consider $N$ as a continuous variable and seek $N^*$ so that $\partial F_0/\partial N = 0$. The result is

$$(N^* - M)\exp(N^* \ln s) = \frac{1 - Mp}{1 - s^2} \tag{C.3}$$

or, because $p < 1/M$ and $s < 1$, $N^* > M + (1 - Mp)/(1 - s^2)$ which implies $N^* > M + 1$. Although these channels are simple, they constitute a useful model for comparison with the channels studied in the text, which are perhaps of greater practical interest.

The special case of $N^* = M$ and $p = r$ should be mentioned. The Gram matrix for this channel is given by (B.4) and the solution to the quantum detection problem is known [17]. The matrix elements $r_{ij} = \langle \alpha_i | p_j \rangle$ are given by

$$r_{ii} = p = q + \sqrt{1 - g} \tag{C.4}$$

$$r_{ij} = q = \frac{\sqrt{1 + (M-1)g} - \sqrt{1-g}}{M} \tag{C.5}$$

where $g = \langle \alpha_i | \alpha_j \rangle = \exp(-\mu^2)$ for all $i, j$. We easily obtain for the cutoff rate

$$F_0^{(M)} = \ln \frac{M}{1 + 2(M-1)pq}. \tag{C.6}$$

Following the method established in Appendix I and based on the inversion of the matrix $G$ as defined by (B.4), with $a = g$, we arrive at

$$F_0^{(M)} = \ln \frac{M}{1 + (M-1)g}. \tag{C.7}$$

Note that (C.7) is also the result given by (C.6) for $g \to 0$. Analysis of (C.6) is most useful. In particular we can prove for $\mu < \mu_0$ with $\mu_0 \approx \ln 2M/2$, that

$$F_0^{(2)} > F_0^{(3)} > F_0^{(4)}, \tag{C.8}$$

which is similar to the result given in [15, p. 318].

## References


[1] J. R. Pierce, E. C. Posner, and E. R. Rodemich, "The capacity of the photocounting channel," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 61–77, Jan. 1981.

[2] J. R. Lesh, "Optical communications research program to demonstrate 2.5 bits/detected photon," *IEEE Commun. Mag.*, vol. 20, pp. 35–37, 1982.

[3] G. Lindblad, "Entropy, information and quantum measurements," *Comm. Math. Phys.*, vol. 33, pp. 305–322, 1973.

[4] M. H. Partovi, "Entropic formulation of uncertainty for quantum measurements," Preprint SLAC-PUB-3100, Apr. 1983.

[5] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1965.

[6] E. B. Davies, *Quantum Theory of Open Systems*. New York: Academic, 1976.

[7] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Probl. Inform. Transm.* (transl. from *Problemy Peredachi Informatsii*), vol. 9, pp. 3–11, July–Sept. 1973.

[8] ——, "Information theoretical aspects of quantum measurements," *Probl. Inform. Transm.* (transl. from *Problemy Peredachi Informatsii*), vol. 9, pp. 31–42, Apr.–June 1973.

[9] C. W. Helstrom, *Quantum Detection and Estimation Theory*. New York: Academic, 1976.

[10] E. B. Davies, "Information and quantum measurement," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 596–599, Sept. 1978.

[11] A. S. Holevo, "Towards the mathematical theory of quantum communications channels," *Probl. Inform. Transm.* (transl. from *Problemy Peredachi Informatsii*), vol. 8, 1972.

[12] V. P. Belavkin and R. L. Stratonovich, "Optimization of processing of quantum signals according to an information criterion," *Radio Eng. Electr. Phys.*, vol. 18, pp. 1349–1354, 1973.

[13] M. Ohya, "On compound state and mutual information in quantum information theory," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 770–774, Sept. 1983.

[14] R. S. Ingarden, "Quantum information theory," *Reps. Math. Phys.*, vol. 10, pp. 43–72, 1976.

