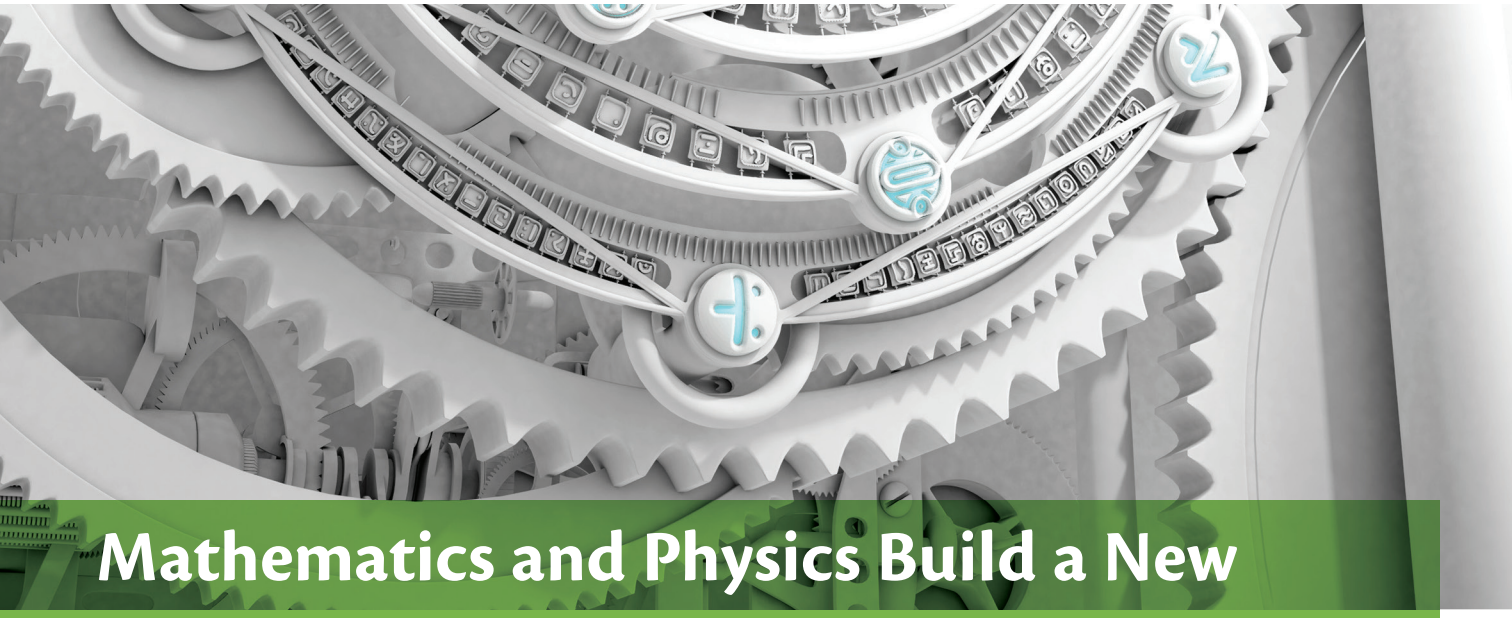

Mathematics and Physics Build a New Future for Secure Communication

Hilarie Orman | Purple Streak
Charles P. Pfleeger | Pfleeger Consulting Group

Once the domain of spies and puzzle solvers, cryptography has grown rapidly over the past 40 years as both an academic discipline and a fundamental technology for security and privacy on the Internet. During that time, it has become heavily computational and deeply mathematical, yet has never left behind its heuristic designs and reliance on randomness. Even the randomness at the heart of quantum mechanics has found a place in practice today.

Cryptography keeps data secret while in transit or at rest, and this property underlies the notions of secure communication, secure identities, and access control on the Internet. These are well-known uses implemented by algorithms and protocols that are the subject of ongoing research and refinement. What has been amazing is the steady discovery of new forms of secure communication, such as secret keys based on names,[1] proof-of-work methods that enable digital money,[2] protocols that prove something is known without revealing it,[3] secure function evaluation,[4] secure secret sharing,[5] and multiparty computation.[6]

There are some physical components in the new era of cryptographic applications. Although quantum computing remains elusive, quantum key distribution is a relatively simple way to send short streams of secret information securely, and there are now practical systems for accomplishing it. In a different research direction, advances in device physics are resulting in sub-Lilliputian computing elements that constitute the Internet of ever-tinier things. This new ecosystem needs cryptographic tools to secure its pervasive reach. In a third dimension, more and more communication is wireless, and wireless signals over very short distances can make physical contacts obsolete.

