

# TIMING CHANNELS, ANONYMITY, MIXES, AND SPIKES

Ira S. Moskowitz  
Center for High Assurance Computer Systems  
Naval Research Laboratory  
Washington, DC 20375, USA  
email: moskowitz@itd.nrl.navy.mil

Richard E. Newman  
CISE Department  
University of Florida  
Gainesville, FL 32611-6120, USA  
email: nemo@cise.ufl.edu

## ABSTRACT

In this paper we consider how timing channels (from high assurance computing) arise in the study of certain anonymity systems. We then discuss how the same type of Shannon analysis for these timing channels applies to spikes (action potentials in the field of neuroscience).

## KEY WORDS

Action Potential, Spike, Neuron, Covert Channel.

## 1 Introduction

In the field of high assurance computing, covert channel analysis is an area concerned with illicit communication channels that exist contrary to system design [1, 2]. In general, covert channels are modeled by two types of Shannon communication channels [2]. The first is the *storage* channel, where all symbols take the same amount of time to pass through the channel. The storage channel “bandwidth” is given by the mutual information and capacity. These bandwidth terms are given in units of bits per symbol which are the same, modulo a normalization constant, as units of bits per unit time. A *timing* channel is more complicated in that the symbols take different amounts of time to pass through the channel. For a timing channel, the capacity should be expressed in units of bits per unit time. But going from bits per symbol to bits per unit time is not simply a matter of normalizing by a constant. Rather, for a timing channel the proper expression of capacity [3] involves optimizing the ratio of the mutual information (given in bits per symbol) to the expected time-cost of the symbols being sent across the channel.

Needless to say the analytic study of timing channels is much more difficult than storage channels, with closed form solutions usually only given for the simpler storage channels. However, closed form capacity results have been given for special cases and bounds have been given for some realistic situations (*e.g.* [4, 5, 6]).

A thrust of this paper is a preliminary timing channel analysis of certain anonymity systems. However, the ability to signal through time has been also looked at in several other areas of interesting research. The first and somewhat related area involves perceived time differences in signaling time in the area of quantum cryptography [7, 8]. However, this work does not seem to perform capacity calcu-

lations. A second, well studied, but apparently unrelated area, is *spikes* [9, 10, 11] from the neurosciences. In this paper we are concerned with the parallels between anonymity systems, timing channels, and spikes.

In [12, 13, 14, 15, 16] covert channels in anonymity systems was put on a firm foundation. However, that work was concerned only with storage channels and timed Mixes.<sup>1</sup> In this paper we look at how timing channels can be used as a metric for quasi-anonymity when studying threshold Mixes (which are designed to give one anonymity). It an irony of the terminology that timed Mixes are analyzed by storage channels, whereas threshold Mixes are analyzed by timing channels. Also, in the area of anonymity [18] has analyzed how (time) latency in the Tor anonymity system can be used to compromise anonymity. We note that their interest was in detecting the loss of perfect anonymity, not a capacity analysis.

As we will show in this paper, timing channels appear as covert channels in the study of Mixes and anonymity. As noted, timing channels also appear in the unrelated field of neuroscience when attempting to analyze the amount of information that is passed when a neuron “spikes”. The study of spikes has used more than a Shannon type analysis of the situation (that is capacity has not been the major concern) and it is hoped that this paper will serve as a motivation (noted in [19] also) for a deeper study of how the mathematical techniques of spikes can be used as metrics for anonymity via capacity. The area of spikes is the second thrust of this paper.

It is our hope that the reader will come away with both the knowledge of the covert channels in anonymity systems and the knowledge of Shannon channels in spikes. More importantly we hope that the reader of this paper will come away with the parallels between the two, and a desire to consider the synergy of the two very different areas.

## 2 Threshold Mix—Preliminaries

We will start by considering a threshold Mix [20] of threshold  $\theta \geq 2$ . This is a very simplistic Mix. The Mix is the exit

---

<sup>1</sup>In [17] Chaum describes a Mix as a communications interface that hides, from an eavesdropper, the correspondence between sender and receiver. Of course the success of this hiding is determined by such factors as the number of senders and the number of receivers. Mix theory comprises an major part of the current research and design of anonymity systems (a system designed to give the user anonymity from prying eyes).

