Research and teaching: **Phillip Rogaway**

For further information visit http://www.cs.ucdavis.edu/∼rogaway/

Overview My work is in *cryptography*, the "mathematical" side of secure communication. Cryptography can be a quite theoretical corner of computer science, rich in connections to algorithms and the theory of computation. At the same time, it can be a quite practical area, both drawing from and contributing to computer security. But the claim that cryptography can be both practical and theoretically rich does not mean that it is routinely both. I have tried to narrow the theory/practice gap, nudging the proof-centered cryptographic tradition in a direction that better reflects the needs of practice.

Provable security began in the early 1980's, as Goldwasser and Micali put forward a definitionally grounded and proof-based approach for understanding what, in principle, cryptography could do. *Practice-oriented* provable security, co-developed with Mihir Bellare, folds into this tradition some fresh sensibilities. One is a focus on problems of direct interest to practice—things like blockcipher-based modes of operations, or the treatment of entity authentication and session-key distribution. Another is the use of finite pseudorandom permutations (blockciphers) as a starting point, turning on its head a conventional view of minimalism. Another aspect is to favor concrete (non-asymptotic) security analyses—not only to drive us towards better protocols and sharper results, but also to surface hidden issues and to directly encompass finitary functions. My work has implicitly urged a catholic view of computational models, welcoming the ideal-cipher model, random-oracle model, random-permutation model, and symbolic models.

I try to write papers both pretty and influential. I would rather write one such paper than a dozen papers that won't mean much. Obversely, I don't have a lot of patience with work that feels careless, incremental, or inbred. The kind of work I like most to do centers around identifying clean and practicable problems, and creating or reshaping foundations for them.

In the last decade I have also become increasingly interested in social issues connected to science and technology. I want to understand the relationships between the disciplinary cultures in which we do our work and the impact that it ends up having on society. Relatedly, a course on ethics-and-technology that I teach continues to occupy my attention.

Recognition ▷ In 2012, I was named a Fellow of the IACR.[1] ▷ In 2011, I won the ACM's Paris Kanellakis Theory and Practice Award,[2] given for "specific theoretical accomplishments that have had a significant and demonstrable effect on the practice of computing." The citation credits Mihir Bellare and me for the "development of the field of practice-oriented provable-security and its widespread impact on the theory and practice of cryptography and security." ▷ In 2013, it was announced that I will give the IACR Distinguished Lecture in 2015.[3] ▷ In 2013, I spoke at the Distinguished Lecture Series for ETH, Zürich. (I will also go there next year as an invited, Visiting Professor.) ▷ In 2012, I spent six weeks as a Visiting Scholar at the Isaac Newton Institute for Mathematical Sciences. The visit was part of a celebration of Alan Turing's 100th birthday. ▷ In 2003, I received the RSA Conference Award for Mathematics.[4] ▷ At CCS 2011, I received the "Test of Time Award" for a paper of ten years earlier. ▷ In 2009, I was happy to give an invited talk at EUROCRYPT, a tier-1 venue in my field. ▷ In 2011, I was the Program Chair for CRYPTO, the other tier-1 venue. ▷ At present, my citation count is at **19,249** and my h-index is **55**. This puts me at #6 in the citation-ordered category "Top authors in security & privacy" on Microsoft Academic Search, and makes me one of the most cited computer science professors in the UC system.[5, 6]

[1] The International Association for Cryptologic Research, the main professional organization in my field. The citation says: "For fundamental contributions to the theory and practice of cryptography and for educational leadership in cryptography." There are 45 IACR Fellows: www.iacr.org/fellows.

[2] Prior winners include, e.g., R. Rivest (1996), R. Tarjan (1999), E. Myers (2001), M. Rabin (2003), and M. Verdi (2005). See http://awards.acm.org/kanellakis for background and the list of all past recipients.

[3] There is one such speaker per year; see http://www.iacr.org/publications/dl/.

