi(u)$ as follows. First we fix $\boldsymbol{p}$ and compute the conditional pdf $\psi(u|\boldsymbol{p})$. Then the end result follows by taking the expectation value over $\boldsymbol{p}$: $\psi(u) = \mathbb{E}_{\boldsymbol{p}}[\psi(u|\boldsymbol{p})]$. Because of the different behavior of positive and negative scores we introduce the notation ψ_+ for $u > 0$ and ψ_- for $u < 0$.

Theorem 1 *Let $T_{y|\boldsymbol{p}}$ and $\tau_{y|\boldsymbol{p}}$ be functions as defined in Sect. 2.3. For a guilty user, the probability distribution of the score conditioned on $\boldsymbol{p}$ is given by*

$$u < 0: \quad \psi_-(u|\boldsymbol{p}) = \sum_{y\in\mathcal{Q}} \delta\left(u - g_0(p_y)\right) \sum_{\boldsymbol{\sigma}} \binom{c}{\boldsymbol{\sigma}} \left(1 - \frac{\sigma_y}{c}\right) \boldsymbol{p}^{\boldsymbol{\sigma}} \theta_{y|\boldsymbol{\sigma}} \tag{25}$$

$$= \sum_{y\in\mathcal{Q}} \delta\left(u - g_0(p_y)\right) \left[\tau_{y|\boldsymbol{p}} - \frac{p_y}{c} \frac{\partial T_{y|\boldsymbol{p}}}{\partial p_y}\right], \tag{26}$$

$$u > 0: \quad \psi_+(u|\boldsymbol{p}) = \sum_{y\in\mathcal{Q}} \delta\left(u - g_1(p_y)\right) \sum_{\boldsymbol{\sigma}} \binom{c}{\boldsymbol{\sigma}} \frac{\sigma_y}{c} \boldsymbol{p}^{\boldsymbol{\sigma}} \theta_{y|\boldsymbol{\sigma}} \tag{27}$$

$$= \frac{1}{c} \sum_{y\in\mathcal{Q}} \delta\left(u - g_1(p_y)\right) p_y \frac{\partial T_{y|\boldsymbol{p}}}{\partial p_y}. \tag{28}$$

Proof See Appendix. □

The asymmetry between positive and negative scores is understood as follows. Even though the score functions g_0, g_1 as defined in (7) have a high degree of symmetry, *their argument* p_y breaks the symmetry: in the g_1 case the p_y refers to the symbol received by the person under scrutiny, but in the g_0 case neither p_y nor $1 - p_y$ is the probability of his symbol.

Next we take the expectation value over $\boldsymbol{p}$.

Theorem 2 *For a guilty user, the distribution function ψ of the score in one segment is given by*

$$u < 0: \quad \psi_-(u) = \frac{2q}{B(\kappa, \kappa[q-1])} \sum_{b=1}^{c-1} \left(1 - \frac{b}{c}\right) \binom{c}{b} \frac{(u^2)^{b+\kappa-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}} K_b, \tag{29}$$

$$u > 0: \quad \psi_+(u) = \frac{2q}{B(\kappa, \kappa[q-1])} \sum_{b=1}^{c} \frac{b}{c} \binom{c}{b} \frac{(u^2)^{c-b+\kappa[q-1]-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}} K_b. \tag{30}$$

Proof See Appendix. □

Table 1 Dominant powers of $\psi(u)$ in the tails and near $u = 0$

Left tail	Right tail	$u \uparrow 0$	$u \downarrow 0$
$\frac{K_{c-1}}{\lvert u\rvert^{3+2\kappa[q-1]}}$	$\frac{K_1}{u^{3+2\kappa}}$	$K_1(c-1)\lvert u\rvert^{1+2\kappa}$	$u^{-1+2\kappa[q-1]}$

All the values above are multiplied by $\frac{2q}{B(\kappa,\kappa[q-1])}$

The expressions (29,30) are rather complicated. We have double-checked their correctness by verifying the normalization and the first moment.

Consistency check 1 *The function $\psi(u)$ given in Theorem 2 is correctly normalized,* $\int_{-\infty}^{\infty} \mathrm{d}u\ \psi(u) = 1$.

Proof See Appendix. □

Consistency check 2 *The function $\psi(u)$ has the correct first moment,* $\int_{-\infty}^{\infty} \mathrm{d}u\ \psi(u)u = \tilde{\mu}/c$.

Proof See Appendix. □

The behavior in the tails and near $u = 0$ is summarized in Table 1. The right tail is dominated by the $b = 1$ term; it is proportional to $(1/u)^{3+2\kappa}$. The integral $\int_0^{\infty} \mathrm{d}u\ \psi_+(u)u^a$ converges for $a < 2+2\kappa$. The left tail is dominated by the $b = c-1$ term, and is proportional to $(1/|u|)^{3+2\kappa[q-1]}$. The integral $\int_{-\infty}^{0} \mathrm{d}u\ \psi_-(u)|u|^a$ converges for $a < 2+2\kappa[q-1]$. Hence, for $\kappa \in \left(0, \frac{1}{2}\right)$, the usual choice, the second moment always exists, but not the third absolute moment. We see that the right tail is heavier than the left tail, meaning that extreme positive scores are more likely than extreme negative scores. Such a property is obviously beneficial for accusing guilty users. In case the chosen strategy is MajV, the right tail is dominated by the $b = \lceil c/q \rceil$ term, which behaves as $(1/u)^{2\lceil c/q\rceil+2\kappa+1}$, which for $c > q$ decreases faster than $(1/u)^{3+2\kappa}$. For MinV the left tail is dominated by $b = \lfloor c/2 \rfloor$, which behaves as $(1/|u|)^{2\lceil c/2\rceil+2\kappa[q-1]+1}$ and decreases faster than $(1/|u|)^{3+2\kappa[q-1]}$ for $c > 2$. Since K_1 is the coefficient associated with the dominant power in the right tail, we find that MinV yields the most pronounced right tail. On the left side it is MajV, the strategy that most emphasizes K_{c-1}. Figure 1 illustrates these trends.

Definition 4 We denote the second moment of the pdf ψ as M_2,

$$M_2 := \int_{-\infty}^{\infty} \mathrm{d}u\ \psi(u)u^2. \tag{31}$$

Definition 5 We denote the variance of the pdf ψ as V,

$$V := M_2 - \tilde{\mu}^2/c^2. \tag{32}$$

Lemma 6 *The second moment M_2 as defined in Def. 4 is given by*

$$M_2 = q \sum_{b=1}^{c} K_b \mathbb{P}_1(b) \left[\left(1 - \frac{b}{c}\right) \frac{b+\kappa}{c-b+\kappa[q-1]-1} + \frac{b}{c} \frac{c-b+\kappa[q-1]}{b+\kappa-1} \right]. \tag{33}$$

Proof See Appendix. □

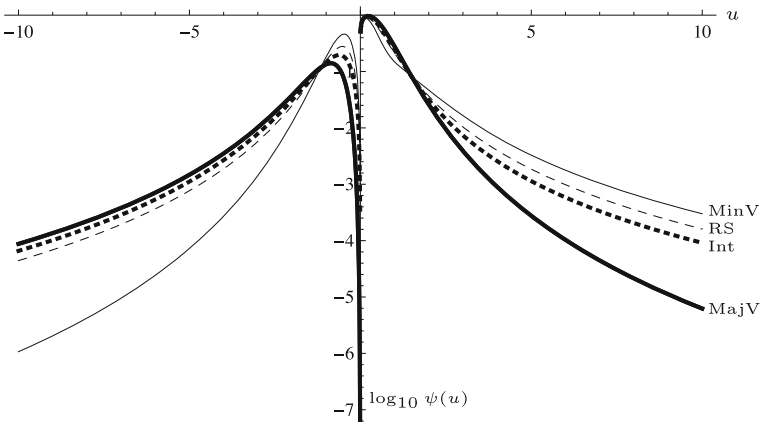

Fig. 1 The pdf ψ of the single-segment score, shown for several strategies. $c = 4$, $q = 3$, $\kappa \approx 1/3$