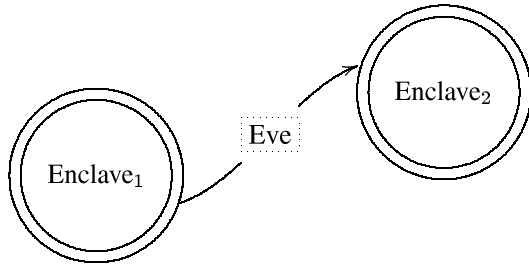


Figure 1. Restricted Passive Adversary Model.

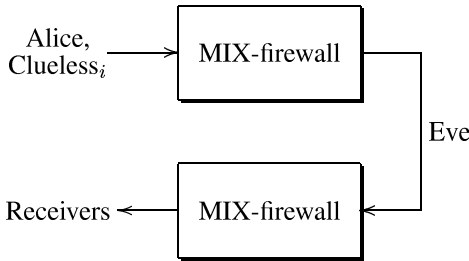


Figure 2. MIX-firewalls with Restricted Passive Adversary.

node of an enclave. Senders in the enclave send their messages to the Mix. The Mix pads the messages to a uniform size, adds a header and encrypts them, then stores them until it fires. The Mix has a buffer of size  $\theta$  (messages) and as soon as the buffer is filled, the Mix fires, forwarding the indistinguishable messages in a random order. We assume that the eavesdropper Eve is monitoring the traffic leaving the Mix. The Mix is actually a Mix-firewall in that Eve does not have direct knowledge of what is happening behind the firewall, thus Eve is a restricted passive adversary (RPA) and that is why we refer to the Mix as a Mix-firewall. Thus the Mix-firewall protects an enclave from prying eyes. In fact, we assume that we have two Mix-firewalls protecting the internal doings of two private enclaves, this is illustrated in Figure 1. Eve can only observe the timing and count the number of messages passing from Enclave<sub>1</sub> to Enclave<sub>2</sub>. We assume that in Enclave<sub>1</sub> there are benign users, referred to as Clueless<sub>*i*</sub> and a malicious user Alice who is attempting to communicate covertly with Eve by influencing the observations that Eve makes. This is illustrated in Figure 2, and was the same model used in [12].

What differs in this paper compared to [12] was that in [12] Eve did a count of the number of messages per unit time leaving the Mix-firewall protecting Enclave<sub>1</sub>. In this paper, since we have a threshold Mix,<sup>2</sup> Eve either counts 0 or  $\theta$  each time unit. That is the Mix-firewall either fires or it does not fire. We denote our units of time as a tick  $t$ . It is assumed that Alice and the Clueless<sub>*i*</sub> either send or do not send at most one message to the Mix-firewall of Enclave<sub>1</sub>

<sup>2</sup>In [12] a timing Mix of time one was considered.

every  $t$ . The messages are destined for the receivers in Enclave<sub>2</sub>, but Eve cannot determine which receivers, only that messages are being passed to Enclave<sub>2</sub>. We further assume that no processing time is involved and that when the Mix-firewall around Enclave<sub>1</sub> has  $\theta$  messages it fires. We also assume that Alice knows when the Mix-firewall fires. This greatly simplifies that mathematics and lets our results be used as a worst-case scenario. Of course the realism of this assumption must be called into question. However, we need these results as a first step for our future work. In this light we also assume that the Mix-firewall does not fire with less than  $\theta$  messages in it, but once at least  $\theta$  messages are in it, it fires all the messages, even if there are more than  $\theta$ . Eve makes no distinction if she sees more than  $\theta$  message leaving the Mix-firewall. Again, this simplifying assumption can be taken as a worst-case scenario.