[15] J. Wozencraft and I. Jacobs, *Principles of Communication Engineering*. New York: Wiley, 1965.

[16] J. L. Massey, "Capacity, cutoff rate and coding for a direct detection optical channel," *IEEE Trans. Commun.*, vol. COM-29, pp. 1615–1622, Nov. 1981.

[17] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimal testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 125–134, Mar. 1975.

[18] V. P. Belavkin, "Optimum distinction of non-orthogonal quantum signals," *Radio Eng. Electr. Phys.*, vol. 25, pp. 39–47, 1973.

[19] J. R. Klauder and E. C. G. Sudarshan, *Fundamentals of Quantum Optics*. New York: Benjamin, 1968.

[20] C. W. Helstrom, M. Charbit, and C. Bendjaballah, "Cut-off rate performance for PSK modulated coherent states," *Opt. Commun.*, vol. 64, pp. 253–255, 1987.

[21] C. Bendjaballah and M. Charbit, "Cut-off rate for phase modulated coherent states," presented at COCT'87, Aug. 24–27, 1987, Karuizawa, Japan.

[22] M. Charbit, C. Bendjaballah, and C. W. Helstrom, "Cut-off rate for $M$-ary PSK modulation channel with optimal quantum detection," to appear in *IEEE Trans. Inform. Theory*.

[23] D. L. Snyder and I. B. Rhodes, "Some implications of the cut-off rate criterion for coded direct detection optical communication systems," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 327–338, May 1980.

[24] J. H. Shapiro, "Quantum noise and excess noise in optical homodyne and heterodyne receivers," *IEEE J. Quant. Electron.*, vol. QE-21, pp. 237–250, 1985.

[25] J. H. Shapiro, "On the near-optimum binary coherent state receiver," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 490–491, July 1980.

[26] H. P. Yuen, "Two-photon coherent states of the radiation field," *Phys. Rev.*, vol. A-13, pp. 2226–2243, 1976.

[27] H. P. Yuen and J. H. Shapiro, "Optical communication with two-photon coherent states, Part I," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 657–668, Nov. 1978.

[28] C. Bendjaballah, M. Charbit, and G. Oliver, "Capacity and cut-off rate for optical communication systems using photon counting techniques," in *Coherence and Quantum Optics V*, L. Mandel and E. Wolf, Eds. New York: Plenum, 1984, pp. 55–62.

[29] R. J. McEliece, "Practical codes for photon communication," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 393–397, July 1981.


# Holographic Dispersal and Recovery of Information

F. P. PREPARATA, FELLOW IEEE

***Abstract*—A simple scheme for dispersal-recovery of digital information based on the discrete Fourier transform is discussed.**

In a recent paper [1] Rabin proposes an attractive information dispersal scheme that is applicable, for example, to fault-tolerant transmission of information in networks and secure data storage. Rabin's method recodes a file $F$ of $L$ characters into $n$ files $F_1, F_2, \cdots, F_n$, each consisting of $L/m$ characters ($m < n$), so that the original file $F$ can be reconstructed using only $m$ of the files $F_1, F_2, \cdots, F_n$. The scheme is based on an $n \times m$ matrix $A$ with the property that any $m$ of its rows form a nonsingular matrix; the reconstruction, for large files, costs $O(m)$ operations per character. Typically, $n$ and $m$ are comparable in size, so that $k \triangleq n - m$, called the "redundancy," is of a lower order of magnitude. In this correspondence we present a different implementation of Rabin's scheme, whose recovery cost is $O(\log m + k)$ operations per character assuming $m = \Theta(n)$; for example, when

Manuscript received December 22, 1988. This work was supported in part by the Joint Services Electronics Program under Contract N00014-84-C-0149.

The author is with the Department of Electrical and Computer Engineering, Coordinated Science Laboratory, University of Illinois, 1101 West Springfield Avenue, Urbana, IL 61801.

IEEE Log Number 8930784.

