Abstract

There has been considerable recent interest in probabilistic packet marking schemes for sending information from nodes (routers) along one or more paths traveled by a stream of packets to the end-host receiving that stream. Such schemes have a number of possible uses, including tracing a sequence of network packets back to an anonymous source. A central consideration for such schemes is the tradeoff between the number B of possible states of the marking bits in a packet($B = 2^b$ if b bits are allocated for the marking), the number of bits n of information being sent by the nodes, and the expected number of packets T required to reconstruct this information. For the case where the packets all travel along the same path, we prove a lower bound of $T \geq \Omega(B2^{2n/(B-1)})$, roughly the square of an earlier lower bound of Adler.

For an upper bound, we consider a model where each of m nodes along a single path must send one of s possible messages (thus $n = m \log_2 s$ total bits are sent). We prove that $T \leq O(m \cdot 2^{2m(\log_2 s)/(B-1)})$ suffices (the implicit constant depends on B and s); this almost matches the lower bound, and is roughly the square root of an earlier upper bound of Adler. The new bound holds for all B and s in two slightly relaxed models, while under the strictest requirements we prove it only for some special values of B and s. This is related to a challenging geometric problem: the existence of an s-reptile $(B-1)$-dimensional simplex, i.e. a simplex S that can be tiled by s congruent simplices similar to S. We also arrive at interesting open problems concerning matrices.

We also consider the case where the packets travel along multiple paths to the same destination. In this case, we present a new protocol and analysis technique that together allow us to significantly generalize over previous work the scenarios where the protocol is effective.

1 Introduction

Probabilistic packet marking (PPM) is a recently discovered, powerful technique for extracting information from nodes (typically routers) along a path travelled by a sequence of packets. In PPM, a small number of header bits in each packet is reserved for this transfer of information, and each node along the path can update these header bits. The goal is to inform the node of the network that receives the sequence of packets of some information stored in a distributed fashion across the nodes along the path. For example, a simple case is where each node along the path has a single bit of information to send to the receiving node. The challenge (and power) of this technique is that each of the intermediate nodes is required to perform this transmission in a memoryless fashion: it can only update the header bits to a value based on its own piece of information, the value of the header bits on the incoming packet, and some number of random bits.

The memoryless requirement is crucial in a network such as the Internet, where routers typically handle a large number of simultaneous flows of packets, and thus it is not conceivable to have per-flow state. This requirement also means that the nodes must mark the packets probabilistically. PPM was first suggested in [4], with the first extensively analyzed protocols being introduced in [17]. This early work used PPM to solve the IP Traceback problem: determine the source of a stream of packets that hides its origin by "spoofing" the source node field in the packet header. Solutions to the IP Traceback problem are crucial to combating Denial-of-Service attacks.

Such a scenario leads to two additional difficulties for designing a PPM scheme. First, a malicious *adversary* sets the initial value of all header bits in the packet, including those allocated to PPM, and thus this adversary will attempt to use this ability to hide the information being transmitted. We henceforth refer to the node receiving the stream of packets, which is trying to determine this information, as the *victim*. Second, many Denial-of-Service attacks are performed in a distributed fashion, with multiple sources sending packets to the victim. In such a scenario, a PPM scheme must be able to handle packets arriving at the victim along multiple paths, where each path has different information to send to the victim, but the victim is not able to determine the path travelled by a given packet.

The application of PPM to the IP Traceback problem has generated considerable interest in this technique [6, 16, 19, 12, 8, 11, 9]. Furthermore, PPM has the potential to be useful in a number of other scenarios as well: congestion control [2], robust routing [6], dynamic network configuration [6], and identification of bottleneck routers [9].

In addition to the potential practical impact of PPM schemes, it turns out that designing optimal PPM techniques is an interesting theoretical problem. In particular, [1] demonstrates that there are inherent tradeoffs between the parameters s, B, m, k, and T, which are defined as follows.

- We assume that each node is given one element from a set of size $s \geq 2$, and it must inform the victim of which element it has.
- We also assume that the header bits can take on B different values. If all possible settings of b binary bits are available, then $B = 2^b$. Let us remark that in [20], an application of packet marking to congestion control is described where $B = 3$, since two bits are available, but one of the possible settings of these bits is reserved for another use.
- We assume that there are m nodes along a path.
- The parameter k represents the number of paths being used by the adversary.
- Finally, T is the number of packets that the victim must receive to reliably reconstruct the messages from the nodes.

In [1], the following results quantifying the tradeoffs between these parameters are presented. For the case where $k = 1$ (i.e., all packets travel along the same path), $s = 2$, and $B = 2^b$ for an integer b, $T \leq 2^{(4+o(1))n/B}$ packets are sufficient with high probability (here $n = m$). An information-theoretic lower bound shows that $T \geq 2^{(1-o(1))n/B}$

*** Should we write these bounds more explicitly??

is necessary, for any values of s and m such that $n = m \log s$. For the case of multiple paths, $B \geq 2k - 1$ must hold, regardless of how large T is. Furthermore, if the adversary sets the initial marking bits to 0 in every packet, then there is a protocol with $B \leq 2k + 1$.

In this paper, we provide several significant improvements to the results of [1]. For the case of a single path, we prove a new lower bound, demonstrating that $T \geq \Omega(B2^{2n/(B-1)})$ packets are necessary, for any values of s and m such that $n = m \log s$. This value is roughly the square of the lower bound shown in [1], and, for the case $B = 2$, matches an upper bound provided in [1].

For brevity, we call protocols (upper bounds) *quasioptimal* if $T \leq 2^{(2+o(1))n/(B-1)}$ is sufficient with high probability. For quasioptimality, we consider k, s and B fixed, and thus asymptotic notation refers to $m \to \infty$. Note that quasioptimality refers to the asymptotics of the exponent and thus leaves plenty of room for improvement, especially for small values of m.

In our efforts to achieve quasioptimality, we provide a reduction from the PPM problem for a given s and B to the problem of finding a $(B-1)$-dimensional simplex that is an *s-reptile*; that is, it can be partitioned into s equal sized pieces all congruent and similar to the whole. This allows us to use known results on s-reptiles to provide quasioptimal protocols for various values of s and B. In particular, we show that if $B = 3$ and s is of the form 2, i^2, $3i^2$, or $i^2 + j^2$ for integers i and

j or if $B \geq 4$ is arbitrary and $s = i^{B-1}$, then there is a quasioptimal protocol. The upper bound provided by these protocols is roughly the square root of the bound shown in [1].

The reduction to finding s-reptiles also allows us to provide a new protocol for the scenario where the marking bits are restricted in their initial distribution. This would be the case in cooperative scenarios, such as applying PPM to congestion control, where the source of the packets sets the initial bits in a predictable fashion. We demonstrate that in this scenario, $T \leq O(s^2 B^2 2^{2m(\log_2 s)/(B-1)})$ is sufficient for any values of B and s. This differs from the new lower bound (which also applies to this cooperative scenario) by a factor of only $s^2 B$, and thus the dependence on m is asymptotically optimal for this scenario. A similar technique also achieves quasioptimality for any values of B and s if the adversary sets the value of the initial bits, but the victim is allowed to lose the information held by a few nodes farthest from it.

Finally, we turn to the case of multiple paths. We remove the assumption made in the protocols of [1] that the adversary sets the initial marking bits to 0 in every packet. While such restrictions on the initial distribution are natural for some scenarios of the single path case, the multiple path case is mostly motivated by Denial-of-Service attacks, and thus the most relevant case is where a malicious adversary is setting the initial value of the header bits. We here introduce a protocol where $B \leq 2k + 1$ is still sufficient, but this protocol makes two alternative assumptions that are much more realistic in terms of the application of PPM to IP Traceback. First, we assume that the element of the set of size s at each of the nodes are chosen randomly (instead of allowing the adversary to choose worst case elements). Note that this is a reasonable assumption for IP Traceback in the Internet, since an adversary cannot chose arbitrary nodes to corrupt; rather, it is only able to target nodes that are compromised. Second, we assume that the intermediate nodes have a small amount of information concerning their location along the path of attack. The exact assumption is described below; this is also a reasonable assumption in the Internet. The lower bound of $B \geq 2k - 1$ from [1] still applies to this case.

2 Models for the PPM Problem

We first describe the model we use for the protocols. For the case of a single path of attack, we assume that packets are traveling across a sequence of intermediate nodes. We shall refer to the node on the path from the victim to the adversary at distance i from the victim as N_i (where the victim is N_0, and the adversary is N_{m+1}). Each node has one of exactly s values to send to the victim. We shall refer to this information as $W = w_1 w_2 \ldots w_m$, where $w_i \in [s]$ indicates the value known by N_i.

Information is sent to the victim via the header bits in the packets traveling from the adversary to the victim. We ignore the contents of each packet other than that allocated to PPM, and thus we simply assume that each packet can take on exactly one of B values. Each node can update the contents of each packet that it forwards towards the victim. However, this update can only be based on the contents of the incoming packet, the value the node holds locally, and probabilistic choices made by the node. The victim does have storage. Typically, we assume that the contents of the packet received by the node N_m is set by a malicious adversary N_{m+1}. However, as was described above, we sometimes assume that the initial distribution of packets is restricted.

For the case of multiple paths, we assume the same model, except that now there are up to k different paths, each of which contains a different set of m nodes. Thus, there are as many as km values that the victim must determine. Each packet travels along one of the k paths, and the contents of that packet can be updated by the nodes along that path. The adversary chooses which path each packet travels on; the victim only sees the contents of the final packet it receives - it does not know which path that packet traveled on. After receiving sufficiently many packets, the victim attempts to determine the strings that were on paths used for a fraction of at least $\frac{\alpha}{k}$ of the packets, for a parameter $\alpha \leq 1$. We provide more details on this model in Section 6.

For the lower bound, we assume a stronger model (i.e., a model where the problem is at least as easy to solve as in the model for the protocols). For the lower bound model, we assume a system consisting of only two parties, called the *Victim* and the *Network*, where we here capitalize Victim to distinguish it from the victim of the upper bound model. The Network has an n-bit string to send to the victim. No communication occurs from the victim to the Network. The Network is allowed to send B-valued packets to the victim, but it is stateless: for each packet it sends, it has no memory of the previous packets that it has sent. This lower bound model actually captures the difficulty of sending information from a memoryless node using packets consisting of a bounded number of bits.

Note that any protocol for the upper bound model implies a protocol for this model as well, and thus lower bounds for this model imply lower bounds for the protocol model. In fact, it might seem like this model is quite a bit more powerful: there is no adversary setting the initial bits of the packets and all of the information to be transmitted is stored at a single node. Despite these seeming advantages, we can prove lower bounds in this model that are close to matching the upper bounds shown in the model for the protocols.

3 Protocols for a Single Path of Attack

Theorem 1 *If (B, s) has one of the forms $(2, i)$, $(3, i^2)$, $(3, 3i^2)$, $(3, i^2 + j^2)$, (i, j^{i-1}) for positive integers i, j, then there is a protocol that recovers all values along the path with high probability as long as the victim receives at least*

$$T \geq Cm \cdot 2^{2m(\log_2 s)/(B-1)}$$

packets, with a suitable constant C depending on B and s. In particular, the protocol is quasioptimal.