### 3 Threshold Mix—No Clueless

In this situation there is only Alice in Enclave<sub>1</sub>. Alice either sends a message or does not send a message to the Mix-firewall. Since only Alice is sending messages, the quickest that the Mix-firewall can fire is at  $t = \theta$ , this happens when Alice acts as quickly as possible by sending a message at  $t = 1$  and then sending a second message at  $t = 2$ , etc. until the Mix buffer is filled and fires when  $\theta$  messages from Alice are received after time  $t = \theta$ . Since Alice can delay as long as she likes to send a message we see that Alice can cause the Mix-firewall to fire at any integer value of  $t \geq \theta$ . Since Alice is the only sender in Enclave<sub>1</sub> she has total control and there is no noise in the channel.

In general a covert communication channel where the output symbols are different time values that is noiseless, discrete and memoryless is called a *simple timing channel* [4]. For a simple timing channel we let  $S_n$  denote all the unique output symbol sequences of duration  $n$  ticks. Then the capacity, in units of bits per tick, [21, 22, 4] of the simple timing channel is given by<sup>3</sup>

$$C = \limsup_{n \rightarrow \infty} \frac{\log |S_n|}{n}. \quad (1)$$

Of course the capacity is the best that one can do. Shannon [21] has shown that capacity is the upper bound for asymptotically error-free communication. In general, designing a pragmatic code to achieve capacity is usually quite problematic. It is shown in [4] that the capacity<sup>4</sup> ( $C$ ) of the simple timing channel for the unbounded case where Eve has the infinite output alphabet  $\{\theta, \theta + 1, \theta + 2, \theta + 3, \dots\}$ , is (surprisingly) given by

$$C = \log \omega_{[\theta, \infty]} \quad (2)$$

where  $\omega_{[\theta, \infty]}$  is the unique positive root of

$$1 - (x^{-\theta} + x^{-1}). \quad (3)$$

<sup>3</sup>Shannon [21] erroneously used limit, instead of the limit superior.

<sup>4</sup>All logarithms are base two.

Of course the capacity slowly decreases from a value of .6942, when  $\theta = 2$  to zero, as  $\theta$  increases (e.g.,  $C = .26$ , when  $\theta = 10$ , and  $C = .0832$ , when  $\theta = 50$ ). The trivial case when  $\theta = 1$  reduces to finding the root of  $1 - 2x^{-1}$ , which is trivially 2, thus resulting in  $C = 1$ .

We note that if Alice is not allowed to delay the Mix firing indefinitely, then the equation changes. Say that Alice may only delay the Mix filling and then firing by  $N$  time increments. That is Eve has the finite output alphabet  $\{\theta, \theta + 1, \dots, \theta + N\}$ , where each output symbol  $\theta + i$  takes time  $\theta + i$  to transit from Alice to Eve. Eq. (1) above still holds, but the polynomial Eq. (3) changes. The capacity is

$$C = \log \omega_{[\theta, N]} \quad (4)$$

where  $\omega_{[\theta, N]}$  is the unique positive root of

$$1 - (x^{-\theta} + x^{-(\theta+1)} + \dots + x^{-(\theta+N)}). \quad (5)$$

Note, as discussed above (see [4, Cor. 3.1]) that as  $N \rightarrow \infty$ , Eq. (4) reduces to Eq. (2). The expression for capacity as given in Eq. (4) follows from Shannon's asymptotic definition of capacity for a noiseless channel [21]. Shannon also showed [21, App. 4] that Eq. (4) could be derived by entropy considerations. Let  $X$  be the random variable that probabilistically models the behavior of Alice. That is  $P(X = \theta + i)$  is the probability that Alice sends the symbol  $\theta + i$  to Eve. Let  $T$  be the random variable that models the arrival time of the symbol that Alice sends to Eve. Since this channel is noiseless  $X$  and  $T$  have the same distributions. The mutual information in this noiseless case is given by  $I_t = \frac{H(X)}{E(T)}$ .

**Theorem 1 (Shannon)** *The maximum of  $I_t$ , over differing  $X$  distributions<sup>5</sup>, is the capacity as given in Eq. (4). In fact the distribution for  $X$  that achieves capacity is given by setting  $P(X = \theta + i) = \omega_{[\theta, N]}^{-(\theta+i)}$ , for  $i = 0, \dots, N$ .*

Now we leave the discussion of anonymous communication systems and turn to the (what seems at first to be) unrelated field of neuroscience.

