Binary and q-ary Tardos codes, revisited

Boris Škorić · Jan-Jaap Oosterwijk

Abstract The Tardos code is a much studied collusion-resistant fingerprinting code, with the special property that it has asymptotically optimal length $m \propto c_0^2$, where c_0 is the number of colluders.
In this paper we give alternative security proofs for the Tardos code, working with the assumption that the strongest coalition strategy is position-independent. We employ the Bernstein inequality and Bennett inequality instead of the typically used Markov inequality. This proof technique requires fewer steps and slightly improves the tightness of the bound on the false negative error probability. We present new results on code length optimization, for both small and asymptotically large coalition sizes.

1 Introduction

1.1 Collusion-resistant forensic watermarking

Watermarking, also known as active fingerprinting, provides a means for tracing the origin and distribution of digital data. Before distribution, the content is modified by embedding an imperceptible watermark, which plays the role of a personalized serial number. Once an unauthorized copy of the content is found, the identities of those users who participated in its creation can be determined. This is done using a tracing algorithm, which outputs a list of suspicious users. The whole process is known as *forensic watermarking.*
In any practical implementation there are two layers [12, 21]: The 'coding' layer determines which message to embed. The underlying watermarking layer hides symbols of the message in segments[1] of the content. The symbols are from a discrete alphabet, binary or larger.
Reliable tracing of content requires security against various attacks on the watermarks. *Collusion attacks* are a particularly strong threat. A coalition of users colludes to compare their copies. As any differences between the copies have to arise from the watermarks and not the content, the comparison tells the coalition where to attack.
To counter this attack, coding theory has produced a number of collusion-resistant codes. The interface between the fingerprinting code and the watermarking system is usually specified in terms of the *Marking Assumption* (MA) plus additional assumptions that are referred to as a 'model'. The MA states that the colluders are able to perform modifications only in those content segments where they received differently marked content. These segments are called detectable positions. The 'model'

[1] The concept of a 'segment' can vary wildly. It can be as simple as a video frame or as complex as a Fourier coefficient spread out over many frames. We will use the concept of segments without defining what they are. Ideally, statements about the coding layer are independent of the embedding process.

specifies the kind of symbol manipulations that the attackers are able to perform in detectable positions. The commonly used *Restricted Digit Model* (RDM) allows them only to choose pieces from their copies of the content, i.e. each segment of the unauthorized copy carries exactly one symbol that the attackers have received. Most other models have unrealistically strong attacks, e.g. putting any symbol from the alphabet in a detectable position, or creating an erasure. Notable exceptions are the 'fusion' attack option in [28] and the Combined Digit Model in [26], which both take into account realistic signal processing attacks.
If the alphabet is binary then all the MA-based attack models are equivalent. In this paper we are primarily interested in larger (q-ary) alphabets. Our interest stems from the fact that the asymptotic (#attackers $\to \infty$) fingerprinting channel capacity[2] in the RDM is known to be an increasing function of the alphabet size q [5], and from the existence of q-ary schemes [25] that perform better asymptotically than their binary counterparts.
Many collusion-resistant codes have been proposed in the literature. Most notable are the Boneh-Shaw construction [6] and the by now famous Tardos code [24]. The former uses a concatenation of an inner code with a random outer code, while the latter is a fully randomized binary code. Tardos' code was the first to achieve the asymptotically optimal property $m \propto c_0^2$, where m is the number of segments, and c_0 is the number of attackers that can be resisted. (Previous codes had higher powers of c_0 or required an alphabet size that is unrealistically large in the context of multimedia watermarking.) This optimality has generated a lot of interest. Papers have appeared containing improved analyses [4,9,11,15,23,27], code modifications [13,18,19], decoder modifications [1,8,16] and various generalizations [7,25,26,28]. In the current paper we improve the analysis of the generalization [25] of the Tardos code to non-binary alphabets.

1.2 Upper-bounding the errors; cutoff parameter

The Tardos code and all its variants are probabilistic in two ways: (1) the code generation is randomized; (2) the tracing procedure allows for a (small) probability of error.
Two types of error are usually studied. The first one is a False Positive (FP) error. The probability of wrongly accusing a *fixed* innocent user has to be upper-bounded by some very small constant, $P_{\rm FP} \leq \varepsilon_1$. The second type of error is a False Negative (FN) error. The probability that the tracing algorithm does not catch any attacker at all has to be bounded as $P_{\rm FN} \leq \varepsilon_2$. Typically $\varepsilon_2 \gg \varepsilon_1$, since a viable deterrent exists even when e.g. $\varepsilon_2 \approx \frac{1}{2}$.
The typical proof technique in the literature is to use the Markov inequality to bound the probability that the 'accusation score' exceeds a certain threshold. For the Markov inequality to work it is required that the scores are finite. They are made finite by introducing a small cutoff parameter 'τ' for the symbol biases (see Section 2.1). It was shown in [25] that for $q \geq 3$ the cutoff is a proof-technical artifact, and one can set $\tau = 0$ without ill effect. This was studied in further detail in [23, 22]. However, for the *binary* Tardos scheme a cutoff is really necessary: it protects the scheme against rare 'tail' events that blow up innocent users' accusation scores.
In this paper we have the cutoff, since we will make use of so-called 'concentration inequalities', which require random variables to be bounded.

1.3 Results on the length of Tardos codes

Tardos [24] proved bounds on the FP and FN errors using Markov inequalities. His construction achieved the asymptotically optimal power law $m \propto c_0^2$, namely $m = 100 c_0^2 \ln \varepsilon_1^{-1}$. The constants appearing in the scheme were far from optimal, especially the coefficient 100 in the code length,

[2] The channel capacity is a fair measure of how efficient a code can theoretically be. It is an upper bound on the achievable fingerprinting rate. The fingerprinting rate of a q-ary code can be interpreted as the number of q-ary symbols needed to isolate one specific user, divided by the length of the code (total number of q-ary symbols transmitted).

which was mostly caused by the choice $\varepsilon_2 = \varepsilon_1^{c_0/4}$. We will denote the code length coefficient as 'A', and write

$$m = Ac_0^2 \ln \varepsilon_1^{-1}. \tag{1}$$

In later work the ε_1 and ε_2 were decoupled, and the numerical constants were tweaked to reduce the code length parameter A. Blayer and Tassa [4] showed that the same proof technique could be maintained while reducing A to some value slightly above 20. In [27] it was shown that for large coalition sizes, A can be reduced to $2\pi^2$. Their asymptotic analysis made use of the fact that the probability distributions of large sums become Gaussian due to the Central Limit Theorem.

In [25] Tardos' accusation score function was modified to make it symmetric in the symbols 0,1. This modification meant that all available information in the forged copy y was utilized, instead of discarding 50% of the information (namely the positions containing 0). The effect was an improvement of the code length by a factor 4. In the same paper, the scheme was generalized to arbitrary alphabet size. Asymptotic analysis using Gaussian distributions showed that asymptotically one can go as low as $A = 2/M^2$, where M is the expected accusation score of the coalition (see Section 4) minimized over the attack strategy. In the binary case this becomes $A = \pi^2/2$.

A different kind of modification of the *binary* Tardos code was used in [20,13,1,10]: The distribution function of the biases was altered. In the current paper we will mostly consider non-binary alphabets, for which no such modifications are known; hence modifying the distribution of the biases is outside the scope of this paper.

A very important development was the development of 'joint decoders' [1,8,16], accusation algorithms that do not only look at single-user scores, but also at tuplets of users. Joint decoders can, in theory, achieve rates close to the fingerprinting capacity. Our interest in 'simple decoders' (which use single-user scores only) stems from the fact that all the proposals for *practical* joint decoders start with a simple decoder as the first stage. Hence, optimization of simple decoding improves the performance of joint decoding.

Recently Laarhoven and de Weger [15] applied the Markov-inequality based proof technique to the symmetric accusation score in the binary case. They obtained the asymptotic result

$$A = \frac{\pi^2}{2}\left[1 + c_0^{-1/3}[\tfrac{12}{\pi^2}]^{\frac{1}{3}}\left(1 + \frac{6\ln\varepsilon_2/\ln\varepsilon_1}{\ln c_0} + \cdots\right)\right] \tag{2}$$

for optimal settings of the tunable parameters in the scheme. In [25] the same kind of analysis had been attempted for general alphabet size, but the results were not tight, sitting a factor 2 above the asymptotic $2/M^2$ known from the Gaussian approximation; the reason for the discrepancy was that one tweakable extra parameter à la [4] was missing in the proof technique.

In [23,22] a semi-analytical method was developed to compute FP error probabilities in Tardos codes. This is especially useful for small ε_1, a regime where simulations cannot penetrate due to the extreme number of runs required. However, explicit pirate strategies have to be given as input; the approach does not yield provable properties against *arbitrary* attacks.

The current state of affairs regarding provable properties of Tardos codes is unsatisfactory in two respects,

- In [25] an opportunity was missed to do a tight analysis of provable bounds on the error probabilities for $q \geq 3$. Such an analysis is still missing.
- The existing proofs, based on Markov inequalities, are very lengthy and cumbersome, and involve several auxiliary variables that have no concrete relation to the system parameters in the code generation and/or score computation.

1.4 Contributions and outline

We present provable bounds on the FP and FN errors for the q-ary symmetric scheme of [25], working with the assumption that the strongest possible coalition attack is position-symmetric. We use the bounds to provide sufficient code lengths that provably guarantee desired FP and FN error rates.

- We base our bounds on the Bernstein inequality and the Bennett inequality. The resulting proofs are shorter than those using the Markov inequality, and do not contain auxiliary variables.
- For $q \geq 3$ this is the first analysis that gives tight bounds. It also is the first to provide asymptotic correction terms to the limiting value $A = 2/M^2$.
- In our analysis we distinguish more clearly between c, the actual number of attackers, and c_0, the system parameter, than previous literature.
- We provide a detailed analysis of the quantity M as a function of the cutoff parameter, and a method to compute M numerically. This has not been done before for $q \geq 3$.
- For $q = 2$ we reproduce the asymptotics of [15], but our proof is less complex. Furthermore, we show that for large but finite c_0, it is possible to get shorter codes by slightly modifying the 'concentration parameter' (see Section 2.1).
- The code rate, obtained from numerics, turns out to be a decreasing function of q at 'small' c_0. Asymptotically, however, we find for $q \in \{2, 3, 4, 5\}$ that the non-binary alphabets have a higher rate than the binary; $q = 3$ has the highest asymptotic code rate. (One has to bear in mind that the results for non-asymptotic c_0 depend on the proof method, i.e. on the bounds obtained from the Bernstein and Bennett inequalities. Sharper bounds on the error probabilities will lead to shorter code length values.)

The organization of this paper is as follows. In Section 2 we summarize the q-ary Tardos scheme and discuss how its performance is measured. We also discuss the inequalities of Bernstein and Bennett. After these preliminaries we prove bounds on the FP and FN error probabilities (Section 3).
In Section 4 we present a number of lemmas about the statistical properties of the accusation scores. In Section 5 these are used to optimize the code length parameter in the asymptotic regime $c_0 \to \infty$. In Section 6 we derive equations for optimizing the code length as a function of ε_1, ε_2 and *finite* c_0. We show numerical solutions for alphabet sizes $q = 3, 4, 5$ and $c_0 \leq 20$. For large (but not asymptotic) c_0 we derive an analytic expression for the code length parameter that contains correction terms to the limiting value $A = 2/M^2$. We summarize in Section 7.
An apology: This could have been a short and elegant paper (consisting only of Sections 1 to 3), due to the brevity of the proofs using Bernstein's and Bennett's inequalities. However, in the presence of a cutoff, the statistical parameter M is a complicated beast, and many pages are spent on taming it (starting at Section 4).

2 Preliminaries

2.1 q-ary Tardos fingerprinting

Tardos [24] introduced the first fingerprinting scheme that achieves optimality in the sense of having the asymptotic behavior $m \propto c_0^2$. He introduced a two-step stochastic procedure for generating the codewords. Here we briefly summarize the generalization to non-binary alphabets [25].
The alphabet is denoted as $\mathcal{Q}$ and has size $|\mathcal{Q}| = q$. There are n users $j \in \{1, \ldots, n\}$. Each user receives a uniquely watermarked version of the content; the content consists of m segments[3], each of which contains one watermark symbol. The symbol of user j in segment i is denoted as X_{ji}. The matrix X is called the code matrix.
Code generation
Step 1: For each segment $i \in \{1, \ldots, m\}$ the content distributor generates a random q-component *bias vector* $\boldsymbol{p}^{(i)} \sim F$, where F is a probability density function that is invariant under permutations of the alphabet. Furthermore, the vector components satisfy $p_\alpha^{(i)} \in [p_{\min}, p_{\max}]$, where $p_{\min} = \tau$ and $p_{\max} = 1 - t$, with $t = (q-1)\tau$, and $\sum_\alpha p_\alpha^{(i)} = 1$. The $\tau \ll 1$ is called the cutoff parameter. For $q \geq 3$

[3] The concept of segments is very general, e.g. they can be combinations of coefficients in any codec.

$\mathcal{Q}$	the alphabet	q	alphabet size $\|\mathcal{Q}\|$
n	number of users	$\mathcal{C}$	set of colluding users
c	number of colluders, $\|\mathcal{C}\|$	c_0	coalition size to be resisted
m	code length	X_{ji}	symbol in segment i for user j
$\boldsymbol{p}^{(i)}$	bias vector for column i	F	distribution of the bias vector, $\boldsymbol{p}^{(i)} \sim F$
κ	'concentration' parameter in F	τ	cutoff parameter for the $\boldsymbol{p}$-space
t	$t = (q-1)\tau$	$\sigma_\alpha^{(i)}$	#occurrences of symbol α in attackers' segment i
y_i	symbol in attacked segment i	$\theta_{y\|\boldsymbol{\sigma}}$	prob. that attackers output symbol y, given $\boldsymbol{\sigma}$
$g_0(p)$, $g_1(p)$	score functions	S_j	score of user j
$S_j^{(i)}$	score of user j in segment i	$S_\mathcal{C}$	coalition score, $S_\mathcal{C} = \sum_{j\in\mathcal{C}} S_j$
$S_\mathcal{C}^{(i)}$	coalition score in segment i	Z	accusation threshold
$\mathcal{L}$	list of accused users	ε_1	max. tolerable prob. of accusing fixed innocent
ε_2	max. tolerable FN prob.	η	$\ln\varepsilon_2/\ln\varepsilon_1$
FP, FN	False Positive, False Negative	$\tilde{\mu}$	expectation $\mathbb{E}[S_\mathcal{C}^{(i)}]$; does not depend on m
$\tilde{\sigma}^2$	variance of $S_\mathcal{C}^{(i)}$	M	minimum of $\tilde{\mu}$ over all strategies θ, for $c = c_0$
M_0	M at $\tau = 0$	M_0^∞	M_0 for $c_0 \to \infty$
$c_0 V^2$	$\max_\theta \tilde{\sigma}^2$ for $c = c_0$	$\nu \in (1,2)$	parameter in the power law $\tau \sim c_0^{-\nu}$

it is allowed to set $\tau = 0$ without ill effects, but for $q = 2$ the cutoff is required to prevent extreme scores (see Eq.6) from popping up and disturbing the statistics. We will take τ nonzero for *all* q, for proof-technical reasons: although the Tardos scheme at $q \geq 3, \tau = 0$ performs fine, concentration inequalities like Bernstein's and Bennett's inequalities require bounded variables.
The probability density F is set to be a symmetric Dirichlet distribution.

$$F(\boldsymbol{p}) = \frac{1}{\mathcal{N}(q,\kappa,\tau)} \prod_{\alpha\in\mathcal{Q}} p_\alpha^{-1+\kappa}, \tag{3}$$

where $\kappa > 0$ is a constant called the 'concentration parameter' and $\mathcal{N}(q,\kappa,\tau)$ is a normalization constant taking care that

$$\int_\tau^{1-t} \mathrm{d}^q p \; \delta(1 - \sum_{\alpha\in\mathcal{Q}} p_\alpha) F(\boldsymbol{p}) = 1 \tag{4}$$

holds.[4] The $\int \mathrm{d}^q p$ denotes q-dimensional integration over all the q variables p_α. In our notation, the integration variable is written immediately after the $\int$ symbol, and integrals are considered to be operators acting on everything to the right. The $\delta(\cdots)$ is the Dirac Delta function, and it takes care that the probabilities p_α add up to 1.
Let $\mathbf{1}_q$ denote a vector consisting of q ones; let B denote the generalized Beta function[5]; then $\mathcal{N}(q,\kappa,0) = B(\kappa\mathbf{1}_q) = [\Gamma(\kappa)]^q/\Gamma(\kappa q)$.
Step 2: Next, the distributor randomly generates the to-be-embedded symbols by employing the bias vectors as categorical probability distributions: $\mathbb{P}[X_{ji} = \alpha] = p_\alpha^{(i)}$. The columns of X are independent, and the rows of X are independent for fixed biases.
<u>Collusion attack</u>
The set of colluders is denoted as $\mathcal{C}$, with $|\mathcal{C}| = c$. According to the Restricted Digit Model, for each segment i the colluders have to output content containing precisely one of the symbols that they have received; they do not have the knowledge to generate any other symbol. The symbol in the forged version is denoted as y_i. Their strategy for choosing y_i is allowed to be probabilistic. The following assumptions are usually made:

[4] In the binary case, Tardos' original scheme is regained by setting $\kappa = 1/2$. We then have $\mathcal{Q} = \{0,1\}$, $\boldsymbol{p} = (p_0, p_1)$ with $p_0 + p_1 = 1$, and $F(\boldsymbol{p}) = \frac{1}{\pi - 4\arcsin\sqrt{\tau}}(p_0 p_1)^{-1/2}$.

[5] The generalized Beta function of a vector $\boldsymbol{v} = (v_1, \cdots, v_n)$ is defined as $B(\boldsymbol{v}) = \Gamma(v_1)\Gamma(v_2)\cdots\Gamma(v_n)/\Gamma(v_1 + \cdots + v_n)$. For $n = 1$ this reduces to 1.

1. The strategy is invariant under permutations of the alphabet.
2. The strategy is fair in the sense that the colluders equally share the risk. (I.e. the strategy is invariant under permutation of the colluder identities.)
3. The same strategy is applied independently for each segment.