Encoding in the probability distribution of packets. The basic idea, introduced in [1], is to encode the given sequence $W \in [s]^n$ into the probability distribution of the packets received by the victim. This probability distribution can be specified by a vector $X = (x_1, x_2, \dots, x_B)$, where x_u is the probability that a packet reaching the victim has value $u \in [B]$. Geometrically, such an X can be regarded as a point of the $(B-1)$-dimensional standard simplex

$$\Delta^{B-1} = \{(x_1, x_2, \dots, x_B) \in \mathbf{R}^B : x_1, x_2, \dots, x_B \geq 0, x_1 + x_2 + \cdots + x_B = 1\}$$

in $\mathbf{R}^B$ (for example, for $B = 3$, Δ^2 is an equilateral triangle placed in $\mathbf{R}^3$).

If the victim receives sufficiently many packets, then he can "read off" the incoming distribution X with a prescribed precision. This allows him to distinguish between different sets of possible distributions, and is expressed quantitatively in the following lemma.

Lemma 2 *Let $X \in \Delta^{B-1}$ be a distribution of the packets. Suppose that the victim receives T packets generated according to X, let Z_u be the number of received packets with value u, $u \in [B]$, and let $Y = (\frac{Z_1}{T}, \frac{Z_2}{T}, \dots, \frac{Z_B}{T})$. Let $\beta > 0$ and $a > 0$ be real parameters (that can be chosen at will) and suppose that $T \geq a/\beta^2$. Then the probability that $\|X - Y\| \geq \beta$ is at most $1/a$.*

Proof: We calculate that the expectation $\mathrm{E}\left[\|X-Y\|^2\right] = 1/T$; then the claim follows from Markov's inequality. By linearity of expectation we have

$$\begin{aligned} \mathrm{E}\left[\|X-Y\|^2\right] &= \sum_{u=1}^{B} \mathrm{E}\left[(x_u - Z_u/T)^2\right] \\ &= T^{-2}\sum_{u=1}^{B} \mathrm{E}\left[(Tx_u - Z_u)^2\right]. \end{aligned}$$

The term in the sum is the variance of Z_u. Now Z_u is the sum of T independent random variables, each attaining value 1 with probability x_u and value 0 with probability $1-x_u$, and its variance is thus bounded above by Tx_u. Hence $\mathrm{E}\left[\|X-Y\|^2\right] \le T^{-1}\sum_{u\in B} x_u = 1/T$. ■

Protocols as affine maps. Now the main question is, how can the nodes encode their messages into the probability distribution of packets received by the victim? Each node, being memoryless, has no way of "knowing" the distribution of the incoming packets. It has to process one packet at a time in a uniform way (but, of course, depending on the message $w \in [s]$ it wants to send). Having received a packet with value u, it must choose in a probabilistic way some value v to put in the packet that it sends. Let $p_{w,uv}$ be the (fixed) probability that when it receives $u \in [B]$, it sends $v \in [B]$. The behavior of the node is fully specified by the choice of $p_{w,uv}$ for every $w \in [s]$ and $u, v \in [B]$. Any such choices that obey the natural restrictions $p_{w,uv} \in [0,1]$ and $\sum_{v\in B} p_{w,uv} = 1$ can be implemented.

Let us assume that the $p_{w,uv}$ are fixed, and that all nodes N_i, $i = 1, 2, \ldots, m$, follow the same protocol given by these values. If the packets reaching N_i have some probability distribution $X_i \in \Delta^{B-1}$, then the packets leaving it have the distribution X_{i-1} given by

$$X_{i-1,v} = \sum_{u\in[B]} p_{w,uv} \cdot X_{i,u}, \tag{1}$$

where $w \in [s]$ is the message N_i wants to send. In other words, we have $X_{i-1} = f(X_i)$, where $f_w\colon \Delta^{B-1} \to \Delta^{B-1}$ is the affine map given by (1). We note that *any* affine map $f\colon \Delta^{B-1} \to \Delta^{B-1}$ can appear as f_w. Indeed, given such an f, the corresponding $p_{w,uv}$ is the vth coordinate of $f(\mathbf{e}_u)$, where $\mathbf{e}_u = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ (with the 1 at position u) is the uth vertex of Δ^{B-1}.

We prefer this way of regarding the protocol executed by the nodes as affine maps. Thus, by a **protocol** for the nodes we mean an s-tuple $F = (f_1, f_2, \ldots, f_s)$ of affine maps $\Delta^{B-1} \to \Delta^{B-1}$, where f_w is the map "executed" by a node with message $w \in [s]$.

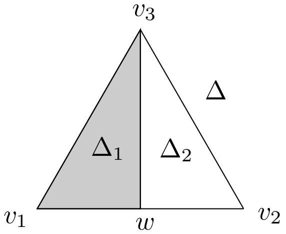
If the adversary (node N_{m+1}) sends packets to N_m with some distribution X_m, the path is described by the string $W = w_1 w_2 \cdots w_m \in [s]^m$, and each node N_i, $i = 1, 2, \ldots, m$, follows the protocol F, then the distribution X_0 "seen" by the victim is $f_W(X_m)$, where f_W is the composed map $f_{w_1} \circ f_{w_2} \circ \cdots \circ f_{w_m}$. In this section we assume X_m arbitrary, i.e., the adversary is free to choose any initial distribution.

Definition 3 *A protocol F as above has **m-step resolution** at least β if for every two distinct strings $W, W' \in [s]^m$, the (Euclidean) distance of the sets $f_W(\Delta^{B-1})$ and $f_{W'}(\Delta^{B-1})$ is at least β.*

By Lemma 2, if F has m-step resolution at least some $\beta > 0$, then the victim can reconstruct the string sent by the m nodes (with probability close to 1) after receiving $T = O(1/\beta^2)$ packets, no matter what initial distribution X_m the adversary chooses. Thus, in order to prove Theorem 1, it suffices to exhibit protocols F with m-step resolution $\Omega(m^{-1}s^{-m/(B-1)})$ for the values of B and s

listed in the theorem. An easy volume argument shows that no protocol can have m-step resolution better than $O(s^{-m/(B-1)})$ (the constant in the $O(\cdot)$ notation may depend on B and s).
*** Even the lower bound of $\Omega(m^{-1/(B-1)}s^{-m/(B-1)})$ can be proved, I believe. To be worked out. Jirka

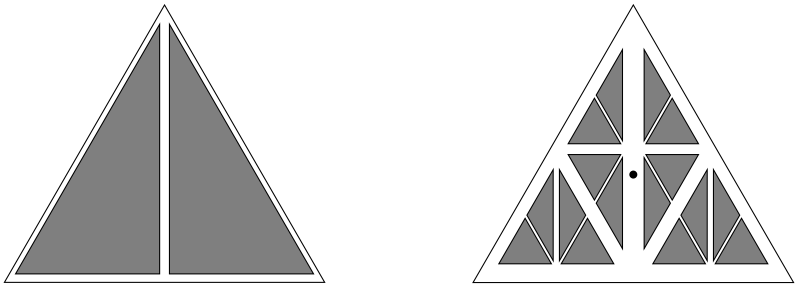
An example. To describe our protocol constructions, we begin with an example where $B = 3$ and $s = 2$. Let $a_1 = \mathbf{e}_1$, $a_2 = \mathbf{e}_2$, $a_3 = \mathbf{e}_3$ be the vertices of the equilateral triangle Δ^2. First we introduce two auxiliary affine maps $g_1, g_2\colon \Delta^2 \to \Delta^2$. The map g_1 is given by $g_1(a_1) = a_1$, $g_1(a_2) = a_3$, and $g_1(a_3) = \bar{a} = \frac{1}{2}(a_1 + a_2)$:



The image $g_1(\Delta^2)$ is the gray triangle Δ_1. Similarly, g_2 is given by $g_2(a_1) = a_3$, $g_2(a_2) = a_2$, $g_2(a_3) = \bar{a}$, and it maps Δ^2 to Δ_2.

For an affine map $f\colon \Delta^{B-1} \to \Delta^{B-1}$, a point $c \in \Delta^{B-1}$, and a real number $\varepsilon \in (0, 1)$, we define the $(1 - \varepsilon)$-*shrinking* of f (with center c) as the affine map $\tilde{f}\colon \Delta^{B-1} \to \Delta^{B-1}$ given by $\tilde{f}(x) = f((1 - \varepsilon)(x - c) + c)$. Intuitively, we first shrink Δ^{B-1} by the factor $1 - \varepsilon$ from the center c and then we apply f.

Continuing with our example, we let c be the center of gravity of Δ^2, we choose a small $\varepsilon > 0$, and we define f_u as the $(1 - \varepsilon)$-shrinking of g_u, $u = 1, 2$. In the illustration below we have $\varepsilon = 0.1$, f_1 maps Δ^2 to the shaded left triangle in the left figure and f_2 maps it to the right shaded triangle:



For $m = 4$, the sets $f_W(\Delta^2)$ for the 16 different strings $W \in [s]^m = [2]^4$ are the 16 small shaded triangles in the right figure.

We claim that if we set $\varepsilon = \frac{1}{m}$ in the above construction, then the m-step resolution of $F = (f_1, f_2)$ is $O(m^{-1}2^{-m/2})$; thus, it is quasioptimal (for $s = 2$ and $B = 3$). The definition below captures properties of g_1 and g_2 used in the proof of this fact, and we state it for arbitrary B and s.

α-tilings. First we introduce, for a map $f\colon \Delta^{B-1} \to \Delta^{B-1}$, the quantity $\operatorname{contr}(f)$, which is defined to be the smallest factor by which f contracts distances; that is,

$$\operatorname{contr}(f) = \inf_{x,y \in \Delta^{B-1}, x \neq y} \frac{\|f(x) - f(y)\|}{\|x - y\|}.$$

Definition 4 *Let $g_1, g_2, \ldots, g_s : \Delta^{B-1} \to \Delta^{B-1}$ be affine maps such that the sets $g_u(\Delta^{B-1})$ for $u \in [s]$ have disjoint interiors. Let $\alpha \in (0,1)$. We call $(g_1, g_2, \ldots, g_s)$ an **α-tiling** (of Δ^{B-1}) if for all $m \geq 1$ and for each $W \in [s]^m$ we have* $\operatorname{contr}(g_W) \geq \delta\alpha^{-m}$ *for a positive constant δ (independent of m but possibly depending on B, s, and the g_u). An $s^{-1/(B-1)}$-tiling is called an **asymptotically optimal tiling**.*

The following lemma shows that a suitable shrinking of an asymptotically optimal tiling leads to quasioptimal protocols.

Lemma 5 *Let $(g_1, \ldots, g_s)$ be an α-tiling of Δ^{B-1} and let c be an interior point of Δ^{B-1}. For a given m and $u \in [s]$, let f_u be the $(1 - \frac{1}{m})$-shrinking of g_u with center c. Then the protocol $(f_1, \ldots, f_s)$ has m-step resolution at least $\Omega(m^{-1}\alpha^m)$ (implicit constants depending on the g_u and on c).*

Proof: Let us write $\varepsilon = \frac{1}{m}$. First we check that $\operatorname{dist}(f_u(\Delta^{B-1}), f_v(\Delta^{B-1})) \geq \beta\varepsilon$ for any $u \neq v$, $u, v \in [s]$, and a constant $\beta > 0$ independent of ε. Indeed, $g_u(\Delta^{B-1})$ is a simplex containing $g_u(c)$ in its interior, thus $f_u(\Delta^{B-1})$ has distance at least $\beta\varepsilon$, for a suitable $\beta > 0$, from the complement $\mathbf{R}^d \setminus g_u(\Delta^{B-1})$, and hence also from $f_v(\Delta^{B-1}) \subseteq g_v(\Delta^{B-1})$, since $g_u(\Delta^{B-1})$ and $g_v(\Delta^{B-1})$ have disjoint interiors.