## 4 Spikes

The neuron [10, 23] is the basis for the nervous system. It is a specialized cell designed to transmit information. The neuron has inputs called *dendrites*, and a CPU-like cell body called the *soma*, and an output device called the *axon*.

There are many dendrites leading into the soma. The soma sends information out to another neuron by causing an electrical pulse to propagate through the axon. The axon communicates this to another neuron via a nerve *synapse*. In neuroscience the sharp change in voltage at the beginning of this pulse (or action potential) is called the spike. The resting potential of the axon across the cell membrane is about -70mV. The spike at the beginning of the pulse

<sup>5</sup>That is the range of  $X$  is fixed, but the probabilistic values may vary, provided they still form a probability distribution.

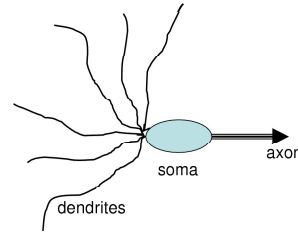


Figure 3. Basic Neuron

jumps to about 50mV and then dissipates back down to the resting potential. It is the existence of the spike that is interpreted as the information, not the particular voltage of the spike. What is important is the *timing* of the spikes.<sup>6</sup> The axon passes information to another neuron via a chemical process between the exiting axon and the entering dendrite over a very small region called the *synaptic cleft*. This transmission is called *synaptic transmission*.

The action potential travels along the axon at speeds less than 1 and up to several hundred kilometers per hour (the size of the axon and whether or not the axon has a myelin covering affect the speed). However, most axons are on the order of  $10^{-2}$  or  $10^{-3}$  meters in length. The duration of a spike is about 1-2ms. Spikes are separated, two spikes cannot “fire” at once. There is a minimum refractory period between spikes. It is the *spike train* that passes information.<sup>7</sup>

Just as the neuron encodes information by the spike train, in either the frequency of spikes or, equivalently, the time between spikes, a covert channel operating through a threshold mix can encode information by the time between mix firings. The insider does this by modulating the rate at which she pours messages into the threshold mix. Likewise, just as the neuron has a refractory period due to the physical transport of ions across the membrane to rebuild the resting potential, a threshold mix has a refractory period during which the senders accumulate messages in its buffers before its threshold trigger condition is met. This minimum time depends on the threshold value,  $\theta$ , and the maximum aggregate sending rate of the senders,  $R = \sum_{i=1}^N R_i$ , where there are  $N$  senders and sender  $i$  has rate  $R_i$ :

$$\text{Min Latency} = \lceil \theta / \sum_{i=1}^N R_i \rceil.$$

Analysis of these two systems modeled in this way should be identical, and each can inform the other.

<sup>6</sup>Thus we see the obvious parallel with threshold Mixes where the timing of an impulse is what sends the information.

<sup>7</sup>There is controversy over whether the shape of the spike also passes information.[24, Sec. 1]. We will not go into this question further in this paper.

## 4.1 MacKay-McCulloch Analysis

In [24] a Shannon-type capacity analysis is performed by the authors.<sup>8</sup> In [24, sec. III], they discuss the limiting information-content of a (synaptic) signal. MacKay and McCulloch state “The limiting *selective information-capacity* of a signal-carrying element will then be the product of the average information-content per signal, with the maximum mean signal-frequency allowable for the modulation-system adopted.” This does not agree with Thm. 1 (as given above). MacKay and McCulloch are saying that  $E(T)$  is maximized independently of  $H(X)$ . This is incorrect, the ratio of the two terms is what must be maximized. MacKay and McCulloch then make a similar second error (this one they catch later in [25]). They state that all symbols should be sent via a uniform distribution. In [25], they note this and state that the probabilities should actually not be uniform, but that their assumption of a uniform distribution still gives one the correct order of magnitude. They correctly note that quicker symbols should be used more often than longer time symbols. We will discuss their “correction” in more detail.