As long as the symbol labels have no physical meaning, i.e. as long as the symbols in $\mathcal{Q}$ have no natural ordering related to the signal processing, assumption 1 does not reduce the strength of the attack. In the setting we work in, namely that the content owner is successful when he traces *at least one* attacker, it is obviously best for the coalition to share the risk equally; hence assumption 2 also does not reduce the attack strength.
Assumption 3 makes a lot of sense intuitively. In a scheme where the code generation and the accusation scores are completely segment-symmetric, it seems obvious that it can only be disadvantageous for the attackers to deviate from this symmetry. Furthermore, in the context of fingerprinting capacities it was shown [17] that the most powerful attack is indeed segment-symmetric. However, all this does not provide a rigorous proof for finite code sizes. (At finite m, the realization of the p_i variables slightly breaks the segment-symmetry; the larger m becomes, the more the symmetry is restored.)
In this paper we will adopt assumptions 1–3. We will need assumption 3 for deriving a bound on the FN probability, but not for the FP.
Given these assumptions, the strategy can depend only on the number of occurrences of each symbol in the coalition. Let $\sigma_\alpha^{(i)} \in \{0, \ldots, c\}$ denote the number of colluders who have the symbol α in segment i, with $\sum_{\alpha\in\mathcal{Q}} \sigma_\alpha^{(i)} = c$. Let $\boldsymbol{\sigma}^{(i)}$ be defined as the vector containing the $\sigma_\alpha^{(i)}$; then for each $\boldsymbol{\sigma}^{(i)}$ independently the attack can be parametrized as a q-component vector $\boldsymbol{\theta}_{\boldsymbol{\sigma}}$ of probabilities $\theta_{y|\boldsymbol{\sigma}} = \mathbb{P}[\text{output } y|\boldsymbol{\sigma}]$, with $\sum_{y\in\mathcal{Q}} \theta_{y|\boldsymbol{\sigma}} = 1$. Given the above assumption 1, the $\theta_{y|\boldsymbol{\sigma}}$ has to be invariant under alphabet permutations. We will use the shorthand notation 'θ' for the complete attack strategy, i.e. the whole set of vectors, $\theta = \{\boldsymbol{\theta}_{\boldsymbol{\sigma}}\}_{\text{all } \boldsymbol{\sigma}}$.

Tracing

For each user j and each segment i independently, the content distributor computes a score $S_j^{(i)}$,

$$S_j^{(i)} = \begin{cases} \text{If } X_{ji} = y_i: & g_1(p_{y_i}) \\ \text{If } X_{ji} \neq y_i: & g_0(p_{y_i}) \end{cases} \tag{5}$$

where

$$g_1(p) = \sqrt{\frac{1-p}{p}} \quad ; \quad g_0(p) = -\sqrt{\frac{p}{1-p}}. \tag{6}$$

The choice (6) of g_0, g_1 is the unique combination of functions that satisfies

$$p g_1(p) + (1-p) g_0(p) = 0 \quad ; \quad p[g_1(p)]^2 + (1-p)[g_0(p)]^2 = 1. \tag{7}$$

This choice has been shown to be 'optimal' for the binary alphabet [9,27], in the sense that, in a certain class of continuous functions, it is the unique choice that minimizes the lower bound on the code length when Tardos' bias distribution function is used in combination with a Markov-inequality-based proof technique. Even though there is no such optimality proof for $q \geq 3$, the properties (7) make the scheme easy to analyze, which was the main motivation for using the score functions (6) in the non-binary case.
The scores per segment are added up to form an overall score S_j for each user,

$$S_j = \sum_{i=1}^{m} S_j^{(i)}. \tag{8}$$

If S_j exceeds a threshold value Z, user j is considered suspicious ('accused'). The list of accused users is denoted as $\mathcal{L}$,

$$\mathcal{L} = \{j : S_j > Z\}. \tag{9}$$

2.2 Measuring the performance

We define the coalition's score as

$$S_{\mathcal{C}} = \sum_{i=1}^{m} S_{\mathcal{C}}^{(i)} \quad ; \quad S_{\mathcal{C}}^{(i)} = \sum_{j\in\mathcal{C}} S_j^{(i)}. \tag{10}$$

Two kinds of error are usually considered: False Positives (FP, accusing an innocent user) and False Negatives (FN, not catching any guilty ones). The corresponding error probabilities are defined as

$$\begin{aligned} P_{\rm FP} &= \mathbb{P}[j \in \mathcal{L}] \text{ for some fixed innocent } j \\ P_{\rm FN} &= \mathbb{P}[\mathcal{L}\cap\mathcal{C} = \emptyset]. \end{aligned} \tag{11}$$

The distributor has the requirement $P_{\rm FP} \leq \varepsilon_1$, $P_{\rm FN} \leq \varepsilon_2$. Typically $\varepsilon_1 < \varepsilon_2$, since accusing innocents is usually more damaging to the tracing system than not catching anyone. The $P_{\rm FP}$ and $P_{\rm FN}$ depend on the following parameters: the alphabet size q; the code length m; the threshold Z; the concentration parameter κ; the cutoff parameter τ; the number of attackers c, unknown to the distributor; the colluder strategy θ, also unknown to the distributor.
Let c_0 denote the coalition size that the code can resist. An often used performance indicator is $m^*(\varepsilon_1, \varepsilon_2, c_0)$, defined as the shortest achievable m as a function of ε_1, ε_2 and c_0. (The dependence on q, κ, τ is not written explicitly.) It is useful to write m^* and the corresponding Z^* as

$$m^* = Ac_0^2 \ln \varepsilon_1^{-1} \quad ; \quad Z^* = Bc_0 \ln \varepsilon_1^{-1}. \tag{12}$$

For finite c_0 the A, B are functions that (weakly) depend on ε_1, ε_2 and c_0. In [25] it was found[6] that asymptotically for $c_0 \to \infty$, the A, B can be expressed in terms of one statistical parameter M,

$$\tilde{\mu} = \frac{1}{m}\mathbb{E}[S_{\mathcal{C}}] = \mathbb{E}[S_{\mathcal{C}}^{(i)}] \tag{13}$$

$$M = \min_{\theta} \tilde{\mu} \quad \text{ for } c = c_0, \tag{14}$$

where the i in $S_{\mathcal{C}}^{(i)}$ is arbitrary. The $\mathbb{E}$ denotes the expectation value (see Section 4) over all stochastic degrees of freedom ($\boldsymbol{p}$, X, y), and θ is the colluder strategy. Note that, for some attack strategies, $\tilde{\mu}$ is a decreasing function of c. (This follows from the fact that adding extra attackers makes the attack more powerful; they can choose to output symbols that will give many attackers a negative score.) Hence for $c \leq c_0$ it holds that $\tilde{\mu} \geq M$. Note that a very bad choice of κ can sometimes lead to $M < 0$ [22]. We will not consider such pathological cases, and always have $M > 0$. The asymptotic values for A and B are

$$A_{\rm asympt} = \frac{2}{M^2} \quad ; \quad B_{\rm asympt} = \frac{2}{M}. \tag{15}$$

For $1 \ll c_0 < \infty$ the M contains a weak dependence on c_0. For $q = 2$, $\kappa = \frac{1}{2}$ it holds that $M = \frac{2}{\pi} - \mathcal{O}(c_0 t)$ (see [24] and Theorem 4). Here $\mathcal{O}()$ denotes Landau O notation. We will use the notation M_0 for M at $\tau = 0$, and $M_0^\infty = \lim_{c_0\to\infty} M_0$.
A second statistical parameter that plays a role is the variance of the scores of guilty users,

$$\tilde{\sigma}^2 = \frac{1}{m}{\rm Var}(S_{\mathcal{C}}) = {\rm Var}(S_{\mathcal{C}}^{(i)}) = \mathbb{E}[(S_{\mathcal{C}}^{(i)})^2] - \tilde{\mu}^2 \tag{16}$$

$$V^2 = \max_{\theta, c\leq c_0} \frac{\tilde{\sigma}^2}{c}. \tag{17}$$

Again, the i is arbitrary. The $\tilde{\sigma}$ is a function of c and the attack strategy, while V is a function of c_0. For all $c \leq c_0$ it holds that $\tilde{\sigma}^2/c \leq V^2$. The parameter V appears in the non-asymptotic properties of the scheme.

[6] In fact the expression $\ln \varepsilon_1^{-1}$ should be replaced by $[{\rm Erfc}^{\rm inv}(2\varepsilon_1)]^2$, which is smaller. E.g. for $\varepsilon_1 = 10^{-10}$ the difference is 12%; for $\varepsilon_1 = 10^{-7}$ it is 16%.

Lemma 1 (Lemma 4 in [25]) *It holds that $\tilde{\mu}^2 + \tilde{\sigma}^2 \leq qc$. This gives upper bounds*

$$M \leq \sqrt{qc_0} \quad \text{and} \quad V^2 \leq q. \tag{18}$$

The proof of Lemma 1 is given in Section 4.2.

2.3 The inequalities of Bernstein and Bennett

We list Bernstein's and Bennett's inequalities, and derive a slightly weakened form of Bennett's inequality. We will use these instead of the Markov inequality which has been employed in previous security proofs of the Tardos scheme. (Note, however, that the Bernstein and Bennett inequalities are typically proven by invoking the Markov inequality.)

Lemma 2 (Bernstein's inequality [3]) *Let $U_1, \cdots, U_m$ be independent zero-mean random variables, with $|U_i| \leq a$ for all i. Let $Z \geq 0$. Then*

$$\mathbb{P}\left[\sum_i U_i > Z\right] \leq \exp\left(-\frac{Z^2/2}{\sum_i \mathbb{E}[U_i^2] + aZ/3}\right).$$

Lemma 3 (Bennett's inequality [2]) *Let $Y_1, \cdots, Y_m$ be independent zero-mean random variables, with $|Y_i| \leq b$ for all i. Let $s^2 = \frac{1}{m}\sum_i \mathbb{E}[Y_i^2]$. Let h be defined as*

$$h(v) = \int_0^v \mathrm{d}x \;\ln(1+x) = (v+1)\ln(v+1) - v. \tag{19}$$

Let $T \geq 0$. Then

$$\mathbb{P}\left[\sum_i Y_i > T\right] \leq \exp\left(-\frac{ms^2}{b^2} h(\frac{b}{ms^2}T)\right).$$

Property 1 For $v > 0$ the fraction $h(v)/v$ is an increasing function of v.

Proof: $\frac{\mathrm{d}}{\mathrm{d}v}\frac{h(v)}{v} = \frac{1}{v^2}(v - \ln[1+v])$, which is positive for $v > 0$. □

Property 2 The function h in Lemma 3 can be lower bounded as

$$v > 0 \implies h(v) > v \ln \frac{v}{e}.$$

Proof: For $v > 0$ we have $h(v) = \int_0^v \mathrm{d}x \;\ln(1+x) > \int_0^v \mathrm{d}x \;\ln x = v \ln \frac{v}{e}$. □

3 Requirements on the code length and threshold

Using Bernstein's and Bennett's inequalities, we derive upper bounds on the FP and FN error probabilities. These are then rewritten as conditions on the code length parameter A and the threshold parameter B, such that $P_{\mathrm{FP}} \leq \varepsilon_1$ and $P_{\mathrm{FN}} \leq \varepsilon_2$ hold. From these conditions we immediately derive the asymptotic behaviour of the code length parameter A for given q, c_0, τ and M.

3.1 Bernstein's inequality applied to the False Positive

Theorem 1 *Let $q \geq 2$. Let the coalition use any attack strategy. The False Positive probability of the q-ary Tardos system, as defined by (11), can be upper bounded as*

$$P_{\rm FP} \leq \exp\left[(\ln \varepsilon_1)\frac{B^2}{2A}\left(1+\frac{B}{3A}\frac{1}{c_0\sqrt{\tau}}\right)^{-1}\right].$$

Proof: For *any* coalition strategy, even one that breaks the segment symmetry, the one-segment scores for an innocent user are independent [24]. Hence we are allowed to use Bernstein's inequality. In Lemma 2 we set $U_i = S_j^{(i)}$ for some innocent user j. This is allowed since $S_j^{(i)}$ has zero expectation value due to the first property in (7). We recall that g_1 and g_0 are decreasing functions. We then have

$$|U_i| \leq \max\{g_1(p_{\rm min}), -g_0(p_{\rm max})\} = g_1(p_{\rm min}) < \frac{1}{\sqrt{p_{\rm min}}} = \frac{1}{\sqrt{\tau}}. \tag{20}$$

Thus we are allowed to set $a = 1/\sqrt{\tau}$. Furthermore, we note that $\mathbb{E}[U_i^2] = 1$ for all i due to the second property in (7). Lemma 2 then gives

$$P_{\rm FP} \leq \exp\left(-\frac{Z^2/2}{m+aZ/3}\right) = \exp\left(-\frac{Z^2}{2m}\cdot\frac{1}{1+aZ/(3m)}\right). \tag{21}$$

Finally substituting $a = 1/\sqrt{\tau}$ and the expressions (12) for m and Z finishes the proof. □
Note: The bound in Theorem 1 does not depend on c (the actual number of attackers), but on the scheme parameter c_0.

Corollary 1 *Theorem 1 allows us to express the requirement $P_{\rm FP} \leq \varepsilon_1$ as a closed-form relation between A and B,*

$$A \leq \frac{B^2}{2} - \frac{1}{c_0\sqrt{\tau}}\frac{B}{3} \implies P_{\rm FP} \leq \varepsilon_1. \tag{22}$$

3.2 Bennett's inequality applied to the False Negative

Theorem 2 *Let $q \geq 3$. Let the coalition employ a segment-symmetric strategy. Let $\tilde{\mu}Ac_0 - Bc > 0$. Let τ be small enough for the following inequality to hold,*

$$\sqrt{\tau} \leq \frac{c}{\tilde{\mu}}(1-\frac{1}{\sqrt{q-1}}). \tag{23}$$

Then the False Negative probability of the q-ary Tardos system, as defined by (11), can be bounded as

$$P_{\rm FN} < \exp\left[\ln \varepsilon_1 \frac{c_0^2\tau A\tilde{\sigma}^2}{c^2}\, h\left(\frac{c}{\tilde{\sigma}^2\sqrt{\tau}}[\tilde{\mu} - \frac{Bc}{Ac_0}]\right)\right]. \tag{24}$$

Proof: We start from $P_{\rm FN} = \mathbb{P}[\mathcal{C}\cap\mathcal{L} = \emptyset] = \mathbb{P}[S_j < Z \text{ for all } j \in \mathcal{C}] < \mathbb{P}[S_\mathcal{C} < cZ] = \mathbb{P}[m\tilde{\mu} - S_\mathcal{C} > m\tilde{\mu} - cZ]$. Due to the segment-symmetry of the attack, the scores in all the segments are independent, which allows us to use Bennett's inequality. We apply Lemma 3 with the following parameters. We set $Y_i = \tilde{\mu} - S_\mathcal{C}^{(i)}$ so that $\mathbb{E}[Y_i] = 0$. We have $\sum_i Y_i = m\tilde{\mu} - S_\mathcal{C}$. We take $T = m\tilde{\mu} - cZ$. As a result we can now write $P_{\rm FN} < \mathbb{P}[\sum_i Y_i > T]$. The condition $\tilde{\mu}Ac_0 - Bc > 0$ ensures that $T > 0$. Next, we have $s^2 = \frac{1}{m}\sum_i \mathbb{E}[Y_i^2] = \frac{1}{m}\sum_i \tilde{\sigma}^2 = \tilde{\sigma}^2$, with $\tilde{\sigma}^2$ as defined in (16). We have

$$\begin{aligned}|Y_i| = |S_\mathcal{C}^{(i)} - \tilde{\mu}| &\leq \max\{cg_1(p_{\rm min}) - \tilde{\mu}, \tilde{\mu} - cg_0(p_{\rm max})\}\\ &= \max\{\frac{c}{\sqrt{\tau}}\sqrt{1-\tau} - \tilde{\mu}, \frac{c}{\sqrt{\tau}}\frac{\sqrt{1-\tau(q-1)}}{\sqrt{q-1}} + \tilde{\mu}\}\\ &< \max\{\frac{c}{\sqrt{\tau}}, \frac{c}{\sqrt{\tau}}\frac{1}{\sqrt{q-1}} + \tilde{\mu}\}.\end{aligned} \tag{25}$$

The condition (23) makes sure that the second argument of the max cannot exceed the first argument. Hence $|Y_i| < c/\sqrt{\tau}$, and we can set $b = c/\sqrt{\tau}$. Finally, substituting these values of T, s^2, b into Lemma 3 and using the parametrization (12) for m and Z in terms of A and B gives the end result. □

Remark 1: We could have chosen b more tightly, e.g. $c/\sqrt{\tau} - M$. However, for typical values of c, $\tilde{\mu}$ and τ the gain would have been less than 1%, and we felt that it was not worth the effort, given the more complicated equations that would result.

Remark 2: The condition (23) does not cause any trouble. Since $c \geq 2$ in coalition attacks, $\tilde{\mu}$ is of order 1, and τ is always set to be very small, (23) is automatically satisfied in practice.

Note that the error bound (24) depends on c_0, c and the attack strategy θ. We get rid of the dependence on c and θ as follows.

Corollary 2 *Let $q \geq 3$ and $2 \leq c \leq c_0$. Let $MA - B > 0$. Let $\sqrt{\tau} \leq \sqrt{\frac{2}{q}}(1 - \frac{1}{\sqrt{q-1}})$. Then the False Negative probability of the q-ary Tardos system, as defined by (11), can be upper bounded as*

$$P_{\rm FN} < \exp\left[\ln \varepsilon_1 \; c_0 \tau A V^2 \; h\left(\frac{M - B/A}{V^2\sqrt{\tau}}\right)\right]. \tag{26}$$

Proof: The conditions $MA - B > 0$ and $c \leq c_0$ imply $\tilde{\mu}Ac_0 - Bc > 0$. Furthermore, we make use of Lemma 1 to bound $\tilde{\mu} < \sqrt{qc}$. Thus, if $\sqrt{\tau} \leq \sqrt{\frac{c}{q}}(1 - \frac{1}{\sqrt{q-1}})$ holds then the condition (23) in Theorem 2 holds. Hence Theorem 2 applies. We use $\tilde{\sigma}^2/c \leq V^2$ (see Section 2.2) in combination with Property 1 in order to replace $\tilde{\sigma}^2/c$ by V^2 in (24). Then we use $c \leq c_0$ and $\tilde{\mu} \geq M$ in combination with the fact that h is an increasing function in order to replace c by c_0 and $\tilde{\mu}$ by M. □

Corollary 2 allows us to formulate a condition on the system parameters (independent of c and θ) such that the FN probability is sufficiently small.