[4] Given annually for "innovation and ongoing contribution to the field of cryptography." M. Bellare and I were co-recipients. The other recipients: D. Boneh, D. Chaum, D. Coppersmith, O. Goldreich, S. Goldwasser, N. Koblitz, A. Lenstra, R. Merkle, S. Micali, J. Pollard, C. Rackoff, J. Stern, J. Quisquater, and S. Vanstone.

[5] Citation counts and h-index are from Google Scholar, as of September 23, 2013, with a query "rogaway".

[6] The ten most cited authors in the security & privacy category are: Shamir, Rivest, Bellare, Boneh, Micali, Rogaway,

Research I have authored about 73 papers, 34 of them falling during this review period. Here I describe some selected topics, mostly more recent ones.

► **Garbling schemes** Some 30 years ago, A. Yao put forward the remarkable idea of a *garbled circuit*. These allow you to evaluate a circuit without understanding *what* you are doing: wires carry seemingly meaningless *tokens*, opaquely transformed by each gate. A startling thing about garbled circuits is that, despite extensive use,[7] there has been no general definition for the *problem* they aimed to solve. The reason, I think, is historical: since the beginning, garbled circuits were described and understood as a *technique*, not as a solution to some specified problem. As a consequence, both rigor and optimized schemes have lagged.

In a series of papers that I view as a single piece of work [A71, A72, A73], my coauthors and I provide foundations for this area. We begin by providing a robust syntax for a *garbling scheme*,[8] a syntax on which multiple definitions can be lain. On top of this syntax we define *privacy*, *obliviousness*, and *authenticity*. Each is defined with respect to both *static* and *adaptive* adversaries. We investigate the relationships among these security notions. We identify gaps in well-known papers that use circuit garbling—bugs ultimately due, I believe, to the (former) absence of a good abstraction boundary. We provide and prove correct the fastest known schemes for garbling circuits, these based on a fixed-key blockcipher (a random permutation). Finally, we implement our schemes, demonstrating order-of-magnitude improvements over prior work.

► **Shuffling, coupling, and format-preserving encryption** A simple question: how can you encipher a credit-card number (CCN)? Formally, we are seeking a PRP-secure blockcipher with a message space of 16-digit strings. This sounds like it must be standard, but, in fact, the modern cryptographic tradition is to create blockciphers on *binary* strings of *conventional* lengths. We want to use such a blockcipher, say AES, to create one with an arbitrary domain. This problem of *format-preserving encryption* (FPE) is eminently practical. As an example, if you replace each CCN in a database by its enciphered / same-format counterpart, the database's schema need not change, facilitating easier security deployment.

My work on FPE goes back to 2002, when my graduate student and I identified the problem and gave some initial solutions [A38]. Later, we offered a much more general treatment [A61]. But quantitative bounds on "medium-sized" domains (things like CCNs) have remained disappointing. A breakthrough of sorts was obtained when I realized that it would be profitable to recast these problems as *card shuffling*, which has a rich tradition in mathematics.[9] In particular, techniques from the analysis of Markov chains—especially *coupling arguments*—could be employed to get new security results.[10] We used the approach to get good bounds for many classical schemes [A63, A64], and also to create a new kind of cipher: a "swap-or-not" network [A70]. Swap-or-not provides a quantitatively better way to create a PRP than prior constructions, and is arguably the first fundamentally new way to construct a blockcipher in decades.

FPE is of much interest to industry. A company I work with, Voltage Security, has done well creating FPE-based solutions for the payment-card industry. The U.S. Government plans to standardize FPE mechanisms in NIST 800-38G, which is based on the FFX algorithm that my colleagues and I proposed [B29, B30].

► **Authenticated encryption** Traditionally, encryption is for privacy. But *authenticated encryption* (AE) is (shared-key) encryption designed to provide authenticity as well. Soon after Bellare and I formalized the goal [A33],[11] I set out to realize it as efficiently as possible. This would result in the scheme OCB1 [A36, A44], inspired by work of C. Jutla.[12] A few years later I published a refinement, OCB2 [A50], to support *associated data* (AD) [A42] and an optimization enabled by a notion from Liskov, Rivest, and Wagner. A

Goldreich, Sandhu, Naor, Vanstone; see http://tinyurl.com/ms-security-and-privacy.