The concern for MacKay and McCulloch is the same as ours, they are concerned with *pulse interval modulation* (symbols take different times to send). This is in contrast to *pulse position modulation* (symbols can be assumed to take the same amount of time).

MacKay and McCulloch set three terms for the spiking across a synaptic link. The term  $T_R$  is the minimum time between spikes. The existence of a minimum “recharging” time as discussed above is based upon biophysical principles. However a spike need not be at  $T_R$ , the spike impulse may be delayed by increments of  $\Delta T$  up to a maximum value of  $T_M$ . The actual arrival time is given as  $T_S$ , where  $T_S = T_R + i\Delta T$ . The interval between  $T_S$  and  $T_M$  is of size  $n\Delta T$ . Therefore, there are  $n + 1$  symbols to play with. We note that MacKay and McCulloch are off by one in their count; they assume that there are  $n$  symbols to use. Clearly, if  $n = 1$ , then there are two symbols:  $T_R$  and  $T_M = T_R + \Delta T$ . The best one could hope for would be for the spike impulses transmit  $\log(n + 1)$  bits of information per  $T_R$ , and the worst would be  $\log(n + 1)$  bits per  $T_M$ . Both of these are unrealistic extremes. The correct capacity is given by Eq. (4), and Thm.(1) shows us that the capacity is the maximum of the ratio of the input entropy to the expected time for a spike to transit. The incorrect formula of MacKay and McCulloch is

$$C = \frac{\log n}{(T_R + T_M)/2} \quad (6)$$

The numerator is simply the log of the (incorrect) number of symbols, and the denominator is the average time for a symbol to be received, provided that every symbol is sent with the same probability.

<sup>8</sup>Unfortunately there is an error in their analysis, which they noted a year later in [25]. However, we feel that their comments in their erratum require further discussion and analysis, which we present here.

## 4.2 Correction of MacKay and McCulloch

Since MacKay and McCulloch has acknowledged their error, not for  $n$  vs.  $n + 1$ , but for their formula in general, we will concentrate mostly on the correct expression for the capacity Eq. 4. Using their example:  $T_R = 1$ msec,  $\Delta T = .05$ msec, and  $T_M = 2$ msec, we see by using Eq. (4) that  $C \approx 3.13$  b/msec. Using the method proposed in [24] we would (incorrectly) divide the maximal entropy (based incorrectly on 20 instead of 21 symbols) by the average time based upon a uniform distribution. This results in  $\frac{\log(20)}{1.5} \approx 2.88$  b/msec (thus, their erroneous results of about 2.9 b/msec). They do comment in [25] that even though their formulas are incorrect that “...The improvement that can be effected does not, however, affect the order of magnitude of the results, and only reinforces our qualitative conclusions.” Certainly the correct result for the above example is the same order of magnitude as their incorrect result. However, their claims about the same order of magnitude do not hold in general as we show below. Thus, a contribution of our work is the correct analysis of the scenario described by MacKay and McCulloch.

Consider the three following channels  $Channel_i, i = 1, 2, 3$  with respective capacities  $C_i$ , with  $T_R = 1$  msec and  $\Delta T = .05$  msec.

$Channel_1$ : This is the channel already discussed,  $T_M = 2$  msec. We have shown that  $C_1 \approx 3.1270$  b/msec. Note that there are 21 distinct timing symbols in this channel. One can consider this a mid-range exploitation.

$Channel_2$ :  $T_M = 1.05$  msec. This is a channel with only two symbols. We have that  $C_2 = .9758$  b/msec.

$Channel_3$ :  $T_M = 6$  msec. This channel has 101 timing symbols and calculations show that  $C_3 = 3.2363$  b/msec.