Corollary 3 *Let $q \geq 3$ and $2 \leq c \leq c_0$. Let $MA - B > 0$. Let $\sqrt{\tau} \leq \sqrt{\frac{2}{q}}(1 - \frac{1}{\sqrt{q-1}})$. Then*

$$c_0 \tau A V^2 \; h\left(\frac{M - B/A}{V^2\sqrt{\tau}}\right) \geq \frac{\ln \varepsilon_2}{\ln \varepsilon_1} \qquad \Longrightarrow \qquad P_{\rm FN} < \varepsilon_2. \tag{27}$$

Proof: Follows directly from Corollary 2. □

Corollary 4 *Let $q \geq 3$ and $2 \leq c \leq c_0$. Let $MA - B > 0$. Let $\sqrt{\tau} \leq \sqrt{\frac{2}{q}}(1 - \frac{1}{\sqrt{q-1}})$. Then*

$$(MA - B)c_0\sqrt{\tau} \; \ln \frac{M - B/A}{eV^2\sqrt{\tau}} \geq \frac{\ln \varepsilon_2}{\ln \varepsilon_1} \qquad \Longrightarrow \qquad P_{\rm FN} < \varepsilon_2. \tag{28}$$

Proof: Follows directly from Corollary 3 and Property 2. □

Corollary 4 is a less tight version of Corollary 3. When the argument of the h function is large (which we will see is the case), the tightness lost in the approximation of $h(v)$ is of relative order $\mathcal{O}(1/v)$, which will turn out to be too small to care about.

For $q = 2$ the above analysis cannot be repeated exactly; a complication arises because condition (23) cannot be satisfied. We get the following, less tight, result.

Theorem 3 *Let $q = 2$. Let $\tilde{\mu}Ac_0 - Bc > 0$. Then the False Negative probability, as defined by (11), can be bounded as*

$$P_{\rm FN} < \exp\left[\ln \varepsilon_1 \frac{c_0^2 \tau A \tilde{\sigma}^2}{c^2(1 + \tilde{\mu}\sqrt{\tau}/c)} \; h\left(\frac{c}{\tilde{\sigma}^2\sqrt{\tau}}[\tilde{\mu} - \frac{Bc}{Ac_0}]\right)\right]. \tag{29}$$

Proof: Follows the same steps as the proof of Theorem 2, with the difference that we have to set $b = c/\sqrt{\tau} + \tilde{\mu}$. Using Property 1 we have, for any $x > 0$, that $b^{-2}h(bx) > (\tau/c^2)(1 + \tilde{\mu}\sqrt{\tau}/c)^{-1}h(\frac{c}{\sqrt{\tau}}x)$, which results in (29). □

From Theorem 3 we can derive corollaries as for $q \geq 3$, but now taking into account the extra factor $1 + \tilde{\mu}\sqrt{\tau}/c$ in the exponent.

Corollary 5 *Let $q = 2$ and $c \le c_0$. Let $MA - B > 0$. Then*

$$(MA - B)\frac{c_0\sqrt{\tau}}{1+\sqrt{2\tau/c_0}}\ \ln\frac{M - B/A}{eV^2\sqrt{\tau}} \ge \frac{\ln\varepsilon_2}{\ln\varepsilon_1} \quad\implies\quad P_{\rm FN} < \varepsilon_2. \tag{30}$$

Proof: Follows the same steps as the proofs of Corollaries 2–4, but with the extra factor $1 + \tilde{\mu}\sqrt{\tau}/c$. We use $\tilde{\mu} < \sqrt{2c}$ (Lemma 1) and $c \le c_0$ to write $c^2 + c\tilde{\mu}\sqrt{\tau} < c_0^2 + c_0^{3/2}\sqrt{2\tau} = c_0^2(1 + \sqrt{2\tau/c_0})$. □
Remark: The difference between the case $q = 2$ and $q \ge 3$ can be seen as an extra factor $1 + \sqrt{2\tau/c_0}$ that slightly modifies the parameter $\eta = \ln\varepsilon_2/\ln\varepsilon_1$ to $\eta(1 + \sqrt{2\tau/c_0})$. We will see in Section 6 that the exact value of η has little effect on the code length parameter A.

3.3 General remarks on optimization and asymptotics

Corollaries 1 and 3 together allow us to draw some conclusions about the optimization of the code length parameter A for given q, c_0, ε_1, ε_2 even before looking at M and V in detail. Note that Corollaries 1 and 3 give upper bounds on the error probabilities. Hence any code lengths derived from these corollaries will be pessimistic; shorter codes will also suffice, but we do not know how much shorter. To explicitly distinguish between the 'really' smallest achievable A and the A for which we can prove that it is still sufficient (given the proof technique above), we introduce the notation $A_{\rm suff}$.

- Corollary 1 and the condition $MA - B > 0$ define an interval in which A must lie as a function of B,

$$A_{\rm suff} \in (\frac{B}{M}, \frac{B^2}{2} - \frac{B}{3c_0\sqrt{\tau}}]. \tag{31}$$

  The interval exists only if

$$B > \frac{2}{M} + \frac{2}{3c_0\sqrt{\tau}}. \tag{32}$$

- From the argument above we get a lower bound

$$A_{\rm suff} > \frac{2}{M^2} + \frac{2}{3Mc_0\sqrt{\tau}}, \tag{33}$$

  which for $c_0 \to \infty$ corresponds to the asymptotic value known from the Gaussian approximation *iff* $c_0\sqrt{\tau} \to \infty$. We conclude that, asymptotically, τ has to depend on c_0 in such a way that $c_0\sqrt{\tau} \to \infty$. On other grounds [24] we know that $c_0\tau \ll 1$. (Otherwise small correction terms for the code length, of order $c_0\tau$, are not small.) Hence, if we assume an asymptotic power law of the form

$$\tau \sim c_0^{-\nu}, \tag{34}$$

  then the parameter ν has to lie in the interval $\nu \in (1, 2)$.
- We consider optimization in the asymptotic case. The $A_{\rm suff}$ is minimized by reducing B as far as possible while still satisfying (27); hence we want to achieve the equality in (27). The function h for large arguments behaves as $h(v) \to v\ln v$. Let us use the notation $M - B/A_{\rm suff} = M\alpha$, where α scales as a function of c_0 such that $\alpha \to 0$ and $\alpha/\sqrt{\tau} \to \infty$. The left hand side of the inequality in (27) has leading order contribution $\alpha(2/M)c_0\sqrt{\tau}\ln(\alpha/\sqrt{\tau})$ which has to go to a constant, $\eta = \ln\varepsilon_2/\ln\varepsilon_1$. By approximately solving the equation $\alpha = M\eta/(2c_0\sqrt{\tau}\ln\frac{\alpha}{\sqrt{\tau}})$ we find that α has to behave as follows,

$$1 - \frac{B}{MA_{\rm suff}} = \alpha = \frac{M}{2}\frac{\eta}{c_0\sqrt{\tau}\ln\frac{1}{c_0\tau}} + \text{ higher order}. \tag{35}$$

We set B very close to the lower bound (32), namely $B = \frac{2}{M} + \frac{2}{3c_0\sqrt{\tau}} + \frac{2}{M}\beta$ with $\beta \ll 1$. From the definition of α it follows that we can write $A_{\rm suff} = \frac{B/M}{1-\alpha}$. This gives

$$A_{\rm suff} = \frac{2}{M^2}[1 + \frac{M}{3c_0\sqrt{\tau}} + \beta + \cdots][1 + \alpha + \cdots] \quad \text{with } \beta > \alpha. \tag{36}$$

The factor $[1 + \alpha + \cdots]$ is the Taylor expansion of $1/(1 - \alpha)$. The requirement $\beta > \alpha$ comes from the fact that the upper boundary in (31) has to be larger than the lower boundary. Finally, putting $\beta = \alpha +$ higher order and substituting (35) into (36) gives

$$A_{\rm suff} = \frac{2}{M^2}\left[1 + \frac{M}{3c_0\sqrt{\tau}}(1 + \frac{3\eta}{\ln 1/c_0\tau}) + \text{ higher order}\right]. \tag{37}$$

(The above reasoning applies to $q = 2$ as well. As we saw in Corollary 5, for $q = 2$ the η effectively changes to $\eta(1+\sqrt{2\tau/c_0})$; the correction $\eta\sqrt{2\tau/c_0}$ gets absorbed into the 'higher order'.) Thus, with relatively little effort compared to previous literature, we obtain the asymptotic form (37) including the logarithmic correction term.

Finding the optimal choice for τ requires knowledge of M as a function of τ. It turns out to be surprisingly difficult to determine what $M(\tau)$ looks like, even for $\tau \ll 1/q$. Section 4 is almost completely devoted to this question. In Sections 5 and 6 we address the optimization of $A_{\rm suff}$.

4 Statistical properties of the accusation scores

4.1 Expectation values

The expectation value over all stochastic degrees of freedom $(\boldsymbol{p}, X, y)$ is denoted as $\mathbb{E}$. For quantities that refer to a single segment and (symmetrically) depend on the attackers' symbols without depending on the codewords of innocent users, i.e. for functions of $\boldsymbol{\sigma}$, the $\mathbb{E}$ can be split up as

$$\mathbb{E}[\cdots] = \mathbb{E}_{\boldsymbol{p}}\mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}}\mathbb{E}_{y|\boldsymbol{\sigma}}[\cdots]. \tag{38}$$

We treat the '$\mathbb{E}$' notation as a linear operator acting to the right. The splitup (38) is natural, since chronologically the first step is to generate $\boldsymbol{p}$; then X is generated for given $\boldsymbol{p}$, leading to counters $\boldsymbol{\sigma}$; finally the (possibly probabilistic) colluder strategy for choosing y depends only on $\boldsymbol{\sigma}$. The three separate expectation values are defined as

$$\mathbb{E}_{\boldsymbol{p}}[\cdots] = \int_{\tau}^{1-t} \mathrm{d}^q p\ \delta(1 - \sum_{\alpha\in\mathcal{Q}} p_\alpha)F(\boldsymbol{p})[\cdots] \tag{39}$$

with F given in (3), and

$$\mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}}[\cdots] = \sum_{\boldsymbol{\sigma}} \binom{c}{\boldsymbol{\sigma}} \boldsymbol{p}^{\boldsymbol{\sigma}}[\cdots] \quad ; \quad \mathbb{E}_{y|\boldsymbol{\sigma}}[\cdots] = \sum_{y\in\mathcal{Q}} \theta_{y|\boldsymbol{\sigma}}[\cdots]. \tag{40}$$

The notation $\boldsymbol{p}^{\boldsymbol{\sigma}}$ stands for $\prod_{\alpha\in\mathcal{Q}} p_\alpha^{\sigma_\alpha}$. In the $\sum_{\boldsymbol{\sigma}}$ summation in (40), it is implicit in the notation that the sum runs only over vectors $\boldsymbol{\sigma}$ that satisfy $\sum_\alpha \sigma_\alpha = c$. The notation $\binom{c}{\boldsymbol{\sigma}}$ stands for the multinomial coefficient $c!/\prod_\alpha(\sigma_\alpha!)$.

We also consider an expectation over $\boldsymbol{\sigma}$ that is *not* conditioned on $\boldsymbol{p}$. For $\tau = 0$ we define $\mathbb{E}^{(0)}_{\boldsymbol{\sigma}}$ as

$$\mathbb{E}^{(0)}_{\boldsymbol{\sigma}}[\cdots] = \sum_{\boldsymbol{\sigma}} \binom{c}{\boldsymbol{\sigma}} \frac{B(\kappa\mathbf{1}_q + \boldsymbol{\sigma})}{B(\kappa\mathbf{1}_q)}[\cdots]. \tag{41}$$

For $\tau = 0$, the integrals over $\boldsymbol{p}$ typically yield Gamma functions and Beta functions. We will occasionally use the following asymptotic properties.

Lemma 4 *For $x \to \infty$ and a, b independent of x with $a, b \ll x$, it holds that*

$$\frac{\Gamma(x+a)}{\Gamma(x+b)} = x^{a-b}[1 + \mathcal{O}(\frac{1}{x})]. \tag{42}$$

Proof: Follows directly from Stirling's approximation $\Gamma(1+x) \approx \sqrt{2\pi x}(x/e)^x$. □

Lemma 5 *For $\lambda \in (0,1)$, $x \to \infty$ and a, b independent of x with $a, b \ll x$ it holds that*

$$B(\lambda x + a, (1-\lambda)x + b) = \frac{\sqrt{2\pi}}{\sqrt{x}} \frac{\lambda^a (1-\lambda)^b}{\sqrt{\lambda(1-\lambda)}} e^{-xE(\lambda)}[1 + \mathcal{O}(\frac{1}{x})], \tag{43}$$

where E denotes the binary entropy function $E(\lambda) = -\lambda \ln \lambda - (1-\lambda)\ln(1-\lambda)$.

Proof: Follows from the definition of the Beta function, $B(x,y) = \Gamma(x)\Gamma(y)/\Gamma(x+y)$, and Stirling's approximation of the Gamma function. □

Lemma 6 *Let w denote the total false positive probability, $w = \mathbb{P}[\mathcal{L} \setminus \mathcal{C} \neq \emptyset]$. Let $m \gg 1$ and $(n-c)P_{\rm FP} \ll 1$. Then*

$$w = (n-c)P_{\rm FP} - \mathcal{O}((n-c)^2 P_{\rm FP}^2). \tag{44}$$

Proof sketch: Let $\alpha_{\bar{\boldsymbol{p}}y}$ denote the probability, for given $\bar{\boldsymbol{p}} = \{\boldsymbol{p}^{(i)}\}_{i=1}^m$ and $y = \{y_i\}_{i=1}^m$, that the score of a fixed innocent user j exceeds the threshold Z. We have $P_{\rm FP} = \mathbb{E}_{\bar{\boldsymbol{p}}y}\alpha_{\bar{\boldsymbol{p}}y}$. Due to the properties (7) the score S_j can be seen as the result of a random walk with steps $S_j^{(i)}$ that have zero mean and variance 1. For large m the statistics of the random walk becomes practically independent of $\bar{\boldsymbol{p}}$ and y, due to the central limit theorem. The threshold Z is fixed in such a way that $\alpha_{\bar{\boldsymbol{p}}y}$ is of order $P_{\rm FP}$ independent of $\bar{\boldsymbol{p}}$ and y. We have

$$1 - w = \mathbb{E}_{\bar{\boldsymbol{p}}y}[(1-\alpha_{\bar{\boldsymbol{p}}y})^{n-c}] = \mathbb{E}_{\bar{\boldsymbol{p}}y}\sum_{k=0}^{n-c}\binom{n-c}{k}(-\alpha_{\bar{\boldsymbol{p}}y})^k, \tag{45}$$

which can be rewritten as

$$w = (n-c)P_{\rm FP} - \sum_{k=2}^{n-c}\binom{n-c}{k}\mathbb{E}_{\bar{\boldsymbol{p}}y}(-\alpha_{\bar{\boldsymbol{p}}y})^k. \tag{46}$$

Since $\alpha_{\bar{\boldsymbol{p}}y} = \mathcal{O}(P_{\rm FP})$ with overwhelming probability, and $(n-c)P_{\rm FP} \ll 1$, each term in the sum in (46) is of a different order of magnitude: the k'th term is of order $[(n-c)P_{\rm FP}]^k$. Eq. (44) follows. □

4.2 Statistics of the guilty accusation scores

The parameters $\tilde{\mu}$ and M, defined in (13,14), as well as $\tilde{\sigma}^2$ and V^2, defined in (16,17), play an important role in the next sections. An upper bound was mentioned in Lemma 1, for which we present the proof here.

Proof of Lemma 1: The single-segment coalition score $S_{\mathcal{C}}^{(i)}$ is $\sigma_y g_1(p_y) + (c - \sigma_y) g_0(p_y)$ which can be rewritten as $\frac{\sigma_y - cp_y}{\sqrt{p_y(1-p_y)}}$. We have $\tilde{\mu}^2 + \tilde{\sigma}^2 = \mathbb{E}[\{S_{\mathcal{C}}^{(i)}\}^2]$, which can be written as

$$\tilde{\mu}^2 + \tilde{\sigma}^2 = \sum_{y \in \mathcal{Q}} \mathbb{E}_{\boldsymbol{p}}\mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}}\theta_{y|\boldsymbol{\sigma}} \frac{(\sigma_y - cp_y)^2}{p_y(1-p_y)}. \tag{47}$$

We use the rather crude bound $\theta_{y|\boldsymbol{\sigma}} \leq 1$ (which holds because probabilities cannot be larger than 1) and then apply the fact that $\mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}}(\sigma_y - cp_y)^2$ is the variance of the binomial-distributed variable σ_y, given by $cp_y(1-p_y)$. The expectation over $\boldsymbol{p}$ becomes trivial, and the sum over y yields a factor q. That proves $\tilde{\mu}^2 + \tilde{\sigma}^2 \leq qc$. Next, $M = \min_\theta \tilde{\mu}|_{c=c_0} \leq \sqrt{qc_0 - \tilde{\sigma}^2} \leq \sqrt{qc_0}$. Finally, $V^2 = \max_{\theta, c \leq c_0} \tilde{\sigma}^2/c \leq \max_{\theta, c\leq c_0}(q - \tilde{\mu}^2/c) = q - M^2/c_0 \leq q$. □

Lemma 7 *The parameter M as defined in (14) can be expressed as*

$$M = \sum_{\boldsymbol{\sigma}} \binom{c_0}{\boldsymbol{\sigma}} \min_{y\colon\, \sigma_y \geq 1} \mathbb{E}_{\boldsymbol{p}} \left[\boldsymbol{p}^{\boldsymbol{\sigma}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}} \right]. \tag{48}$$

<u>*Proof:*</u> The expectation value $\tilde{\mu} = \mathbb{E}[S_{\mathcal{C}}^{(i)}]$ for $c = c_0$ is given by

$$\tilde{\mu}|_{c=c_0} = \mathbb{E}_{\boldsymbol{p}} \mathbb{E}_{\boldsymbol{\sigma}|\boldsymbol{p}} \mathbb{E}_{y|\boldsymbol{\sigma}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}} = \sum_{\boldsymbol{\sigma}} \binom{c_0}{\boldsymbol{\sigma}} \mathbb{E}_{y|\boldsymbol{\sigma}} \mathbb{E}_{\boldsymbol{p}} \left[\boldsymbol{p}^{\boldsymbol{\sigma}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}} \right]. \tag{49}$$

The minimum over θ is achieved when the strategy picks $y \in \mathcal{Q}$ such that, for a given $\boldsymbol{\sigma}$, the lowest possible value of $\mathbb{E}_{\boldsymbol{p}}[\cdots]$ is selected. Due to the Marking Assumption there is the constraint that y cannot be chosen when $\sigma_y = 0$. □

Lemma 7 has a large overlap with [25], but the notation differs and here we make a clearer distinction between c and c_0. The summation in (48) contains a large number of terms ($\propto c_0^{q-1}$). Since the argument of the 'min' depends only on the numbers $\{\sigma_\alpha\}_{\alpha\in\mathcal{Q}}$, and not on their location in the vector $\boldsymbol{\sigma}$, the $\boldsymbol{\sigma}$-summation can be replaced by a sum over partitions, which contains fewer terms.