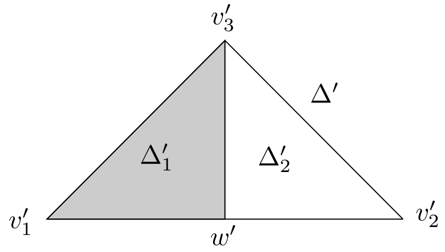
Now we consider arbitrary words W and W' of length m and we let t be the first position where they differ; that is, we can write $W = UuV$ and $W' = UvV'$, $u \neq v$ (so U has length $t-1$). Then we have

$$\begin{aligned}
\operatorname{dist}(f_W(\Delta^{B-1}), f_{W'}(\Delta^{B-1})) &\geq \operatorname{contr}(f_U) \cdot \\
&\qquad \operatorname{dist}(f_u(f_V(\Delta^{B-1})), f_v(f_{V'}(\Delta^{B-1}))) \\
&\geq (1-\varepsilon)^{t-1}\delta\alpha^t \cdot \operatorname{dist}(f_u(\Delta^{B-1}), f_v(\Delta^{B-1})) \\
&\geq (1-\varepsilon)^m \delta\alpha^m \cdot \beta\varepsilon \\
&= \beta\delta \left(1 - \frac{1}{m}\right)^m \frac{1}{m} \cdot \alpha^m \\
&= \Omega\left(m^{-1}\alpha^m\right).
\end{aligned}$$

Lemma 5 is proved. ■

For our example above, it remains to verify that (g_1, g_2) is an asymptotically optimal tiling. The condition that is not obvious is $\operatorname{contr}(g_W) \geq \Omega(2^{-m/2})$ for all $W \in [2]^m$. It can be checked by direct geometric arguments, but we offer a more conceptual proof that generalizes easily.

Let us consider the affine map h that maps the right isosceles triangle S to the equilateral triangle Δ^2, with $h(a'_j) = a_j$:



The map $r_1 = h^{-1} \circ g_1 \circ h\colon S \to S$ maps S to its left half S_1, and $r_2 = h^{-1} \circ g_2 \circ h$ maps S to S_2. The important point is that both S_1 and S_2 are similar to S with ratio $2^{-1/2}$, and r_1 and r_2 are isometries followed by scaling by the factor $2^{-1/2}$. Hence $\mathrm{contr}(r_W) = 2^{-m/2}$ for any $W \in [2]^m$. For g_W we then have

$$\begin{aligned} g_w &= g_{w_1} \circ g_{w_2} \circ \cdots \circ g_{w_n} \\ &= h \circ r_{w_1} \circ h^{-1} \circ h \circ r_{w_2} \circ h^{-1} \circ \cdots \circ h \circ r_{w_n} \circ h^{-1} \\ &= h \circ r_W \circ h^{-1}. \end{aligned}$$

Therefore $\mathrm{contr}(g_W) \geq \mathrm{contr}(h) \cdot \mathrm{contr}(r_W) \cdot \mathrm{contr}(h^{-1}) = \Omega(2^{-n/2})$, and we have thus verified that (g_1, g_2) is an asymptotically optimal tiling.

We conclude the discussion of our example by remarking that there are several affine maps that map the equilateral triangle Δ^2 to its left half Δ_1, and not all of them can be chosen for g_1 if we want to get an asymptotically optimal tiling. For example, if we defined $g_1(a_1) = a_1$, $g_1(a_2) = \bar{a}$, and $g_1(a_3) = a_3$, then the image of Δ^2 under an m-fold iteration of g_1 would be much too flat.

Asymptotically optimal tilings and simplex *s*-reptiles. The technique for showing that our example yields an asymptotically optimal tiling can be generalized in an obvious manner and it connects the problem to a classical area of combinatorial geometry.

The following notion has been studied in various contexts (see, e.g., [3, 18, 10, 15]): A closed set $S \subset \mathbf{R}^d$ with nonempty interior is called an ***s*-reptile** (sometimes written "s rep tile" or "s rep-tile") if there are sets $S_1, S_2, \ldots, S_s$ with disjoint interiors and with $S = S_1 \cup S_2 \cup \cdots \cup S_s$ that are all congruent and similar to S. For each S_u, let $r_u\colon S \to S_i$ be an affine map of S onto S_u that witnesses the similarity of S_u to S; that is, it is an isometry followed by scaling by the factor $s^{-1/d}$. We call $r_1, r_2, \ldots, r_s$ a *reptiling map system* of S. (If S has a symmetry, then the reptiling map system is not unique.)

The above example was based on the fact that the right isosceles triangle S is a 2-reptile. The following result establishes a close connection between asymptotically optimal tilings and simplex reptiles:

Theorem 6 (i) *Let S be a $(B-1)$-dimensional simplex that is an s-reptile, and let $h\colon S \to \Delta^{B-1}$ be an affine bijection. Let us put $g_u = h \circ r_u \circ h^{-1}$, $u \in [s]$. Then $(g_1, g_2, \ldots, g_s)$ is an asymptotically optimal tiling of Δ^{B-1}.*

(ii) *Every asymptotically optimal tiling of Δ^{B-1} can be obtained from some s-reptile simplex as in* (i). *Moreover, given affine maps $g_1, g_2, \ldots, g_s\colon \Delta^{B-1} \to \Delta^{B-1}$ such that the sets $g_u(\Delta^{B-1})$ have disjoint interiors, it can be checked in polynomial time whether $(g_1, \ldots, g_s)$ is an asymptotically optimal tiling.*

The algorithmic claim in (ii) should be understood properly: We do not claim to be able to check in polynomial time that the images $g_u(\Delta^{B-1})$ tile Δ^{B-1}; we assume this as given. The algorithm only checks the condition involving $\mathrm{contr}(g_W)$. We also do not consider in detail the (nontrivial) issue of how the g_u can be given; see a remark in the proof.

ADDED FI

Proof: Part (i) is proved by repeating the considerations in the above example almost verbatim. It remains to deal with part (ii).

Let us assume that $(g_1, \ldots, g_s)$ is an asymptotically optimal tiling of Δ^{B-1}. Easy volume considerations show that the simplices $g_u(\Delta^{B-1})$ have equal volumes and tile Δ^{B-1} without overlap.

Let us write $d = B - 1$ and let us assume that Δ^d is isometrically embedded in $\mathbf{R}^d$. Let $\ell_u\colon \mathbf{R}^d \to \mathbf{R}^d$ be the "linear part" of g_u, given by $\ell_u(x) = g_u(x) - g_u(0)$. Then $\mathrm{contr}(g_W) = \mathrm{contr}(\ell_W) = \inf\{\|\ell_W(x)\| : x \in \mathbf{R}^d, \|x\| = 1\}$.

Next, let L_u be ℓ_u scaled by $s^{1/d}$, i.e., $L_u(x) = s^{1/d} \cdot \ell_u(x)$. Then L_u is volume-preserving.

For $W \in [s]^m$ we set $C_W = L_W(B^d) = \{L_W(x) : x \in \mathbf{R}^d, \|x\| \leq 1\}$, and we let

$$C = \bigcap\{C_W : W \in [s]^m, m = 1, 2, \ldots\}.$$

Each C_W is convex, and thus C is convex as well. Since each L_u is a nonsingular linear map, C_u is bounded, and hence C is bounded. Since $(g_1, \ldots, g_s)$ is an $s^{-1/d}$-tiling, there is some $\delta > 0$ such that $\mathrm{contr}(L_W) \geq \delta$ for all W. Then C contains the ball of radius δ centered at 0.

We have $L_u(C_W) = C_{uW}$, and so $L_u(C) \subseteq C$. Since L_u preserves volume and since the volume of C is finite and positive, we have $L_u(C) = C$ for all $u \in [s]$.

Let E be the ellipsoid of the smallest volume containing C (the Löwner-John ellipsoid). As is well known, the smallest-volume ellipsoid containing a given convex body is unique (see [5] for references). Hence we have $L_u(E) = E$ for all $u \in [s]$ (for otherwise, E and $L_u(E)$ would be two different smallest-volume ellipsoids containing C).

Let $h\colon \mathbf{R}^d \to \mathbf{R}^d$ be a linear map that maps the unit ball B^d onto the ellipsoid E. Then each of the linear maps $R_u = h^{-1} \circ L_u \circ h$ maps B^d to B^d, and hence it is an isometry. Thus each of the affine maps $r_u = h^{-1} \circ g_u \circ h$ is an isometry followed by scaling by $s^{-1/d}$. The simplex $S = h^{-1}(\Delta^d)$ is tiled by the images $r_u(S)$ without overlap, and it follows that S is an s-reptile.

Next, we consider the algorithmic question: Do given g_u constitute an asymptotically optimal tiling? By what we have already proved it is enough to check whether there exists a nonsingular linear map $h\colon \mathbf{R}^d \to \mathbf{R}^d$ such that each $r_u = h^{-1} \circ g_u \circ h$ is an isometry followed by scaling by $s^{-1/d}$.

The affine map g_u has the form $g_u(x) = A_u x + b_u$, where A_u is a nonsingular $d \times d$ matrix and b_u is a translation vector. In order to describe the input to the algorithm easily, we suppose that the A_u and b_u are rational (using standard machinery, the algorithm can be extended to work with algebraic numbers, say).

In the matrix language, we ask whether there is a nonsingular $d \times d$ matrix T (the matrix of h) such that all the matrices $Q_u = s^{1/d} \cdot T^{-1} A_u T$, $u \in [s]$, are orthogonal, i.e. such that $Q_u^T = Q_u^{-1}$. This condition can be rewritten to $s^{2/d} \cdot P A_u^T = A_u^{-1} P$ for all u, where P is the matrix TT^T. As is well known, a square matrix P can be written in the form TT^T iff it is positive semidefinite. So we have a semidefinite programming problem with an unknown matrix P, which is solvable in polynomial time (see, e.g., [13]). We do not know whether there is any more direct algorithm. ■

We are thus led to the question, for what s and d does there exist a d-dimensional simplex that is an s-reptile? Obviously, the answer is positive for $d = 1$ and all s. For $d = 2$, all s-reptile triangles have been characterized [18], and in particular, they exist iff s is of the form i^2, $3i^2$, or $i^2 + j^2$, for integers i and j. The only known examples for $d \geq 3$ seem to be the Hill simplices (or Hadwiger-Hill simplices; see, e.g., [7]), which provide s-reptile d-simplices for all s of the form $s = i^d$. These examples and the above discussion conclude the proof of Theorem 1.

Further research.

1. No s-reptile simplex is known for $d \geq 3$ and $s < 2^d$. Motivated by the present paper, it was shown in [14] that no 2-reptile simplices exist for $d \geq 3$. The general existence problem for d-dimensional s-reptile simplices appears challenging.

2. We have shown that an asymptotically optimal tiling has to come from an s-reptile simplex. It would be interesting to decide whether this is also the only possible way to obtain a *quasioptimal tiling* of Δ^{B-1}, i.e. one with the condition on $\mathrm{contr}(g_W)$ weakened to $\mathrm{contr}(g_w) \geq (1-o(1))^m s^{-m/(B-1)}$.

   *** Here an immediate problem comes from the matrix (Jordan cell) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, whose mth power expands distances by the (subexponential) factor m. J.