Considering  $Channel_3$ , if we use MacKay and McCulloch’s Eq. (6) we have that  $C = 1.9023$  (using  $n = 101$ ), or 1.8982 (using  $n = 100$ ). These are still within the same order of magnitude as 3.2363. We may rewrite MacKay and McCulloch’s Eq. (6) as

$$C = \frac{\log n}{T_R + n\frac{\Delta T}{2}} \quad (7)$$

As  $n \rightarrow \infty$ , Eq. (7) implies that  $C \rightarrow 0$ . This is not true thus dispelling the notion in [25] that their error does not affect the order of magnitude of the correct capacity. By using Eq. (2) (from [4, Cor. 3.1]) we can show that the limiting capacity as  $n$  grows without bound is  $C_\infty = 3.2364$  b/msec. In fact, as discussed in [4, Cor. 3.1], the larger  $T_M$  is the larger the capacity is. Of course, as we can see in our own examples, the rate of increase greatly slows as  $n$  grows, so in reality we can get close to asymptotic capacity with a pragmatic choice of  $n$ .

Thus, MacKay and McCulloch’s capacity expressions, nor their conclusions should be relied upon. However, this is not to take away from their interesting and novel exposition of the physical problem of the information theoretic capacity of the neuronal action potential (spike). MacKay and McCulloch made the error that many make

thinking that a uniform distribution and averaging things out is about the best you can do. For timing channels we see that this is not true. However, for certain storage channels this is true as we discuss below.

## 5 Comparison of Fixed Baud and Variable Baud Channels

At this point we wish to bring up an interesting distinction between discrete memoryless channels (DMC) where the symbols take the same amount of time, versus DMCs with varying time symbols. For a constant symbol time 2-input DMC [26] Majani and Rumsey showed that the optimal distribution for  $X$  was such that each of the two symbols was sent with a probability between  $\frac{1}{e}$  and  $1 - \frac{1}{e}$ . They further went on to show that if one used a uniform distribution for 2-valued distribution of  $X$  that one would not be too far off from the capacity. They conjectured similar results for a  $n$ -input constant symbol time DMC. Recently, Liang [27] was able to prove Majani and Rumsey's conjectures. For a DMC where the symbols take different amounts of time, the Majani and Rumsey results do not carry over (they never implied that they would). We see this directly from the probability distribution described in Thm. 1. A concrete counterexample is given in [28].

## 6 Conclusions

We have shown how the same type of information theoretic analysis correctly applied to spikes is the same model for threshold Mixes when there is only a malicious user Alice in the first enclave. Thus, we have corrected results from early work in the neurosciences. In reality we need to extend our information theoretic analysis to include the situations where the  $\text{Clueless}_i$  are also in  $\text{Enclave}_1$ . It is not clear how this applies to spikes. Since the  $\text{Clueless}_i$  act as noise, and lessen the capacity in the anonymity system one must consider how noise could be introduced (if at all) into the spike model. We leave this for future work. However, we end with a brief discussion of how to deal with the  $\text{Clueless}_i$ .

The  $\text{Clueless}_i$  act as noise, because of that we can no longer use an algebraic approach as given by Thm. 1. We are in the situation of a noisy timing channel. The only algebraic approach that we know of is given in [28], and this is for a very specialized and simplistic noisy timing channel. Instead of using  $I_t = \frac{H(X)}{E(T)}$ , we must instead maximize  $I_t = \frac{H(X) - H(X|Y)}{E(T)}$ , which is much more complicated. The conditional entropy term  $H(X|Y)$  is needed to model the noise from the  $\text{Clueless}_i$ .

## 7 Acknowledgments

Research supported by the Office of Naval Research. We appreciate the time of Ira Schwartz and Thomas O'Shaughnessy of NRL. We also thank the anonymous reviewers and Keye Martin for their helpful comments.