Lemma 8 *Let $\mathcal{P}_q^c$ denote the set of (ordered) partitions of the integer c into exactly q nonnegative integers (i.e. allowing zeroes). For $\boldsymbol{a} \in \mathcal{P}_q^c$ let $R(\boldsymbol{a})$ be a tuple containing the frequencies of the numbers appearing in $\boldsymbol{a}$. For $y \in \{1, \cdots, q\}$ let a_y denote the y'th entry in $\boldsymbol{a}$. Then M can be written as*

$$M = \sum_{\boldsymbol{a}\in\mathcal{P}_q^{c_0}} \binom{c_0}{\boldsymbol{a}} \binom{q}{R(\boldsymbol{a})} \min_{y\in\{1,\ldots,q\}\colon\, a_y\geq 1} \mathbb{E}_{\boldsymbol{p}} \left[\boldsymbol{p}^{\boldsymbol{a}} \frac{a_y - c_0 p_y}{\sqrt{p_y(1-p_y)}} \right]. \tag{50}$$

<u>*Proof:*</u> We start from (48). A permutation of $\boldsymbol{\sigma}$ will not affect the outcome of $\min_y \mathbb{E}_{\boldsymbol{p}}[\cdots]$, due to the permutation symmetry of $F(\boldsymbol{p})$. The $\boldsymbol{a} \in \mathcal{P}_q^{c_0}$ is an ordered version of $\boldsymbol{\sigma}$, e.g. in decreasing order of σ_α values. Hence $\binom{c_0}{\boldsymbol{a}} = \binom{c_0}{\boldsymbol{\sigma}}$. The multinomial factor $\binom{q}{R(\boldsymbol{a})}$ counts how many different $\boldsymbol{\sigma}$-vectors can be constructed by permuting $\boldsymbol{a}$. The total number of permutations of q elements is $q!$. Re-occurrence of some integer in $\boldsymbol{a}$, say f-fold, reduces the number of permutations by $f!$. □

Example 1 For $c_0 = 5, q = 3$, the partitions are $(5,0,0)$, $(4,1,0)$, $(3,2,0)$, $(3,1,1)$, $(2,2,1)$, with $R((5,0,0)) = (1,2)$, $R((4,1,0)) = (1,1,1)$, $R((3,2,0)) = (1,1,1)$, $R((3,1,1)) = (1,2)$, and $R((2,2,1)) = (2,1)$.

For ($c_0 \gg 1$, $q = \mathcal{O}(1)$), it is known [14] that the number of terms in the $\sum_{\boldsymbol{a}}$ summation, i.e. the number of partitions of c_0 into at most q parts, scales as $\frac{c_0^{q-1}}{q!(q-1)!}$. For comparison: direct summation over $\boldsymbol{\sigma}$ consists of $\approx c_0^{q-1}/(q-1)!$ terms (the volume of a $(q-1)$-dimensional simplex). Hence the speedup in Lemma 8 is approximately a factor $q!$.

Next we list a number of results about the behaviour of M.

Lemma 9 *It holds that*

$$M_0 = \mathbb{E}_{\boldsymbol{\sigma}}^{(0)} \min_{y\colon\, \sigma_y\geq 1} W(\sigma_y) \tag{51}$$

$$W(\sigma_y) = c_0\{\tfrac{1}{2} - \kappa + \frac{\sigma_y}{c_0}(\kappa q - 1)\} \frac{\Gamma(\kappa + \sigma_y - \frac{1}{2})\Gamma(\kappa[q-1] + c_0 - \sigma_y - \frac{1}{2})}{\Gamma(\kappa + \sigma_y)\Gamma(\kappa[q-1] + c_0 - \sigma_y)}.$$

For $c_0 \to \infty$ the function W behaves as

$$W(c_0 x) \to \frac{\frac{1}{2} - \kappa + x(\kappa q - 1)}{\sqrt{x(1-x)}}. \tag{52}$$

Proof: It has been shown (Eq.12 in [22]) that for $\tau = 0$ we have $\tilde{\mu} = \mathbb{E}_{\boldsymbol{\sigma}}^{(0)} \sum_y \theta_{y|\boldsymbol{\sigma}} W(\sigma_y)$. Equation (51) immediately follows. The asymptotic result (52) was derived in section 3.2 of [22]. □

Lemma 10 *Let $q \geq 3$. Then*

$$M_0^\infty = \frac{1}{\mathcal{N}(q,\kappa,0)} \int_0^1 \mathrm{d}^q p \; \delta(1 - \sum_{\alpha\in\mathcal{Q}} p_\alpha) \; \boldsymbol{p}^{-1+\kappa} \min_{y\in\mathcal{Q}} \frac{\frac{1}{2} - \kappa + p_y(\kappa q - 1)}{\sqrt{p_y(1-p_y)}}. \tag{53}$$

Proof: We start from Lemma 9, with $W(\sigma_y) = W(c_0 \cdot \sigma_y/c_0)$ expressed as in (52), and take the limit $c_0 \to \infty$. In this limit $\boldsymbol{\sigma}$ goes to its expectation value $c_0\boldsymbol{p}$, with decreasing relative variance. Hence in the limit $c_0 \to \infty$ the expectation over $\boldsymbol{\sigma}$ ($\mathbb{E}^{(0)}_{\boldsymbol{\sigma}}$) in (51) becomes an expectation over $\boldsymbol{p}$, and σ_y/c_0 is replaced by p_y. We use the definition of $\mathbb{E}_{\boldsymbol{p}}$ as given in (39), with $\tau = 0$. Finally, the condition $\sigma_y > 0$ in the minimization becomes $p_y > 0$, which is automatically satisfied. □

The M_0^∞ is plotted in Fig. 1 for q = 3, 4 and 5. (For large q, numerical evaluation of the integral in (53) turns out to be very time consuming. We leave evaluation for $q \geq 6$ for future work.) We observe maxima around $\kappa \approx 1/q$. The maxima are sharp, with discontinuous derivatives. In [25] it was observed that when c is not infinite, the curves are smooth, while the maxima lie at somewhat larger κ. Fig. 1 shows that asymptotically it is optimal to choose κ equal to $1/q$ or very close to $1/q$.

We can read off from Fig. 1 which *fingerprinting rate* can be achieved asymptotically. The rate R of a fingerprinting code is defined as $R = (\log_q n)/m$, i.e. the number of q-ary symbols needed to uniquely determine one out of n users, divided by the number of symbols in the codeword. Thus, it measures which *fraction* (or percentage) of the watermark actually contains the message[7] that is conveyed by the codeword. The rest is redundancy required to achieve collusion resistance. Being a percentual measure of efficiency, the fingerprinting rate can be used as a figure of merit to compare codes that have different alphabet size.

In the limit $c_0 \to \infty$, we have that $n \to \infty$, while the total FP probability $w \approx n\varepsilon_1$ (see Lemma 6) stays constant, yielding $\ln \varepsilon_1^{-1} = \ln n[1 + \mathcal{O}(1/\ln n)]$. [8] Furthermore, the code length parameter A goes to $2/(M_0^\infty)^2$. Hence the fingerprinting rate $R = (\log_q n)/m = (\log_q n)/(Ac_0^2 \ln \varepsilon_1^{-1})$ goes to $(M_0^\infty)^2/(c_0^2\, 2\ln q)$.

Evaluation of the fraction $(M_0^\infty)^2/(2\ln q)$ at $\kappa = 1/q$ for $q \in \{2,3,4,5\}$ yields $\{0.29, 0.36, 0.33, 0.33\}$. We tentatively conclude that the asymptotic rate is best at alphabet size $q = 3$. This result shows that, *in the case of very large coalitions*, the score system of the q-ary Tardos code using the g_0, g_1 functions is far from optimal, in the sense that the code rate is far away from the fingerprinting capacity $(q-1)/(c_0^2\, 2\ln q)$ [5] and even decreases as a function of q for $q > 3$ instead of increasing.

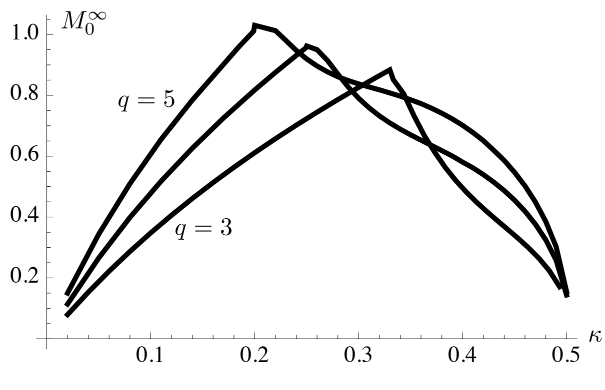

Fig. 1 *M_0^∞ as a function of κ, plotted for $q = 3$, $q = 4$ and $q = 5$. The graphs were obtained by numerical evaluation of the integral in (53). For $\kappa > 1/q$ there is some inaccuracy in the numerical evaluation.*

[7] In case of an error-correcting code one counts the number of (q-ary) message symbols. In the fingerprinting case in the catch-one-colluder scenario, the communicated message contains entropy $\log_q n$, counted in q-ary symbols.

[8] The relation $\ln \varepsilon_1^{-1} = \ln n[1 + \mathcal{O}(1/\ln n)]$ also holds more generally: e.g. for $w = f(n\varepsilon_1)$ where f is some invertible function.

Lemma 11 *Let $\tau \ll 1$. The normalizaton factor $\mathcal{N}$ in $F(\boldsymbol{p})$ can be expressed as an expansion in powers of τ as follows*

$$\mathcal{N}(q,\kappa,\tau) = B(\kappa\mathbf{1}_q)+\sum_{x=0}^{\infty}\sum_{b=1}^{q-1}\tau^{x+b\kappa}\binom{q}{b}(-1)^{x+b}B(\kappa\mathbf{1}_{q-b})\binom{-1+\kappa[q-b]}{x}\sum_{\substack{\boldsymbol{s}\in\mathbb{N}_0^b:\\ \sum_j s_j=x}}\binom{x}{\boldsymbol{s}}\prod_{\alpha=1}^{b}\frac{1}{\kappa+s_\alpha}. \tag{54}$$

Proof: See Appendix A.1.

Corollary 6 *Let $\kappa<1$. For $q=2$ the leading order behaviour of $\mathcal{N}$ is*

$$\mathcal{N}(2,\kappa,\tau) = B(\kappa,\kappa) - \frac{2}{\kappa}\tau^\kappa + \mathcal{O}(\tau^{\kappa+1}) \tag{55}$$

while for $q\geq 3$ it is

$$\mathcal{N}(q,\kappa,\tau) = B(\kappa\mathbf{1}_q) - \frac{q}{\kappa}B(\kappa\mathbf{1}_{q-1})\tau^\kappa + \mathcal{O}(\tau^{2\kappa}). \tag{56}$$

Proof: Follows from Lemma 11. The leading order term in the summations is ($b=1$, $x=0$), yielding a factor τ^κ. The two binomials that contain x then both reduce to 1; $\binom{q}{b}=q$; the summation vector $\boldsymbol{s}$ reduces to a scalar s_1 that has to be equal to x (i.e. 0); the product $\prod_a$ contains a single factor, namely $1/(\kappa+s_1)=1/\kappa$. Thus, the leading order term after $B(\kappa\mathbf{1}_q)$ is $-\frac{q}{\kappa}B(\kappa\mathbf{1}_{q-1})\tau^\kappa$. For $q=2$ the Beta function $B(\kappa\mathbf{1}_{q-1})$ reduces to 1 since the argument has only one component.
For $q\geq 3$ the next order term is the one with ($b=2$, $x=0$), yielding $\tau^{2\kappa}$. This is not an option for $q=2$, however, since the b-sum runs only till $q-1$. For $q=2$ the next order term occurs at ($b=1$, $x=1$). □
For the next lemma we first introduce some extra notation. Let $\mathcal{A}\subseteq\mathcal{Q}$. The notation $\boldsymbol{s}\in\mathbb{N}^{\mathcal{A}}$ means that $\boldsymbol{s}$ is a $|\mathcal{A}|$-component vector such that for every $\alpha\in\mathcal{A}$ there is a component $s_\alpha\in\mathbb{N}$. Furthermore we define the vector $\boldsymbol{\sigma}_{\mathcal{A}}$ as the restriction of $\boldsymbol{\sigma}$ to the components $(\sigma_\alpha)_{\alpha\in\mathcal{A}}$, and we define the scalar $\sigma_{\mathcal{A}}=\sum_{\alpha\in\mathcal{A}}\sigma_\alpha$.

Lemma 12 *Let $q=2$ and $\kappa=\frac{1}{2}+\psi$, with $\psi\neq 0$ and $|\psi|<\frac{1}{2}$. Let $\tau<|\psi|^{\frac{1}{1+\psi}}/c_0$. Let B_u^v denote the incomplete Beta function,*

$$B_u^v(x,y) := \int_u^v \mathrm{d}p\; p^{-1+x}(1-p)^{-1+y}. \tag{57}$$

Then for sufficiently large c_0, M can be expressed as

$$\begin{aligned} M^{(q=2,\kappa\neq\frac{1}{2})} &= \frac{2c_0}{\mathcal{N}}[1+\operatorname{sign}\psi]B_\tau^{1-\tau}(1+\psi,c_0+\psi) \\ &\quad -\frac{2\operatorname{sign}\psi}{\mathcal{N}}\frac{c_0!}{[\Gamma(\frac{c_0}{2}+\frac{1}{2})]^2}B_\tau^{1-\tau}(\tfrac{c_0}{2}+\tfrac{1}{2}+\psi,\tfrac{c_0}{2}+\tfrac{1}{2}+\psi). \end{aligned} \tag{58}$$

Proof: See Appendix A.2.

Corollary 7 *Let $q=2$ and $\kappa=\frac{1}{2}+\psi$, with $\psi\neq 0$ and $|\psi|<\frac{1}{2}$. Then*

$$M_0^\infty = \frac{2}{\sqrt{\pi}}\frac{\Gamma(1+\psi)}{\Gamma(\frac{1}{2}+\psi)}\operatorname{sign}(-\psi). \tag{59}$$

Proof: See Appendix A.3
Remark 1: This result tells us[9] that choosing $\kappa>\frac{1}{2}$ is very bad asymptotically! The scheme becomes so bad that the coalition's expected score is negative, whereas innocent users have zero expected score.
Remark 2: Eq. (59) is an increasing function of ψ on $\psi\in(-1/2,0)$. The limit $\psi\uparrow 0$ yields $M_0^\infty\to 2/\pi$, the known result for $\kappa=\frac{1}{2}$.
In the rest of the paper we will mainly consider $\kappa\leq\frac{1}{2}$.

[9] In [22] it was already noted that $\kappa>1/2$ is problematic, leading to negative terms in the $\sum_{\boldsymbol{\sigma}}$ for any q.

Lemma 13 *Let $q \geq 3$ and $\tau \ll 1$. The expectation value in (48) is evaluated as*

$$\mathbb{E}_{\boldsymbol{p}}[\boldsymbol{p}^{\boldsymbol{\sigma}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}}] = \frac{I_1 + I_2}{\mathcal{N}}, \tag{60}$$

with

$$\begin{aligned} I_1 = &\sum_{j=0}^{\infty} \sum_{\substack{\mathcal{A}\subset\mathcal{Q}:\\ y\in\mathcal{A}}} \tau^{j+\kappa|\mathcal{A}|+\sigma_{\mathcal{A}}-\frac{1}{2}}(-1)^{j+|\mathcal{A}|} B(\kappa \mathbf{1}_{q-|\mathcal{A}|} + \boldsymbol{\sigma}_{\mathcal{Q}\setminus\mathcal{A}}) \sum_{\substack{\boldsymbol{s}\in\mathbb{N}_0^{\mathcal{A}}:\\ s_{\mathcal{A}}\leq j}} \binom{-\frac{1}{2}}{j - s_{\mathcal{A}}} \\ &\binom{\kappa[q-|\mathcal{A}|] + \sigma_{\mathcal{Q}\setminus\mathcal{A}} - 1}{s_{\mathcal{A}}} \binom{s_{\mathcal{A}}}{\boldsymbol{s}} \left[\prod_{\alpha\in\mathcal{A}\setminus\{y\}} \frac{1}{\kappa + \sigma_\alpha + s_\alpha}\right] \\ &\left(\frac{\sigma_y}{\kappa + \sigma_y + s_y + j - s_{\mathcal{A}} - \frac{1}{2}} - \frac{c_0\tau}{\kappa + \sigma_y + s_y + j - s_{\mathcal{A}} + \frac{1}{2}}\right) \end{aligned} \tag{61}$$

$$\begin{aligned} I_2 = &\sum_{z=0}^{\infty} \sum_{\mathcal{A}\subseteq\mathcal{Q}\setminus\{y\}} \tau^{z+\kappa|\mathcal{A}|+\sigma_{\mathcal{A}}}(-1)^{z+|\mathcal{A}|} \left[\prod_{\beta\in(\mathcal{Q}\setminus\mathcal{A})\setminus\{y\}} \Gamma(\kappa+\sigma_\beta)\right] \\ &\frac{\Gamma(\kappa+\sigma_y-\frac{1}{2})\Gamma(\kappa[q-|\mathcal{A}|-1] + \sigma_{\mathcal{Q}\setminus\mathcal{A}} - \sigma_y - z - \frac{1}{2})}{\Gamma(\kappa[q-|\mathcal{A}|-1] + \sigma_{\mathcal{Q}\setminus\mathcal{A}} - \sigma_y - z)\Gamma(\kappa[q-|\mathcal{A}|] + \sigma_{\mathcal{Q}\setminus\mathcal{A}} - z - 1)} \\ &\left(\sigma_y - c_0 \frac{\kappa+\sigma_y-\frac{1}{2}}{\kappa[q-|\mathcal{A}|] + \sigma_{\mathcal{Q}\setminus\mathcal{A}} - z - 1}\right) \sum_{\substack{\boldsymbol{s}\in\mathbb{N}_0^{\mathcal{A}}:\\ s_{\mathcal{A}}=z}} \prod_{\alpha\in\mathcal{A}} \frac{1}{(\kappa+\sigma_\alpha+s_\alpha)s_\alpha!}. \end{aligned} \tag{62}$$

Proof: See Appendix A.4.
Note: The notation $\mathcal{A} \subset \mathcal{Q}$ does not include $\mathcal{A} = \mathcal{Q}$.
Eqs. (61) and (62) look daunting, but they are useful: they allow us to numerically evaluate M for nonzero τ with sufficient accuracy. Cutting off the j and z summations yields a result up to a certain power of τ. The ensuing finite summations are far easier to compute numerically than the original q-dimensional integration.

