

The Mathematics Community and the NSA

POST-PUBLICATION EDITOR'S NOTE: This article is a part of the ongoing series "Mathematicians Discuss the Snowden Revelations". At the time of the writing of this piece Michael Wertheimer was the Director of Research at the NSA; he recently retired from that position. He can be reached at nsapao@nsa.gov.

This is the latest installment in the *Notices* discussion of the National Security Agency (NSA). Previous *Notices* pieces on this topic are:

"AMS Should Sever Ties with the NSA" (Letter to the Editor), by Alexander Beilinson (December 2013); "Dear NSA: Long-Term Security Depends on Freedom", by Stefan Forcey (January 2014); "The NSA Backdoor to NIST", by Thomas C. Hales (February 2014); "The NSA: A Betrayal of Trust", by Keith Devlin (June/July 2014); "The Mathematical Community and the National Security Agency", by Andrew Odlyzko (June/July 2014); "NSA and the Snowden Issues", by Richard George (August 2014); "The Danger of Success", by William Binney (September 2014); "Opposing an NSA Boycott" (Letter to the Editor), by Roger Schlafly (November 2014).

See also the Letters to the Editor in this issue.

Unsolicited submissions on this topic are welcome. Inquiries and submissions may be sent to notices-snowden@ams.org. Articles of 800 words or less are preferred. Those of 400 words or less can be considered as Letters to the Editor and should be sent to notices-letters@ams.org.

— *Allyn Jackson*
Notices Deputy Editor
axj@ams.org

Encryption and the NSA Role in International Standards

Michael Wertheimer

Michael Wertheimer is Director of Research at the National Security Agency. His email address is mawerth@nsa.gov.

DOI: <http://dx.doi.org/10.1090/noti1213>

Over the past several months a discussion about the role of mathematics, mathematicians, and the activities of the National Security Agency has been hosted on the pages of the *Notices*. As an NSA mathematician I would like to provide some context to what has been reported in the press and share with the American Mathematical Society important facts and information. In particular I would like to address two hot-button issues shaping this conversation: "weakening" Internet encryption and impacts of data on privacy.

The US National Institute for Standards and Technology (NIST), the American National Standards Institute (ANSI), the Internet Engineering Task Force (IETF), and the International Standards Organization (ISO) are the four main bodies with which the NSA participates in developing standards for cryptography. NSA has worked with each of these for over twenty-five years. We value and are committed to the important work of these groups in producing secure cryptographic standards that protect global communications. NSA has a long and documented record of providing security enhancements to openly published international standards. However, recently our work has been questioned in several standards that are elliptic curve based, the most significant of which is an NIST-proposed random number generator that I discuss below.

NSA mathematicians remain steadfast in advocating secure international standards. Nevertheless, we are mindful that there has been considerable discussion regarding NIST publication SP 800-90A. This publication is entitled "Recommendation for Random Number Generation Using Deterministic Random Bit Generators" and contains specifications for four pseudorandom number generations for use in cryptographic applications. One of these describes a particular random number generator associated with NSA: the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG). The discussion centers on NSA's role in the design and advocacy for this algorithm despite a mathematical demonstration of the potential for a trapdoor.

A trapdoor, simply put, is information that allows the inverse of a seemingly one-way function to be computed easily. In other words, compute x from $f(x)$. In cryptographic applications, functions f are specifically designed to make the x to $f(x)$ computation very fast but the inverse computation intractable (hence, the term one-way). If an attacker knows “secret” information about f that allows an inverse to be calculated, the attacker might be able to decrypt messages or, in the case of the Dual_EC_DRBG, predict future outputs.

During the development of the ANSI standard based on the NIST publication, members of X9F1 (the ANSI-approved working group responsible for cryptographic tools) raised concerns about the potential that elliptic curve points used as parameters for the Dual_EC_DRBG could harbor a trapdoor secret known only to, and exploitable only by, the person who generated the points. As a result, the X9F1 committee expanded the standard to include verifiable random point generation. Since the NSA was using the algorithm at the time and had generated elliptic curve points for protecting Department of Defense users, the NSA-generated points were included in the standard. In other words, any implementation that used the NSA-generated points would be deemed compliant. Shortly thereafter, NIST negotiated with ANSI to use the ANSI Random Number Generation Standard as the basis for an NIST Random Number Generation Standard. ANSI also approved submitting a version of this standard to the ISO.

In 2007 several Microsoft researchers, including Microsoft’s representative to the ANSI X9F1 committee that created the ANSI version of the standard, raised concerns in a talk at a cryptographic conference about the trapdoor potential in the Dual_EC_DRBG. These concerns were picked up by the media and widely disseminated. NIST and ANSI reviewed this information and elected to retain both the verifiable point generation scheme and the NSA-generated points.

In 2013 the same concerns were again raised and promulgated by the media. This time NSA’s actions were portrayed as a subversion of standards. However, the facts remain:

- The Dual_EC_DRBG was one of four random number generators in the NIST standard; it is neither required nor the default.
- The NSA-generated elliptic curve points were necessary for accreditation of the Dual_EC_DRBG but only had to be implemented for actual use in certain DoD applications.
- The trapdoor concerns were openly studied by ANSI X9F1, NIST, and by the public in 2007.

With hindsight, NSA should have ceased supporting the dual EC_DRBG algorithm immediately after security researchers discovered the potential for a trapdoor. In truth, I can think of no better way to describe our failure to drop support for the Dual_EC_DRBG algorithm as anything other than regrettable. The costs to the Defense Department to deploy a new algorithm were not an adequate reason to sustain our support for a questionable algorithm. Indeed, we support NIST’s April 2014 decision to remove the algorithm. Furthermore, we realize that our advocacy for the DUAL_EC_DRBG casts suspicion on the broader body of work NSA has done to promote secure standards. Indeed, some colleagues have extrapolated this single action to allege that NSA has a broader agenda to “undermine Internet encryption.” A fair reading of our track record speaks otherwise. Nevertheless, we understand that NSA must be much more transparent in its standards work and act according to that transparency. That effort can begin with the AMS now.