Remark The scores of guilty users are not independent. As a consequence, the variance of the coalition score $S_{\mathcal{C}}^{(i)}$ is not a simple multiple of V. Let the covariance between two guilty user scores be $K_{jj'} = \mathbb{E}[S_j^{(i)} S_{j'}^{(i)}] - \tilde{\mu}^2/c^2$. Then we have

$$\mathbb{E}[(S_{\mathcal{C}}^{(i)})^2] = \mathbb{E}[\sum_{j,j' \in \mathcal{C}} S_j^{(i)} S_{j'}^{(i)}] = c\mathbb{E}[(S_j^{(i)})^2] + \sum_{j \neq j'} (\mathbb{E}[S_j^{(i)} S_{j'}^{(i)}] - \tilde{\mu}^2/c^2) + \tilde{\mu}^2(1 - \frac{1}{c}). \tag{34}$$

which yields

$$\tilde{\sigma}^2 := \mathrm{Var}(S_{\mathcal{C}}^{(i)}) = cV + \textstyle\sum_{j \neq j'} K_{jj'}. \tag{35}$$

In [29] the variance was bounded as $\tilde{\sigma}^2 < qc - \tilde{\mu}^2$. From this bound we learn that the sum $\sum_{j \neq j'} K_{jj'}$ scales at most linearly in c, even though it contains two sums over the coalition. A study of the covariances is left for future work.

Remark In the case of the Interleaving attack, we have $\Psi_b(\boldsymbol{x}) = b/c$ and $K_b = b/c$. The $\sum_b$ summations in Theorem 2 can be evaluated exactly, and yield

$$\psi_-^{\mathrm{Int}}(u) = (1 - \tfrac{1}{c}) \frac{2q}{B(\kappa, \kappa[q-1])} \frac{(u^2)^{\kappa+1/2}}{(1+u^2)^{2+\kappa q}} \tag{36}$$

$$\psi_+^{\mathrm{Int}}(u) = \frac{1}{c} \frac{2q}{B(\kappa, \kappa[q-1])} (c + u^2) \frac{(u^2)^{\kappa[q-1]-1/2}}{(1+u^2)^{2+\kappa q}}. \tag{37}$$

The left tail has dominant power $(1/|u|)^{3+2\kappa[q-1]}$ and the right tail $(1/u)^{3+2\kappa}$, which corresponds to the longest possible tails as listed in Table 1. This does not come as a surprise; the Interleaving attack has the same tail behavior in the case of innocent users.

3.2 Fourier transform

Definition 6 Let $\chi : \mathbb{R} \to \mathbb{C}$ be a function. The Fourier transform of χ is denoted as $\tilde{\chi}$ and defined as

$$\tilde{\chi}(k) = \int_{-\infty}^{\infty} \mathrm{d}x \; e^{-ikx} \chi(x) \quad \text{with } k \in \mathbb{R}. \tag{38}$$

Lemma 7 *Let χ be a probability distribution function, and X a random variable with $X \sim \chi$. Then*

$$\left. \frac{\mathrm{d}^n \tilde{\chi}(k)}{\mathrm{d}k^n} \right|_{k=0} = (-i)^n \mathbb{E}\left[X^n\right]. \tag{39}$$

Proof $\frac{\mathrm{d}^n \tilde{\chi}(k)}{\mathrm{d}k^n} = \int \mathrm{d}x \left[\frac{\mathrm{d}^n}{\mathrm{d}k^n} e^{-ikx}\right] \chi(x) = (-i)^n \int \mathrm{d}x \; x^n e^{-ikx} \chi(x)$. Setting $k = 0$ gives the result. □

Lemma 8 *(*From *[22],* Sect. 2.5.9*) Let $k \in \mathbb{R}$,* Re $v > -\frac{1}{2}$*, and $d > 0$. Let the function Λ be defined as the following convergent integral,*

$$\Lambda(d, v; k) := \int_0^{\infty} \mathrm{d}u \; \frac{u^{2d-1}}{(u^2+1)^{v+d}} e^{iku}. \tag{40}$$

This integral can be expressed as

$$\begin{aligned} \Lambda(d, v; k) &= (-ik)^{2v} \Gamma(-2v) \; {}_1F_2(v+d; v+\frac{1}{2}, v+1; \frac{k^2}{4}) \\ &+ \frac{1}{2} \sum_{j=0}^{\infty} \frac{(ik)^j}{j!} B(d+\frac{j}{2}, v-\frac{j}{2}) \end{aligned} \tag{41}$$

where ${}_1F_2$ is a hypergeometric function.

Notice that in general $\Lambda(d, v; k)$ is not an entire function of k due to the appearance of the factor k^{2v} in the first term, which for general v is not an entire function. The hypergeometric function ${}_1F_2$ has the sum representation ${}_1F_2(\alpha; \beta_1, \beta_2; z) = \sum_{j=0}^{\infty} \frac{(\alpha)_j}{j!(\beta_1)_j (\beta_2)_j} z^j$ where $(\alpha)_j = \alpha(\alpha+1)\cdots(\alpha+j-1)$ is the Pochhammer symbol. The radius of convergence is infinity.

Theorem 3 *The Fourier transform of ψ is given by*

$$\tilde{\psi}(k) = \frac{2q}{B(\kappa, \kappa[q-1])} \sum_{b=1}^{c} \binom{c}{b} K_b \cdot \left[\left(1 - \frac{b}{c}\right) \Lambda(d_b, v_b; k) + \frac{b}{c} \Lambda(D_b, V_b; -k) \right], \tag{42}$$

with Λ as defined in Lemma 8, and

$$\begin{aligned} d_b &= b + \kappa \quad ; \quad v_b = c - b + \kappa[q-1] \\ D_b &= c - b + \kappa[q-1] \quad ; \quad V_b = b + \kappa. \end{aligned} \tag{43}$$

Proof We use the expression for ψ given in Theorem 2. The Fourier integral for the summands in ψ_+ is immediately of the form (41) and yields $\Lambda(D_b, V_b; -k)$. The integral over the ψ_- terms is of the form $\int_{-\infty}^{0} \mathrm{d}u \; f(u^2) e^{-iku}$, which can be rewritten as $\int_0^{\infty} \mathrm{d}u \; f(u^2) e^{iku}$; this too has the form (41) and yields $\Lambda(d_b, v_b; k)$. □

Corollary 2 *For $q \geq 3$ and $\frac{1}{2(q-1)} \leq \kappa < \frac{1}{2}$, the $\tilde{\psi}$ has the following power series expansion,*

$$\tilde{\psi}(k) = 1 - i\frac{\tilde{\mu}}{c}k - \frac{1}{2}M_2k^2 + A(-ik)^{2+2\kappa} + O(k^3), \tag{44}$$

$$\text{where } A := \frac{2q}{B(\kappa, \kappa[q-1])}K_1\Gamma(-2-2\kappa). \tag{45}$$

Proof Trivially $\mathbb{E}[u^0] = 1$. From Consistency check 2 and Lemma 6 we know that $\mathbb{E}[u] = \frac{\tilde{\mu}}{c}$ and $\mathbb{E}[u^2] = M_2$. Hence by Lemma 7 we have $\tilde{\psi}(0) = 1$, $\tilde{\psi}'(0) = -i\frac{\tilde{\mu}}{c}$ and $\tilde{\psi}''(0) = -M_2$. The expansion in (44) is consistent with these values. After k^2 the powers can be non-integer. The next term in the series expansion is $k^{2+2\kappa}$. The exponent comes from the application of Lemma 8 in Theorem 3: in the first term of (41) the k^{2v} factor can build irrational powers of k. The minimum value generated is for $V_1 = 1 + \kappa$, with V_b as defined in (43). Note that the Λ term obtained from v_c is not present because it is multiplied by $1 - b/c$. The next contribution is $v_{c-1} = 1 + \kappa[q-1]$ which (for $q \geq 3$) is larger than V_1. Finally, the coefficient A follows from the $\Lambda(D_1, V_1, -k)$ term in (42), taking only the leading term (=1) in the sum representation of the ${}_1F_2$ function. □

In order to apply the CSE method we will have to work with a zero-mean pdf. For this reason we introduce a 'centered' version of ψ.