3. How efficiently can we find (or approximate) the largest α such that given affine maps $g_1, \ldots, g_s \colon \Delta^{B-1} \to \Delta^{B-1}$, such that the images $g_u(\Delta^{B-1})$ have disjoint interiors, constitute an α-tiling? If we rephrase this in a matrix language, we arrive at the at the following (more general) problem, about which we haven't found anything in the literature: Given $d \times d$ matrices $M_1, M_2, \ldots, M_s$, can we decide (at least in some approximate sense) whether

$$\sup \left\{ \|M_W x\| : x \in \mathbf{R}^d, \|x\| \leq 1, W \in [s]^m, m = 1, 2, \ldots \right\} < \infty\,?$$

   *** The answer is yes IFF there is a convex body C with $M_u C \subseteq C$ for all $u \in [s]$. In principle, all possible C could be searched, up to some accuracy. How efficiently can this be done? Unlike in the asymptotically optimal case, we no longer suffice with ellipsoids! Jirka

   A powerful necessary condition for the last inequality is that all eigenvalues of every M_W, $W \in [s]^m$, have absolute value at most 1 (this is proved by fixing W and considering large powers of M_W). We don't know how to check this condition either, but it provides an useful upper bound on α in the α-tiling question.

4. What is the best possible m-step resolution of a protocol, for given s and B? Our current bounds are between $O(m^{-1/(B-1)} s^{-m/(B-1)})$ (always) and $\Omega(m^{-1} s^{-m/(B-1)})$ (if an asymptotically optimal tiling exists). Suppose that for some B and s and for infinitely many m there is a protocol with m-step resolution $\Omega(m^{-1} s^{-m/(B-1)})$. Does this imply the existence of an asymptotically optimal tiling?
   *** Can we claim, say using Jeff's lower bound argument, that every protocol achieving an asymptotically optimal number of packets has an asymptotically optimal m-step resolution, or something of that sort?? Jirka

4 Restricted Protocols for Any B and s

In the previous section we have constructed quasioptimal protocols for certain combinations of values of B and s. For other cases, such as $s = 2$, $B \geq 4$ we suspect that no quasioptimal protocols exist, although we cannot prove it.

In such cases, several approaches are possible. First, we can try to construct suboptimal but still good protocols, under the same requirements. The results of [1] yields a protocol with $T \leq s^{4n/B}$. One can try to look for α-tilings of Δ^{B-1} with α as large as possible. In this context, the problems raised at the end of the last section become even more relevant, since we would like to be able to estimate the best α for given candidate tilings. Another possibility is to relax the requirements on the protocol. In the following theorem we offer two versions (attaining quasioptimality).

Theorem 7 (i) *For every s and B there exist a region $D \subset \Delta^{B-1}$ (convex and with nonempty interior) and a protocol such that such that if the distribution X_m of packets generated by the adversary is guaranteed to lie in D, then the victim can reconstruct all m messages sent by the nodes (with constant probability) using $T \leq O(s^2 B^2 2^{2m(\log_2 s)/(B-1)})$ packets.*

(ii) *For every s, B, and every function φ on the natural numbers with $\lim_{n\to\infty}\varphi(n) = \infty$, there exists a (quasioptimal) protocol such that no matter what distribution X_m is generated by the adversary, the victim can reconstruct (with high probability) the messages of the nodes $N_{m-\varphi(m)}$ through N_1 using $T \leq 2^{(2+o(1))m(\log_2 s)/(B-1)}$ packets.*

*** Proofs from the old version need to be adjusted (change notation and explain the explicit constants).

Part (i) is proved using a suitable s-reptile, in a way similar to Theorem 6(i). This time the s-reptile is not a simplex, but rather, a suitable d-dimensional rectangular box R, where write $d = B - 1$. First we define an auxiliary simplex $S = \{X \in \mathbf{R}^d : x_1, \ldots, x_d \geq 0, \sum_{i=1}^d x_i \leq 1\}$. Then we set $\rho = s^{-1/d}$ and $\lambda = 1 - \rho$, and we define R as the rectangular box $\prod_{i=1}^d [0, \lambda\rho^{i-1}]$. The reptiling map r_u is given by $r_u(x_1, x_2, \ldots, x_d) = (\rho x_d + \frac{\lambda}{s}(u-1), \rho x_1, \rho x_2, \ldots, \rho x_{d-1})$. That is, the box is sliced into s congruent boxes by parallel slices perpendicular to the longest side. We let $h\colon S \to \Delta^{B-1}$ be an affine bijection, and we define a protocol $(f_1, f_2, \ldots, f_s)$ by $f_u = h \circ r_u \circ h^{-1}$. It is easily checked that $r_u(S) \subseteq S$, and hence the maps f_u indeed map Δ^{B-1} into Δ^{B-1} and constitute a protocol.

To define the region D where the initial distributions X_m are permitted to lie, we define $R' = \prod_{i=1}^d [\frac{\lambda}{4}\rho^{i-1} \frac{3\lambda}{4}\rho^{i-1}]$ as the $\frac{1}{2}$-shrinking of R from its center and we set $D = h(R')$. It remains to verify that the protocol restricted to D has m-resolution $\Omega((sB)^{-1}s^{-m/(B-1)})$. This is a simple calculation which we omit.

For part (ii), we start with the protocol $(f_1, \ldots, f_s)$ as in (i). Then we choose a parameter $\eta > 0$, depending on s, B and φ and tending to 0 as $m \to \infty$ but very slowly, and we replace the reptiling maps r_u at the beginning of the construction by their $(1-\eta)$-shrinking with center at the origin (i.e. at a vertex of S; this is different from our previous shrinking operations, where the center was always an interior point of the considered region). Let $(\tilde{f}_1, \ldots, \tilde{f}_u)$ be the protocol obtained by the construction from the shrunk r_u's. The m-step resolution decreases somewhat by the $(1-\eta)$-shrinking of the r_u but asymptotically this won't matter. The point is that no matter what initial distribution X_m is generated by the adversary, its images after $\varphi(m)$ steps, i.e. $\tilde{f}_V(X_m)$ for all $V \in [s]^{\varphi(m)}$, are guaranteed to lie in the region $h(R)$, for which the protocol already "works." This is verified by a direct, although not entirely short, calculation.

This finishes a sketch of the proof of Theorem 7.

*** Rewrite!!!

Proof: We prove as follows that the first $n_0 = (\ln(4s^2/Ld\varepsilon)/\ln s)d \in \omega(1)$ nodes of the path are guaranteed to shrink the full space Δ to be contained within D, i.e., for all $W \in [s]^{n_0}$, $f_W(\Delta) \subseteq D$. The protocol then continues our analysis as before assuming that the "Attacker" is the $(n-n_0)^{th}$ node who provides a distribution $X_{n-n_0} \in D$.

What remains to prove is that Δ shrinks to D. For each $u \in [1, d]$, consider how the value x_u changes as it passes through d nodes. Each of the first $d - u$ applications of f_w multiplies x_u by

$[(1-\varepsilon)s^{-1/d}]$ and cycles the coordinate to the right bringing it to the d^{th} coordinate. The next application again multiplies it by $[(1-\varepsilon)s^{-1/d}]$, adds $w \cdot \frac{L}{s} \leq \frac{s-1}{s} \cdot L$ to it and rotates it to the first coordinate. The remaining $u-1$ applications multiples this new amount by $[(1-\varepsilon)s^{-1/d}]$ and rotates it back to the u^{th} coordinate. The complete effect is that for $W' \in [s]^d$ and $f_{W'}(\langle x_1, \dots, x_d \rangle) = \langle x'_1, \dots, x'_d \rangle$, we have that $x'_u \leq [(1-\varepsilon)s^{-1/d}]^d \cdot x_u + [(1-\varepsilon)s^{-1/d}]^{u-1} \cdot \frac{s-1}{s} \cdot L \leq (1-\frac{d\varepsilon}{2})\frac{1}{s} \cdot x_u + s^{-(u-1)/d} \cdot \frac{s-1}{s} \cdot L = a \cdot x_u + b$ for the appropriate a and b. The initial value of $x_u \leq 1$. Hence, after $n_0 = m \cdot d$ nodes, the coordinate x''_u has become at most $b + a \cdot (b + a \cdot (b + \dots a \cdot (b + a \cdot 1))) = \frac{b(1-a^m)}{1-a} + a^m \leq b/[1-(1-\frac{d\varepsilon}{2})\frac{1}{s}] + [\frac{1}{s}]^{\ln(4s^2/Ld\varepsilon)/\ln s} \leq [s^{-(u-1)/d} \cdot \frac{s-1}{s} \cdot L]/[\frac{s-1}{s} + \frac{d\varepsilon}{2s}] + \frac{Ld\varepsilon}{4s^2} \leq [s^{-(u-1)/d} \cdot L] \cdot [1 - \frac{d\varepsilon}{4(s-1)}] + \frac{1}{s}L \cdot \frac{d\varepsilon}{4s} \leq s^{-(u-1)/d} \cdot L$, which is within the required range to have $f_W(X) \in D$. ■

5 Lower bound for a single path of attack

Theorem 8 *For any protocol $\mathcal{P}$, let T be the expected number of packets received by the Victim and $w(\mathcal{P})$ be the probability that the Victim does not return the input string given to the Network when that input is chosen uniformly at random from the set of all 2^n possible n-bit strings. If $w(\mathcal{P}) \leq 1/2$, then $T \geq \Omega\left(B \cdot 2^{2n/(B-1)}\right)$.*

Proof: (Sketch.) Let *permutation oblivious* protocols be the restricted class of protocols where the Victim waits until it has received exactly T packets, where T depends only on n and B. It then ignores the order that the packets arrive and considers only the *receipt profile* X, which is the B-tuple from $\Delta_{\langle B,T \rangle} = \left\{X = (x_1, \dots, x_B) : \sum_{u=1}^{B} x_u = T\right\}$, where x_u is the number of packets of type u received by the Victim. In a permutation oblivious protocol, the Victim's strategy is specified by the function $V(X, W)$ which is the probability that when the Victim receives receipt profile X, it guesses that the Network's n-bit string is W.

Adler in [1] proves that for any general protocol $\mathcal{P}$, there is a permutation oblivious protocol $\mathcal{P}'$ for the Victim, where $w(\mathcal{P}') \leq w(\mathcal{P}) + 1/4$, and $\mathcal{P}'$ uses at most 4 times as many packets as $\mathcal{P}$. Intuitively, this is because the Network has no memory and thus no sense of time, and so the order in which the packets arrive is not useful information for the Victim. Thus, to prove the lower bound for general protocols that make a mistake with probability at most 1/2, it suffices to prove a lower bound on permutation oblivious protocols that make a mistake with probability at most 1/4.

The lower bound in [1] follows from the fact that if the n-bit string W is communicated by the Network "sending" a receipt profile X, then the number of packets T must be large enough that the number of different receipt profiles is at least the number of possible values held by the Network. We improve on this idea via a technique to account for the fact that the Network does not have full control over the receipt profile that it sends. In particular, all that a protocol is able to do is specify the probability $N(W, u)$ that the Network sends a packet of type u when its n-bit string is W. This same probability is used independently when sending each of the T packets. This in turn induces the probability $N(W, X)$ that receipt profile X is "sent" by the Network when its n-bit string is W. We demonstrate that no matter what the Network does, the probability that it sends a particular profile X is exponentially small.