About This Issue

These developments make for a vibrant, emerging landscape for privacy and authentication on

 Copublished by the IEEE Computer and Reliability Societies

an ever-shifting physical substrate. In this special magazine issue, we explore four different parts of that landscape. All the technologies in these articles are usable today, yet all are cutting edge, facing practical challenges in deployment and proving their utility for real-world, everyday applications.

One article explores the energy requirements for small, wireless devices. Unattended sensors are adapted for all kinds of monitoring uses, including agriculture, wildlife management, hospitals, and even the human body. Battery life is a critical design constraint, and wireless communication and cryptography can eat into that energy budget. The problems that beset designers of secure, low-energy communication devices are the subject of Wade Trappe, Richard Howard, and Robert S. Moore's thoughtful article, "Low-Energy Security: Limits and Opportunities in the Internet of Things."

The emergence of outsourced computation is an interesting evolution of Internet services. More and more computation happens in the cloud, but how can data privacy be assured when the computers are owned by an outside party? In "Computing with Data Privacy: Steps toward Realization," David W. Archer and Kurt Rohloff tell us how, in the future, we might see a few innovative solutions. One is to encrypt the data in a way that lets someone carry out computations and return an answer without learning anything about the unencrypted data. Or, the data could be masked and split among several different parties in a way that allows the originator to recombine the separately computed results into the correct answer.

One of the most surprising discoveries in physics in the 20th century was that randomness rules the world of subatomic particles. Cryptography needs randomness, but it needs controlled randomness. Quantum key distribution (QKD) achieves this and allows two parties to communicate in a way that prevents eavesdropping. This technology is in use today. Can it become a widespread way of distributing the secrets used by cryptography on more conventional communication lines? What are the design tradeoffs to consider? Logan O. Mailloux and his colleagues describe their evaluation tool for QKD designs in "Performance Evaluations of Quantum Key Distribution System Architectures."

Finally, we have an article that examines communication in which security depends on proving proximity. People often use physical presence as a component of security in verifying identities in everyday life, but proving it in a digital environment is quite difficult. Ioana Boureanu and Serge Vaudenay's article, "Challenges in Distance Bounding," reviews the state of the art in protocols that protect against various ways of thwarting distance bounding.

We hope that these four glimpses into the new trends in cryptography and secure communication will pique your interest. All security professionals must keep up with new developments and their implications to understand the tools for addressing today's security needs. And someday, cryptography research might yield further surprising magic for protecting our digital lives. Cryptography and computing research are synergistic in some deep sense, and both will continue to shape the future. ■

References

1. D. Boneh et al., "IBE Secure E-mail," Stanford Univ., 2002; http://crypto.stanford.edu/ibe.
2. "How Does BitCoin Work?," Bitcoin, 2014; https://bitcoin.org/en/how-it-works.
3. O. Goldreich, "Zero-Knowledge Tutorial," 2010; www.wisdom.weizmann.ac.il/~oded/PS/zk-tut10.ps.
4. T. Schneider, Engineering Secure Two-Party Computation Protocols: Design, Optimization, and Applications of Efficient Secure Function Evaluation, Springer, 2012.
5. R. Cramer, I. Damgård, and S. Dziembowski, "On the Complexity of Verifiable Secret Sharing and Multiparty Computation," *Proc. 32nd Ann. ACM Symp. Theory of Computing*, 2000, pp. 325–334.
6. M. Hirt, J.B. Nielsen, and B. Przydatek, "Cryptographic Asynchronous Multi-party Computation with Optimal Resilience," *Advances in Cryptology—EUROCRYPT 2005*, LNCS 3494, 2005, pp. 322–340.

Hilarie Orman is a security guru and software developer at Purple Streak. Contact her at president@purplestreak.com

Charles P. Pfleeger is a researcher, consultant, and textbook author with the Pfleeger Consulting Group. Contact him at chuck@pfleeger.com.

Letters for the editor? Please email your comments or feedback to editor Brian Kirk (bkirk@computer.org). All letters will be edited for brevity, clarity, and language.