Definition 7 We define the pdf χ as a shifted version of ψ,

$$\chi(r) := \psi\left(\frac{\tilde{\mu}}{c} + r\right). \tag{46}$$

We will use shorthand notation $r = u - \tilde{\mu}/c$. From the definition it trivially follows that $\mathbb{E}[r] = 0$ and $\mathbb{E}[r^2] = V$.

Lemma 9 *The Fourier transform of χ is given by*

$$\tilde{\chi}(k) = e^{ik\frac{\tilde{\mu}}{c}}\tilde{\psi}(k). \tag{47}$$

Proof $\tilde{\chi}(k) = \int_{-\infty}^{\infty} \mathrm{d}r\, e^{-ikr}\chi(r) = \int_{-\infty}^{\infty} \mathrm{d}u\, e^{-ik\left(u-\frac{\tilde{\mu}}{c}\right)}\psi(u) = e^{ik\frac{\tilde{\mu}}{c}}\tilde{\psi}(k)$. □

Corollary 3 *Let $\frac{1}{2[q-1]} < \kappa < \frac{1}{2}$ and let χ be as given in Definition 7. Then $\tilde{\chi}$ has the following power series expansion,*

$$\tilde{\chi}(k) = 1 - \frac{1}{2}Vk^2 + A(-ik)^{2+2\kappa} + O(k^3) \tag{48}$$

with A as given in (45).

Proof From (47) we can rewrite $\tilde{\chi}(k)$ as a product of the series expansions of $e^{ik\frac{\tilde{\mu}}{c}}$ and $\tilde{\psi}(k)$. Since $e^{ik\frac{\tilde{\mu}}{c}} = 1 + i\frac{\tilde{\mu}}{c}k - \frac{1}{2}\frac{\tilde{\mu}^2}{c^2}k^2 + O(k^3)$, and the $\tilde{\psi}(k)$ expansion was given in (44), we have

$$e^{ik\frac{\tilde{\mu}}{c}}\tilde{\psi}(k) = \left[1 + i\frac{\tilde{\mu}}{c}k - \frac{1}{2}\frac{\tilde{\mu}^2}{c^2}k^2 + O(k^3)\right]\left[1 - i\frac{\tilde{\mu}}{c}k - \frac{1}{2}M_2k^2 + A(-ik)^{2+2\kappa} + O(k^3)\right] \tag{49}$$

$$= 1 + 0k + \left(-\frac{M_2}{2} - \frac{\tilde{\mu}^2}{2c^2} + \frac{\tilde{\mu}^2}{c^2}\right)k^2 + A(-ik)^{2+2\kappa} + O(k^3), \tag{50}$$

and (48) follows after some simplification. □

Remark The $1 - \frac{1}{2}Vk^2$ part of (48) can be also found using Lemma 7, since we know that $\mathbb{E}[r] = 0$ and $\mathbb{E}[r^2] = V$.

In the expression (48) there are no powers between k^0 and k^2. This makes it possible for us to use the CSE method.

4 Applying the CSE method to the guilty user score

We are now finally in a position to compute accusation probabilities for guilty users. The Fourier transform $\tilde{\chi}$ serves as the basis; raising it to the power m yields the Fourier-transformed pdf of the total accusation S_j. The computational steps are almost identical to the case of the innocent score distribution [25], with two minor differences: (i) The variance of the single-segment pdf is V instead of 1; (ii) The pdf has non-zero average.

In Sect. 4.1 we show how these differences affect the theory. In Sect. 4.2 we discuss how the one-pirate probability $\Pr[S_j > Z]$ is used to obtain an upper bound on P_{FP}. In Sect. 4.3 we present plots that demonstrate the convergence of our numerical implementation. Furthermore, we present an ROC curve combining innocent and guilty accusation probabilities.

4.1 Adaptations

Below we list the (slight) modifications in the CSE method, as compared to [25], induced by the $V \neq 1$ variance and the nonzero mean. First, the tail of the Gaussian distribution changes.

Definition 8 We define the function Ω as the probability mass in the right tail of the normal distribution, $\Omega(z) := \frac{1}{\sqrt{2\pi}} \int_z^\infty \mathrm{d}x\ e^{-x^2/2}$.

Lemma 10 *Let $V > 0$ be the variance defined in (32). Then, for $x \in \mathbb{R}$ it holds that*

$$\frac{1}{2\pi i} \int_{-\infty}^{\infty} \mathrm{d}k\ \frac{e^{ikx}}{k} e^{-\frac{V}{2}k^2} = \frac{1}{2} - \Omega(x/\sqrt{V}). \tag{51}$$

Proof From Eq. 9.254.1 in [9] we have that $\frac{1}{2\pi i} \int_{-\infty}^{\infty} \mathrm{d}k\ \frac{e^{ikx}}{k} e^{-k^2/2} = \frac{1}{2} - \Omega(x)$. Changing the integration variable in (51) to $k' = k\sqrt{V}$ immediately yields the result. □

The modified Gaussian tail leads to modifications in all the integrals involving the tail.

Lemma 11 *Let $V > 0$ be the variance defined in (32). For $x \in \mathbb{R}$ and $\nu > 0$ it holds that*

$$\int_{-\infty}^{\infty} \frac{\mathrm{d}k}{2\pi} (i \operatorname{sgn} k)^{\alpha-1} |k|^{\nu-1} e^{-\frac{V}{2}k^2} e^{ikx} = \frac{1}{\pi V^{\frac{\nu}{2}}} \Gamma(\nu) 2^{\nu/2} \operatorname{Im}\left[i^{-\alpha} H_{-\nu}\left(\frac{ix}{\sqrt{2V}} \right) \right]. \tag{52}$$

Here $H_{-\nu}$ is a Hermite function.

Proof Corollary 2 in [25] states that for $x \in \mathbb{R}$ and $\nu > 0$:

$$\int_{-\infty}^{\infty} \frac{\mathrm{d}k}{2\pi} (i \operatorname{sgn} k)^{\alpha-1} |k|^{\nu-1} e^{-k^2/2} e^{ikx} = \frac{1}{\pi} \Gamma(\nu) 2^{\nu/2} \operatorname{Im}\left[i^{-\alpha} H_{-\nu}\left(\frac{ix}{\sqrt{2}} \right) \right]. \tag{53}$$

A change of integration variable to $k\sqrt{V}$ in (52) directly leads to the end result. □

The nonzero expectation value $\mathbb{E}[S_j] = m\tilde{\mu}/c$ gives rise to a 'shifted' version of the formula for the accusation probability. We introduce a shifted accusation threshold Δ,

$$\Delta := Z - m\tilde{\mu}/c \quad ; \quad \tilde{\Delta} := \Delta/\sqrt{m}. \tag{54}$$

The accusation probability can be expressed as a function of $\tilde{\Delta}$, as shown in the following two theorems.

Theorem 4 *Let j be a guilty user. Let R_m denote the accusation probability $\Pr[S_j > Z]$. Then*

$$R_m(\tilde{\Delta}) = \frac{1}{2} + \frac{i}{2\pi} \int_{-\infty}^{\infty} \mathrm{d}k \, \frac{\exp ik\tilde{\Delta}}{k} \left[\tilde{\chi}\left(\frac{k}{\sqrt{m}}\right)\right]^m. \tag{55}$$

Proof Exactly the same as the proof of (Theorem 3 in [25]), but with $\tilde{\Delta}$ replacing $\tilde{Z}$. □

Theorem 5 *Let j be a guilty user and $\frac{1}{2[q-1]} < \kappa < \frac{1}{2}$. Then it is possible to write*

$$\left[\tilde{\chi}\left(\frac{k}{\sqrt{m}}\right)\right]^m = \exp(-\frac{1}{2}Vk^2)\left[1 + \sum_{t=0}^{\infty} \omega_t(m)(i \operatorname{sgn} k)^{\alpha_t}|k|^{\nu_t}\right] \tag{56}$$

where α_t are real numbers; the coefficients $\omega_t(m)$ are real; the powers ν_t satisfy $\nu_0 = 2+2\kappa$ and $\nu_{t+1} > \nu_t$. The ν_t are not necessarily integer. All the coefficients $\omega_t(m)$ are decreasing functions of m. The probability of accusing user j is given by

$$R_m(\tilde{\Delta}) = \Omega(\tilde{\Delta}/\sqrt{V}) + \tfrac{1}{\pi}\sum_{t=0}^{\infty} \omega_t(m)\Gamma(\nu_t)(2/V)^{\nu_t/2} \operatorname{Im}\left[i^{-\alpha_t} H_{-\nu_t}(i\tilde{\Delta}/\sqrt{2V})\right]. \tag{57}$$

Proof See Appendix. □

4.2 Relation between $\Pr[S_j > Z]$ and the False Negative probability

The quantity that we compute, $\Pr[S_j > Z]$, is not equal to the quantity we are most interested in, P_{FN}. Below we explain how we obtain a bound on P_{FN} based on $\Pr[S_j > Z]$.