Lemma 9 *Given n-bit string W and any receipt profile $X = (x_1, \dots, x_B)$, the probability $N(W, X)$ that the Network "sends" X when having W is at most $N(X) = \frac{\sqrt{T}}{\mathbf{e}} \cdot \Pi_{u=1}^{B} \frac{\mathbf{e}}{\sqrt{x_u}}$.*

Before proving this, we will consider an easier situation in which each packet is obtained by an independent Bernoulli trial. If the Network can color each packet either red or blue independently with any fixed probability p of its choice and it wants to color exactly x of them red, then the best it can do is to set $p = \frac{x}{T}$. As such, the expected number of red packets is $x = pd$. Furthermore, with constant probability the actual number of packets is fairly uniformly distributed within a range of $\sqrt{x} = \sqrt{pT}$ of this expected number. As a result of this, the probability of getting exactly x reds is approximately $\frac{\mathbf{e}}{\sqrt{x}}$. Note that this probability does not depend on the number of packets T. The reason that the probability of the Network sending exactly X is at most $\frac{\sqrt{T}}{\mathbf{e}} \cdot \Pi_{u=1}^{B} \frac{\mathbf{e}}{\sqrt{x_u}}$ is that it must get the exact number x_u of each type of packet.

Lemma 10 *Given any number $x \leq \frac{T}{2}$ and any single way of coloring each of T packets independently, the probability of there being exactly x red packets is at most $\frac{\mathbf{e}}{\sqrt{x}}$.*

Proof: Fix $x \leq \frac{T}{2}$. If the probability of a packet being red is chosen to be p, then the probability that there are exactly x red packets is $P(p) = \binom{T}{x} p^x (1-p)^{T-x}$. To maximize this probability with respect to p, it is equivalent to maximize $\ln(P(p)) = \ln(\binom{T}{x}) + x \ln p + (T-x)\ln(1-p)$. Differentiating and setting to zero gives $\frac{x}{p} = \frac{T-x}{1-p}$ and solving gives $p = \frac{x}{T}$. Fix $p = \frac{x}{T}$.
Let $P_x = \binom{T}{x} \left(\frac{x}{T}\right)^x \left(\frac{T-x}{T}\right)^{T-x}$ be the probability that there are exactly x red packets.
Let $P_{(x+h)} = \binom{T}{x+h} \left(\frac{x}{T}\right)^{x+h} \left(\frac{T-x}{T}\right)^{T-x-h}$ be the probability that there are exactly $x+h$ red packets, where $h \leq \frac{1}{2}\sqrt{x}$. We bound the ratio between these as follows.

$$\begin{aligned} \frac{P_{(x+h)}}{P_x} &= \frac{(T-x)}{(T-x)} \cdots \frac{(T-x-h+1)}{(T-x)} \cdot \frac{x}{(x+h)} \cdots \frac{x}{(x+1)} \\ &\geq \left(1 - \frac{h}{T-x}\right)^h \cdot \left(1 - \frac{h}{x}\right)^h \approx \mathbf{e}^{-\frac{h^2}{T-x}} \cdot \mathbf{e}^{-\frac{h^2}{x}} \geq \mathbf{e}^{-1} \end{aligned}$$

Similarly, we can bound $\frac{P_{(x-h)}}{P_x} \geq \mathbf{e}^{-1}$. This gives us that probability of there being x plus or minus $\frac{1}{2}\sqrt{x}$ red balls is $1 \geq \sum_{h=-1/2\sqrt{x} \ldots 1/2\sqrt{x}} P_{(x+h)} \geq \sqrt{x} \cdot \mathbf{e}^{-1} \cdot P_x$. This gives the result that $P_x \leq \frac{\mathbf{e}}{\sqrt{x}}$.
■

Proof (of Lemma 10): Consider any n-bit string W and any desired receipt profile $X = (x_1, \ldots, x_B)$. Assume WLOG that x_B is the largest x_u. Let $X' = (x'_1, \ldots, x'_B)$ be the profile that is actually produced.

$$\begin{aligned} N(W, X) &= \Pr\left[x'_1 = x_1, \ldots, x'_B = x_B \mid W\right] \\ &= \Pi_{u=1}^{B-1} \Pr\left[x'_u = x_u \mid x'_1 = x_1, \ldots, x'_{u-1} = x_{u-1} \;\&\; W\right] \end{aligned}$$

Note that we do not worry about $x'_B = x_B$ because $\sum_{u=1}^{B} x_u = \sum_{u=1}^{B} x'_u = T$. In the experiment $\Pr\left[x'_u = x_u \mid x'_1 = x_1, \ldots, x'_{u-1} = x_{u-1} \;\&\; W\right]$, the contents of $\sum_{i=1}^{u-1} x_i$ of the packets have been fixed leaving some $T' = \sum_{i=u}^{B} x_i$ left to be determined. Note that $x_u \leq \frac{T'}{2}$, because x_B is assumed to be at least x_u. We will say that one of these T' packet is colored red by the Network if it is of type u. Lemma **??** then gives that the probability that the number of packets with contents u is exactly x_u is at most $\frac{\mathbf{e}}{\sqrt{x_u}}$. This gives

$$N(W,X) \quad = \quad \Pi_{u=1}^{B-1} \frac{\mathbf{e}}{\sqrt{x_u}} \leq \frac{\sqrt{T}}{\mathbf{e}} \cdot \Pi_{u=1}^{B} \frac{\mathbf{e}}{\sqrt{x_u}}$$

■

We use this Lemma to prove Theorem 8. We consider the quantity $\rho(\mathcal{P}) = (1 - w(\mathcal{P})) \cdot 2^n$. Since $1 - w(\mathcal{P})$ is the probability that using $\mathcal{P}$, the Victim returns the input string given to the Network when that input is chosen uniformly at random from the set of all 2^n possible n-bit strings, we have $\frac{1}{4} \cdot 2^n \leq \rho(\mathcal{P})$. Furthermore, $\rho(\mathcal{P}) = \sum_{W \in \{0,1\}^n} \Pr\left[\text{Victim returns } W \mid \text{Network has } W\right] = \sum_{W \in \{0,1\}^n} \sum_{X \in \Delta_{\langle B,T \rangle}} \Pr[$ Network sends profile X and Victim returns W | Network has $W]$ $= \sum_{W \in \{0,1\}^n} \sum_{X \in \Delta_{\langle B,T \rangle}} N(W,X) \cdot V(X,W)$. Computing this sum becomes difficult because of the interplay between what the Network and the Victim do. However, we decouple them by not forcing the Network to run a fixed protocol when it has the message W, but instead for each distribution of packets X allow it to use the protocol that will maximize its probability of sending X. This can increase the probability of success. However, we know from Lemma 10 that no matter what the Network does, $N(W,X) \leq N(X)$. This conveniently decouples our sum, giving us that $\rho(\mathcal{P}) \leq \sum_{X \in \Delta_{\langle B,T \rangle}} N(X) \cdot \sum_{W \in \{0,1\}^n} V(X,W) \leq \sum_{X \in \Delta_{\langle B,T \rangle}} N(X) \cdot 1$. By plugging in the value for $N(X)$, we get $\rho(\mathcal{P}) \leq \sum_{X \in \Delta_{\langle B,T \rangle}} \frac{\sqrt{T}}{\mathbf{e}} \cdot \Pi_{u=1}^{B} \frac{\mathbf{e}}{\sqrt{x_u}}$. We then can use Lemma 11 to bound this by $\sqrt{T}\mathbf{e}^{B-1} \cdot \left[\frac{\pi(3.4\sqrt{T})^{B-2}}{\sqrt{(B-1)!}}\right] \leq \frac{\frac{\pi}{3.4} \cdot (3.4\mathbf{e}\sqrt{T})^{B-1}}{\sqrt{((B-1)/\mathbf{e})^{B-1}}} \leq \left(\frac{3.4^2\mathbf{e}^3 T}{B-1}\right)^{(B-1)/2}$. Solving $\frac{1}{4} \cdot 2^n \leq \left(\frac{3.4^2\mathbf{e}^3 T}{B-1}\right)^{(B-1)/2}$ gives that $T \geq \Omega\left(B \cdot 2^{2n/(B-1)}\right)$. ■

Lemma 11 *If* $\Delta_{\langle B,T \rangle} = \left\{x = (x_1, \ldots, x_B) \mid \sum_{u=1}^{B} x_u = T\right\}$, *then* $\sum_{x \in \Delta_{\langle B,T \rangle}} \Pi_{u=1}^{B} \frac{1}{\sqrt{x_u}} \leq \frac{\pi(3.4\sqrt{T})^{B-2}}{\sqrt{(B-1)!}}$

For intuition, the requirement that $\sum_{u=1}^{B} x_u = T$ leaves $B-1$ independent values of x_u, each roughly T/B. Hence, there are approximately $(T/B)^{B-1}$ terms in the sum $\sum_{x \in \Delta_{\langle B,T \rangle}} \Pi_{u=1}^{B} \frac{1}{\sqrt{x_u}}$. Each term is roughly $(\frac{1}{\sqrt{T/B}})^B$. This gives a total of about $(T/B)^{B-1} \cdot (\frac{1}{\sqrt{T/B}})^B = \sqrt{T/B}^{B-2}$.

Proof: The proof is by induction on B. For $B = 2$, Maple gives that the sum $\sum_{x=1}^{T} \frac{1}{\sqrt{x}} \cdot \frac{1}{\sqrt{T-x}}$ is at most π. Assuming that the hypothesis is true for $B-1$, for B we have $\sum_{x \in \Delta_{\langle B,T \rangle}} \Pi_{u=1}^{B} \frac{1}{\sqrt{x_u}} = \sum_{x=1}^{T} \frac{1}{\sqrt{x}} \cdot \left[\sum_{x' \in \Delta_{\langle B-1,T-x \rangle}} \Pi_{u=1}^{B-1} \frac{1}{\sqrt{x_u}}\right]$, which by induction hypotheses is at most $\sum_{x=1}^{T} \frac{1}{\sqrt{x}} \cdot \left[\frac{\pi(3.4\sqrt{T-x})^{B-3}}{\sqrt{(B-2)!}}\right] = \frac{\pi(3.4)^{B-3}}{\sqrt{(B-2)!}} \cdot \left[\sum_{x=1}^{T} \frac{(T-x)^c}{\sqrt{x}}\right]$, where $c = \frac{B-3}{2}$. Lemma 12 then gives that this is at most $\frac{\pi(3.4)^{B-3}}{\sqrt{(B-2)!}} \cdot \left[\frac{2.4}{\sqrt{c+1}} \cdot T^{c+1/2}\right] = \frac{\pi(3.4)^{B-3}}{\sqrt{(B-2)!}} \cdot \left[\frac{2.4 \cdot \sqrt{2}}{\sqrt{B-1}} \cdot T^{(B-2)/2}\right] \leq \frac{\pi(3.4\sqrt{T})^{B-2}}{\sqrt{(B-1)!}}$. ■

Lemma 12 $\sum_{x=1}^{T} \frac{(T-x)^c}{\sqrt{x}} \leq \frac{2.4}{\sqrt{c+1}} \cdot T^{c+1/2}$.