NSA strongly endorses the NIST outline for cryptographic standards development, which can be found at csrc.nist.gov/groups/ST/crypto-review/process.html. One significant, and correct, change is that all NSA comments will be in writing and published for review. In other words, we will be open and transparent about our cryptographic contributions to standards. In addition, we will publish algorithms before they are considered for standardization to allow more time for public scrutiny (as we did recently with the new SIMON and SPECK algorithms, eprint.iacr.org/2013/404.pdf). With these measures in place, even those not disposed to trust NSA’s motives can determine for themselves the appropriateness of our submissions, and we will continue to advocate for better security in open-source software, such as Security Enhancements for Linux and Security Enhancements for Android (selinuxproject.org).

We hope this open affirmation and our adherence to it will chart a course that all mathematicians will agree is appropriate and correct.

Data and Privacy

NSA mathematicians carry on a long and storied tradition of making and breaking codes and ciphers. Perhaps most celebrated are feats that our forebearers, American and Allied, made in breaking German and Japanese ciphers in World War II. Ironically, less than 5 percent of the encrypted material collected during that war was successfully decrypted, and of that amount only a scant fraction contributed to any sort of measurable action. Such is the nature of intelligence.

Today’s communications environment makes 5 percent appear staggeringly large. The simple act of using a particular encryption algorithm no longer identifies the sender or receiver (as the

ENIGMA cipher did in World War II); the variety of protocols, products, and services for secure communications numbers in the thousands; and the ease and frequency of changing identifiable features is unprecedented. To achieve our foreign intelligence mission lawfully and effectively, NSA mathematicians lead efforts that determine how we “filter,” “select,” and “process” data while continuously verifying that our processes and procedures adhere to all legal and policy regulations.

Filtering algorithms decide what material is defeated, i.e., neither collected nor stored for analysis. Using aggregate numbers, of the exceedingly small proportion of the world’s foreign communications we access, NSA algorithms filter out approximately 99.998 percent of the data it sees. The importance of these algorithms cannot be overstated: they form the bulwark of the legal and privacy protections in executing our mission. After the filtering process, surviving data must meet exacting criteria to be “selected” for subsequent processing and analysis. NSA mathematicians are at the forefront in designing the methods by which the selection criteria are expressed. The precision and accuracy of these methods are constantly improving and with those improvements come increased privacy protections.

I am reminded of an event shortly after the 9/11 attacks that may help to impress the importance of getting filtering and selection “right.” Soon after allied operations launched in Afghanistan we came into possession of laptops left behind by retreating Taliban combatants. In one case we were able to retrieve an email listing in the customary to/from/subject/date format. There was only one English language email listed. The “to” and “from” addresses were nondescript (later confirmed to be combatants) and the subject line read: CONSOLIDATE YOUR DEBT. It is surely the case that the sender and receiver attempted to avoid allied collection of this operational message by triggering presumed “spam” filters. Indeed, this is exactly how intelligence and counterintelligence work: an escalating series of moves to discover and avoid discovery of information.

Adapting our filters and selectors to stay relevant while always operating within our legal and policy framework can never be perfect—but it is nearly so. Indeed, in a much-publicized account of 2,776 deviations from the rule set in 2012, a full 75 percent of these incidents occurred when an individual roamed from foreign soil to US soil and we failed to catch the fact in real time. The remaining 25 percent, about 700 in total, were human error (e.g., typing mistakes). Put into perspective, the average analyst at NSA makes a compliance mistake once every ten years.

The collection and analysis of data that lie between filtering (what we know we do not want) and selection (what we know we do want) is governed

by a complex set of laws, policies, and implementing rules. This type of data, lawfully obtained and properly evaluated, helps us to avoid surprise. It is used to discover new threats, refine both our filters and selectors, and ultimately create a rising tide that lifts our intelligence insights and privacy protections. Mathematicians are leading the way to design and implement the algorithms that create this rising tide. Here we share many common interests with industry: e.g., big data analytics, cloud computing, machine learning, and advanced search. So-called metadata (intelligence information that can be ascertained without examining the actual content of a communication) plays a big role here, as our governing rules generally do not permit deep inspection when the aperture into our data set widens. Getting this right is paramount: the average NSA mathematician takes fourteen courses each year to be up-to-date on the procedures that govern these activities.

Some Parting Thoughts

I fondly recall the opportunity NSA gave me early in my career to return to the University of Pennsylvania and complete my PhD. During those formative years I had many opportunities to present results at AMS conferences, and I remember the warm embrace of colleagues who encouraged and supported my studies. I felt then, and I feel now, a connection to the mathematics community that goes beyond scholarship. That is why NSA Research is a major provider of grants for pure mathematical research, a participant in the National Physical Sciences Consortium, a sponsor of local high school teams for the American Regions Mathematics League, and sponsors of both undergraduate and graduate summer programs. Our research mathematicians serve on editorial boards, publish papers, teach at universities, and contribute time and energy to the AMS.

More broadly, NSA mathematicians are also fighters in the war on international terrorism, weapons of mass destruction proliferation, narcotics trafficking, and piracy. In fact, the overwhelming bulk of what we do is universally acknowledged as proper, measured, and important. We do so quietly and honorably.

It is my sincerest hope that the AMS will always see NSA mathematicians as an important part of its membership. I further hope that dialogue on important issues will always be respectful, informed, and focused on inclusivity.