Lemma 12 *Let $j \in \mathcal{C}$. Let $\mathcal{L}$ be the set of accused users, and $\mathcal{A} = \mathcal{L} \cap \mathcal{C}$ the set of attackers that end up in $\mathcal{L}$. Then the False Negative probability can be expressed as*

$$P_{\mathrm{FN}} = 1 - c\Pr[j \in \mathcal{L}] + (c-1)\Pr[\mathcal{A} = \mathcal{C}]. \tag{58}$$

Proof We start by writing

$$\begin{aligned}\Pr[j \in \mathcal{L}] = \Pr[\mathcal{A} = \{j\}] + \sum_{k \in \mathcal{C}\setminus\{j\}} \Pr[\mathcal{A} = \{j,k\}] + \sum_{(k,\ell):k,\ell \in \mathcal{C}\setminus\{j\}} \Pr[\mathcal{A} = \{j,k,\ell\}] \\ + \cdots + \Pr[\mathcal{A} = \mathcal{C}],\end{aligned} \tag{59}$$

where (k,ℓ) is a pair with $k \neq \ell$, and the dots denote summation over all tuplets in $\mathcal{C}\setminus\{j\}$ up to and including size $c-2$. Next we take the sum $\sum_{j\in\mathcal{C}}$ over the whole equation (59). This yields $c\Pr[j \in \mathcal{L}] = \sum_{s=1}^{c-1}\Pr[|\mathcal{A}| = s] + c\Pr[\mathcal{A} = \mathcal{C}]$. Finally we use $1 - P_{\mathrm{FN}} = \sum_{s=1}^{c}\Pr[|\mathcal{A}| = s]$. □

The CSE method applied to *one* guilty user does not allow us to compute $\Pr[\mathcal{A} = \mathcal{C}]$. In order to upper bound the P_{FN} we will therefore use the following corollary.

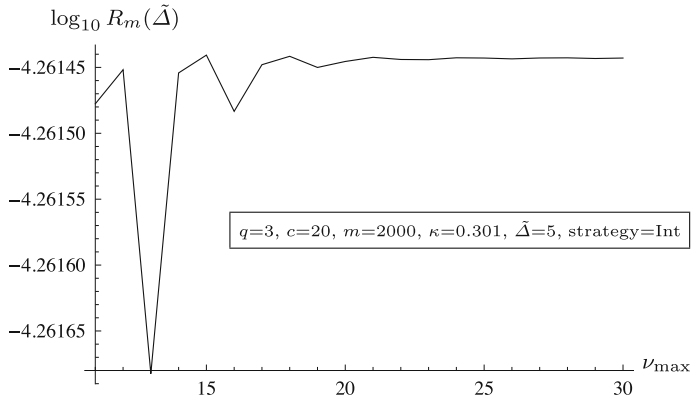

Fig. 2 Convergence example. Estimated $R_m(\tilde{\Delta})$ as a function of the cutoff power $\nu_{\max}$

Corollary 4 *Let $j \in \mathcal{C}$. It holds that $P_{\mathrm{FN}} < 1 - \Pr[S_j > Z]$.*

Proof Use $\Pr[\mathcal{A} = \mathcal{C}] < \Pr[j \in \mathcal{A}] = \Pr[j \in \mathcal{L}] = \Pr[S_j > Z]$ in Lemma 12. □

Remark The bound provided in Corollary 4 is not always tight. Note that $\Pr[\mathcal{L} = \mathcal{C}] \ll \Pr[j \in \mathcal{L}]$ if Z is 'significantly' larger than $m\tilde{\mu}/c$, yielding $P_{\mathrm{FN}} \approx 1 - c\Pr[S_j > Z]$. This is a much smaller number than what Corollary 4 gives us. However, we have not been able to prove a tight upper bound on P_{FN}.

4.3 Numerical results

We have implemented the CSE formulas of Sect. 4.1 in Wolfram Mathematica. In this section we present graphs to demonstrate that our implementation works and that we can generate ROC curves with it; we do not yet put the method to work to derive many "useful" results, e.g. exhaustive comparison of strategies for a large region of parameter space. That is left for future work.

4.3.1 Convergence

The convergence of (57) turns out to be rather quick. Often it suffices to take powers only up to $\nu_t \approx 10$ in order to get good accuracy. An example is shown in Fig. 2. (The parameters were chosen such that we are not in the Gaussian regime but in the right tail.)

4.3.2 Consistency check: power law in the tails

In Table 1 we see that the single-segment pdf has a power law $(1/u)^{3+2\kappa}$ in the right tail (provided that $K_1 \neq 0$). Hence the integrated probability mass beyond Z scales as $(1/Z)^{2+2\kappa}$. For large Z we expect to see the $(1/Z)^{2+2\kappa}$ scaling also in the $R_m(\tilde{\Delta})$ curves. (Due to the Central Limit Theorem, the $R_m(\tilde{\Delta})$ goes to a Gaussian shape, but only for small $\tilde{\Delta}$; for large $\tilde{\Delta}$ the original single-segment tail is still there.) We use this as a consistency check on our CSE implementation. Figure 3 shows a log-log plot of the right tail for various strategies. The tails in this plot indeed have the same slope as the $m = 1$ curve.

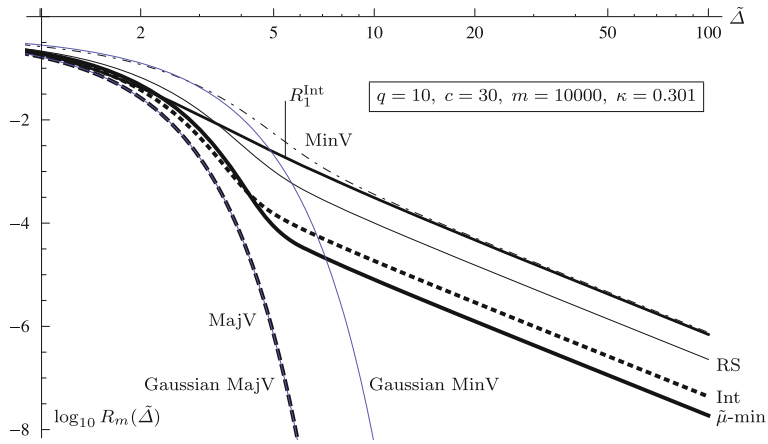

Fig. 3 Log–log plot of $R_m(\tilde{\Delta})$ for several strategies. The single-segment tail integral $R_1(\tilde{\Delta})$ for the Int attack is also shown. Two Gaussian tails are plotted: for the V value corresponding to the MajV and MinV strategies. The MajV curve coincides with its Gaussian approximation

4.3.3 ROC curves

One of the most useful types of graph for decision-making problems is the Receiver Operating Characteristic (ROC). We take a slightly different graph, with ε_1 and (our upper bound on) P_{FN} on the axes. This way, being closer to the origin means better accusation performance. Conversely, a stronger attack pushes points further from the origin. An example is shown in Figs. 4(a, b). Each curve corresponds to tracing the threshold Z from very low (lots of users get accused: high FP and low FN) to very high (almost nobody gets accused: low FP and high FN).

In Fig. 4(a) most of the relevant Z values lie outside the Gaussian regime, i.e. for all the attacks except MajV and $\tilde{\mu}$-min Z lies in the linear tail of the *innocent*-user score pdf.