Proof: We break the sum into two at $r = \frac{0.35T}{c+1}$. First, $\sum_{x=1}^{r} \frac{(T-x)^c}{\sqrt{x}} \leq T^c \cdot \sum_{x=1}^{r} \frac{1}{\sqrt{x}} \leq T^c \cdot 2\sqrt{r} \leq \frac{1.2}{\sqrt{c+1}} \cdot T^{c+1/2}$. Second, $\sum_{x=r}^{T} \frac{(T-x)^c}{\sqrt{x}} \leq \frac{1}{\sqrt{r}} \cdot \sum_{x=r}^{T} (T-x)^c \leq \frac{1}{\sqrt{r}} \cdot \frac{1}{c+1}(T-r)^{c+1} = \frac{1}{\sqrt{0.35T/(c+1)}} \cdot \frac{1}{c+1}(T - 0.35T/(c+1))^{c+1} = \frac{1}{\sqrt{0.35}} \cdot (1 - \frac{0.35}{c+1})^{c+1} \cdot \frac{1}{\sqrt{c+1}} \cdot T^{c+1/2} \leq \frac{1}{\sqrt{0.35}} \cdot \mathbf{e}^{-0.35} \cdot \frac{1}{\sqrt{c+1}} \cdot T^{c+1/2} \leq \frac{1.2}{\sqrt{c+1}} \cdot T^{c+1/2}$.
■

6 Protocol for Multiple Paths

In this section, we provide our new protocol for the case of multiple paths of attack. Recall that for this case of the problem, there are up to k different paths, each of which contains a different set of m nodes. The adversary chooses which path each packet travels on; the victim only sees the contents of the final packet it receives - it does not know which path that packet traveled on. The goal is to design a protocol where the victim can determine the strings that were on paths used for a fraction of at least $\frac{\alpha}{k}$ of the packets, for a parameter $\alpha \leq 1$. We refer to the string of information along the jth path as W_j. Also, we refer to the node at distance i from the victim on the jth path as N_i^j.

The minimum value of B required by this protocol is $2k+1$, which is the same as that achieved by a protocol provided in [1]. The main improvement of the new protocol is the assumptions made on the underlying network. In particular, the protocol from [1] assumes that the adversary always sets the initial bits to 0. Thus, it would be quite easy for the adversary to disable that protocol. We here provide a protocol that works for *any* scheme by the adversary to set the initial bits. Instead, we show that the combination of two other and more realistic assumptions is sufficient. We point out that the lower bound of $B \geq 2k-1$, shown in [1], still applies with the two assumptions made here.

First, we assume that the value to be sent by each node in the system is chosen independently and uniformly at random. This is justified in the IP Traceback scenario, since the attacks these techniques protect against occur from compromised nodes in the Internet. Our assumption here corresponds to the assumption that the descriptions of the paths to compromised nodes are distributed randomly, as opposed to being a worst case distribution.

Our second assumption is that the nodes along each path have a small amount of information as to their location along that path. Note that this is also a reasonable assumption in the Internet, since a node has access to the destination of a given packet, and nodes are likely to have some knowledge of whether that destination is close by or not. In particular, we assume that each node N_i^j has a predicate C such that if N_i^j has distance of at most $2\log k+1$ hops from the victim of the attack, then $C(N_i^j) = \text{TRUE}$, and if i is the node adjacent to the adversary, then $C(N_i^j) = \text{FALSE}$ (and hence $m \geq 2\log k+2$). For the remainder of the nodes along the path, the value of $C(N_i^j)$ can be either TRUE or FALSE. For example, if $2\log k < m/2$, it is sufficient for a node to know if it is in the first or second half of the routing path. For ease of presentation, we make two assumptions that are not difficult to remove: (1) we assume here that $C(N_i^j)$ is constant for all j, and we assume that all N_i^j for which $C(N_i^j) = \text{TRUE}$ are closer to the victim than any N_i^j for which $C(i) = \text{FALSE}$. We denote by $C_{\max}$ the number of i for which $C(N_i^j) = \text{TRUE}$.

We also point out that the protocol we describe here is based on that introduced in [1], with a number of changes. The real innovation of the result presented here is not as much these changes as a greatly improved analysis technique. This new analysis technique allows us to prove these results. It also has considerable potential to address the question of tight tradeoffs for the number of packets required in the multiple path case, an interesting open problem.

6.1 The protocol

We here describe the protocol for the case where $s = 2$ (i.e., each node has a single bit), but our technique can easily be adapted to any s that is a power of 2. We here assume that the protocol is designed for a specific upper bound on k: the protocol is not required to know how many paths the adversary is using. Instead, it works (with high probability), as long as the the adversary does not use more than k paths. For simplicity, we also here assume that $B = 2k + 1$. For larger values of B, the remaining states of the marking bits are treated as being equivalent to state 0, and thus are not used. Let $d = 2k = B - 1$. We define two different mappings from a probability distribution over packets to a probability distribution over packets. For each of these, let $p_{u,v}$ be the probability that the packet u gets mapped to packet v. Consider first the mapping **zero**:

- For $0 < u \leq d$, $p_{u,u} = 2^{-u}$, and $p_{u,0} = 1 - 2^{-u}$.
- For $u \neq v$, and $v \neq 0$, $p_{u,v} = 0$.
- $p_{0,0} = 1$.

The second mapping is called **one**:

- For $1 \leq u \leq v \leq d$, $p_{u,v} = 2^{2u-3v}\binom{v}{u} + 2^{-3v}$.
- For $1 \leq v < u \leq d$, or $u = 0 < v \leq d$, $p_{u,v} = 2^{-3v}$.
- For $v = 0 \leq u \leq d$, $p_{u,v} = 1 - \sum_{v=1}^{d} p_{u,v}$.

The protocol from [1] consists of a node with the bit 0 simply applying mapping **zero**, and a node with the bit 1 applying mapping **one**. In the new protocol, a node N_i^j with the bit 0 and $C(N_i^j) =$ TRUE applies the mapping **zero** twice, followed by the mapping **one** once, followed by three more applications of the mapping **zero**. A node N_i^j with the bit 1 and $C(N_i^j) =$ TRUE applies the same process, except that the last mapping **zero** is replaced with a **one**. A node N_i^j with the bit 0 and $C(N_i^j) =$ FALSE applies the mapping **zero** $ck + 1$ times, for a suitable constant c to be described below. A node N_i^j with the bit 1 and $C(N_i^j) =$ FALSE applies the mapping **zero** ck times, followed by the mapping **one**. This completes the description of the encoding portion of the protocol.

Theorem 13 *For any α, and any $\delta > e^{-\frac{2}{3}k} + 2^{2\log k - C_{\max}}$, there is a value $T(\alpha, \delta)$, such that after the victim has received at least $T(\alpha, \delta)$ packets, with probability at least $1 - \delta$, he has enough information to determine every string that is on a path used for at least a fraction of $\frac{\alpha}{k}$ of the packets the adversary sends.*

We point out that the lower bound on δ is due to a requirement that the set of k strings "look" random (in a manner we make formal below). For any set of strings that meet this requirement, the probability of success can be made arbitrarily close to 1.

Proof: Assume first that the adversary sets the initial value of every packet to 0 (as was assumed throughout in the protocol of [1]). Later, we shall see how to relax this assumption. Let $p_u(W_j)$ be the probability that a packet, with initial value 0, sent on a path with string W_j, arrives at the victim set to the value u. Let w_i^j be the ith bit (starting from the victim) of the string W_j. Let

$$\begin{aligned} X_{W_j} \quad = \quad & \sum_{i=1}^{C_{\max}} (\frac{1}{2})^{6(i-1)+1}(w_i^j + \frac{1}{8}) + \\ & \sum_{i=C_{\max}+1}^{m} (\frac{1}{2})^{(ck+1)(i-C_{\max}-1)+6C_{\max}+1} w_i^j . \end{aligned}$$

We shall refer to X_{W_j} as the value of the string W_j. Note that X_{W_j} is the real number with a binary representation where the bit representing 2^{-t} is a 1 if and only if the tth mapping (counting from last to first) applied to the probability distribution is the mapping **one**. Thus, if the victim is informed of the value of a string or even a sufficiently good estimate of this value, then this gives it sufficient information to determine all the bits of that string. With the assumption that the initial bits are set to 0, Claim 9 from [1] demonstrates that for $0 < u \leq d$:

$$p_u(W_j) = \left(\frac{X_{W_j}}{4}\right)^u, \tag{2}$$

Thus, if the victim could determine a sufficiently good estimate on $p_u(W_j)$, for any u, $0 < u \leq d$, it would have enough information to determine the string W_j. However, the adversary is able to "hide" the $p_u(W_j)$s by choosing what fraction of the packets are sent on each of the different paths. Let λ_j be the fraction of the received packets that are sent by the adversary with string W_j. The probability that a randomly chosen packet from the set of packets received by the victim has its bits set to u is $q_u = \sum_{j=1}^{k} \lambda_j p_u(W_j)$. The set of received packets provides the victim with an estimate on the values of the q_u. Although the stochastic variance inherent to the communication process means that it is unlikely for the victim to know the q_us exactly, we first assume that the victim is given the exact values of the q_us, and demonstrate that this uniquely determines the entire set of strings used by the adversary. This allows us to build some intuition for why the victim is able to decode the set of strings in the actual scenario. We shall then remove both this assumption, as well as the assumption that the adversary set the initial bits to 0.

We show that if we assume that the q_us do not determine the strings uniquely, this leads to a contradiction. Let $V(W_j)$ be the $2k$-dimensional vector where component u of $V(W_j)$, for $1 \leq u \leq 2k$, is $p_u(W_j)$. We shall refer to $V(W_j)$ as the *string vector* for W_j. Assume that there is some set of strings $W_{k+1} \dots W_{2k}$ and probabilities $\lambda_{k+1} \dots \lambda_{2k}$ such that $\sum_{j=1}^{k} \lambda_j V(W_j) = \sum_{j=k+1}^{2k} \lambda_j V(W_j)$. For the set of strings to not be uniquely determined, it must be the case that there is some string W_j with $\lambda_j > 0$ such that if $j \leq k$ then $W_j \notin \{W_{k+1}, \dots, W_{2k}\}$, and if $j > k$ then $W_j \notin \{W_1, \dots, W_k\}$. Assume here that such a string is W_{2k}; the case where $j \leq k$ is similar. In this case, we see that

$$\lambda_{2k} V(W_{2k}) = \sum_{j=1}^{k} \lambda_j V(W_j) - \sum_{j=k+1}^{2k-1} \lambda_j V(W_j). \tag{3}$$

There may be strings that appear in both $W_1, \dots, W_k$ and $W_{k+1}, \dots, W_{2k}$. However, by replacing any such string with another unused string, we see that (3) implies that there is some set of $2k$ distinct strings $W'_1 \dots W'_{2k}$ and real numbers $\lambda'_1 \dots \lambda'_{2k}$, with $\lambda'_{2k} > 0$, such that

$$\lambda'_{2k} V(W'_{2k}) = \sum_{j=1}^{2k-1} \lambda'_j V(W'_j). \tag{4}$$

Now, consider the $2k \times 2k$ matrix M where entry $M_{u,j} = p_u(W'_j)$. From (4), we see that M does not have full rank. However, from (2), we see that $M_{u,j} = \left(\frac{X_{W'_j}}{4}\right)^u$. The $2k \times 2k$ matrix M', where entry $M'_{u,j} = \left(\frac{X_{W'_j}}{4}\right)^{u-1}$, is a Vandermonde matrix. Since the strings $W'_1 \dots W'_{2k}$ are distinct, if $j \neq j'$ then $X_{W'_j} \neq X_{W'_{j'}}$, and thus M' has full rank. Since, for all strings W_j, $X_{W_j} \neq 0$, the matrix M must have full rank as well, which is a contradiction. Therefore, the exact values of the q_u exactly determines all strings W_j, $1 \leq j \leq k$, such that $\lambda_j > 0$.

We next examine the effect of removing our two assumptions. In particular, 1) instead of the victim knowing the values of the q_u exactly, it only has the information provided by the packets it has received: a series of samples from the probability distribution. Also, 2) the adversary, instead of being restricted to setting the initial bits to 0 on each packet, is allowed to employ any strategy it wants for the initial bits.