[7] More than 3000 papers reference Yao's original work on this, these covering more than 30 cryptographic applications.

[8] Garbling schemes, not garbled circuits, are the definitional focus: an early realization is that one might garble anything that computes—not just a circuit, but a DFA, RAM, TM, or whatever. Indeed there were already such inventions in the literature, but no unifying definitional view.

[9] In fact, Naor and his coauthors had earlier connected enciphering and card shuffling, although not in order to obtain or analyze practical enciphering schemes.

[10] Coupling too had made a prior appearance in the cryptographic literature, in a result by Mirinov on RC4. It had not been used to prove a symmetric technique sound.

[11] Katz and Yung did so too, concurrently, while Bellare and Namprempre offered an influential exploration of the idea.

[12] The "1" of OCB1 has been added retrospectively, to distinguish it from its successors. The name OCB is meant to suggest *offset codebook*, which is vaguely suggestive of the technique.

final refinement, OCB3, came in 2011. It incorporates tricks that arose by closely coupling experimentation and design. OCB (in all of its forms) is far more efficient than competing alternatives, CCM and GCM; see the charts at http://www.cs.ucdavis.edu/∼rogaway/ocb/performance/. Besides OCB, I developed differently-motivated AE schemes EAX [A46] and SIV [A56], the latter achieving *deterministic* and *misuse-resistant* AE. All of these methods are in standards (eg, EAX and OCB2 are in ISO/IEC 19772).

Maybe it is fitting that *OCB* looks like *OCD*; the mode, and AE more generally, has been an obsession. Yet it seems appropriate. The state of real-world symmetric encryption has been an embarrassment: twenty years after the emergence of provable security, cryptographic practice was still employing (nearly exclusively and often incorrectly) the blockcipher modes of FIPS 81 (1980). There was no effort to figure out what the goal for a general-purpose symmetric-encryption standard should be, let alone how to achieve it. The answer I have pushed is that AE (nonce based, with AD) *is* that basic goal. I have repeatedly maintained this would assist correct use. I think this has now become the conventional wisdom.

► **Hash functions** I have been heavily involved in foundational issues connected to cryptographic hash functions. ▷ A logically-first paper [A48] sorts out the terms that had been strewn about (collision-resistance, preimage resistance, second-preimage resistance), providing rigorous definitions and investigating the relationships among them, painting a fairly complete picture of the keyed-hash-function world. ▷ In another well-known piece of work [A41, A65], we reconsider the family of methods described by Preneel, Govaerts, and Vandewalle (PGV) for turning a blockcipher into a cryptographic hash function. Combining attacks and ideal-cipher-model proofs, we prove a taxonomy of PGV's 64 constructions, along the lines of what they did, but more formally established. ▷ My oddly titled *Formalizing Human Ignorance* [A54] explores the following well-known dilemma: "For any fixed hash function $H\colon \{0,1\}^* \to \{0,1\}^n$, there *is* an efficient algorithm to output a collision—the algorithm that prints one out—the only problem is that us dumb humans don't know what the algorithm is. Not a mathematically-amenable complaint, defining collision-intractability requires adopting a richer signature for H—reimagining it as a family of hash function." I explain why this reasoning is specious—that all we really need to do is adopt a more constructive way to state our theorems. Effectively, we have been trapped by our linguistic traditions.[13] ▷ In a pair of related papers with John Steinberger [A59, A60], we look at how well one can do in constructing cryptographic hash functions from *permutations*—fixed-key blockciphers—giving both upper and lower bounds. Results are analyzed in the random-permutation model (RPM). The viewpoint that random permutations are a good starting point for making cryptographic hash functions would go on to shape many SHA-3 designs.