The order of the curves for the different strategies is consistent with [26]: the most powerful attack is MinV, then RS, Int, and MajV/$\tilde{\mu}$-min. (The MajV and $\tilde{\mu}$-min are identical for the chosen parameters.) The quick transition from almost 1 to almost 0 on the vertical axis occurs when Z passes through the peak of the guilty-user score pdf. The FP probability changes little during this transition, since Z lies in the tail of the innocent-user score pdf.

In Fig. 4(b) we used the same settings as in Fig. 3. This is an example of a choice of parameters such that the Z visits the innocent-user Gaussian regime during the FN-transition. When Z is lowered (downward and to the right in the figure) into the innocent-user Gaussian regime, $\tilde{\mu}$-min becomes the most powerful attack. This is not surprising, as $\tilde{\mu}$-min is designed to be the strongest attack under the Gaussian assumption. Note that the FN-transition is much wider than in Fig. 4(a). This is caused by the fact that $\tilde{\mu}$ enters the steep Gaussian part of the innocent-user score pdf. This is particularly the case for the $\tilde{\mu}$-min attack, which has the lowest $\tilde{\mu}$ value.

5 Conclusions

We have adapted the CSE method so that we can compute accusation probabilities for individual guilty users, in the q-ary Tardos scheme, in the Restricted Digit Model. We use this to

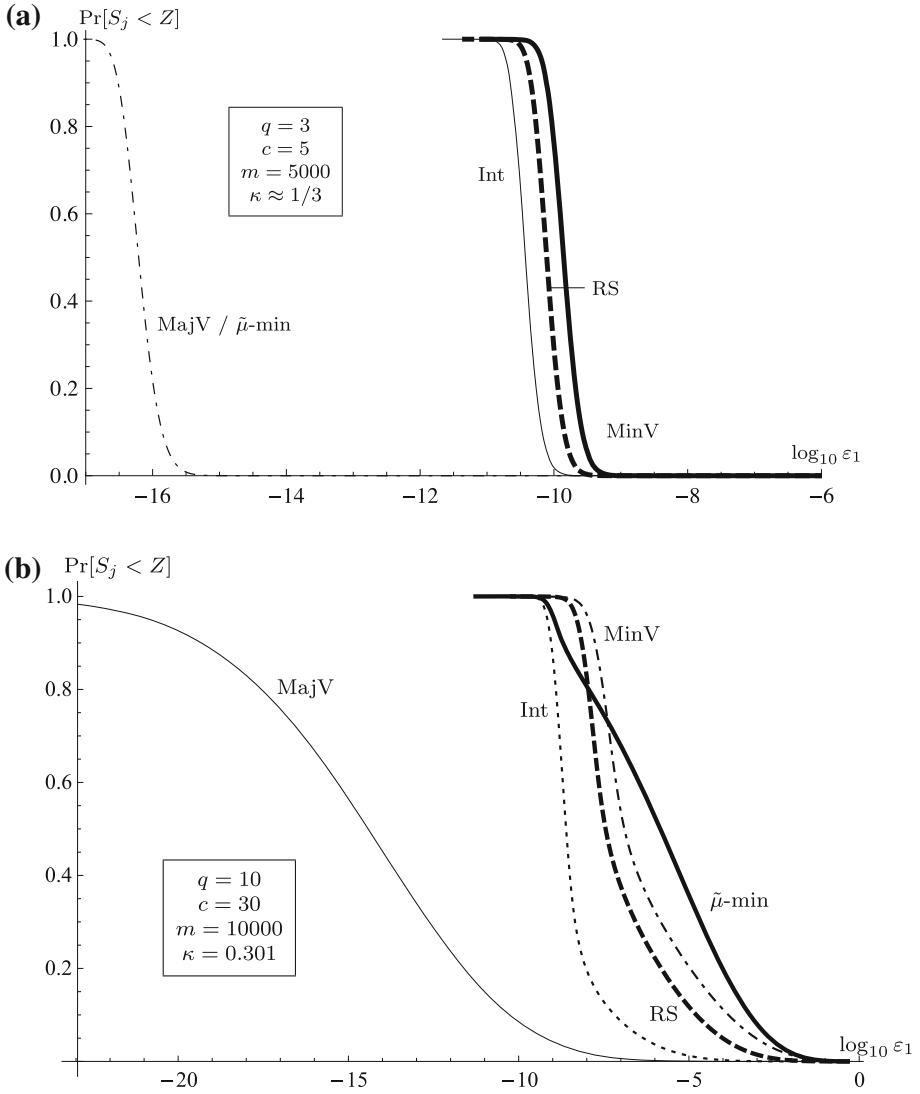

Fig. 4 Example 'ROC' curves. Our upper bound $\Pr[S_j < Z]$ on P_{FN} versus the probability ε_1 of accusing a fixed innocent user. The ε_1 data is taken from [26]

bound the overall FN probability as $P_{\text{FN}} < \Pr[S_{\text{guilty}} < Z]$. The main steps are the derivation of $\psi(u)$ (Theorem 2), taking the Fourier transform (Theorem 3), and executing the changes due to $\mathbb{E}[u] \neq 0$ and $\text{Var}(u) \neq 1$ (Sect. 4.1). The rest of the work is precisely as for the innocent score pdf. We have implemented the thus adapted CSE method and done a number of tests. Convergence of the series expansion seems to be faster than for the innocent pdf. The large-Z tails have the expected power law $(1/\tilde{\Delta})^{2+2\kappa}$. Having the CSE method at our disposal for guilty as well as innocent user scores, it now becomes possible to make full ROC curves. These can serve for choosing optimal parameter settings in the Tardos scheme (even though our bound $P_{\text{FN}} < \Pr[S_{\text{guilty}} < Z]$ is not tight), especially when there are attack

crossovers such as occur in Fig. 4(b). An exhaustive study of ROC curves is left for future work.

Appendix

Proof of Lemma 1

The proof is similar to the steps taken in Appendix D of [25]. First we split the q-dimensional integration $\int \mathrm{d}^q\boldsymbol{p}\ F(\boldsymbol{p})r(\boldsymbol{p})$ as follows,

$$\mathbb{E}_{\boldsymbol{p}}[r(\boldsymbol{p})] = \frac{1}{B(\kappa\mathbf{1}_q)} \int_0^1 \mathrm{d}p_y\ p_y^{-1+\kappa} \int_0^{1-p_y} \mathrm{d}^{q-1}\boldsymbol{p}_{\setminus y}\,\delta\left(1 - p_y - \sum_{\beta\in\mathcal{Q}\setminus\{y\}} p_\beta\right)\boldsymbol{p}_{\setminus y}^{-1+\kappa} r(\boldsymbol{p}). \tag{60}$$

Then we write $\boldsymbol{p}_{\setminus y} = (1-p_y)\boldsymbol{t}$. We get $\delta(1 - p_y - \sum_{\beta\in\mathcal{Q}\setminus\{y\}} p_\beta) = (1-p_y)^{-1}\delta(1 - \sum_{\beta\in\mathcal{Q}\setminus\{y\}} t_\beta)$. Furthermore, $\mathrm{d}^{q-1}\boldsymbol{p}_{\setminus y} = (1-p_y)^{q-1}\mathrm{d}^{q-1}\boldsymbol{t}$ and $\boldsymbol{p}_{\setminus y}^{-1+\kappa} = (1-p_y)^{(q-1)(-1+\kappa)}\boldsymbol{t}^{-1+\kappa}$. Combined with the fact that $B(\kappa\mathbf{1}_q) = B(\kappa, \kappa[q-1])B(\kappa\mathbf{1}_{q-1})$, these steps yield the end result. □

Proof of Theorem 1

The guilty user's symbol is denoted as X. The one-segment score is either $g_0(p_y)$ (when $X \neq y$) or $g_1(p_y)$ (when $X = y$). Since no other values are possible, the probability distribution at given $\boldsymbol{p}$ will consist of delta-function peaks. Each peak is multiplied by the probability that the corresponding event occurs

$$\psi_-(u|\boldsymbol{p}) = \sum_{y\in\mathcal{Q}} \delta\left(u - g_0(p_y)\right)\Pr[u = g_0(p_y)|\boldsymbol{p}] \tag{61}$$

$$\psi_+(u|\boldsymbol{p}) = \sum_{y\in\mathcal{Q}} \delta\left(u - g_1(p_y)\right)\Pr[u = g_1(p_y)|\boldsymbol{p}]. \tag{62}$$