We can think of the values q_u as a point in B-dimensional space, where the coordinate for dimension u is q_u. The effect of removing both of the two assumptions above is that instead of knowing the exact point defined by the q_us, we instead know a point that we shall show is (whp) sufficiently close to determine any string that is used to send a large enough fraction of the packets. Let Q be the point defined by the q_us. Let $D_0 = \frac{6}{2^{6C_{\max}+(ck+1)(m-C_{\max})}}$. The estimate of the point Q that is used is as follows: the victim collects $T = \frac{6k}{D_0^2} \ln \frac{2k}{\delta}$ packets. For $1 \leq u \leq B$, let Y_u be the number of times that packet u is seen in the T packets. We set $\bar{q}_u = Y_u/T$.

The victim only returns sets of strings that are likely to lead to seeing the $\bar{q}_u$s that it computes. Furthermore, it restricts its attention to those sets of strings that are not too close together, since it is unlikely that randomly chosen strings will be too close together.

Definition 14 *We say that a set of k strings $W_1, \ldots, W_k$ is* well dispersed *if $\forall j, 1 \leq j \leq k, \Pi_{i \neq j} |X_{W_i} - X_{W_j}| \geq 2^{-32k}$.*

The victim returns any string W_j such that W_j is contained in a convex combination of at most k string vectors, with the coefficient associated with W_j being at least $\frac{\alpha}{k}$, such that (a) the Euclidean distance of the resulting convex combination from the corresponding point defined by the $\bar{q}_u$s is at most D_0, and (b) the set of k strings is well dispersed. We first point out that it is likely that the adversary has a set of strings that is well dispersed.

Claim 15 *Say we choose a set R of k strings independently and uniformly at random. The probability that R is not well dispersed is at most $e^{-\frac{2}{3}k} + 2^{2\log k - C_{\max}}$.*

Proof: Note that the value X_{W_j} for a randomly chosen string W_j, when represented in binary, has a first bit that is chosen randomly, with five subsequent bits that are fixed, and then every 6th bit is chosen randomly with the subsequent 5 bits fixed, until $C_{\max}$ bits have been chosen randomly. After that, one in every $ck + 1$ bits is chosen randomly.

The probability that any randomly chosen pair of strings W_i and W_j have a value that agrees on the first $6C_{\max}$ bits is at most $2^{-C_{\max}}$. Thus, by a union bound, the probability that any pair of strings agrees on the first $6C_{\max}$ bits is at most $2^{-C_{\max}+2\log k}$. Thus, we henceforth assume that any pair of string values disagrees somewhere on the first $6C_{\max}$ bits.

We next examine a single string W_j, and bound the probability that the pairwise products with respect to this string are too small. We see that the distribution on $|X_{W_j} - X_{W_i}|$ stochastically dominates the distribution on $(\frac{1}{2} - \frac{1}{64})^{6h+1}$, where h is the number of heads seen before the first tail in a sequence of flips of a fair coin. Thus, for a fixed W_j, $\Pi_{i \neq j} |X_{W_j} - X_{W_i}|$ stochastically dominates $(\frac{31}{64})^{6\hat{h}_k + k}$, where $\hat{h}_k$ is the number of heads seen before a total of k tails have been seen in a sequence of flips of a fair coin. Standard Chernoff bound techniques suffice to show that $\Pr[\hat{h}_k \geq 5k] \leq e^{-\frac{4}{3}k}$.

Thus, by taking a union bound over all possible strings j, $\Pr[\exists j \text{ s.t. } \Pi_{i \neq j}|X_{W_j} - X_{W_i}| \geq (\frac{31}{64})^{31k}] \leq e^{-\frac{4}{3}k + \ln k} \leq e^{-\frac{2}{3}k}$. The claim now follows from the fact that $(\frac{31}{64})^{31k} \geq (\frac{1}{2})^{32k}$ ■

We demonstrate that with probability at least $1 - \delta$, the victim returns every string P such that a fraction of at least $\frac{\alpha}{k}$ of the packets travel on P, and no strings that are not used by the adversary at all. To do so, we prove two lemmas: We first demonstrate that (whp) the point determined by the victim is not more than D_0 distance from Q. We then demonstrate that every convex combination of string vectors that has a coefficient associated with string W_j of at least $\frac{\alpha}{k}$, where W_j is not used by the adversary, has a Euclidean distance from Q of more than $2D_0$. Let $D_q = \sqrt{\sum_{i=1}^{2k}(q_u - \bar{q}_u)^2}$.

Lemma 16 *$\Pr[D_q > D_0] \leq \delta$.*

Proof: Note that for each u, $|\bar{q}_u - \mathrm{E}[\bar{q}_u]|$ is the distance caused by stochastic variation, and $|q_u - \mathrm{E}[\bar{q}_u]|$ is the distance caused by the adversary not setting the initial bits to 0. Standard Chernoff bound techniques demonstrate that with N packets, $\Pr[\sqrt{\sum_{i=1}^{2k}(\mathrm{E}[\bar{q}_u] - \bar{q}_u)^2} \geq D_0/2] \leq \delta$. Thus, we only need to demonstrate that the effect of the adversary setting the initial bits arbitrarily cannot cause the distance from the point Q to be more than $D_0/2$.

To examine the effect of arbitrary settings of the initial bits, note that since the mappings performed by the nodes are linear, it is sufficient for us to consider each of the cases where the adversary always sets the initial bits to the same value, for all possible values, and to show that for each of these individually, the distance from Q is at most $D_0/2$. This is sufficient, since the strategy used by the adversary must be some convex combination of these strategies.

Claim 17 *For u a positive integer, let $\mu(u) = \max(0, u - 2)$. After a packet has had $\ell \geq 1$ sets of three mappings applied to it, where the first two mappings in each set are the mapping* **zero**, *$|q_u - E[\bar{q}_u]| \leq \frac{1}{2^{3\ell + \mu(u)}}$.*

Proof: We prove this by induction on ℓ. For the base case, consider $\ell = 1$. When the last mapping in the set of three is **zero**, the claim follows simply from the definition of the mapping **zero**. When the last mapping is **one**, the portion of the mapping from u to v (which is only relevant when $v \geq u$) is $\binom{v}{u}\frac{2^u}{4^v}$. With the combination of the 2 **zero** mappings that are applied before the **one**, we see that the amount of u that goes to v is $\binom{v}{u}\frac{2^u}{2^{4v}}$. For $v = 1$, only $u = 1$ is relevant, and thus we see that in the case that the incoming packet is a 1, after the first node has applied its mapping, $|q_1 - \mathrm{E}[q_1]| \leq \frac{1}{8}$, as desired. For $v > 1$, we see that the amount of u that goes to v is at most $\frac{1}{2^{2v}}$. Summing over all relevant u, we get at most $\frac{v}{2^{2v}}$, which is at most $\frac{1}{2^{v+1}}$, as desired.

For the inductive step, if we assume that the inductive hypothesis holds, then the case where the last mapping is a **zero** is easy. For the case where the last mapping is a **one**, we saw for the base case that the total relevant probability of going from $u = 1$ to $v = 1$ is at most $\frac{1}{8}$, and so the inductive step works for $|q_1 - \mathrm{E}[q_1]|$. For the case of $v > 1$ we also saw in the base case that the total relevant probability of being v after this step is at most $\frac{1}{2^{v+1}}$. Even if this all comes from the largest possible value at the previous node (i.e., $u = 1$), this is still sufficient for the inductive step. ■ This implies the Lemma, since the distance from Q is at most $\frac{3}{2^{6C_{\max} + (ck+1)(m - C_{\max})}}$. ■

Note that Lemma 16 implies that with high probability, the victim returns all strings that it is required to return. To show that with high probability the victim does not return any strings that it should not return, we show that $D_q \leq D_0$ also implies that there can be no string P not used by the adversary such that P is returned by the victim.

Lemma 18 *If the set of strings used by the adversary is well dispersed, then every convex combination of k well dispersed string vectors that contains a string W_j, not used by the adversary, with a coefficient of more than $\frac{\alpha}{k}$, has a Euclidean distance from Q of at least $2D_0$.*

Proof: If a string W_j as described by the Lemma exists, then there must be some set of strings $W_1 \ldots W_{2k}$, where $W_1 \ldots W_k$ are the well dispersed strings used by the adversary, $W_{k+1} \ldots W_{2k}$ are the well dispersed strings contained in the incorrect convex combination, and W_{2k} is the string returned incorrectly. Thus, $W_{2k} \notin \{W_1, \ldots, W_k\}$, and there exist probabilities $\lambda_1 \ldots \lambda_{2k}$, with $\lambda_{2k} \geq \frac{\alpha}{k}$, such that

$$\sqrt{\sum_{u=1}^{B} \left(\sum_{j=k+1}^{2k} \lambda_j p_u(W_j) - \sum_{j=1}^{k} \lambda_j p_u(W_j) \right)^2} \leq 2D_0$$

This implies that there are $2k$ distinct strings $W'_1, \ldots, W'_{2k}$ and real numbers $\lambda'_1 \ldots \lambda'_{2k}$, with $\lambda'_{2k} \geq \frac{\alpha}{k}$, such that

$$\sqrt{\sum_{u=1}^{B} \left(\lambda'_{2k} p_u(P'_{2k}) - \sum_{j=1}^{2k-1} \lambda'_j p_u(P'_j) \right)^2} \leq 2D_0 \tag{5}$$

Let D_1 be the Euclidean distance in $\Re^{2k}$ from the point $\lambda'_{2k} V(W'_{2k})$ to the subspace spanned by $V(W'_1), \ldots V(W'_{2k-1})$. For (5) to be true, it must be the case that $D_1 \leq 2D_0$. Thus, to demonstrate that no such incorrectly returned string W_{2k} can exist, it is sufficient to show that $D_1 > 2D_0$. Let $\mathcal{V}_{2k}$ be the $2k$-dimensional volume of the parallelepiped defined by the vectors $V(W'_1), \ldots, V(W'_{2k-1}), \lambda_{2k} V(W'_{2k})$ in $\Re^{2k}$. Let $\mathcal{V}_{2k-1}$ be the $(2k-1)$-dimensional volume of the parallelepiped defined by the vectors $V(W'_1), \ldots, V(W'_{2k-1})$ in $\Re^{2k}$. We see that $D_1 = \frac{\mathcal{V}_{2k}}{\mathcal{V}_{2k-1}}$, and thus we consider each of $\mathcal{V}_{2k}$ and $\mathcal{V}_{2k-1}$ separately. In what follows, for any string W_i, let $Y_{W_i} = \frac{X_{W_i}}{4}$.

Lemma 19

$$\mathcal{V}_{2k} = \lambda_{2k} \prod_{1 \leq i < j \leq 2k} \left| Y_{W'_i} - Y_{W'_j} \right| \prod_{i=1}^{2k} Y_{W'_i}.$$

Proof: Due to the convenient form of the vectors $V(W'_1), \ldots, V(W'_{2k})$, we can easily determine $\mathcal{V}_{2k}$. In particular, a standard result from linear algebra is that $\mathcal{V}_{2k}$ is equal to the absolute value of the determinant of the matrix T, where column j of T, for $1 \leq j \leq 2k-1$, is $V(W'_j)$, and column $2k$ is the vector $\lambda_{2k} V(W'_{2k})$.

