

## PUBLISHER

Randolph A. Nanna  
Tel: 301-209-3102  
rnanna@aip.org

## ASSOCIATE PUBLISHER/EDITOR

Kenneth J. McNaughton  
Tel: 301-209-3051  
kmcnaugh@aip.org

## ART DIRECTOR

Steven R. Black

## SENIOR CONTRIBUTING EDITOR

Patrick Young

## CONTRIBUTING EDITORS

Jay C. Cherniak  
Nancy Forbes  
Eric J. Lerner  
Jennifer Ouellette

## CIRCULATION DIRECTOR

Jeff Bebee

## PUBLISHING ASSISTANT

Stephanie Jankowski

## ADVISORY COMMITTEE

Don Christiansen (chair),  
Peter Brown, Vincent M. Donnelly,  
William H. Prest, Thomas R. Steele,  
Richard E. Swanson, Mark Talwani,  
Randolph A. Nanna (staff liaison)

## ADVERTISING MANAGER

Abby Singer Klar

## SR. ADVERTISING PRODUCTION MANAGER

Christine DiPasca

## SENIOR PRODUCTION ASSISTANT

Rita C. Wehrenberg

## EDITORIAL OFFICES

One Physics Ellipse  
College Park, MD 20740-3842  
Tel: 301-209-3051  
Fax: 301-209-0842  
e-mail: tip@aip.org

## ADVERTISING OFFICES

Tel: 800-247-2242

## WORLD WIDE WEB

www.tipmagazine.com

AMERICAN  
INSTITUTE  
OF PHYSICS

## EXECUTIVE DIRECTOR AND CEO

Marc H. Brodsky

## MEMBER SOCIETIES

The American Physical Society  
Optical Society of America  
Acoustical Society of America  
The Society of Rheology  
American Association of Physics Teachers  
American Crystallographic Association  
American Astronomical Society  
American Association of Physicists in Medicine  
American Vacuum Society  
American Geophysical Union

## OTHER MEMBER ORGANIZATIONS

Corporate Associates  
Sigma Pi Sigma Physics Honor Society  
Society of Physics Students

# Nobel Prizes

I was pleased to read Marc Brodsky's comment about the Nobel Prize in Physics recently awarded to Jack Kilby for his part in the invention of the integrated circuit (*The Industrial Physicist*, December 2000, pp. 8–11). The lack of recognition of the significance of engineers is hardly a recent phenomenon. Scientists traditionally have received the credit for advancing the cause of mankind with discoveries that might never have benefited anybody without the added value of innovative engineering skill. Let us all keep in mind that neither could function without the other.

Alvin G. Sydnor  
Boothwyn, Pennsylvania

I wish to add my two cents worth to your article "Nobel Prizes Honor Innovations in Electronics." Although innovations in semiconductor devices were seldom the work of a single individual, I acknowledge the vigorous pursuit and the patents generated by Kilby and Noyce, and I stand in strong support of this award. However, in the period from 1956 to 1958, virtually everyone capable of fabricating silicon transistors attempted to fabricate some kind of multiple-transistor structure. At the Raytheon Research Division, we beat out both Texas Instruments and Transatron in the fabrication of Device No. 15, a 5-W, 1,000°C power transistor for the Signal Corps. Warren Erricson was assigned the task of building a four-transistor bridge circuit, which he did.

Contrary to the opinion of my good friend Marshall Nathan, which is given in your article, although the yield of these transistors was very low, suggesting the improbability of such circuits, the yield in certain portions of each slice was 100%, making such circuits attainable. Raytheon, however, only patented devices in manufacturing, and as a consequence, the Texas Instruments patent portfolio has been extensive, while Raytheon's is nonexistent.