Lemma 14 *Let $q \geq 2$. For $\kappa \in [\frac{1}{2(q-1)}, \frac{1}{2}]$ it holds that $M_0 \geq M_0^\infty > 0$ with $M_0^\infty = \mathcal{O}(1)$. Furthermore, in the limit $c_0 \to \infty$ it holds for any κ that $M_0 = M_0^\infty\{1 + \mathcal{O}(\frac{1}{c_0})\}$.*

Proof: See Appendix A.5.

Theorem 4 *Let τ asymptotically follow the power law $\tau \sim c_0^{-\nu}$ with $\nu \in (1,2)$. Then the leading order asymptotic behaviour of M for various combinations of q and κ is given by*

q	κ	ν	M/M_0^∞
≥ 3	$(\frac{1}{q}, \frac{1}{2})$	$(1,2)$	$1 - c_0\tau^{\frac{1}{2}+\kappa} \frac{q(q-1)}{M_0^\infty(\frac{1}{2}+\kappa)} \frac{\Gamma(\kappa q)\Gamma(\kappa+c_0-1)}{[\Gamma(\kappa)]^2\Gamma(\kappa[q-1]+c_0-1)}$ + *higher order*
≥ 3	$< \frac{1}{q}$	$(1, \frac{1}{1-\kappa})$	$1 - (\cdots)c_0\tau$ + *higher order*
		$(\frac{1}{1-\kappa}, 2)$	$1 - \tau^\kappa \frac{1}{\kappa}\left[\frac{M_0^{\infty(q-1)}}{M_0^\infty} - \frac{q}{B(\kappa,\kappa[q-1])}\right]$ + *higher order*
2	$\frac{1}{2}$	$(1,2)$	$1 - 2c_0\tau$ + *higher order*
2	$< \frac{1}{2}$	$(1,2)$	$1 + \tau^\kappa \frac{2}{\kappa B(\kappa,\kappa)}$ + *higher order*

Proof: See Appendix A.6.

5 Code length optimization for $c_0 \to \infty$

5.1 Asymptotic correction terms

By combining the asymptotic expression for the code length parameter A (37) and Theorem 4, we can find the optimal choice for the cutoff τ so as to minimize A (for given κ). If we write $M/M_0^\infty = 1-\omega$, with ω given in the table in Theorem 4, then from (37) we have

$$A = \frac{2}{(M_0^\infty)^2}\left[1 + 2\omega + \frac{M_0^\infty}{3c_0\sqrt{\tau}} + \text{higher order}\right]. \tag{63}$$

Several situations can occur.

- ω is positive and proportional to a positive power of τ, e.g. $\omega \sim c_0^a \tau^b$ for some $b > 0$ and some a. In this case the best code length is obtained by letting ω and $\frac{1}{c_0\sqrt{\tau}}$ scale in the same way, if possible. We have $\omega \sim c_0^{a-\nu b}$ and $\frac{1}{c_0\sqrt{\tau}} \sim c_0^{-1+\nu/2}$; ν has to be set such that $a - \nu b = -1 + \nu/2$, if allowed by the constraints on ν.
- $\omega = \mathcal{O}(c_0^{-1})$. In this case ω loses against $\frac{1}{c_0\sqrt{\tau}} \sim c_0^{-1+\nu/2}$, since $\nu > 0$. The best code length is obtained by making $\frac{1}{c_0\sqrt{\tau}}$ as small as possible, i.e. ν as small as possible.
- ω is negative. In this case the best code length is obtained by setting ν such that ω beats $\frac{1}{c_0\sqrt{\tau}}$ by the largest possible margin. If this turns out to be impossible, then $\frac{1}{c_0\sqrt{\tau}}$ should be made as small as possible, as above.

The above considerations lead to the following result.

Theorem 5 *Let κ be given. Let the asymptotic behavior of A be parametrized as $A = \frac{2}{(M_0^\infty)^2}[1+\delta]$, where δ depends among others on the choice of τ. Let τ be parametrized as $\tau \sim c_0^{-\nu}$. Then the optimal ν, which minimizes A, is given in the table below, for various combinations of q and κ. The sign and the order of the ensuing δ are also listed.*

q	κ	ν range	optimal ν	δ from optimal ν
≥ 3	$(\frac{1}{q}, \frac{1}{2})$	$(1, 2)$	$\frac{2}{1+\kappa}$	$+\mathcal{O}(c_0^{-\kappa/(1+\kappa)})$
≥ 3	$< \frac{1}{q}$	$(1, \frac{1}{1-\kappa})$	$4/3$	$+\mathcal{O}(c_0^{-1/3})$
			or $\frac{1}{1-\kappa}$	$+\mathcal{O}(c_0^{-1+1/(2[1-\kappa])})$
		$(\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}]$ and $\omega < 0$	$\frac{1}{1-\kappa}$	$-\mathcal{O}(c_0^{-\kappa/(1-\kappa)})$
		$(\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}]$ and $\omega > 0$	$\frac{2}{1+2\kappa}$	$+\mathcal{O}(c_0^{-2\kappa/(1+2\kappa)})$
		$(\max\{\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}\}, 2)$	$\max\{\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}\}$	$+\mathcal{O}(c_0^{-1+\nu/2})$
2	$\frac{1}{2}$	$(1, 2)$	$4/3$	$+\mathcal{O}(c_0^{-1/3})$
2	$< \frac{1}{2}$	$(1, \frac{2}{1+2\kappa})$	$1 + 0^+$	$-\mathcal{O}(c_0^{-\kappa-0^+})$
2		$(\frac{2}{1+2\kappa}, 2)$	$\frac{2}{1+2\kappa}$	$+\mathcal{O}(c_0^{-2\kappa/(2\kappa+1)})$

Proof: See Appendix A.7.
Theorem 5 allows us to draw conclusions about the optimization of the code length. For a given q, we are allowed to choose some κ and τ so as to minimize A. The M_0^∞ depends on q and κ only; hence κ should be chosen such that M_0^∞ is (close to) maximal. Then τ must be set such that the leading order correction δ is as negative as possible. (If δ cannot be negative, then it should be made as close to zero as possible.)

5.2 Asymptotic optimization for $q = 2$

From Corollary 7 we see that for $q = 2$ the largest value of M_0^∞ is achieved at $\kappa = 1/2$. Hence the best code length for '$c_0 = \infty$' is achieved at $\kappa = 1/2$. According to Theorem 5 (3rd row from below

in the table), the corresponding best choice for the cutoff is $\tau \sim c_0^{-4/3}$, leading to $\delta \sim c_0^{-1/3}$. This matches the result of Laarhoven and de Weger [15].
However, it is possible to achieve a smaller δ for 'intermediate' large values of c_0. As can also be seen from Theorem 5 (2nd row from below in the table), by setting κ slightly smaller than 1/2 the asymptote becomes worse, but is approached with a power law $\approx c_0^{-1/2}$, which falls off faster than $c_0^{-1/3}$. For this regime we can formulate the following result.

Theorem 6 *Let $q = 2$, $\kappa = \frac{1}{2} - \varepsilon$, $\tau = Tc_0^{-1-\rho}$, with $\varepsilon \ll 1$, $\varepsilon > 0$, $\rho < \frac{\varepsilon}{1-\varepsilon}$ and T some positive constant. For $c_0 > (T/\varepsilon)^{1/\rho}$ the code length parameter is given by*

$$A = \frac{\pi^2}{2}[1 + \varepsilon \cdot 4\ln 2 + \mathcal{O}(\varepsilon^2)] \left[1 - \frac{4}{\pi}\sqrt{T}c_0^{-\frac{1}{2}+\varepsilon-\frac{\rho}{2}+\varepsilon\rho} + \frac{2}{3\pi\sqrt{T}}c_0^{-\frac{1}{2}+\frac{\rho}{2}} + \textit{higher order}\right]. \quad (64)$$

The negative correction term dominates the positive correction term for $c_0 > (\frac{1}{6T})^{\frac{1}{\varepsilon-\rho+\varepsilon\rho}}$.

<u>Proof:</u> See Appendix A.8.
Note that the bound $c_0 > (\frac{1}{6T})^{\frac{1}{\varepsilon-\rho+\varepsilon\rho}}$ is typically an extremely large number; hence, in practice, the positive term in (64) is dominant. The positive correction term of order $\approx c_0^{-1/2}$ can be better than the $+\mathcal{O}(c_0^{-1/3})$ that is obtained at $\kappa = 1/2$, $\nu = 4/3$. Fig. 2 shows an example of a better correction term than (2) for large but finite c_0.

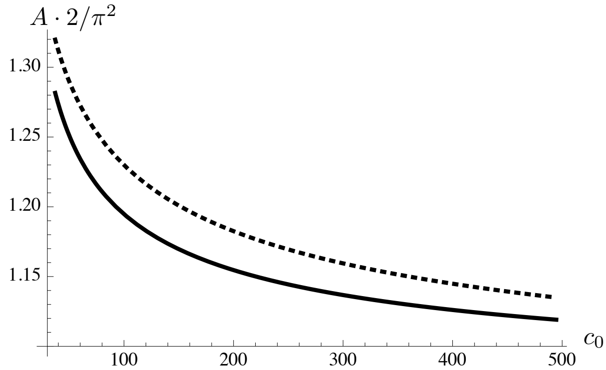

Fig. 2 *The dotted line is the expression $1 + (12/\pi^2)^{1/3}c_0^{-1/3}$ from [15]. The solid line corresponds to (64) with the ε^2 term neglected, for $\varepsilon = \rho = 0.02$, $T = 0.0215$.*

5.3 Asymptotic optimization for $q \geq 3$

For $q \geq 3$ it is a bit harder to decide which parameter settings are optimal. If we set[10] $\kappa = 1/q + 0^+$, then line 1 of the table in Theorem 5 tells us that the best choice is $\tau \sim c_0^{-2q/(1+q)+0^+}$, with a positive correction term of approximate order $\mathcal{O}(c_0^{-1/(q+1)})$; not a very good result. Setting $\kappa = 1/q - 0^+$ allows for better correction terms.

– For $q = 3$, $\kappa = 1/3 - 0^+$, the interval $(\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}]$ does not exist (see lines 3 and 4 in the table of Theorem 5). Hence there is no possibility to achieve the corresponding negative correction term. The best option is to set $\nu = 4/3$, which yields a positive correction term of order $\mathcal{O}(c_0^{-1/3})$.

[10] The notation 0^+ stands for an infinitesimally small positive number.

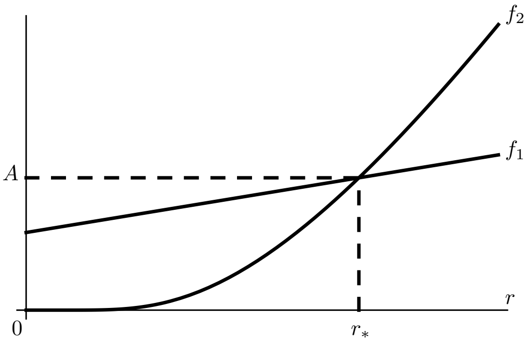

Fig. 3 *Schematic plot of the functions f_1 and f_2 as a function of r for fixed τ.*

- For $q \geq 4$, $\kappa = 1/q - 0^+$, the interval $(\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}]$ *does* exist. Furthermore, from the numerical results on M_0^∞ (part of which is shown in Fig. 1) we find that $\omega < 0$ for $q = 4, 5, 6$. Hence the *negative* correction term of order $\mathcal{O}(c_0^{-1/[q-1]})$ applies when ν is set to $\nu = \frac{1}{1-\kappa} + 0^+$. For larger q we do not have numerical results, and there it might be the case that $\omega > 0$. Then the best option is to set $\nu = \frac{1}{1-\kappa} - 0^+$, yielding a positive correction term of order approximately $\mathcal{O}(c_0^{-1+\frac{1}{2[1-\kappa]}}) = \mathcal{O}(c_0^{-\frac{q-2}{2[q-1]}})$. Note that this decreases for increasing alphabet size.

It would be nice to derive a result like Theorem 6 for general alphabet size, but that requires precise knowledge of the ω in the expression $M/M_0^\infty = 1 - \omega$.

6 Optimization of the code length for finite c_0

6.1 Formulas for finite coalition size

Based on Corollaries 1 and 4 we provide analytic equations for finding the optimal code length for non-asymptotic c_0. They take the form of coupled implicit equations.

Theorem 7 *Let $q \geq 3$ and $2 \leq c \leq c_0$. Let $\sqrt{\tau} \leq \sqrt{\frac{2}{q}}(1 - \frac{1}{\sqrt{q-1}})$ and $\sqrt{\tau} < \frac{M}{2eq}$. Let the functions f_1 and f_2 be defined as*

$$f_1(\tau, r) = \frac{1}{M^2}\left[1 + \frac{M}{c_0\sqrt{\tau}}(\frac{1}{3} + \eta r) + \sqrt{D(\tau, r)}\right] \tag{65}$$

$$f_2(\tau, r) = \frac{\eta}{eq}\frac{r}{c_0\tau}e^{-1/r} \tag{66}$$

$$D(\tau, r) = 1 + \frac{2M}{c_0\sqrt{\tau}}(\frac{1}{3} + \eta r) + \frac{M^2}{9c_0^2\tau}. \tag{67}$$

Then there exists an $r_*(\tau) > 0$ such that $f_1(\tau, r_*(\tau)) = f_2(\tau, r_*(\tau))$, and the following choice of A and B

$$\begin{aligned} A &= f_1(\tau, r_*) \\ B &= M f_1(\tau, r_*) - \frac{\eta r_*}{c_0\sqrt{\tau}} \end{aligned} \tag{68}$$

achieves both $P_{\mathrm{FP}} \leq \varepsilon_1$ and $P_{\mathrm{FN}} \leq \varepsilon_2$.

Proof: See Appendix A.9.
For small (non-asymptotic) c_0 it is quite difficult to determine which value of τ is optimal. The main difficulty is the complicated dependence of M on τ. If $\partial M/\partial\tau$ is known, then τ can be optimized in the following way.

Theorem 8 *The code length parameter A is minimized by choosing A, B according to Theorem 7 and by setting the cutoff parameter to τ_*, where τ_* and r_* are obtained by solving the following system of equations for τ and r,*

$$f_1(\tau, r) = f_2(\tau, r) \quad ; \quad \tau \frac{\partial(f_1 - f_2)/\partial\tau}{\partial(f_1 - f_2)/\partial r} = -\frac{r^2}{r+1}. \tag{69}$$

Proof: See Appendix A.10.
Note that the derivative $\partial f_1/\partial\tau$ contains $\partial M/\partial\tau$. This hinders straightforward application of Theorem 8. An approximation for $\partial M/\partial\tau$ can be based on Lemmas 11 and 13.

6.2 Numerical results for 'small' coalition sizes

In this section we present numerical results for $q = 3$, $q = 4$ and $q = 5$. For fixed q, c_0 and η we used Theorem 7 to find κ and τ values that minimize the code length parameter A. Table 1 shows κ, τ and A for $q = 3$ at several c_0. In Fig. 4 we plotted A versus c_0 in two different ways: (i) the parameter A itself; (ii) the expression $A \cdot \log_2 q$. The first way reflects the number of q-ary symbols, since A is defined according to $m = Ac_0^2 \ln \varepsilon_1^{-1}$, with m the number of symbols in a codeword. The second way measures the amount of 'space' occupied by the watermark, and is a more fair way to compare the use of different alphabet sizes; $A \log_2 q$ is inversely proportional to the code rate (see Section 4.2).
From Fig. 4 we see that the rate at $c_0 \leq 20$ *worsens* when the alphabet size is increased, even though the code length (number of q-ary symbols) is reduced. We have to be careful drawing conclusions from this graph. It shows values of A that are optimal *with respect to the chosen proof method* and therefore does not necessarily tell what is 'really' happening.[11] Furthermore, the results in Section 4.2 demonstrate that for $c_0 \to \infty$ the opposite behaviour occurs: there the code rate increases with growing q.

$q = 3$						
	$\eta = \frac{\ln 1/2}{\ln 10^{-10}} \approx 0.030$			$\eta = \frac{\ln 1/2}{\ln 10^{-3}} \approx 0.100$		
c_0	A	κ	τ	A	κ	τ
3	14.3	0.309	0.0017	15.4	0.309	0.0017
4	12.3	0.309	0.0013	13.2	0.302	0.0017
5	10.9	0.304	0.0013	11.7	0.304	0.0013
6	10.0	0.305	0.0011	10.7	0.305	0.0011
8	8.85	0.305	0.0009	9.43	0.304	0.0009
10	8.09	0.305	0.0007	8.60	0.303	0.0008
13	7.33	0.302	0.0006	7.77	0.301	0.0006
20	6.38	0.294	0.00046	6.70	0.299	0.00042

Table 1 *Results of numerical optimization of the code length parameter A for $q = 3$, using Theorem 7. For various combinations of c_0 and η, the optimal A is shown as well as the κ and τ values required to get the optimal A.*

6.3 Formulas for 'large' c_0

It is interesting to see what happens to the finite-c_0 formulas in Theorem 7 when the coalition size is increased. For $c_0 \gg 1$ we can solve the crossover point $r_*(\tau)$ approximately, and also approximately determine how τ must be chosen as a function of c_0 in order to minimize the code length. The cutoff τ has to be chosen as a decreasing function of c_0 such that $c_0\tau^{1/2+\kappa} \to 0$ and $c_0\sqrt{\tau} \to \infty$.