Notice that

$$\Pr[u = g_0(p_y)|\boldsymbol{p}] = \Pr[X \neq y \wedge Y = y|\boldsymbol{p}] \quad ; \quad \Pr[u = g_1(p_y)|\boldsymbol{p}] = \Pr[X = y \wedge Y = y|\boldsymbol{p}] \tag{63}$$

and that

$$\Pr[X \neq y \wedge Y = y|\boldsymbol{p}] + \Pr[X = y \wedge Y = y|\boldsymbol{p}] = \Pr[Y = y|\boldsymbol{p}] = \tau_{y|\boldsymbol{p}}. \tag{64}$$

Next step is to compute $\Pr[u = g_1(p_y)|\boldsymbol{p}]$ in (62). Let be $\boldsymbol{e}_y$ a q-ary vector entirely set to 0 except for the y-th element that is instead equal to 1.

$$\Pr[u = g_1(p_y)|\boldsymbol{p}] = \Pr[X_{ji} = y]\Pr[Y = y|X_{ji} = y, \boldsymbol{p}] = p_y \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}} \binom{c-1}{\boldsymbol{\sigma} - \boldsymbol{e}_y} \boldsymbol{p}^{\boldsymbol{\sigma}-\boldsymbol{e}_y}\theta_{y|\boldsymbol{\sigma}}. \tag{65}$$

The last equation is obtained as follows: $\Pr[X_{ji} = y] = p_y$; $\Pr[Y = y|X_{ji} = y, \boldsymbol{p}]$ is equal to the sum over all the possible $\boldsymbol{\sigma}$ vectors that have at least one occurrence of y (expressed

with the condition $\sigma_y > 0$). Knowing that $X_{ji} = y$, the multinomial factor is needed to count the remaining $c-1$ pirate symbols in $\boldsymbol{\sigma}$, subtracting 1 from σ_y (using the $\boldsymbol{e}_y$ vector).

$$\Pr[u = g_1(p_y)|\boldsymbol{p}] = \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}} \frac{\sigma_y}{c}\binom{c}{\boldsymbol{\sigma}}\boldsymbol{p}^{\boldsymbol{\sigma}}\theta_{y|\boldsymbol{\sigma}}. \tag{66}$$

In the last equation we used $\boldsymbol{p}^{\boldsymbol{\sigma}} = p_y\boldsymbol{p}^{\boldsymbol{\sigma}-\boldsymbol{e}_y}$ and $\binom{c-1}{\boldsymbol{\sigma}-\boldsymbol{e}_y} = \frac{\sigma_y}{c}\binom{c}{\boldsymbol{\sigma}}$. Then the condition $\sigma_y > 0$ becomes superfluous and (27) trivially follows. Notice that

$$p_y\frac{\partial T_{y|\boldsymbol{p}}}{\partial p_y} = p_y\frac{\partial}{\partial p_y}\sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\boldsymbol{p}^{\boldsymbol{\sigma}}\theta_{y|\boldsymbol{\sigma}} = \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\theta_{y|\boldsymbol{\sigma}}\,p_y\frac{\partial\boldsymbol{p}^{\boldsymbol{\sigma}}}{\partial p_y} = \sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\theta_{y|\boldsymbol{\sigma}}\,\sigma_y\boldsymbol{p}^{\boldsymbol{\sigma}} \tag{67}$$

proving that (28)=(27) and (26)=(25). Finally, from (64) combined with (63) we have

$$\psi_-(u|\boldsymbol{p}) = \sum_{y\in\mathcal{Q}}\delta\left(u - g_0(p_y)\right)\left(\tau_{y|\boldsymbol{p}} - \Pr[X = y \wedge Y = y|\boldsymbol{p}]\right). \tag{68}$$

This, together with (66), completes the proof. □

Proof of Theorem 2

The full $\psi(u)$, without conditioning, is obtained by taking the expectation over $\boldsymbol{p}$ of (25)+(27).

$$\psi(u) = \mathbb{E}_{\boldsymbol{p}}[\psi(u|\boldsymbol{p})] = \Theta(-u)\mathbb{E}_{\boldsymbol{p}}[\psi_-(u|\boldsymbol{p})] + \Theta(u)\mathbb{E}_{\boldsymbol{p}}[\psi_+(u|\boldsymbol{p})]. \tag{69}$$

We first prove (29) starting from $\mathbb{E}_{\boldsymbol{p}}[\psi_-(u|\boldsymbol{p})]$ with $\psi_-(u|\boldsymbol{p})$ as given in (25).

$$\mathbb{E}_{\boldsymbol{p}}[\psi_-(u|\boldsymbol{p})] = \mathbb{E}_{\boldsymbol{p}}\left[\sum_{y\in\mathcal{Q}}\delta\left(u - g_0(p_y)\right)\sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\left(1-\frac{\sigma_y}{c}\right)\boldsymbol{p}^{\boldsymbol{\sigma}}\theta_{y|\boldsymbol{\sigma}}\right] \tag{70}$$

$$= \sum_{y\in\mathcal{Q}}\sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\left(1-\frac{\sigma_y}{c}\right)\theta_{y|\boldsymbol{\sigma}}\,\mathbb{E}_{\boldsymbol{p}}\left[\delta\left(u - g_0(p_y)\right)\boldsymbol{p}^{\boldsymbol{\sigma}}\right]. \tag{71}$$

From Lemma 1 and $\boldsymbol{p}_{\setminus y}^{\boldsymbol{\sigma}_{\setminus y}} = \left(1-p_y\right)^{c-\sigma_y}\prod_{\alpha\in\mathcal{Q}\setminus\{y\}}t_\alpha^{\sigma_\alpha}$ we have that

$$\mathbb{E}_{\boldsymbol{p}}\left[\delta\left(u - g_0(p_y)\right)\boldsymbol{p}^{\boldsymbol{\sigma}}\right] = \frac{1}{B(\kappa\mathbf{1}_q)}\int_0^1 \mathrm{d}p_y\;\delta\left(u - g_0(p_y)\right)p_y^{\sigma_y+\kappa-1}(1-p_y)^{c-\sigma_y+\kappa[q-1]-1}$$

$$\int_0^1 \mathrm{d}^{q-1}\boldsymbol{t}\;\delta(1-\sum_{\beta\in\mathcal{Q}\setminus\{y\}}t_\beta)\prod_{\alpha\in\mathcal{Q}\setminus\{y\}}t_\alpha^{\sigma_\alpha+\kappa-1}. \tag{72}$$

The second integral in (72) evaluates to $B(\boldsymbol{\sigma}_{\setminus y} + \kappa\mathbf{1}_{q-1})$, having the structure shown in Def. 1. In order to evaluate the p_y-integral we have to rewrite the delta function into the form $\delta\left(p_y - \cdots\right)$. We use the rule

$$\delta\left(u - w(p)\right) = \frac{\delta\left(p - w^{\mathrm{inv}}(u)\right)}{|\mathrm{d}w/\mathrm{d}p|} \tag{73}$$

for any monotonic function $w(p)$. This gives

$$\delta\left(u - g_0(p)\right) = \Theta(-u)\frac{2|u|}{\left(1+u^2\right)^2}\delta\left(p - \frac{u^2}{1+u^2}\right). \tag{74}$$

We substitute (74) into (72) and solve the integral

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{p}}\left[\delta\left(u - g_0(p_y)\right)\boldsymbol{p}^{\boldsymbol{\sigma}}\right] &= 2|u|\Theta(-u)\left(\frac{1}{1+u^2}\right)^2 \frac{B(\boldsymbol{\sigma}_{\setminus y}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)} \int_0^1 \mathrm{d}p_y\, \delta\left(p_y - \frac{u^2}{1+u^2}\right) \\
&\qquad p_y^{\sigma_y+\kappa-1}(1-p_y)^{c-\sigma_y+\kappa[q-1]-1} \\
&= 2|u|\Theta(-u)\left(\frac{1}{1+u^2}\right)^2 \frac{B(\boldsymbol{\sigma}_{\setminus y}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)} \\
&\qquad \left(\frac{u^2}{1+u^2}\right)^{\sigma_y+\kappa-1}\left(\frac{1}{1+u^2}\right)^{c-\sigma_y+\kappa[q-1]-1} \\
&= 2\Theta(-u)\frac{B(\boldsymbol{\sigma}_{\setminus y}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)}\frac{(u^2)^{\sigma_y+\kappa-1/2}}{(1+u^2)^{c+\kappa q}}.
\end{aligned} \tag{75}$$