$k = \Theta(\log n)$ this cost drops from $O(m)$ to $O(\log m)$ per character. Since our implementation is based on the Fourier transform, it is appropriate to name it "holographic."

Let $n$ and $m$ be two given integers ($n > m$). The integer $n$ is chosen highly composite, typically a power of 2. It is known [2] that there exists a prime $p$ of the form $p = cn + 1$ which is representable with $s = \Theta(\log n)$ bits. Then $\mathscr{Z}_p$, the field of integers modulo $p$, contains a primitive root of unity $\omega$ of order $n$ and supports an $O(n \log n)$-step fast Fourier transform on $n$ points. Without loss of generality, we may assume that $F$ consists of $m$ characters of $(s-1)$ bits each (each character being an element of $\mathscr{Z}_p$), since the same process is applicable to each of the $m(s-1)$-bit blocks into which the original file can be segmented. We shall encode $F$ into $n$ elements of $\mathscr{Z}_p$ in the following manner. Let $V$ be the $n \times n$ Fourier matrix corresponding to primitive root $\omega$, i.e., $(V)_{ij} = \omega^{ij}$ and $(V^{-1})_{ij} = \omega^{i(n-j)} n^{-1}$, $0 \le i, j < n$. Let $F = \{f_1, \cdots, f_m\}$, $f_j \in \mathscr{Z}_p$, and let $\boldsymbol{f} = (0, \cdots, 0, f_1, f_2, \cdots, f_m)$ be an $n$-component vector. The vector $\boldsymbol{g} = (g_1, g_2, \cdots, g_n)$ defined by

$$\boldsymbol{g}^T = V\boldsymbol{f}^T$$

is the discrete Fourier transform of $\boldsymbol{f}$ and gives the $n$-character encoding of file $F$. We now show how to reconstruct $\{f_1, \cdots, f_m\}$ from an arbitrary $m$-term subsequence $(g_{i_1}, g_{i_2}, \cdots, g_{i_m})$ of $(g_1, \cdots, g_n)$.

We define $J \triangleq \{j_1, \cdots, j_k\} = \{1, \cdots, n\} - \{i_1, \cdots, i_m\}$. We also let $\tilde{V}$ denote the $k \times n$ matrix consisting of the first $k$ rows of $V^{-1}$ and $\tilde{V}_J$ the $k \times k$ matrix consisting of the columns of $\tilde{V}$ corresponding to index set $J$. Then, from the definition of $\boldsymbol{f}$ we obtain

$$\tilde{V}\boldsymbol{g}^T = (0, \cdots, 0)^T$$

and consequently the unknown $(g_{j_1}, \cdots, g_{j_k})$ are obtained from

$$\tilde{V}_J (g_{j_1}, \cdots, g_{j_k})^T = (c_1, \cdots, c_k)^T,$$

where the terms $c_1, \cdots, c_k$ are computable with $2km$ operations in $\mathscr{Z}_p$ from $\tilde{V}$ and the known quantities $(g_{i_1}, \cdots, g_{i_m})$. We now observe that $\tilde{V}_J$ is proportional (by the factor $n^{-1}$) to a Vandermonde matrix for any choice of $J$ and is therefore invertible in time $O(k^2)$ [3, p. 122]. Once $\tilde{V}_J^{-1}$ is available, the values of the unknowns $g_{j_1}, \cdots, g_{j_k}$ are computed with $2k^2$ operations in $\mathscr{Z}_p$ and the vector $\boldsymbol{g}$ is fully reconstructed; vector $\boldsymbol{f}$ is then obtained as the inverse Fourier transform of $\boldsymbol{g}$ with $O(n \log n)$ operations in $\mathscr{Z}_p$. Combining the above observations and using the facts that $k \ll m$ and $m \sim n$, we use $O(k + \log m)$ operations in $\mathscr{Z}_p$ to recover each character (itself an element of $\mathscr{Z}_p$) of the original file $F$.