► **Other works** ▷ Traditional definitions for encryption-scheme security do not allow the plaintext to depend on the secret key. My work on KDM (key-dependent message) security relaxed this constraint [A29, A37, A40], allowing you to encrypt messages depend on the key. This has inspired much follow-on work. ▷ The classical way to make a message authentication code (MAC) out of a blockcipher, the CBC MAC, completely fails when inputs can have varying lengths. A paper with John Black sought the simplest correct variant [A32, A51]. The resulting scheme,[14] CMAC, is already a widely used cryptographic standard (NIST SP800-38B). ▷ For years, many of my proofs have used "game playing" arguments, wherein a cryptographic scenario is analyzed by slowly bleeding one "game" into another, quantitatively accounting for each loss in fidelity. The games are embodied by fragments of code, and rewriting rules can be used to justify each transition. Bellare and I have advocated this approach [A55], illustrating its power by using it to prove the security of triple encryption in the ideal-cipher model.[15] Follow-on work in the programming-languages community, by Gilles Barthe and others, has fashioned tools, like EasyCrypt and CryptoVerif, enabling computer-verified proofs for code-based games. ▷ In a little-noticed paper at CCS [A58], Bellare and I give a unified and long-overdue account of secret-sharing goals: perfect, statistical, and computational secret sharing; static and dynamic adversaries; schemes with or without robustness; schemes where a participant recovers the secret, and those where an external party does so.

[13] This does not mean that keyed hash functions are of no use. It does mean that, in proving security for hash-function based protocols where that hash function is to be instantiated by something like SHA-1 or SHA-3, provable security is not forfeit by sticking with an unkeyed view of what the underlying hash function is.

[14] Renamed and slightly modified.

[15] This does not mean that a proof could not be found *without* code-based games, only that they enabled *us* to arrive at a proof. Also, some bugs in that proof, all correctable, were later found by Gaži and Maurer, who extended our results.

The above enumeration ignores most of my early work, on topics that include: entity authentication and key distribution [A7, A11, A31]; modes of operation [A9, A12, A13, A16, A20, A23, A24, A27, A28, A30, A34]; public-key schemes OAEP, PSS, and DHIES [A10, A15, A21, A35]; the random-oracles paradigm [A6]; and bridging of the gap between computation and symbolic views of cryptography [A29, A37]. Many of these works have had an enduring influence on my field.

▶ **Further research-related comments** Regarding funding, I have always brought in enough of it to support the number of students I like to advise (1–2 at a time), and my other scientific needs. (I dislike requesting money, but have usually been successful when I do.) At present, I have more funding than I need, and have been able to fund one of Matt Franklin's students on the overage. All of my current funding is from the NSF (apart from old gift money from Cisco and Intel).

It is my belief that we should be mindful of *who* is funding our work and *what* are their institutional aims. I am distressed by the extent to which universities support military agencies and socially-undesirable aims.

In recent years I've become convinced that the sociology of my community—scientifically inessential aspects of our disciplinary culture—strongly impacts what we all do. In recent invited talks I have taken to speaking about this.[16] Many of the problems I have worked on have been open, I now understand, because of a systematic neglect of a class of problems that fell outside of a prevailing ethos. Recognition of this fact has helped me identify similarly neglected topics.

Teaching I teach towards the top few students of each class, losing, I'm afraid, a rather large fraction of the rest. One might expect to be "punished" for this in teaching evaluations, but that hasn't been the case. Most of the time, my median teaching-evaluation score has been 10 (out of 10).[17] Over the last decade, I've had mean teaching-evaluations of about 9.24 (out of 10).[18, 19] In 2010, I won College of Engineering's Distinguished Teaching Award. Random comments on my teaching can be found on ratemyprofessors.com.

The class I've come to care most about teaching is ECS 188, *Ethics in an Age of Technology*. I designed the class, and continually work on it. Evolving the course reader (available at tinyurl.com/ecs188) is never-ending. Every time I teach the class, a student or two will tell me how it changed his worldview or life direction. There aren't many things more rewarding.

I don't produce a lot of Ph.D. students, but I work with them intently. All but one has gone to academia. My "best" placements are John Black (University of Colorado, Boulder) and John Steinberger (Tsinghua University, China). My most recent student, Viet Tung Hoang, graduated in Spring 2013 with six excellent papers (3×CRYPTO, 1×CCS, 1×S&P 1×Asiacrypt) and has taken a postdoc at UCSD.