[11] For a given attack strategy, the method of [23,22] can be used to obtain *exact* results.

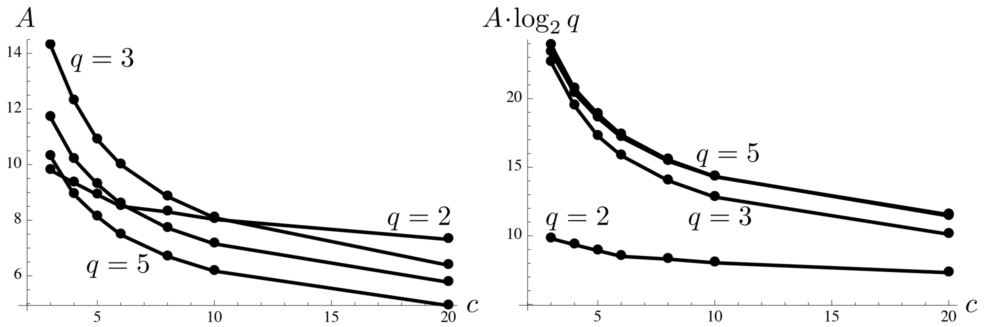

Fig. 4 *Optimal code length parameter, obtained numerically using Theorem 7, as a function of c_0, for $\eta = 0.03$ and $q = 2, 3, 4, 5$. The data for $q = 2$ were taken from [15].* **Left:** *The parameter A, related to the number of q-ary symbols.* **Right:** *The product $A \log_2 q$, inversely proportional to the rate of the code.*

Theorem 9 *Let the following inequalities be satisfied,*

$$\sqrt{\tau} < \frac{M}{2qe} \tag{70}$$

$$c_0\tau \ln(\frac{1}{c_0\tau}) < \frac{M^2\eta}{2e^2 q} \tag{71}$$

$$c_0\sqrt{\tau}\frac{\ln[\ln(1/c_0\tau)\frac{2eq}{M^2\eta}]}{\ln(1/c_0\tau)} \geq M(\tfrac{1}{3}+\eta). \tag{72}$$

Then the choice $A = \hat{A}$, $B = \hat{B}$, with

$$\hat{A} = \frac{2}{M^2}\left[1 + \frac{M}{3c_0\sqrt{\tau}}(1+3\eta\hat{r})\right] \tag{73}$$

$$\hat{B} = \frac{2}{M}\left[1 + \frac{M}{3c_0\sqrt{\tau}}(1+\tfrac{3}{2}\eta\hat{r})\right] \tag{74}$$

$$\hat{r} := 1/\ln\left[(c_0\tau\ln\frac{1}{c_0\tau})^{-1}\frac{M^2\eta}{2eq}\right], \tag{75}$$

achieves both $P_{\rm FP} \leq \varepsilon_1$ and $P_{\rm FN} \leq \varepsilon_2$.

Proof: See Appendix A.11.
Note that the inequalities (70–72) are not difficult to satisfy.
Theorem 9 provides a shorter sufficient code length (by a factor ≈ 2) than the proofs in [25]. (Although the asymptotic value $2/M^2$ was already derived in [25] using the Gaussian approximation.) The code length parameter (73), unsurprisingly, has the same form as (37), with an explicit expression for the 'higher order' terms in (37). Theorem 9 captures the large-c_0 behaviour of the provably secure code without specifying an asymptotic relation for τ as a function of c_0.

7 Summary

Use of the Bernstein inequality (for FP, leading to Corollary 1) and the Bennett inequality (for FN, leading to Corollaries 4 and 5), instead of the Markov inequality, shortens the security proofs for Tardos codes. Furthermore, for $q \geq 3$ the obtained FN bound is tighter than previously available. With very little effort the lower bound (37) on the large-c_0 code length parameter is derived, as well as the general-c_0 optimization equations given in Theorem 7. It must be noted that our use of Bennett's inequality for the FN bound is conditional on the assumption that the strongest coalition attack strategy is segment-symmetric.

Our paper could have ended at this point. However, the parameter M has a nontrivial dependence on c_0, q, the concentration parameter κ and the cutoff τ. For a serious analysis of optimal code lengths this dependence has to be known precisely. Section 4 is completely devoted to this problem, and most of the appendices too. The limit $\tau \to 0$, $c_0 \to \infty$ is difficult to compute, because it requires a $(q-1)$-dimensional integration over $\boldsymbol{p}$.
Numerics for $q = 3, 4, 5$ (Fig. 1) indicate that the asymptotic code rate is best at alphabet size $q = 3$. One has to be careful how to interpret this result. On the one hand, it seems to indicate that the q-ary scheme of [25] fails to make use of the fact that the fingerprinting capacity is an increasing function [5] of q. However, one must also bear in mind that the *provably secure* code length may be significantly larger than the *actually secure* code length. Unfortunately, the proof method does not reveal how much tightness is lost in the inequalities.
The lemmas that give finite-c_0 correction terms (Lemmas 11, 12 and 13) are not pretty. However, they have enabled us to derive optimal asymptotic power laws for the sufficient code length parameter. For $q = 2$ we have found that setting κ slightly below $1/2$ allows for shorter codes (Fig. 2). Furthermore, the ugly lemmas made it possible to do the small-c_0 code length optimization in Section 6.2. This optimization shows that for $c_0 \leq 20$ the binary code has a better rate than $q \geq 3$. However, all the 'optimality' results are again valid only *with respect to the employed proof technique*, which makes it hard to draw final conclusions about the real performance of the Tardos scheme.

Acknowledgements We thank Dion Boesten, Jeroen Doumen, Thijs Laarhoven, Antonino Simone, and Benne de Weger for useful discussions. We thank Wil Kortsmit for his help with numerical integrations. This research was funded by STW Sentinels (CREST project, 10518).

References

1. E. Amiri and G. Tardos. High rate fingerprinting codes and the fingerprinting capacity. In *Proc. 20th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 336–345, 2009.
2. G. Bennett. Probability Inequalities for the Sum of Independent Random Variables. *Journal of the American Statistical Association*, 57(297):33–45, 1962.
3. S.N. Bernstein. *Theory of Probability.* 1927.
4. O. Blayer and T. Tassa. Improved versions of Tardos' fingerprinting scheme. *Designs, Codes and Cryptography*, 48(1):79–103, 2008.
5. D. Boesten and B. Škorić. Asymptotic fingerprinting capacity for non-binary alphabets. In *Information Hiding 2011*, volume 6958 of *LNCS*, pages 1–13. Springer, 2011.
6. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5):1897–1905, 1998.
7. A. Charpentier, C. Fontaine, T. Furon, and I.J. Cox. An asymmetric fingerprinting scheme based on Tardos codes. In *Information Hiding*, volume 6958 of *LNCS*, pages 43–58. Springer, 2011.
8. A. Charpentier, F. Xie, C. Fontaine, and T. Furon. Expectation maximization decoding of Tardos probabilistic fingerprinting code. In *Media Forensics and Security*, volume 7254 of *SPIE Proceedings*, page 72540, 2009.
9. T. Furon, A. Guyader, and F. Cérou. On the design and optimization of Tardos probabilistic fingerprinting codes. In *Information Hiding*, volume 5284 of *Lecture Notes in Computer Science*, pages 341–356. Springer, 2008.
10. T. Furon and L. Pérez-Freire. Worst case attacks against binary probabilistic traitor tracing codes. *CoRR*, abs/0903.3480, 2009.
11. T. Furon, L. Pérez-Freire, A. Guyader, and F. Cérou. Estimating the minimal length of Tardos code. In *Information Hiding*, volume 5806 of *LNCS*, pages 176–190, 2009.
12. S. He and M. Wu. Joint coding and embedding techniques for multimedia fingerprinting. *TIFS*, 1:231–248, June 2006.
13. Y.W. Huang and P. Moulin. Capacity-achieving fingerprint decoding. In *IEEE Workshop on Information Forensics and Security*, pages 51–55, 2009.
14. C. Knessl and J.B. Keller. Partition asymptotics from recursion equations. *Siam J. Appl. Math.*, 50(2):323–338, 1990.
15. T. Laarhoven and B.M.M. de Weger. Optimal symmetric Tardos traitor tracing schemes, 2011. `http://arxiv.org/abs/1107.3441`.
16. P. Meerwald and T. Furon. Towards joint Tardos decoding: the 'Don Quixote' algorithm. In *Information Hiding*, volume 6958 of *LNCS*, pages 28–42. Springer, 2011.
17. P. Moulin. Universal fingerprinting: Capacity and random-coding exponents. In *Preprint arXiv:0801.3837v2, avilable at http://arxiv.org/abs/0801.3837*, 2008.

18. K. Nuida. Short collusion-secure fingerprint codes against three pirates. In *Information Hiding*, volume 6387 of *LNCS*, pages 86–102. Springer, 2010.
19. K. Nuida, S. Fujitsu, M. Hagiwara, T. Kitagawa, H. Watanabe, K. Ogawa, and H. Imai. An improvement of discrete Tardos fingerprinting codes. *Des. Codes Cryptography*, 52(3):339–362, 2009.
20. K. Nuida, M. Hagiwara, H. Watanabe, and H. Imai. Optimal probabilistic fingerprinting codes using optimal finite random variables related to numerical quadrature. *CoRR*, abs/cs/0610036, 2006.
21. H.G. Schaathun. On error-correcting fingerprinting codes for use with watermarking. *Multimedia Systems*, 13(5-6):331–344, 2008.
22. A. Simone and B. Škorić. Asymptotically false-positive-maximizing attack on non-binary Tardos codes. In *Information Hiding*, volume 6958 of *LNCS*, pages 14–27. Springer, 2011.
23. A. Simone and B. Škorić. Accusation probabilities in Tardos codes: beyond the Gaussian approximation. *Designs, Codes and Cryptography*, 63(3):379–412, 2012.
24. G. Tardos. Optimal probabilistic fingerprint codes. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 116–125, 2003.
25. B. Škorić, S. Katzenbeisser, and M.U. Celik. Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. *Designs, Codes and Cryptography*, 46(2):137–166, 2008.
26. B. Škorić, S. Katzenbeisser, H.G. Schaathun, and M.U. Celik. Tardos fingerprinting codes in the Combined Digit Model. *IEEE Transactions on Information Forensics and Security*, 6(3):906–919, 2011.
27. B. Škorić, T.U. Vladimirova, M.U. Celik, and J.C. Talstra. Tardos fingerprinting is better than we thought. *IEEE Transactions on Information Theory*, 54(8):3663–3676, 2008.
28. F. Xie, T. Furon, and C. Fontaine. On-off keying modulation and Tardos fingerprinting. In *Proc. 10th Workshop on Multimedia & Security (MM&Sec)*, pages 101–106. ACM, 2008.

A Proofs

A.1 Proof of Lemma 11

We take the alphabet labeling $\mathcal{Q} = \{1, 2, \ldots, q\}$ in this proof, without loss of generality. The normalization constant $\mathcal{N}$ in (3) is defined as $\mathcal{N} = \int_\tau^{1-t} \mathrm{d}^q p\; \delta(1 - \sum_\alpha p_\alpha)\boldsymbol{p}^{-1+\kappa}$. The upper bound $1-t$ on the integration can be replaced by ∞, since the delta function makes sure that only the relevant part of the integration region plays a role. We split the integration operator $\int \mathrm{d}^q p$ into a product of q operators, and then further split each of them according to $\int_\tau^\infty = \int_0^\infty - \int_0^\tau$. This gives rise to a sum over 2^q integration operators, which due to symmetry can be grouped according to the number of $\int_0^\tau$ factors appearing.

$$
\begin{aligned}
\mathcal{N} &= \left[\prod_{\alpha\in\mathcal{Q}} \Big(\int_0^\infty \mathrm{d}p_\alpha - \int_0^\tau \mathrm{d}p_\alpha\Big)\right] \boldsymbol{p}^{-1+\kappa}\delta(1 - \sum_{\gamma\in\mathcal{Q}} p_\gamma) \\
&= B(\kappa\mathbf{1}_q) + \sum_{b=1}^{q-1}\binom{q}{b}(-1)^b \left[\prod_{\alpha=1}^{b}\int_0^\tau \mathrm{d}p_\alpha\right]\left[\prod_{\beta=b+1}^{q}\int_0^\infty \mathrm{d}p_\beta\right] \boldsymbol{p}^{-1+\kappa}\delta(1 - \sum_{\gamma\in\mathcal{Q}} p_\gamma).
\end{aligned}
$$

The maximum value of the index b is $q-1$, since at $b = q$ the delta function can no longer be satisfied. We write $p_A := \sum_{\alpha=1}^{b} p_\alpha$ and $p_\beta = (1 - p_A)s_\beta$, with $s_\beta \in [0, 1]$. Provided that $\tau < 1/q$ (which in practice is always the case) we can then evaluate the p_β integrals,

$$
\begin{aligned}
\mathcal{N} - B(\kappa\mathbf{1}_q) &= \sum_{b=1}^{q-1}\binom{q}{b}(-1)^b \left[\prod_{\alpha=1}^{b}\int_0^\tau \mathrm{d}p_\alpha\, p_\alpha^{-1+\kappa}\right](1-p_A)^{-1+\kappa(q-b)}\int_0^\infty \mathrm{d}^{q-b}s\; \boldsymbol{s}^{-1+\kappa}\delta(1 - \sum_{a=b+1}^{q} s_a) \\
&= \sum_{b=1}^{q-1}\binom{q}{b}(-1)^b B(\kappa\mathbf{1}_{q-b})\left[\prod_{\alpha=1}^{b}\int_0^\tau \mathrm{d}p_\alpha\, p_\alpha^{-1+\kappa}\right](1-p_A)^{-1+\kappa(q-b)}. \qquad (76)
\end{aligned}
$$

We expand in τ, using the fact that $p_A = \mathcal{O}(\tau)$. We write $p_\alpha = \tau u_\alpha$, with $u_\alpha \in [0, 1]$. Using the binomial expansion of $(1 - p_A)^{\cdots}$ we get

$$
(1-p_A)^{-1+\kappa(q-b)} = \sum_{x=0}^{\infty}\tau^x\binom{-1+\kappa[q-b]}{x}(-\sum_\alpha u_\alpha)^x. \qquad (77)
$$

Substitution into (76) and doing a multinomial expansion of $(\sum u_\alpha)^x$ yields

$$
\begin{aligned}
\mathcal{N} &= B(\kappa\mathbf{1}_q) + \sum_{b=1}^{q-1}\binom{q}{b}(-1)^b B(\kappa\mathbf{1}_{q-b})\sum_{x=0}^{\infty}\tau^{x+b\kappa}(-1)^x\binom{-1+\kappa[q-b]}{x}\zeta_{bx} \\
\zeta_{bx} &:= \int_0^1 \mathrm{d}^b u\; \boldsymbol{u}^{-1+\kappa}(\sum_{\alpha=1}^{b} u_\alpha)^x = \sum_{\boldsymbol{s}\colon \sum_j s_j = x}\binom{x}{\boldsymbol{s}}\prod_{\alpha=1}^{b}\frac{1}{\kappa+s_\alpha}. \qquad (78)
\end{aligned}
$$

A.2 Proof of Lemma 12

For $q = 2$, the minimization $\min_y$ in (48) reduces to choosing one out of two expectation values. Because of the $0 \leftrightarrow 1$ symbol symmetry these two values turn out to be identical, up to a minus sign. The negative contribution is always chosen, except where the marking assumption prohibits it. The sum over the vector $\boldsymbol{\sigma}$ reduces to a sum over a scalar σ. Also because of symbol symmetry, the contribution from $c_0 - \sigma$ equals the one from σ. Hence the range of the σ-sum can be restricted to the lower half.
Without loss of generality we take c_0 odd. Then

$$\begin{aligned} M &= \frac{2c_0}{\mathcal{N}} J_1 - \frac{2}{\mathcal{N}} \sum_{\sigma=1}^{(c_0-1)/2} \binom{c_0}{\sigma} |J_2| \\ J_1 &:= \int_\tau^{1-\tau} \mathrm{d}p \, p^\psi (1-p)^{c_0-1+\psi} \\ J_2 &:= \int_\tau^{1-\tau} \mathrm{d}p \, p^{\sigma-1+\psi} (1-p)^{c_0-\sigma-1+\psi} (\sigma - c_0 p). \end{aligned} \tag{79}$$

Further evaluation of the integrals yields

$$\begin{aligned} J_1 &= B(1+\psi, c_0+\psi) - \int_0^\tau \mathrm{d}p \, p^\psi (1-p)^{c_0-1+\psi} - \int_0^\tau \mathrm{d}k \, k^{c_0-1+\psi} (1-k)^\psi \\ &= B(1+\psi, c_0+\psi) - \frac{\tau^{1+\psi}}{1+\psi} [1 + \mathcal{O}(c_0\tau)] \end{aligned} \tag{80}$$

$$\begin{aligned} J_2 &= \int_\tau^{1-\tau} \mathrm{d}p \, [p(1-p)]^\psi \frac{\mathrm{d}}{\mathrm{d}p} [p^\sigma (1-p)^{c_0-\sigma}] \\ &= -\psi \frac{c_0 - 2\sigma}{c_0 + 2\psi} B(\sigma+\psi, c_0-\sigma+\psi) - \tau^{\sigma+\psi} \frac{\sigma}{\sigma+\psi} [1 + \mathcal{O}(c_0\tau)]. \end{aligned} \tag{81}$$

In the last step we used integration by parts and made use of $c_o\tau \ll 1$.
Next we look at the Beta function term in (81) and compare its magnitude to the factor $\tau^{\sigma+\psi}$ in the last term. We distinguish between two cases:

- $\underline{\sigma \ll c_0}$. In this case we apply Lemma 4 and obtain

$$\psi B(\sigma+\psi, c_0-\sigma+\psi) = \psi \Gamma(\sigma+\psi) c_0^{-\sigma-\psi} [1 + \mathcal{O}(1/c_0)]. \tag{82}$$

  The condition $\tau < |\psi|^{\frac{1}{1+\psi}}/c_0$ that we imposed in the lemma makes sure that the $\tau^{\sigma+\psi}$ term 'loses': we get $\tau^{\sigma+\psi} < |\psi|^{\frac{\sigma+\psi}{1+\psi}} c_0^{-\sigma-\psi} \le |\psi| c_0^{-\sigma-\psi}$.
- $\underline{\sigma \text{ of the same order as } c_0}$. We write $\sigma = \alpha c_0$, with $\alpha < \frac{1}{2}$, $\alpha \gg 1/c_0$. Applying Lemma 5 we find

$$\psi B(\sigma+\psi, c_0-\sigma+\psi) = \psi \frac{\sqrt{2\pi}}{\sqrt{c_0}} [\alpha(1-\alpha)]^{-\frac{1}{2}+\psi} e^{-c_0 E(\alpha)} [1 + \mathcal{O}(\frac{1}{c_0})]. \tag{83}$$

  Again, the imposed condition on τ causes the $\tau^{\sigma+\psi}$ term to 'lose': we have $\tau^{\sigma+\psi} < |\psi| c_0^{-\sigma-\psi} = |\psi| c_0^{-\psi} \exp[-c_0 \alpha \ln c_0]$. Since $\alpha \ln c_0 > E(\alpha)$ for $\alpha \gg 1/c_0$ and large enough c_0, we have an expression that is exponentially smaller than (83) in the limit $c_0 \to \infty$.