I also disagree with my good friend Nick Holonyak about Bob Hall's invention of the GaAs semiconductor laser. If any one of the three teams deserved being called the first in the invention of the semiconductor laser, Bob Rediker and his group at Lincoln Laboratory receive my accolades. These people discovered the luminous efficiency of GaAs p-n junctions, publicized their work in *Lincoln Laboratory Quarterly Reports*, verbally communicated their findings to everyone in the field, and handed out recipes for making GaAs LEDs. If one may judge by published or verbal statements, it was not until the seminal paper delivered by the Lincoln Laboratory people at the Device Conference in June 1963 in Durham, New Hampshire, that the researchers from General Electric and IBM jumped into the act.

I also strongly support Herb Kroemer's award (one of three sharing the Nobel Prize in Physics). I would, however, like to point out two slightly incorrect statements. When



THE INDUSTRIAL PHYSICIST (ISSN 1082-1848; CODEN INPHFA), volume 7, number 1,

Copyright © 2001 American Institute of Physics. **Subscriptions:** *The Industrial Physicist* is available free to qualified parties in the USA who complete, sign and return the qualification cards in each issue. Mail to *The Industrial Physicist*, P.O. Box 96000, Collingswood, NJ 08108, fax to 856-488-6188, or log onto [www.tipmagazine.com](http://www.tipmagazine.com) and click on the free subscription button. **Readers outside the USA** can receive the magazine at the following rates: members of AIP-related societies \$57/year, all other individuals \$66/year. **Libraries and institutions** in the USA pay \$76/year, those outside the USA \$106 (airfreight delivery only). **To order a paid subscription**, please send your request with name, address and payment—a check for \$U.S. drawn on a U.S. bank, or credit card information (indicating VISA/MC/AMEX, credit card #, expiration date, name as it appears on the card, and billing address)—to AIP, Attn: TIP Payments, P.O. Box 503284, St. Louis, MO 63150-3284. **Change of address:** Log onto [www.tipmagazine.com](http://www.tipmagazine.com), click on the free subscription button, and complete the entire subscription form. In the box where you are asked to provide your old address, please provide the numbers from the top line of your mailing label to reduce risk of receiving duplicate magazines. Allow 8 weeks advance notice. **Cancellation, duplicate copies:** Please fax the mailing label(s) from the front cover(s) of your magazine(s) to 856-488-6188, and indicate clearly the necessary changes. **Back copies** are available for \$20 each postage paid from the AIP office listed under "Qualified readers outside the USA," using the same pre-payment instructions. **Republication** or systematic or multiple reproduction of any material in this publication is permitted only under license from AIP. Please send requests for permission to AIP Office of Rights and Permissions, Two Huntington Quadrangle, Suite 1N01, Melville, NY 11747-4502; fax (631-576-2450); phone (631-576-2268); email ([rights@aip.org](mailto:rights@aip.org)). Copies of articles may be made upon payment of a copying fee of \$17 per copy through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. **Subscription problems?** E-mail [jbebee@aip.org](mailto:jbebee@aip.org)

Kroemer delivered his heterojunction paper to the Device Conference in 1957, he was employed at the RCA Research Division, but the paper described work he had initiated in his thesis at Gottingen University. This paper described increasing the bandgap of the emitter to improve emitter efficiency, rather than narrowing the bandgap of the base, which would have added complications to the collector junction.

Jerome M. Lavine  
Sudbury, Massachusetts  
lavine@world.std.com

## Raman spectroscopy

I enjoyed your article on the rise to prominence of Raman scattering as a diagnostic tool (October, pp. 12–14). Four years ago, when I set up a poster on remote laser-induced breakdown spectroscopy (LIBS) at the Lunar and Planetary Science Conference, I found that Paul Lucey (University of Hawaii) was setting up a poster on remote Raman

spectroscopy right next to me. We talked and found that essentially the same instrumental components are used for both techniques. The logical conclusion was to start working together to design a single instrument capable of providing rapid mineralogical (via Raman) and elemental (via LIBS) composition information on rocks or soil samples anywhere within 20 m of the rover or lander that the instrument would be mounted on. We are currently developing these capabilities for the National Aeronautics and Space Administration, but they could have widespread use in other contexts as well.