*Remark:* From a coding theorist's viewpoint, the above dispersal-recovery scheme is a $k$-erasure correcting code of length $n$ over $\mathscr{Z}_p$. As an erasure-correcting code, in the very special case where $p - 1 = n = 2^s$, it has efficiency comparable to that of a Reed–Solomon code of length $(n-1)$ over GF($2^s$) (see, e.g., [4, sec. 8.6]).

## References


[1] M. O. Rabin, "Efficient dispersal of information for security load balancing and fault tolerance," *JACM*, vol 36, no. 2, pp. 335–348, Apr. 1989.

[2] S. S. Wagstaff, Jr., "Greatest of the least primes in arithmetic progressions having a given modulus," *Math. Comput.*, 33, pp. 1073–1083, 1979.

[3] G. H. Golub and C. F. van Loan, *Matrix Computations*. Baltimore, MD: Johns Hopkins Univ. Press, 1983.

[4] R. J. McEliece, *The Theory of Information and Coding*. Reading, MA: Addison-Wesley, 1977.


# A Simple Window Random Access Algorithm with Advantageous Properties


MICHAEL PATERAKIS, MEMBER, IEEE, AND
P. PAPANTONI-KAZAKOS, SENIOR MEMBER, IEEE



***Abstract*—A simple full feedback sensing window random access algorithm is proposed and analyzed. The throughput of the algorithm is 0.429; its delay and resistance to feedback channel errors are better than those induced by the Capetanakis's window algorithm. In addition, the simple operations of the algorithm allow for the analytical evaluation of the output traffic interdeparture distribution.**


## I. Introduction

In systems where independent users transmit through a single common channel, the deployment of random access transmission algorithms is frequently desirable for three reasons. 1) They are implemented independently by each user, without a priori coordination among the users. 2) They are insensitive to changing user population. 3) They induce low delays for low input rates when the user traffic is bursty.

We propose and analyze a full feedback sensing window random access algorithm. The algorithm was first proposed for systems with strict delay limitations [3] and requires that each user know the overall feedback history (full feedback sensing). The proposed algorithm has the following interesting properties. 1) It can be easily modified to operate under limited feedback sensing, where each user follows the feedback history from the time s/he generates a message to the time when this message is successfully transmitted. 2) When the Poisson user model is adopted, the algorithm attains the same throughput as that attained by Capetanakis's dynamic algorithm [1], while it induces lower delays for arrival rates above 0.30, and better resistance to feedback channel errors. 3) The simple operations of the algorithm allow analytical evaluation when strict delay limitations exist [3]. Its simplicity, together with its regenerative properties, provide the means for the analytical evaluation of the output traffic interdeparture distribution induced by the algorithm. The analysis of the latter distribution is important when several systems that use some random access algorithm (RAA) for internal transmissions interact; the corresponding distribution is far more difficult to obtain when either Capetanakis's [1] or Gallager's [2] algorithm is deployed. 4) Compared to Gallager's algorithm [2], the proposed algorithm operates and can be analyzed in systems where the Poisson user model is not valid (e.g., when more than one packet can be generated at a given time instant). The feasibility of the analysis depends on the specific arrival statistics.

In Section II the system model is presented, and the algorithm is described. In Section III throughput and delay analysis for the Poisson user model is presented. In Section IV the performance of the algorithm in the presence of feedback channel errors and


Manuscript received February 8, 1988; revised December 1988. This work was supported in part by the U.S. Office of Naval Research under Contract N00014-86-K-0742 and in part by the National Science Foundation under Grant ECS-85-06916. The material in this correspondence was presented at the IEEE Infocom Conference, New Orleans, LA, March 1988.



M. Paterakis is with the Computer and Information Science Department, Smith Hall, University of Delaware, Newark, DE 19716.

P. Papantoni-Kazakos is with the Electrical Engineering Department, Thornton Hall, University of Virginia, Charlottesville, VA 22901.



IEEE Log Number 8930785.