Substituting (75) into (71) we have

$$\mathbb{E}_{\boldsymbol{p}}[\psi_-(u|\boldsymbol{p})] = 2\sum_{y\in\mathcal{Q}}\sum_{\boldsymbol{\sigma}\in\mathcal{S}_{qc}}\binom{c}{\boldsymbol{\sigma}}\left(1-\frac{\sigma_y}{c}\right)\frac{B(\boldsymbol{\sigma}_{\setminus y}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)}\frac{(u^2)^{\sigma_y+\kappa-1/2}}{(1+u^2)^{c+\kappa q}}\theta_{y|\boldsymbol{\sigma}}. \tag{76}$$

Now we change the summations as follows: the $\sum_{\boldsymbol{\sigma}}$ can be written as $\sum_b\sum_{\boldsymbol{x}}$ with $b=\sigma_y$ and $\boldsymbol{x}=\boldsymbol{\sigma}_{\setminus y}$, so $\theta_{y|\boldsymbol{\sigma}} = \Psi_b(\boldsymbol{x})$. Then the summand is a function of only b and $\boldsymbol{x}$, which allows us to write

$$\sum_y\sum_{\boldsymbol{\sigma}}\binom{c}{\boldsymbol{\sigma}} \to q\sum_{b=0}^{c}\sum_{\boldsymbol{x}}\binom{c}{b}\binom{c-b}{\boldsymbol{x}}. \tag{77}$$

Now we have

$$\mathbb{E}_{\boldsymbol{p}}[\psi_-(u|\boldsymbol{p})] = 2q\sum_{b=0}^{c}\sum_{\boldsymbol{x}}\binom{c}{b}\binom{c-b}{\boldsymbol{x}}\frac{c-b}{c}\frac{B(\boldsymbol{x}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)}\frac{(u^2)^{b+\kappa-1/2}}{(1+u^2)^{c+\kappa q}}\Psi_b(\boldsymbol{x}) \tag{78}$$

where

$$\sum_{\boldsymbol{x}}\binom{c}{b}\binom{c-b}{\boldsymbol{x}}\frac{B(\boldsymbol{x}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_q)}\Psi_b(\boldsymbol{x}) = \binom{c}{b}\sum_{\boldsymbol{x}}\binom{c-b}{\boldsymbol{x}}\frac{B(\boldsymbol{x}+\kappa\mathbf{1}_{q-1})}{B(\kappa\mathbf{1}_{q-1})B(\kappa,\kappa[q-1])}\Psi_b(\boldsymbol{x}) \tag{79}$$

$$= \binom{c}{b}\frac{1}{B(\kappa,\kappa[q-1])}\sum_{\boldsymbol{x}}\mathbb{P}_{q-1}(\boldsymbol{x}|b)\Psi_b(\boldsymbol{x})$$

$$= \binom{c}{b}\frac{K_b}{B(\kappa,\kappa[q-1])}. \tag{80}$$

In the last line we used Definition 3. Substituting (80) into (78) and removing 0 and c from the b-range, we have (29).

We can use exactly the same steps to obtain (30) from (27). The only significant difference is the delta function which in this case will be

$$\delta\left(u - g_1(p)\right) = \Theta(u)\frac{2u}{\left(1+u^2\right)^2}\delta\left(p - \frac{1}{1+u^2}\right). \tag{81}$$

□

Proof of consistency check 1

Integration of (29) and (30) gives

$$\int_{-\infty}^{\infty} \mathrm{d}u\, \psi(u) = \frac{2q}{B(\kappa, \kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(1-\frac{b}{c}\right)\int_{-\infty}^{0}\mathrm{d}u\,\frac{\left(u^2\right)^{b+\kappa-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}} + \frac{b}{c}\int_{0}^{\infty}\mathrm{d}u\,\frac{\left(u^2\right)^{c-b+\kappa[q-1]-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}}\right]. \tag{82}$$

Let be $\lambda{:=}b+\kappa$ and $w{:=}c-b+\kappa[q-1]$. Applying Lemma 2 we have

$$\frac{2q}{B(\kappa, \kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(1-\frac{b}{c}\right)\frac{1}{2}B(\lambda, w) + \frac{b}{c}\frac{1}{2}B(w, \lambda)\right] = \frac{q}{B(\kappa, \kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b B(\lambda, w). \tag{83}$$

The result follows applying Lemma 3 followed by Lemma 4. □

Proof of consistency check 2

Taking (29) and (30), the integral $\int_{-\infty}^{\infty}\mathrm{d}u\, u\psi(u)$ can be written as

$$\frac{2q}{B(\kappa, \kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(1-\frac{b}{c}\right)\int_{-\infty}^{0}\mathrm{d}u\,\frac{u\left(u^2\right)^{b+\kappa-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}} + \frac{b}{c}\int_{0}^{\infty}\mathrm{d}u\,\frac{u\left(u^2\right)^{c-b+\kappa[q-1]-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}}\right]. \tag{84}$$

Let $\lambda{:=}b+\kappa-\frac{1}{2}$ and $w{:=}c-b+\kappa[q-1]-\frac{1}{2}$. Applying Lemma 2 and the property $\Gamma(x+1) = x\Gamma(x)$ we have

$$\int_{-\infty}^{\infty}\mathrm{d}u\, u\psi(u) = \frac{2q}{B(\kappa, \kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(\frac{b}{c}-1\right)\frac{\Gamma(\lambda)\Gamma(w)\lambda}{2\Gamma(c+\kappa q)} + \frac{b}{c}\frac{\Gamma(\lambda)\Gamma(w)w}{2\Gamma(c+\kappa q)}\right]. \tag{85}$$

To obtain $\tilde{\mu}$ as in (24) we use Lemma 3 to substitute $\binom{c}{b}\frac{1}{B(\kappa,\kappa[q-1])}$ with $\frac{\mathbb{P}_1(b)}{B(\lambda+1/2,w+1/2)}$. After some simplifications, the result follows. □

Proof of Lemma 6

The integral $\int_{-\infty}^{\infty} \mathrm{d}u\, u^2\psi(u)$ can be written as

$$\frac{2q}{B(\kappa,\kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(1-\frac{b}{c}\right)\int_{-\infty}^{0}\mathrm{d}u\,\frac{u^2\left(u^2\right)^{b+\kappa-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}}\right.$$
$$\left.+\frac{b}{c}\int_{0}^{\infty}\mathrm{d}u\,\frac{u^2\left(u^2\right)^{c-b+\kappa[q-1]-\frac{1}{2}}}{\left(1+u^2\right)^{c+\kappa q}}\right]. \tag{86}$$

Let $\lambda{:=}c-b+\kappa[q-1]$ and $w{:=}b+\kappa$. Applying Lemma 2 with (2) and the property $\Gamma(x+1)=x\Gamma(x)$, we get

$$\frac{2q}{B(\kappa,\kappa[q-1])}\sum_{b=1}^{c}\binom{c}{b}K_b\left[\left(1-\frac{b}{c}\right)\frac{\Gamma(\lambda-1)\Gamma(w-1)w(w-1)}{2\Gamma(c+\kappa q)}\right.$$
$$\left.+\frac{b}{c}\frac{\Gamma(\lambda-1)\Gamma(w-1)\lambda(\lambda-1)}{2\Gamma(c+\kappa q)}\right]. \tag{87}$$