Roger C. Wiens  
Los Alamos, New Mexico  
rwiens@nis-pop.lanl.gov

## Delay in a pill

With regard to the camera in a pill (*October 2000*, p. 9), there is probably a timer chip that controls light, camera, and transmission. A small modification might delay

system start-up (enable) for several hours with only minor use of battery capacity. This might require two versions of the pill—the present version for the upper gastrointestinal tract and a new delay version for the lower tract—to get more from an already great product.

Tom Turner  
Emerald Electronics, Inc.  
Newport, Rhode Island  
emeraldtom@earthlink.net

## Cryptography strikes again

Fred Schaff's letter on cryptography (*October 2000*, p. 6) seems to presume that cryptography is controlled by government agencies (in the U.S. by the National Security Agency and perhaps the Central Intelligence Agency; elsewhere by those same agencies or some local variant). According to Schaff, the control is exercised in such a way that it is not possible to avoid having one's encrypted communi-

cations read at will. What the U.S. or any other government may want, and what it is capable of doing as a result of some (unnamed and not even suggested) cryptographic aspect, need not be the same. And in fact, they are not. It has been possible to encrypt any material in an unbreakable manner since the algorithm was invented more than 80 years ago (at the end of World War I), and that algorithm has been publicly known to have been proved unbreakable since publications in the late 1940s by Claude Shannon in the Bell System *Technical Journal* and Warren Weaver in the *Mathematical Theory of Communications*. Shannon's results were as significant for cryptography as Gödel's 1930s proofs were for the foundations of mathematics. That algorithm—the “one-time pad”—is as secure as any algorithm can ever be, regardless of what any government may wish. However, it is also monumentally impractical; if it were not, everyone would be using it exclusively.

Practical algorithms are another story. No publicly known practical cryptographic algorithm is known to be unbreakable. And there are theoretical reasons to believe that all, or at least most, might be breakable. In practice, however, several publicly known algorithms are widely believed by the cryptography community to be so difficult to break analytically that they are effectively secure. It must be understood that this is an engineering evaluation and that advances in cryptanalysis or mathematical theory (e.g., in factoring or some branches of number theory) could easily change that evaluation. Furthermore, many of these algorithms are available in source code. Competent examination of the source code for an algorithm can establish, to a very high degree of certainty, that no additional functionality (e.g., a National Security Agency “backdoor”) is present.

Reimplementation of the algorithm without using any of the available source code will offer additional assurance that no hostile functionality is present. The only way a backdoor could exist in such an algorithm would be if the inherent operation of the algorithm were vulnerable. Since at least


some of the algorithms in this class have been developed outside the U.S. by non-U.S. citizens, and since all have been published and are available for examination by the public cryptography community worldwide, it is unlikely that—for these algorithms at least—there are “trapdoors” built into them in some obscure manner.

It is certainly true that assorted government agencies (e.g., the NSA, FBI, and CIA in the U.S. and the KGB and its successor, the FSB, in Russia) would like to have trapdoor access to encrypted communications. And it is true that there have been persistent proposals from within the U.S. government for statutes mandating the use of this or that NSA-developed algorithm that has a publicly known “key escrow” feature and perhaps a secret trapdoor feature. And the NSA is widely thought to have reduced the key length of what became the DES algorithm to something that allowed more or less practical brute force searches (at the time perhaps only by the NSA, but recently even by civil liberties organizations).

However, if your cryptography system is well designed, uses sensible, publicly known algorithms, and is correctly used, a trapdoor of the kind feared by Mr. Schaff is not likely. Other noncryptographic security problems are much more probable.

In actual cryptographic practice, the greatest sources of insecurity include the following:

- Inadequate cryptography system design (e.g., bad protocols, insecure use of algorithms, and poor key scheduling).
- Poor security for physical plaintexts (at the sender, receiver, or both).
- Insecure use of even good cryptography systems end users.
- Poor organizational security policies.
- Hostile action by insiders who have been permitted legitimate access to confidential information.

Will Wilgus  
Slocum and Spray  
Yonkers, New York 

#### CORRECTION

In the December issue, p. 12, third paragraph, NIST stands for the National Institute of Standards and Technology.