We conclude that the term containing the Beta function determines the sign of J_2. Furthermore, the factor $c_0 - 2\sigma$ is positive. The Beta function is also positive. Hence for sufficiently large c_0 we have $|J_2| = J_2 \cdot \mathrm{sign}(-\psi)$ for all $\sigma \in \{1, \cdots, \frac{c_0-1}{2}\}$.
Then we go back to (79): we move the $\sum_\sigma$ into the J_2-integral and use the following summation equality,

$$\sum_{\sigma=1}^{(c_0-1)/2} \binom{c_0}{\sigma} p^\sigma (1-p)^{c_0-\sigma} (\sigma - c_0 p) = c_0 p (1-p)^{c_0} - \frac{c_0!}{[(\frac{c_0-1}{2})!]^2} [p(1-p)]^{(c_0+1)/2}. \tag{84}$$

Finally we express the integrals as incomplete Beta functions.

A.3 Proof of Corollary 7

In the limit $c_0 \to \infty$ we have $\tau \downarrow 0$, so that the incomplete Beta functions become complete. We look at the first term in (58). If $\psi < 0$ then it vanishes. Using Lemma 4 we see that the Beta function scales as

$$c_0 B(1+\psi, c_0+\psi) \sim c_0^{-\psi}. \tag{85}$$

Hence this term disappears for $\psi > 0$ as well. In the second term we use the doubling formula for the Gamma function, $c_0! = (2^{c_0}/\sqrt{\pi})\Gamma(c_0/2+1/2)\Gamma(c_0/2+1)$ and, again using Lemma 4,

$$B(c_0/2+\kappa, c_0/2+\kappa) = \frac{\sqrt{\pi}}{2^{c_0+2\kappa-1}} \frac{\Gamma(c_0/2+\kappa)}{\Gamma(c_0/2+1/2+\kappa)} \sim \frac{\sqrt{\pi}}{2^{2\psi}} \frac{(c_0/2)^{-1/2}}{2^{c_0}} \tag{86}$$

We divide by $[\Gamma(c_0/2+1/2)]^2$ and use $\Gamma(c_0/2+1)/\Gamma(c_0/2+1/2) \sim \sqrt{c_0/2}$. Using the doubling formula again we rewrite the normalization factor $\mathcal{N}$ as

$$\mathcal{N}(2, \tfrac{1}{2}+\psi, 0) = B(\tfrac{1}{2}+\psi, \tfrac{1}{2}+\psi) = 2^{-2\psi}\sqrt{\pi}\frac{\Gamma(\frac{1}{2}+\psi)}{\Gamma(1+\psi)}. \tag{87}$$

Combining all the ingredients yields the end result.

A.4 Proof of Lemma 13

We write $\mathbb{E}_{\boldsymbol{p}}[\frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}}\boldsymbol{p}^{\boldsymbol{\sigma}}] = \frac{I}{\mathcal{N}}$, where I is a q-dimensional integral, split up as in Appendix A.1,

$$I = [\prod_{\alpha\in\mathcal{Q}}(\int_0^1 \mathrm{d}p_\alpha - \int_0^\tau \mathrm{d}p_\alpha)]\delta(1-\sum_{\beta\in\mathcal{Q}} p_\beta)\boldsymbol{p}^{-1+\kappa+\boldsymbol{\sigma}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}}. \tag{88}$$

The product $\prod_\alpha$ can be rewritten as a sum of different q-dimensional integrals; in each if these integrals a different choice is made which of the α are integrated in the $(0,\tau)$ interval. We denote the set of these symbols as $\mathcal{A}$. For brevity we will use the notation $a = |\mathcal{A}|$, $\mathcal{B} = \mathcal{Q}\setminus A$, $\sigma_{\mathcal{A}} = \sum_{\alpha\in\mathcal{A}}\sigma_\alpha$, $\sigma_{\mathcal{B}} = \sum_{\beta\in\mathcal{B}}\sigma_\beta$, $P_{\mathcal{A}} = \sum_{\alpha\in\mathcal{A}} p_\alpha$, $P_{\mathcal{B}} = \sum_{\beta\in\mathcal{B}} p_\beta$.

$$I = \sum_{\mathcal{A}\subset\mathcal{Q}} (-1)^a \int_0^\tau \mathrm{d}^a p_{\mathcal{A}}\, \boldsymbol{p}_{\mathcal{A}}^{-1+\kappa+\boldsymbol{\sigma}_{\mathcal{A}}} \int_0^{1-P_{\mathcal{A}}} \mathrm{d}^{q-a} p_{\mathcal{B}}\, \boldsymbol{p}_{\mathcal{B}}^{-1+\kappa+\boldsymbol{\sigma}_{\mathcal{B}}} \delta(1-P_{\mathcal{A}}-P_{\mathcal{B}}) \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}}. \tag{89}$$

(Note that $\mathcal{A} = \mathcal{Q}$ does not occur in the sum.) We split the $\sum_{\mathcal{A}}$ into two parts: one with $y \in \mathcal{A}$ (giving rise to a contribution to I denoted as I_1) and one with $y \in \mathcal{B}$ (giving rise to I_2). In both parts we write, for $\beta \in \mathcal{B}$, $p_\beta = (1-P_{\mathcal{A}})s_\beta$, with $s_\beta \in (0,1)$. We have $\delta(1-P_{\mathcal{A}}-P_{\mathcal{B}}) = (1-P_{\mathcal{A}})^{-1}\delta(1-\sum_{\beta\in\mathcal{B}} s_\beta)$. The integrals over the '$\mathcal{B}$' degrees of freedom can be evaluated to Beta functions.
We first derive the result for I_1.

$$I_1 = \sum_{\substack{\mathcal{A}\subset\mathcal{Q}:\\ y\in\mathcal{A}}} (-1)^a B(\kappa\mathbf{1}_{q-a}+\boldsymbol{\sigma}_{\mathcal{B}}) \int_0^\tau \mathrm{d}^a p_{\mathcal{A}}\, \boldsymbol{p}_{\mathcal{A}}^{-1+\kappa+\boldsymbol{\sigma}_{\mathcal{A}}} \frac{\sigma_y - c_0 p_y}{\sqrt{p_y(1-p_y)}} (1-P_{\mathcal{A}})^{-1+\kappa[q-a]+\sigma_{\mathcal{B}}}. \tag{90}$$

We use binomial and multinomial expansions to write

$$\begin{aligned} \frac{1}{\sqrt{1-p_y}} &= \sum_{x=0}^\infty \binom{-1/2}{x} p_y^x, \\ (1-P_{\mathcal{A}})^u &= \sum_{z=0}^\infty \binom{u}{z}(-P_{\mathcal{A}})^z \\ &= \sum_{z=0}^\infty \binom{u}{z}(-1)^z \sum_{\boldsymbol{s}\in\mathbb{N}^{\mathcal{A}}:\, s_{\mathcal{A}}=z} \binom{z}{\boldsymbol{s}} \prod_{\alpha\in\mathcal{A}} p_\alpha^{s_\alpha}. \end{aligned} \tag{91}$$

Substitution into (90) yields an expression containing a independent integrals that can be evaluated analytically. Furthermore we re-arrange the x and z summations by introducing $j := x + z$,

$$\sum_{x=0}^\infty \sum_{z=0}^\infty f(x,z) = \sum_{j=0}^\infty \sum_{z=0}^j f(j-z, z). \tag{92}$$

Thus we obtain

$$\begin{aligned} I_1 = &\sum_{j=0}^\infty \sum_{\mathcal{A}\subset\mathcal{Q}:\, y\in\mathcal{A}} (-1)^{j+a} \tau^{j+\kappa a+\sigma_{\mathcal{A}}-\frac{1}{2}} B(\kappa\mathbf{1}_{q-a}+\boldsymbol{\sigma}_{\mathcal{B}}) \sum_{z=0}^j \binom{-\frac{1}{2}}{j-z} \\ &\binom{-1+\kappa[q-a]+\sigma_{\mathcal{B}}}{z} \sum_{\boldsymbol{s}\in\mathbb{N}^{\mathcal{A}}:\, s_{\mathcal{A}}=z} \binom{z}{\boldsymbol{s}} \left[\prod_{\alpha\in\mathcal{A}\setminus y} \frac{1}{\kappa+\sigma_\alpha+s_\alpha}\right] \\ &(\frac{\sigma_y}{\kappa+\sigma_y+s_y+j-z-\frac{1}{2}} - \frac{c_0\tau}{\kappa+\sigma_y+s_y+j-z+\frac{1}{2}}). \end{aligned} \tag{93}$$

We use the constraint $s_{\mathcal{A}} = z$ to eliminate the z-sum,

$$I_1 = \sum_{j=0}^{\infty} \sum_{\mathcal{A}\subset\mathcal{Q}:\ y\in\mathcal{A}} (-1)^{j+a} \tau^{j+\kappa a+\sigma_{\mathcal{A}}-\frac{1}{2}} B(\kappa \mathbf{1}_{q-a} + \boldsymbol{\sigma}_{\mathcal{B}}) \sum_{\boldsymbol{s}\in\mathbb{N}^{\mathcal{A}}:\ s_{\mathcal{A}}\leq j} \binom{-\frac{1}{2}}{j-s_{\mathcal{A}}}$$
$$\frac{\Gamma(\kappa[q-a]+\sigma_{\mathcal{B}})}{\Gamma(\kappa[q-a]+\sigma_{\mathcal{B}}-s_{\mathcal{A}})} \frac{1}{\prod_\alpha s_\alpha!} \left[\prod_{\alpha\in\mathcal{A}\setminus\{y\}} \frac{1}{\kappa+\sigma_\alpha+s_\alpha}\right]$$
$$\left(\frac{\sigma_y}{\kappa+\sigma_y+s_y+j-s_{\mathcal{A}}-\frac{1}{2}} - \frac{c_0\tau}{\kappa+\sigma_y+s_y+j-s_{\mathcal{A}}+\frac{1}{2}}\right) \tag{94}$$

Next we do a similar derivation for I_2. Integration over the '$\mathcal{B}$' degrees of freedom gives

$$I_2 = \sum_{x=0}^{\infty} \binom{-\frac{1}{2}}{x} \sum_{\mathcal{A}\subseteq\mathcal{Q}\setminus\{y\}} (-1)^{x+a} \int_0^\tau \mathrm{d}^a p_{\mathcal{A}}\, \boldsymbol{p}_{\mathcal{A}}^{-1+\kappa+\boldsymbol{\sigma}_{\mathcal{A}}} (1-P_{\mathcal{A}})^{-\frac{3}{2}+\kappa[q-a]+\sigma_{\mathcal{B}}+x}$$
$$\left\{\sigma_y B(\kappa\mathbf{1}+\boldsymbol{\sigma}_{\mathcal{B}}+\boldsymbol{e}_y[x-\tfrac{1}{2}]) - c_0(1-P_{\mathcal{A}})B(\kappa\mathbf{1}+\boldsymbol{\sigma}_{\mathcal{B}}+\boldsymbol{e}_y[x+\tfrac{1}{2}])\right\}. \tag{95}$$

Expansion of $(1-P_{\mathcal{A}})^{\cdots}$ as in (91) folowed by $\int \mathrm{d}^a p_{\mathcal{A}}$ integration yields

$$I_2 = \sum_{z=0}^{\infty} \sum_{\mathcal{A}\subseteq\mathcal{Q}\setminus\{y\}} (-1)^{z+a} \tau^{z+\kappa a+\sigma_{\mathcal{A}}} \left[\prod_{\beta\in\mathcal{B}\setminus\{y\}} \Gamma(\kappa+\sigma_\beta)\right]$$
$$\left[\sum_{x=0}^{\infty} \binom{-\frac{1}{2}}{x} (-1)^x \{\sigma_y \xi_x - c_0 \xi_{x+1}\}\right] \sum_{\boldsymbol{s}\in\mathbb{N}^{\mathcal{A}}:\ s_{\mathcal{A}}=z} \binom{z}{\boldsymbol{s}} \frac{1}{z!} \left[\prod_{\alpha\in\mathcal{A}} \frac{1}{\kappa+\sigma_\alpha+s_\alpha}\right]$$
$$\xi_x = \frac{\Gamma(\kappa+\sigma_y+x-\frac{1}{2})}{\Gamma(\kappa[q-a]+\sigma_{\mathcal{B}}-z+x-\frac{1}{2})}. \tag{96}$$

Finally we use the following identity to get rid of the x-sum,

$$\sum_{x=0}^{\infty} \binom{-\frac{1}{2}}{x} (-1)^x \frac{\Gamma(u+x)}{\Gamma(w+\frac{1}{2}+x)} = \frac{\Gamma(u)\Gamma(w-u)}{\Gamma(w-u+\frac{1}{2})\Gamma(w)}, \tag{97}$$

with $u = \kappa + \sigma_y - \frac{1}{2}$, $w = \kappa[q-a] + S_B - z - 1$.

A.5 Proof of Lemma 14

For $\tau = 0$, the $(q-1)$-dimensional integral $\mathbb{E}_p$ occurring in (48) can be evaluated exactly, yielding generalized Beta functions. These can be rearranged [25,22] to yield $M_0 =$

$$\mathbb{E}_{\boldsymbol{\sigma}}^{(0)}\left[\min_{y:\ \sigma_y\geq 1} \frac{\Gamma(\kappa+\sigma_y-\frac{1}{2})\Gamma(\kappa[q-1]+c_0-\sigma_y-\frac{1}{2})}{\Gamma(\kappa+\sigma_y)\Gamma(\kappa[q-1]+c_0-\sigma_y)} \{c_0(\tfrac{1}{2}-\kappa)+\sigma_y(\kappa q-1)\}\right]. \tag{98}$$

All the Gamma functions are positive, since $\sigma_y \geq 1$ causes all their arguments to be nonnegative. Furthermore, the condition $\kappa \in [\frac{1}{2(q-1)}, \frac{1}{2}]$ makes sure that the expression $\{\cdots\}$ is positive[12] at $\sigma_y \leq c_0 - 1$ and nonnegative at $\sigma_y = c_0$. That proves that $M_0 > 0$ independent of c_0.
It was shown in [25] that (98) is of order $\mathcal{O}(1)$ in the limit $c_0 \to \infty$. Finally, a series expansion of (98), of which we omit the details, shows that the correction to the leading order is $+\mathcal{O}(\frac{1}{c_0})$. □

A.6 Proof of Theorem 4

The case $q \geq 3$
We start from Lemma 13. The M_0 part follows from setting $z = 0$, $\mathcal{A} = \emptyset$ in I_2. We use the notation Y for the symbol choice y that achieves the minimum in (48). Note that Y is a function of $\boldsymbol{\sigma}$. For the sub-leading term, there are several competitors (1 to 4 listed below). Furthermore, there is a positive $\mathcal{O}(1/c_0)$ term from $M_0/M_0^\infty = 1+\mathcal{O}(1/c_0)$, which has to be taken into account as well.

[12] The case $q = 2, \kappa = \frac{1}{2}$ is special. Here the $\Gamma(-\frac{1}{2} + \kappa[q-1] + c_0 - \sigma_y)$ at $\sigma_y = c$ has to be combined with the expression $\{\cdots\} = 0$ in order to obtain a non-divergent value $0 \cdot \Gamma(0) = \Gamma(1) = 1$.

1. Set $j=0$, $\mathcal{A}=\{Y\}$ in I_1 and take the $\tau=0$ part of $\mathcal{N}$. This yields the following contribution to M:

$$\triangle M_1 = \frac{-1}{B(\kappa \mathbf{1}_q)} \sum_{\boldsymbol{\sigma}} \binom{c_0}{\boldsymbol{\sigma}} \tau^{\kappa+\sigma_Y-\frac{1}{2}} B(\kappa + \boldsymbol{\sigma}_{\mathcal{Q}\setminus\{Y\}}) \frac{\sigma_Y}{\kappa+\sigma_Y-1/2}. \tag{99}$$

We have to determine if it is possible for $\sigma_Y=1$ to occur, since this gives the lowest power of τ. Close inspection of the function W (52) reveals that asymptotically $W(c_0-1)-W(1)\to \frac{\sqrt{c_0}}{\sqrt{1-1/c_0}}(\kappa q-1)(1-2/c_0)$. For $\kappa>\frac{1}{q}$ we have $W(1)<W(c_0-1)$, which means that $\boldsymbol{\sigma}$-vectors of the form $(1,c_0-1,0,\cdots,0)$ will indeed lead to the selection of the symbol that occurs once, i.e. $\sigma_Y=1$. Furthermore, $W(c_0-2)<W(1)$, which means that the above form of $\boldsymbol{\sigma}$ is the only one that can yield $\sigma_Y=1$. Substitution of this form into (99) gives

$$\triangle M_1 = \frac{-\tau^{\kappa+\frac{1}{2}}}{B(\kappa \mathbf{1}_q)} \sum_{\boldsymbol{\sigma}} \sum_{y\in\mathcal{Q}} \delta_{\sigma_y,1} \sum_{\alpha\in\mathcal{Q}\setminus y} \delta_{\sigma_\alpha,c_0-1} \binom{c_0}{\boldsymbol{\sigma}} \frac{[\Gamma(\kappa)]^{q-2}\Gamma(\kappa+c_0-1)}{\Gamma(\kappa[q-1]+c_0-1)} \frac{1}{\kappa+\frac{1}{2}} \tag{100}$$

which reduces to the expression in the first row of the table. For $\kappa<1/q$ it does not occur that $\sigma_Y=1$, and $\triangle M_1$ (99) does not contain dominant contributions.