Then using (18) we have

$$\int_{-\infty}^{\infty}\mathrm{d}u\,u^2\psi(u)=q\sum_{b=1}^{c}K_b\mathbb{P}_1(b)\left[\left(1-\frac{b}{c}\right)\frac{w}{\lambda-1}+\frac{b}{c}\frac{\lambda}{w-1}\right] \tag{88}$$

and (33) follows after some rewriting. □

Proof of Theorem 5

We start from Corollary 3 and write a general power series expansion,

$$\tilde{\chi}(k)=1-(V/2)k^2+\sum_{t=0}^{\infty}\gamma_t|k|^{r_t}, \tag{89}$$

where the $r_t\geq 2+2\kappa$ are powers and the $\gamma_t\in\mathbb{C}$ are coefficients of the form $i^{\beta_t\,\mathrm{sgn}\,k}$ times a real factor. In this expression the desired relation $\tilde{\chi}(-k)=[\tilde{\chi}(k)]^*$ evidently holds, and the properties $\tilde{\chi}(0)=1$, $\tilde{\chi}'(0)=0$, $\tilde{\chi}''(0)=-V$ are clearly present. Then we write

$$[\tilde{\chi}(k/\sqrt{m})]^m=\exp[m\ln\tilde{\chi}(k/\sqrt{m})]=e^{-\frac{V}{2}k^2}\exp\left[m\sum_{t=0}^{\infty}(\frac{|k|}{\sqrt{m}})^{r_t'}\delta_t\right], \tag{90}$$

where the powers $r_t'\geq 2+2\kappa$ and coefficients $\delta_t\propto i^{\beta_t'\mathrm{sgn}\,k}$ are obtained (laboriously) by substituting (89) into the Taylor series for the logarithm, $\ln(1+\varepsilon)=\varepsilon-\varepsilon^2/2+\varepsilon^3/3-\varepsilon^4/4+\cdots$. It is worth noting that m disappears from the k^2 term, but not from the others. Equation (56) is obtained from (90) by using the Taylor series for the exp function,

$$\exp\varepsilon=1+\varepsilon+\varepsilon^2/2!+\varepsilon^3/3!+\cdots \tag{91}$$

and (again laboriously) collecting terms with equal powers of k. Since we started out with powers $r_t \geq 2 + 2\kappa$, we end up with powers $\nu_t \geq 2 + 2\kappa$. Finally, (57) follows by applying Lemma 10 and Lemma 11 to evaluate the integrals that arise when (56) is substituted into Theorem 4. □

References

1. Amiri E., Tardos G.: High rate fingerprinting codes and the fingerprinting capacity. In: ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 336–345 (2009).
2. Blayer O., Tassa T.: Improved versions of Tardos' fingerprinting scheme. Des. Codes Cryptogr. **48**(1), 79–103 (2008).
3. Boesten D., Škorić B.: Asymptotic fingerprinting capacity for non-binary alphabets. In: Information Hiding. Lecture Notes in Computer Science, vol. 6958, pp. 1–13. Springer, Heidelberg (2011).
4. Boneh D., Shaw J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inf. Theory **44**(5), 1897–1905 (1998).
5. Charpentier A., Xie F., Fontaine C., Furon T.: Expectation maximization decoding of Tardos probabilistic fingerprinting code. In: SPIE Proceedings of Media Forensics and Security, vol. 7254, p. 72540 (2009).
6. Furon T., Pérez-Freire L.: Worst case attacks against binary probabilistic traitor tracing codes. In: IEEE Workshop on Information Forensics and Security (WIFS). http://arxiv.org/abs/0903.3480 (2009).
7. Furon T., Pérez-Freire L., Guyader A., Cérou F.: Estimating the minimal length of Tardos code. In: Information Hiding. Lecture Notes in Computer Science, vol. 5806, pp. 176–190. Springer, Berlin (2009).
8. Furon T., Guyader A., Cérou F.: On the design and optimization of Tardos probabilistic fingerprinting codes. In: Information Hiding. Lecture Notes in Computer Science, vol. 5284, pp. 341–356. Springer, Berlin (2008).
9. Gradshteyn I.S., Ryzhik I.M.: Table of Integrals, Series, and Products, 5th edn. Academic Press, New York (1994).
10. He S., Wu M.: Joint coding and embedding techniques for multimedia fingerprinting. IEEE Trans. Inf. Forensics Secur. **1**, 231–248 (2006).
11. Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.: On codes with the identifiable parent property. J. Comb. Theory **82**, 472–479 (1998).
12. Huang Y.W., Moulin P.: On fingerprinting capacity games for arbitrary alphabets and their asymptotics. In: IEEE International Symposium on Information Theory (ISIT), pp. 2571–2575 (2012).
13. Huang Y.W., Moulin P.: Saddle-point solution of the fingerprinting capacity game under the marking assumption. In: IEEE International Symposium on Information Theory (ISIT), pp. 2256–2260 (2009).
14. Kilian J., Leighton F.T., Matheson L.R., Shamoon T.G., Tarjan R.E., Zane F.: Resistance of digital watermarks to collusive attacks. In: IEEE International Symposium on Information Theory (ISIT), p. 271 (1998).
15. Kuribayashi M., Akashi N., Morii M.: On the systematic generation of Tardos's fingerprinting codes. In: IEEE International Workshop on Multimedia Signal Processing (MMSP), pp. 748–753 (2008).
16. Laarhoven T., de Weger B.: Optimal symmetric Tardos traitor tracing schemes. Des. Codes Cryptogr. (2012). doi:10.1007/s10623-012-9718-y.
17. Laarhoven T., Doumen J., Roelse P., Škorić B., de Weger B.M.M.: Dynamic Tardos traitor tracing schemes. IEEE Trans. Inf. Theory **59**, 1–13 (2013).
18. Meerwald P., Furon T.: Towards joint Tardos decoding: the 'Don Quixote' algorithm. In: Information Hiding. Lecture Notes in Computer Science, vol. 6958, pp. 28–42. Springer, Prague (2011).
19. Moulin P.: Universal fingerprinting: capacity and random-coding exponents. http://arxiv.org/abs/0801.3837 (2008).
20. Nuida K.: Short collusion-secure fingerprint codes against three pirates. In: Information Hiding. Lecture Notes in Computer Science, vol. 6387, pp. 86–102. Springer, Calgary (2010).
21. Nuida K., Hagiwara M., Watanabe H., Imai H.: Optimal probabilistic fingerprinting codes using optimal finite random variables related to numerical quadrature. CoRR, abs/cs/0610036 (2006).
22. Prudnikov A.P., Brychkov Y.A., Marichev O.I.: Integrals and Series, vol. 1. CRC Press, Boca Raton (1994).
23. Schaathun H.G.: On error-correcting fingerprinting codes for use with watermarking. Multimedia Syst. **13**(5–6), 331–344 (2008).

24. Simone A., Škorić B.: Asymptotically false-positive-maximizing attack on non-binary Tardos codes. In: Information Hiding. Lecture Notes in Computer Science, vol. 6958, pp. 14–27. Springer, Berlin (2011).
25. Simone A., Škorić B.: Accusation probabilities in Tardos codes: beyond the Gaussian approximation. Des. Codes Cryptogr. **63**(3), 379–412 (2012).
26. Simone A., Škorić B.: False Positive probabilities in q-ary Tardos codes: comparison of attacks. http://eprint.iacr.org/2012/522 (2012).
27. Somekh-Baruch A., Merhav N.: On the capacity game of private fingerprinting systems under collusion attacks. IEEE Trans. Inf. Theory **51**, 884–899 (2005).
28. Tardos G.: Optimal probabilistic fingerprint codes. In: ACM Symposium on Theory of Computing (STOC), pp. 116–125 (2003).
29. Škorić B., Katzenbeisser S., Celik M.U.: Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. Des. Codes Cryptogr. **46**(2), 137–166 (2008).
30. Škorić B., Katzenbeisser S., Schaathun H.G., Celik M.U.: Tardos fingerprinting codes in the combined digit model. In: IEEE Workshop on Information Forensics and Security (WIFS), pp. 41–45 (2009)
31. Škorić B., Vladimirova T.U., Celik M.U., Talstra J.C.: Tardos fingerprinting is better than we thought. IEEE Trans. Inf. Theory **54**(8), 3663–3676 (2008).
32. Xie F., Furon T., Fontaine C.: On-off keying modulation and Tardos fingerprinting. In: ACM Workshop on Multimedia and Security (MM&Sec), pp. 101–106 (2008).