Service At the Departmental and College levels, I've been chairing our department's undergraduate (UG) committee (CSUGA) and representing us on UG matters at the college (UGEP). As such, I meet one-on-one with numerous UG students. I've ushered through my department's UG curriculum changes, including the creation of new classes, the addition of a minor in Computational Biology, and the requirement (in CSE) for a senior-design project. I organized an update of all UG course descriptions in the department, a highly time-consuming effort. I helped us through the last ABET review (Dipak Ghosal was the lead), and no doubt the ones before (by now pleasantly forgotten). I was a member of the CoE/physics committee that studied changes in the Physics-9 series. I was a vocal member of the Advising Working Group (at the CoE level). I fought, unsuccessfully, against a formula-driven approach to TA-allocation that seemed unfair to CS. With respect to graduate education, I chair the GGCS[20] committee of Graduate Advisors, which generates lots of paperwork and meetings with students. I led the preparation of a highly critical response to the College's IT-centralization directions (another battle we lost, and at great cost). I routinely cover events for CS, things like picnic day, decision day, and commencement.

[16] See *Practice-Oriented Provable Security and the Social Construction of Cryptography*, a near-transcript of my Eurocrypt 2009 invited talk: http://www.cs.ucdavis.edu/ rogaway/papers/cc.pdf. My interest in the sociology of science began with a chance discovery of Ludwik Fleck's under-appreciated gem, *Genesis and Development of a Scientific Fact* (1935/1981).

[17] This has been true for 9 of the last 10 classes taught (F10–S13), and 22 of the last 32 classes taught (F03–S13).

[18] This number is the median of 32 means, the classes I've taught between Fall 2003 to Spring 2013.

[19] Regarding the anomalous 6.60/10.00 instructor rating for ECS 188 in SQ 2007: I took over this class (Thurs of week-3) from an instructor that had employment issues. It was a no-win situation for everyone.

[20] Graduate Group in Computer Science.

At the campus level, I served as member and then Chair for the Academic Senate's Committee on International Studies and Exchanges (CISE). I was a member of the system-wide University Committee on International Education (UCIE). These positions were very time-consuming and frustrating. I have often served as our department's rep for the Representative Assembly of the Academic Senate.

I interact with NIST a fair amount. In recent years I championed adoption of CTR mode (NIST 800-38A), co-designed CMAC (NIST 800-38B), and co-designed FFX (NIST 800-38G; draft). FFX will be my twelfth cryptographic mechanism to find its way into a cryptographic standard.[21]

I've been on the Program Committee for about a dozen conferences during this review period, including serving as Program Chair for CRYPTO 2011. I've been on the editorial board for *Information and Computation* and *J. of Cryptology*.[22] I serve on the usual parade of NSF panels, and sometimes help the NSF's foreign counterparts (eg, grant reviews for Ireland or the EU; and some algorithmic reviews for the government of Japan). I've been on the dissertation committee for doctoral students at ETH and Lund.

I believe it is important for scientists and technologists, especially well-known ones, to take a public stance when important social and ethical matters intersect our work.[23] I am one of (at most) a handful of cryptographers in the USA, and the most high-stature one, who has taken a public position against our country's unconscionable mass-surveillance activities; see the link from my homepage.

Phillip Rogaway
Davis, California, USA
October 1, 2014

[21] CMAC (message authentication), DHIES and ECIES (public-key encryption), EAX (authenticated encryption), EME2 (wide-blocksize blockcipher), FFX (format-preserving encryption), OAEP (public-key encryption), OCB (authenticated encryption), PSS (digital signatures) PSS-R (digital signatures with message recovery), SIV (authenticated encryption), UMAC (message authentication code), and XTS (tweakable blockcipher).

[22] I am not a good editor. I don't like asking people to do stuff for me.

[23] Many physicists have internalized this imperative—perhaps a legacy of having built "the bomb" and having observed the behavior of leaders like Hans Bethe. But, among computer scientists, a willingness to do anything that could be seen as "political" or "unprofessional" is amazingly rare.