2. Take M_0 and the leading order correction to $\mathcal{N}(q,\kappa,0)$. From Corollary 6 we get

$$\triangle M_2 = M_0 \frac{q}{\kappa B(\kappa,\kappa q-\kappa)} \tau^\kappa. \tag{101}$$

Note that for $\kappa>1/q$ we have $\triangle M_2/\triangle M_1 = \mathcal{O}(1/c_0\sqrt{\tau}) \ll 1$.

3. Take $\mathcal{N}(q,\kappa,0)$ and set $\mathcal{A}=\emptyset$, $z=1$ in I_2. This yields a contribution

$$\triangle M_3 = c_0\tau \mathbb{E}^{(0)}_{\boldsymbol{\sigma}} \left[(\kappa q + c_0 -1) \frac{\Gamma(\kappa+\sigma_Y-\frac{1}{2})\Gamma(\kappa[q-1]+c_0-\sigma_Y-\frac{3}{2})}{\Gamma(\kappa+\sigma_Y)\Gamma(\kappa[q-1]+c_0-\sigma_Y-1)} \{\frac{\sigma_Y}{c_0}(2-\kappa q) - (\tfrac{1}{2}-\kappa)\} \right], \tag{102}$$

with $\mathbb{E}^{(0)}_{\boldsymbol{\sigma}}$ as defined in (41). Using Lemma 4 we see that $\triangle M_3$ is of order $\mathcal{O}(c_0\tau)$ when $\sigma_Y=\mathcal{O}(c_0)$ and even smaller if $\sigma_Y=\mathcal{O}(1)$. Thus for $\kappa>1/q$ we have $\triangle M_3/\triangle M_1 = o(\tau^{1/2-\kappa}) \ll 1$. In the case $\sigma_Y=\mathcal{O}(c_0)$ we can write

$$\triangle M_3 \to c_0\tau \mathbb{E}^{(0)}_{\boldsymbol{\sigma}} \left[\frac{\frac{\sigma_Y}{c_0}(2-\kappa q) - (\frac{1}{2}-\kappa)}{\sqrt{\frac{\sigma_Y}{c_0}(1-\frac{\sigma_Y}{c_0})}} \right]. \tag{103}$$

4. Take $\mathcal{N}(q,\kappa,0)$ and set $\mathcal{A}=\{\gamma\}$ (with $\gamma\neq Y$), $\sigma_\gamma=0$, $z=0$ in I_2. The contribution to M is

$$\begin{aligned}\triangle M_4 &= \frac{-\tau^\kappa}{\kappa} \mathbb{E}^{(0),q\to q-1}_{\boldsymbol{\sigma}} \left[\frac{\Gamma(\kappa+\sigma_Y-\frac{1}{2})\Gamma(\kappa[q-2]+c_0-\sigma_Y-\frac{1}{2})}{\Gamma(\kappa+\sigma_Y)\Gamma(\kappa[q-2]+c_0-\sigma_Y)} \{c_0(\tfrac{1}{2}-\kappa)+\sigma_Y(\kappa[q-1]-1)\} \right] \\ &= \frac{-\tau^\kappa}{\kappa} M_0^{q\to q-1} \end{aligned} \tag{104}$$

where the "$q\to q-1$" denotes that the alphabet has effectively been reduced by the exclusion of the symbol γ. The largest possible contributions occur when $\sigma_Y=1$ (case $\kappa>1/q$); the corresponding form of $\boldsymbol{\sigma}=(1,c_0-1,0,\cdots,0)$ happens with probability $\mathcal{O}(c_0^{-\kappa[q-1]})$. Again using Lemma 4 we conclude that $\triangle M_4 = \mathcal{O}(\tau^\kappa c_0^{1/2-\kappa[q-1]})$. We have $\triangle M_4/\triangle M_1 = \mathcal{O}(c_0^{-(\kappa q-1)-(1/2-\kappa)}/(c_0\sqrt{\tau}))$. Finally, with $\kappa q>1$,$\kappa<\frac{1}{2}$ and $c_0\sqrt{\tau}\to\infty$ we find $\triangle M_4 \ll \triangle M_1$.
In the case $\kappa<1/q$, we have $\sigma_Y=\mathcal{O}(c_0)$, yielding $\triangle M_4=\mathcal{O}(\tau^\kappa)$.

For $\kappa>1/q$, the $\triangle M_1$ is of larger order than $\triangle M_2$, $\triangle M_3$, $\triangle M_4$. Furthermore, $\triangle M_1$ is also of larger order than the $\mathcal{O}(1/c_0)$ correction. This is seen as follows: $c_0\tau^{\kappa+1/2}/[1/c_0]=(c_0\sqrt{\tau})(c_0\tau^\kappa)$; use $\kappa<1/2$ and $c_0\sqrt{\tau}\to\infty$.
For $\kappa<1/q$, the contestants are $\triangle M_3=\mathcal{O}(c_0\tau)$ ($\triangle M_3>0$) and $\triangle M_2+\triangle M_4=\mathcal{O}(\tau^\kappa)$. Their quotient is $\tau^\kappa/\triangle M_3 \sim c_0^{-1}\tau^{\kappa-1} \sim c_0^{-1+\nu(1-\kappa)}$.

- For $\nu<1/(1-\kappa)$, the $c_0\tau$ wins. Note that $c_0\tau$ dominates the $1/c_0$ correction, since $c_0\tau/[1/c_0]=(c_0\sqrt{\tau})^2$ with $c_0\sqrt{\tau}\to\infty$.
- For $\nu>1/(1-\kappa)$, the τ^κ wins. Note that τ^κ dominates the $1/c_0$ correction, since we have $\tau^\kappa/(1/c_0)\sim c_0^{1-\nu\kappa}$ with $\nu<1/\kappa$.

The case $q=2$

We start from Lemma 12. The τ^κ term in the last row of the table comes from taking all the p-integrals with $\tau=0$ and then dividing by $\mathcal{N}$ as given in Corollary 6.
All the other leading order corrections to M_0 are obtained from the Marking Assumption term (the first term) and from the $\sigma=1$ term in the summation; in both cases the correction can be computed as an integration $\int_0^\tau \mathrm{d}p(\cdots)$, and the leading order correction is proportional to $\int_0^\tau \mathrm{d}p\, p^{-1/2+\kappa}=\tau^{1/2+\kappa}/(1/2+\kappa)$. It turns out that for $\sigma=1$ the sign of the integral is $\mathrm{sgn}(1/2-\kappa-0^+)$. For $\kappa\geq\frac{1}{2}$ the leading order corrections add up, yielding $\mathcal{O}(c_0\tau^{1/2+\kappa})$. However, for $\kappa<\frac{1}{2}$ the leading order corrections cancel each other, and the next terms (of relative order $c_0\tau\ll 1$) become dominant.

A.7 Proof of Theorem 5

We give the proof case by case. We refer to the table in Theorem 4 as 'the table'.
$q \geq 3, \kappa \in (\frac{1}{q}, \frac{1}{2}), \nu \in (1, 2)$:
From line 1 of the table we get $\delta = \mathcal{O}(c_0 \tau^{1/2+\kappa}) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = \mathcal{O}(c_0^{1-\nu(1/2+\kappa)}) + \mathcal{O}(c_0^{\nu/2-1})$. The contributions are of the same order if we set $\nu = 2/(1+\kappa)$.
$q \geq 3, \kappa < \frac{1}{q}, \nu \in (1, \frac{1}{1-\kappa})$, assuming $\omega > 0$:
Line 2 of the table gives $\delta = \mathcal{O}(c_0\tau) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = \mathcal{O}(c_0^{1-\nu}) + \mathcal{O}(c_0^{\nu/2-1})$. The contributions are of the same order if we set $\nu = 4/3$. However, κ may be so small that $4/3$ lies outside the given range $\nu \in (1, \frac{1}{1-\kappa})$. In that case, the $\mathcal{O}(c_0^{1-\nu})$ wins and we want to make ν as large as possible.
$q \geq 3, \kappa < \frac{1}{q}, \nu \in (1, \frac{1}{1-\kappa})$, assuming $\omega < 0$:
We have $\delta = -\mathcal{O}(c_0\tau) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = -\mathcal{O}(c_0^{1-\nu}) + \mathcal{O}(c_0^{\nu/2-1})$. We want the $c_o\tau$ to win by as large a margin as possible. This is achieved by setting $\nu = 1 + 0^+$.
$q \geq 3, \kappa < \frac{1}{q}, \kappa < \frac{1}{4}, \nu \in (\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}], \omega < 0$:
Line 3 of the table gives $\delta = -\mathcal{O}(\tau^\kappa) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = -\mathcal{O}(c_0^{-\nu\kappa}) + \mathcal{O}(c_0^{\nu/2-1})$. By setting ν as small as possible, $\nu_* = \frac{1}{1-\kappa} + 0^+$, we let the negative term win as much as possible. This can be seen by comparing the powers: $-\nu_*\kappa - (\nu_*/2 - 1) = (\frac{1}{2} - 2\kappa)/(1-\kappa) - 0^+$, which is positive by virtue of $\kappa < \frac{1}{4}$.
$q \geq 3, \kappa < \frac{1}{q}, \kappa < \frac{1}{4}, \nu \in (\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}], \omega > 0$:
Now we have $\delta = +\mathcal{O}(c_0^{-\nu\kappa}) + \mathcal{O}(c_0^{\nu/2-1})$. The two terms are of equal order if we set $\nu = \frac{2}{1+2\kappa}$.
$q \geq 3, \kappa < \frac{1}{q}, \nu \in (\max\{\frac{1}{1-\kappa}, \frac{2}{1+2\kappa}\}, 2)$:
Now we have $\delta = \pm\mathcal{O}(c_0^{-\nu\kappa}) + \mathcal{O}(c_0^{\nu/2-1})$, but the second term always wins. The optimum is to set ν as small as possible.
$q = 2, \kappa \in [\frac{1}{2}, 1), \nu \in (1, \frac{4}{1+2\kappa})$:
Line 4 of the table gives $\delta = \mathcal{O}(c_0\tau^{1/2+\kappa}) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = \mathcal{O}(c_0^{1-\nu(1/2+\kappa)}) + \mathcal{O}(c_0^{\nu/2-1})$. The balance lies at $\nu = \frac{2}{1+\kappa}$, which is inside $(1, \frac{4}{1+2\kappa})$.
$q = 2, \kappa \in [\frac{1}{2}, 1), \nu \in (\frac{4}{1+2\kappa}, 2)$:
Line 5 of the table gives $\delta = \mathcal{O}(c_0^{-1}) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}})$. The c_0^{-1} always loses. The optimum is to set ν as small as possible.
$q = 2, \kappa < \frac{1}{2}, \nu \in (1, \frac{2}{1+2\kappa})$:
Line 6 of the table gives $\delta = -\mathcal{O}(\tau^\kappa) + \mathcal{O}(\frac{1}{c_0\sqrt{\tau}}) = -\mathcal{O}(c_0^{-\nu\kappa}) + \mathcal{O}(c_0^{\nu/2-1})$. Let $\kappa = \frac{1}{2} - \psi$ and $\nu = 1 + \varepsilon$. The negative term wins as long as $\varepsilon < \psi/(1-\psi)$.
$q = 2, \kappa < \frac{1}{2}, \nu \in (\frac{2}{1+2\kappa}, 2)$:
Again we have $\delta = -\mathcal{O}(c_0^{-\nu\kappa}) + \mathcal{O}(c_0^{\nu/2-1})$, but now the positive term always wins. The optimum is to set ν as small as possible.

A.8 Proof of Theorem 6

Lemma 12 (from which the correction terms were derived) is applicable only for $\tau < \varepsilon/c_0$. This translates to $Tc_0^{-\rho} < \varepsilon$, i.e. $c_0 > (T/\varepsilon)^{1/\rho}$. This explains the condition on c_0. Applying a Taylor expansion to Corollary 7 for $\psi = -\varepsilon$ gives

$$\frac{\Gamma(1-\varepsilon)}{\Gamma(\frac{1}{2}-\varepsilon)} = \frac{1}{\sqrt{\pi}}[1 - \varepsilon \cdot 2\ln 2 + \mathcal{O}(\varepsilon^2)], \tag{105}$$

which leads to the factor after $\frac{\pi^2}{2}$ in (64). In Theorem 6, the quotient of the positive correction term divided by the negative one is $\frac{1}{6T} c_0^{-\varepsilon+\rho(1-\varepsilon)}$. The condition $\rho < \varepsilon/(1-\varepsilon)$ makes sure that the negative correction term dominates for sufficiently large c_0. The above mentioned quotient is smaller than 1 for $c_0 > (1/6T)^{1/(\varepsilon-\rho+\varepsilon\rho)}$.

A.9 Proof of Theorem 7

τ is given. We define $r = c_0\sqrt{\tau}(MA - B)/\eta$, with $r \geq 0$. Instead of the variables (A, B) we consider (A, r) as our independent variables of interest. We are allowed to apply Corollary 4, since the condition $MA - B > 0$ is satisfied by the A, B solution given in Theorem 7. Using Corollary 4 and $V^2 < q$ (Lemma 1), we find

$$A \le f_2(\tau, r) \implies P_{\rm FN} \le \varepsilon_2. \tag{106}$$

Rewriting (22) in terms of A, r is a bit more laborious. It results in a quadratic inequality for A,

$$0 \le \frac{M^2}{2}A^2 - A\left\{1 + \frac{M}{c_0\sqrt{\tau}}(\frac{1}{3} + \eta r)\right\} + \frac{\eta r}{c_0^2\tau}(\frac{1}{3} + \frac{1}{2}\eta r) \qquad \implies \qquad P_{\rm FP} \le \varepsilon_1. \tag{107}$$

The quadratic function in A has two positive roots. We concentrate on the largest root,

$$A \ge f_1(\tau, r) \qquad \implies \qquad P_{\rm FP} \le \varepsilon_1. \tag{108}$$

We have $f_1(\tau, 0) > 0$, $f_2(\tau, 0) = 0$, $\frac{\partial f_1}{\partial r}(\tau, r \to \infty) = 2\eta/(Mc_0\sqrt{\tau})$ and $\frac{\partial f_2}{\partial r}(\tau, r \to \infty) = \eta/(eqc_0\tau)$. Since it was given that $\sqrt{\tau} < \frac{M}{2eq}$, it holds at large enough r that $\partial f_2/\partial r > \partial f_1/\partial r$. Hence there exists a point $r_*(\tau)$ where $f_1(\tau, r_*) = f_2(\tau, r_*)$. See Fig. 3. The value $r_*(\tau)$ is the smallest value of r for which both conditions $A \ge f_1(\tau, r)$ and $A \le f_2(\tau, r)$ can hold simultaneously. □

A.10 Proof of Theorem 8

We have the following derivatives,

$$\frac{\partial f_2}{\partial \tau} = -\frac{1}{\tau}f_2 < 0 \qquad \frac{\partial f_2}{\partial r} = \frac{r+1}{r^2}f_2 > 0 \qquad \frac{\partial f_1}{\partial r} = \frac{\eta}{Mc_0\sqrt{\tau}}(1 + \frac{1}{2\sqrt{D}}) > 0. \tag{109}$$

The implicit function theorem gives us

$$\frac{{\rm d}r_*(\tau)}{{\rm d}\tau} = -\left.\frac{\partial(f_1 - f_2)/\partial\tau}{\partial(f_1 - f_2)/\partial r}\right|_{r=r_*(\tau)}. \tag{110}$$

Minimizaton of $A = f_2(r_*)$ with respect to τ can be written as

$$0 = \frac{{\rm d}f_2(\tau, r_*(\tau))}{{\rm d}\tau} = \frac{\partial f_2}{\partial \tau}(\tau, r_*) + \frac{\partial f_2}{\partial r}(\tau, r_*)\frac{{\rm d}r_*(\tau)}{{\rm d}\tau}. \tag{111}$$

Substitution of (110) and the $\partial f_2/\partial\tau$ and $\partial f_2/\partial r$ from (109) into (111) yields

$$0 = -\frac{1}{\tau}f_2(\tau, r_*) - \frac{r_* + 1}{r_*^2}f_2(\tau, r_*)\left.\frac{\partial(f_1 - f_2)/\partial\tau}{\partial(f_1 - f_2)/\partial r}\right|_{r=r_*(\tau)}. \tag{112}$$

Multiplication by τ/f_2 and some slight rearranging yields the end result. □

A.11 Proof of Theorem 9

The idea is to pick a value $\hat{r}$ (75) slightly larger than r_*, and set A to some value $\hat{A} \in [f_1(\tau, \hat{r}), f_2(\tau, \hat{r})]$. The condition (70) is necessary so that we can use Theorem 7.
We introduce the abbreviation $y = \ln[\ln(1/c_0\tau)\frac{2eq}{M^2\eta}]/\ln(1/c_0\tau)$. The condition (71) ensures that $y < 1$. We then have

$$f_2(\tau, \hat{r}) = \frac{2}{M^2}\cdot\frac{1}{1-y} > \frac{2}{M^2}(1+y). \tag{113}$$

Condition (71) also ensures that $\hat{r} < 1$. For f_1 we get

$$f_1(\tau, \hat{r}) \le \frac{2}{M^2}\left[1 + \frac{M}{3c_0\sqrt{\tau}}(1 + 3\eta\hat{r})\right] < \frac{2}{M^2}\left[1 + \frac{M}{3c_0\sqrt{\tau}}(1 + 3\eta)\right], \tag{114}$$

where the first inequality follows from neglecting a part of the determinant D (67) and the second inequality from $\hat{r} < 1$. Condition (72) ensures that the lower bound on $f_2(\tau, \hat{r})$, i.e. the last expression in (113), lies higher than the upper bound on $f_1(\tau, \hat{r})$, so that indeed we have $f_2(\tau, \hat{r}) > f_1(\tau, \hat{r})$ as planned. Furthermore, the first inequality in (114), together with the definition of $\hat{A}$ in (73) tells us that indeed $f_1(\tau, \hat{r}) < \hat{A} < f_2(\tau, \hat{r})$. The choice for B follows by setting $\hat{B} = M\hat{A} - \frac{\eta\hat{r}}{c_0\sqrt{\tau}}$ just as in Theorem 7. □