## References

- [1] Butler W. Lampson. A note on the confinement problem. *CACM*, 16(10):613–615, 1973.
- [2] Ira S. Moskowitz and Myong H. Kang. Covert channels — here to stay? In *Proc. COMPASS'94*, pages 235–243, Gaithersburg, MD, June 27- July 1 1994. IEEE Press.
- [3] Sergio Verdú. On channel capacity per unit cost. *IEEE Transactions on Information Theory*, 36(5):1019–1030, 1992.
- [4] Ira S. Moskowitz and Allen R. Miller. Simple timing channels. In *IEEE Computer Society Symposium on Research in Security and Privacy*, pages 56–64, Oakland, CA, May 16-18 1994.
- [5] Allen R. Miller and Ira S. Moskowitz. Reduction of a class of Fox-Wright psi functions for certain rational parameters. *Computers & Mathematics with Applications*, 30(11):73–82, 1995.
- [6] Myong H. Kang, Ira S. Moskowitz, and Daniel C. Lee. A network Pump. *IEEE Transactions on Software Engineering*, 22(5):329–328, 1998.
- [7] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled two-photon source for quantum communication. *Physical Review Letters*, 82(12):2594–2597, 22 March 1999.
- [8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Physical Review Letters*, 84(20):4737–4740, 15 May 2000.
- [9] Fred Rieke, David Warland, Rob de Ruyter van Steveninck, and William Bialek. *Spikes — Exploring the Neural Code*. MIT Press, 1999.
- [10] Wulfram Gerstner and Werner Kistler. *Spiking Neuron Models — Single Neurons, Populations, Plasticity*. Cambridge Univ. Press, 2002.
- [11] Hugh R. Wilson. *Spikes, Decisions and Actions*. Oxford Univ. Press, 1999.
- [12] Ira S. Moskowitz, Richard E. Newman, Daniel P. Crepeau, and Allen R. Miller. Covert channels and anonymizing networks. In *ACM WPES*, pages 79–88, Washington, October 2003.

- [13] Ira S. Moskowitz, Richard E. Newman, and Paul F. Syverson. Quasi-anonymous channels. In *IASTED CNIS*, pages 126–131, New York, December 2003.
- [14] Ira S. Moskowitz, Richard E. Newman, Daniel P. Crepeau, and Allen R. Miller. A detailed mathematical analysis of a class of covert channels arising in certain anonymizing networks. NRL Memorandum Report NRL/MRL/5540–03-8691, NRL, August 2003.
- [15] Richard E. Newman, Vipin R. Nalla, and Ira S. Moskowitz. Covert channels and simple timed mix-firewalls. NRL Memorandum Report NRL/MR/5540–04-8812, NRL, 2004.
- [16] Richard E. Newman, Vipin R. Nalla, and Ira S. Moskowitz. Anonymity and covert channels in simple timed mix-firewalls. In *WPES*, pages 1–16, Toronto, May 2004. Springer, LNCS 3424.
- [17] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
- [18] Steven J. Murdoch and George Danezis. Low-cost traffic analysis of Tor. *Preprint*, 2005.
- [19] Venkat Anantharam and Sergio Verdú. Reflections on the 1998 information theory society paper award: Bits through queues. *IEEE Information Theory Newsletter*, pages 100–102, 1999.
- [20] Andrei Serjantov, Roger Dingledine, and Paul Syverson. From a trickle to a flood: Active attacks on several mix types. In *Proc. IH 2002*, pages 36–52, Oct. 2002.
- [21] C. E. Shannon. The mathematical theory of communication. *Bell Sys. Tech. J.*, 30:50–64, 1948.
- [22] Ralph M. Krause. Channels which transmit letters of unequal duration. *Information and Control*, 5:13–24, 1992.
- [23] Richard F. Thompson. *The Brain*. W.H. Freeman and Co., 1985.
- [24] Donald M. MacKay and Warren S. McCulloch. The limiting information capacity of a neuronal link. *Bulletin of Mathematical Biophysics*, 14:127–135, 1952.
- [25] Donald M. MacKay and Warren S. McCulloch. Erratum—The limiting information capacity of a neuronal link. *Bulletin of Mathematical Biophysics*, 15:107, 1953.
- [26] E.E. Majani and H. Rumsey. Two results on binary input discrete memoryless channels. In *IEEE International Symposium on Information Theory*, page 104, June 1991.
- [27] Xue-Bin Liang. An algebraic, analytic and algorithmic investigation on the capacity and capacity-achieving input probability distributions of finite-input finite-output discrete memoryless channels. *Preprint*, April 2004.
- [28] Ira S. Moskowitz, Steven J. Greenwald, and Myoung H. Kang. An analysis of the timed Z-channel. *IEEE Transactions on Information Theory*, 44(7):3162–3168, 1998.