To compute $|det(T)|$, consider the matrix T', where column j of T', for $1 \leq j \leq 2k$, is $\frac{V_j}{Y_{W'_j}}$. By (2), the matrix T' is Vandermonde, and thus

$$det(T') = \prod_{1 \leq i < j \leq 2k} \left| Y_{W'_i} - Y_{W'_j} \right|.$$

The lemma then follows from the fact that to get T from T', we merely multiply each column i of T' by Y_{W_i}, with the exception of column $2k$, which is multiplied by $\lambda_{2k} Y_{W_i}$. ■

Lemma 20

$$\mathcal{V}_{2k-1} \le \prod_{1\le i<j\le 2k-1} \left|Y_{W'_i} - Y_{W'_j}\right| \prod_{i=1}^{2k-1} [Y_{W'_i}(1+Y_{W'_i}^{2k-1})].$$

Proof: Let $V^2(W_j)$ be the vector consisting of the components $1, Y_{W_j}, Y_{W_j}^2, \ldots, Y_{W_j}^{2k-1}$. Let $V^3(W_j)$ be the vector consisting of the components $0, Y_{W_j}, Y_{W_j}^2, \ldots, Y_{W_j}^{2k-1}$. Let $V^4(W_j)$ be the vector consisting of the components $0, 1, Y_{W_j}, Y_{W_j}^2, \ldots, Y_{W_j}^{2k-2}$.

For $e \in \{2,3,4\}$, let $\mathcal{V}_{2k-1}^e$ be the $(2k-1)$-dimensional volume of the parallelepiped defined by the vectors $V^e(W'_1), \ldots, V^e(W'_{2k-1})$ in $\Re^{2k}$.

Since $V(W_j)$ is simply $V_2(W_j)$ with every component multiplied by Y_{W_j}, $\mathcal{V}_{2k-1} = \mathcal{V}_{2k-1}^2 \cdot \prod_{i=1}^{2k-1} Y_{W'_i}$. Similarly, $\mathcal{V}_{2k-1}^3 = \mathcal{V}_{2k-1}^4 \cdot \prod_{i=1}^{2k-1} Y_{W'_i}$. Since $\mathcal{V}_{2k-1}^4$ is the $2k-1$ dimensional volume of a set of $2k-1$ vectors in $2k-1$ dimensions, $\mathcal{V}_{2k-1}^4$ is the absolute value of the determinant of the matrix formed by the vectors $V^4(W'_1), \ldots, V^4(W'_{2k-1})$. Since this matrix is Vandermonde, its determinant is

$$\prod_{1\le i<j\le 2k-1} \left|Y_{W'_i} - Y_{W'_j}\right|.$$

Claim 21 $\mathcal{V}_{2k-1}^2 \le \mathcal{V}_{2k-1}^3 \prod_{i=1}^{2k-1} \frac{1+Y_{W'_i}^{2k-1}}{Y_{W'_i}}$.

Proof: Consider the process of changing from the vectors $V^2(W'_1), \ldots, V^2(W'_{2k-1})$ to the vectors $V^3(W'_1), \ldots, V^3(W'_{2k-1})$, and consider the pairing of each vector of the type V^2 with the corresponding vector of the type V^3. This process has two effects on the parallelepiped defined by these vectors: it changes the length of the vectors, and it changes the angle between vectors. Note first that for any two pairs of corresponding vectors, the angle between those two vectors for V^3 is at least as large as the angle between those two vectors for V^2. Since all angles are between 0 and 90 degrees, the effect of the change in angles can only increase the volume of the parallelepiped. Thus, we only need to consider the change in length for each vector.

Let L_1 be the length of $V^2(W_j)$, and L_2 the length of $V^3(W_j)$. Since $L_1 = \sqrt{1 + Y_{W_j}^2 + Y_{W_j}^4 + \ldots + Y_{W_j}^{4k-2}}$ and $L_2 = \sqrt{Y_{W_j}^2 + Y_{W_j}^4 + \ldots + Y_{W_j}^{4k-2}}$, it is easy to see that $\forall j, L_1 \le \frac{1+Y_{W_j}^{2k-1}}{Y_{W_j}} L_2$. ■

The Lemma follows. . ■

Since $D_1 = \frac{\mathcal{V}_{2k}}{\mathcal{V}_{2k-1}}$, we see that D_1 is at least

$$\frac{\lambda_{2k} Y_{W'_{2k}} \prod_{i=1}^{2k-1}\left(Y_{W'_i} - Y_{W'_{2k}}\right)}{\prod_{i=1}^{2k-1}(1+Y_{W'_i}^{2k-1})} \ge \frac{\lambda_{2k}}{128} \prod_{i=1}^{2k-1}\left(Y_{W'_i} - Y_{W'_{2k}}\right),$$

where the second inequality follows from the fact that for $1 \le i \le 2k$, $\frac{1}{64} \le Y_{W'_i} \le \frac{1}{4}$. To complete the proof, we need to demonstrate that for any set of $2k$ string vectors formed from two well dispersed sets of k string vectors, this quantity will not be too large.

Claim 22 *Let $S_1 = \{Y_{W_1}, \ldots, Y_{W_k}\}$ and $S_2 = \{Y_{W_{k+1}}, \ldots, Y_{W_{2k}}\}$ be two sets of well dispersed string vectors such that $Y_{W_{2k}} \notin S_1$.*

$$\prod_{Y_{W_i} \in S_1 \cup S_2 - Y_{W_{2k}}} |Y_{W_i} - Y_{W_{2k}}| \geq \frac{1}{2^{65k+6C_{\max}+(m-C_{\max}-1)(ck+1)+2}}.$$

Proof: Let Y_{W_m} be the element of S_1 that minimizes $|Y_{W_m} - Y_{W_{2k}}|$. Note that since the last bit of the strings must be different, $|Y_{W_m} - Y_{W_{2k}}| \geq \frac{1}{2^{6C_{\max}+(m-C_{\max}-1)(ck+1)+3}}$. Since S_2 is well dispersed,

$$\prod_{Y_{W_i} \in S_2 - Y_{W_{2k}}} |Y_{W_i} - Y_{W_{2k}}| \geq \frac{1}{2^{32k}}.$$

Since S_1 is well dispersed,

$$\prod_{Y_{W_i} \in S_1 - Y_{W_m}} |Y_{W_i} - Y_{W_m}| \geq \frac{1}{2^{32k}}.$$

Furthermore, since $Y_{W_{2k}}$ is closer to Y_{W_m} than any other element in S_1, it must be the case that $\forall W_i \in S_1, |Y_{W_i} - Y_{W_{2k}}| \geq |Y_{W_i} - Y_{W_m}|/2$. Thus,

$$\prod_{Y_{W_i} \in S_1 - Y_{W_m}} |Y_{W_i} - Y_{W_{2k}}| \geq \frac{1}{2^{33k-1}}.$$

The claim follows. ■

Lemma 18 (and hence the Theorem) now follows by observing that if we set $c = 72 + \log \frac{1}{\alpha}$, then for $k \geq 2$ it must be the case that $D_1 > 2D_0$. ■

■

Finally, we mention the computational efficiency of the decoding procedure. A simple solution is to try all possible $\binom{2^m}{k}$ sets of k paths, and for each set, (a) check if it is well dispersed, and (b) check to see if the corresponding string vectors have a convex combination that is sufficiently close to the observed sample from the received packets. Part (b) can be done via linear programming (strictly speaking, this requires using an L_1 norm, instead of the L_2 norm we have used in the proofs, but adapting our proofs to L_1 is not difficult). While this procedure is not very fast, the number of packets that are required is $2^{\Omega(mk)}$, and thus the decoding procedure is polynomial in the number of packets received. Determining if there exists a faster decoding algorithm is an interesting open problem.

Acknowledgments

We thank Uri Zwick for fruitful discussions at the beginning of this research. We also thank William Hesse for being the first to point out a protocol of the type depicted in Figure 1. The third author (JM) would like to thank the following people for kindly answering his queries concerning reptiles, matrix powers, and other things related to this paper: Christoph Bandt, Maurice Cochand, David Eppstein, Eike Hertel, Marie Hušková, Krystyna Kuperberg, Wlodzimierz Kuperberg, Petr Plecháč, and Jiří Rohn. We are particularly indebted to Yuri Lyubich for a suggestion that eventually led to the use of the convex body C in the proof of Theorem 6, and to Pavel Valtr for the right remark about smallest-volume ellipsoids at the right moment.

References

[1] M. Adler, Tradeoffs in Probabilistic Packet Marking for IP Traceback, In *Proc. of ACM Symposium on Theory of Computing*, May 2002.

[2] M. Adler, J. Cai, J. K. Shapiro, and D. Towsley, Estimation of Congestion Price Using Probabilistic Packet Marking. In *Proceedings of Infocom* 2003.

[3] C. Bandt, Self-similar sets. V. Integer matrices and fractal tilings of $\mathbf{R}^n$. *Proc. Amer. Math. Soc.*, 112(2):549–562, 1991.

[4] H. Burch and B. Cheswick, Tracing Anonymous Packets to Their Approximate Source. In *Proc. Usenix LISA '00*, 2000.

[5] L. Danzer, B. Grünbaum, and V. Klee, Helly's theorem and its relatives. In *Convexity*, volume 7 of *Proc. Symp. Pure Math.*, pages 101–180. American Mathematical Society, Providence, 1963.

[6] D. Dean, M. Franklin, and A. Stubblefield, An Algebraic Approach to IP Traceback. In *Proc. 2001 Network and Distributed System Security Symposium.*

[7] H. E. Debrunner, Tiling Euclidean d-space with congruent simplexes. In *Discrete geometry and convexity (New York, 1982)*, volume 440 of *Ann. New York Acad. Sci.*, pages 230–261. New York Acad. Sci., New York, 1985.

[8] T. Doeppner, P. Klein, and A. Koyfman, Using router stamping to identify the source of IP packets. In*Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 184–189, Athens, Greece, November 2000.

[9] Q. Dong, M. Adler, and K. Hirata, Efficient Schemes for Probabilistic Packet Marking. University of Massachusetts, Amherst Technical Report 2004-67.

[10] G. Gelbrich, Crystallographic reptiles. *Geom. Dedicata*, 51(3):235–256, 1994.

[11] M. Goodrich, Efficient Packet Marking for Large-Scale IP Traceback. *Proc. of 9th ACM Conf. on Computer and Communications Security (CCS)*, 2002, 117-126.

[12] S. Lee and C. Shields, Tracing the Source of Network Attack: A Technical, Legal and Societal Problem. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, June 2001.

[13] L. Lovász, Semidefinite programs and combinatorial optimization. In B. Reed and C. Linhares-Sales, editors, *Recent Advances in Algorithms and Combinatorics*, pages 137–194. Springer, New York, 2003.

[14] J. Matoušek, Nonexistence of 2-reptile simplices. *Discrete Comput. Geom.*, 2004. Submitted.

[15] S.-M. Ngai, V. F. Sirvent, J. J. P. Veerman, and Y. Wang, On 2-reptiles in the plane. *Geom. Dedicata*, 82(1-3):325–344, 2000.

[16] K. Park and H. Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In *Proc. IEEE INFOCOM '01*, pp. 338–347, 2001.

[17] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, Practical Network Support for IP Traceback. In *Proceedings of ACM SIGCOMM 2000* , pp. 295–306, August 2000.

[18] S. L. Snover, C. Waiveris, and J. K. Williams, Rep-tiling for triangles. *Discrete Math.*, 91(2):193–200, 1991.

[19] D. X. Song and A. Perrig, Advanced and authenticated marking schemes for IP traceback. In *Proc. IEEE INFOCOM '01*, 2001.

[20] R. Thommes and M. J. Coates, Deterministic Packet Marking for Congestion Price Estimation. In *Proc. IEEE INFOCOM '04*.