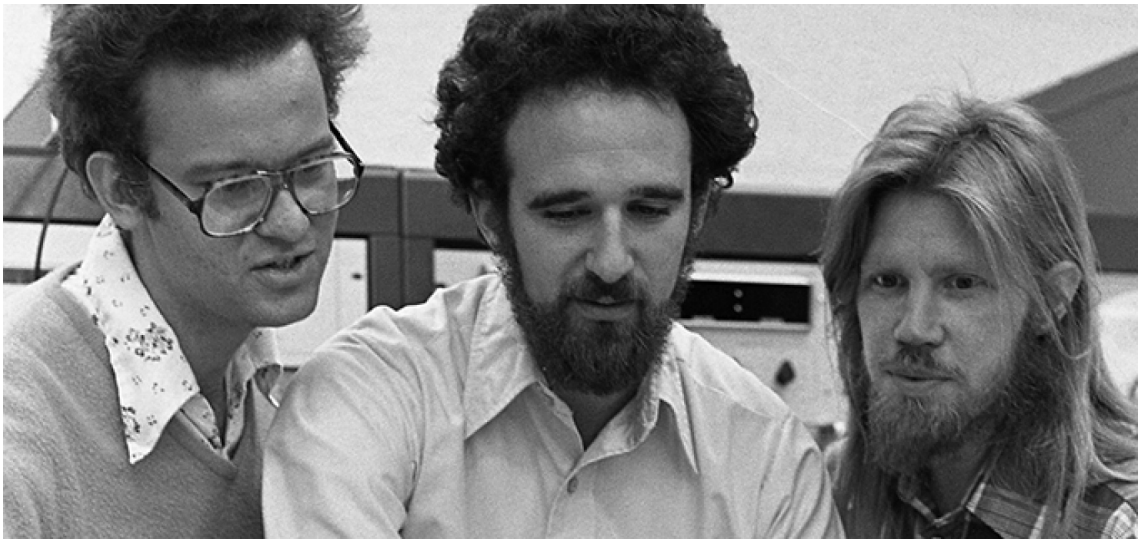
Stanford cryptography pioneers win the ACM 2015 A.M. Turing Award

A groundbreaking algorithm from Martin Hellman and Whitfield Diffie enabled a secure Internet.

March 1, 2016
By Steve Fyffe and Tom Abate



Stanford's Martin Hellman, center, and Whitfield Diffie, right, winners of the 2015 A.M. Turing Award, are shown with Ralph Merkle of UC Berkeley in this 1977 photo. | Chuck Painter / Stanford News Service

Stanford cyber-security innovators Whitfield Diffie and Martin Hellman, who brought cryptography from the shadowy realm of classified espionage into the public space and created a major breakthrough that enabled modern e-commerce and secure communications over the Internet, are being honored with the Association for Computing Machinery's 2015 A.M. Turing Award.

The award is often referred to as the "Nobel Prize of computing" and comes with a $1 million prize funded by Google.

The Association for Computing Machinery (ACM) made the official announcement this morning at the RSA conference in San Francisco – one of the largest gatherings of cryptographers working on Internet security.

Diffie and Hellman's 1976 paper, "New Directions in Cryptography," stunned the academic and intelligence communities by providing a blueprint for a revolutionary new technique that would allow people to communicate over an open channel, with no prearrangement, but keep their information secret from any potential eavesdroppers.

They called it public-key cryptography.

They also showed how, by reversing the order of operations, it was possible to create a "digital signature." Like a written signature, this has to be easy for the legitimate signer to create and for everyone else to verify. But it has to be difficult – preferably impossible – for anyone else to sign new messages. Unlike a written signature, which looks the same even if it's taken from a $1 check and forged onto a $1,000,000 check, a digital signature can only be used with the specific message that was signed.

Digital signatures and the "digital certificates" or "certs" they can produce are critical components in the modern security architecture. They allow your browser to know that your bank is really who it claims to be, and they allow iPhones to only run software signed by Apple.

"Their 1976 invention is widely viewed as the birth of modern cryptography," said Dan Boneh, Stanford professor of computer science and electrical engineering and co-director of the Stanford Cyber Initiativ.

"Simply put, without their work, the Internet could not have become what it is today," Boneh said. "Billions of people all over the planet use the Diffie-Hellman protocol on a daily basis to establish secure connections to their banks, e-commerce sites, e-mail servers, and the cloud."

Threat of jail time

It was a feat made even more impressive by the fact that little serious academic scholarship on cryptography existed at the time of their invention outside the realm of classified research conducted under the purview of secretive government agencies such as the National Security Agency. Hellman said academic colleagues had tried to discourage him from pursuing his interest in cryptography early in his career because of the NSA's virtual monopoly on the subject.

"They said, 'You're wasting your time working on cryptography because the NSA has such a huge budget and a several-decades head start," said Hellman, Stanford professor emeritus of electrical engineering. "How are you going to come up with something they don't already know? And if you come up with something good, they'll classify it.'"

Diffie and Hellman clashed with the NSA over their publications, including one that claimed that the agency had pressured IBM to weaken the National Bureau of Standards' Data Encryption Standard (DES) by limiting the key size to 56 bits instead of a stronger option of 64 bits or higher.

After the publication of "New Directions in Cryptography" and another paper on the DES key size, the conflict intensified as the NSA waged a concerted campaign to limit the distribution of Diffie and Hellman's research.

An NSA employee even sent a letter to the publishers warning that the authors could be subject to prison time for violating U.S. laws restricting export of military weapons.

These skirmishes became known as the first of the "crypto wars."

Ultimately, the NSA failed to limit the spread of their ideas, and public key cryptography became the backbone of modern Internet security.

"Cryptography is the one indispensable security technique," said Diffie, who was a part-time researcher at Stanford at the time he and Hellman invented public-key cryptography. "There are lots of other things needed, but if the government had succeeded in blocking people from having strong cryptographic systems … it would have meant you could not have had security on the Internet."

Cryptography's starring role

Diffie and Hellman said the U.S. government's recent demands that Silicon Valley companies build so-called back doors into their products so law enforcement and intelligence agencies could access encrypted messages reminded them of the first crypto war. As then, the government did not have a workable proposal for how to create those back doors without undermining the security of those products.

Diffie and Hellman both said they sided with Apple in the current legal standoff over the FBI's request that Apple provide access to an iPhone belonging to one of the San Bernardino terrorists by writing software to bypass some of its security features.

"All the computer security experts that I talk with – I don't think there's been one who believes that we should do what the government wants," Hellman said. "While in this one case it might not do much harm, it establishes a dangerous precedent where Apple is then likely to be inundated with thousands upon thousands of requests that they'll have to either fight or comply with at great risk to the security of the iPhone system."

Diffie said giving in to the FBI's request would also make it harder for Apple to resist similar requests from foreign governments who want to spy on their citizens and crush internal dissent.

"We do not wish to support the ability of totalitarian regimes to do this kind of thing when they are persecuting people for their free speech," Diffie said.

Diffie and Hellman are both currently affiliated with Stanford's Center for International Security and Cooperation (CISAC), where they regularly attend seminars on a diverse range of national security issues and mentor young pre- and postdoctoral fellows on issues of cyber security.

"What's great about both Whit Diffie and Marty Hellman is the way in which they contribute to the ongoing intellectual discourse of the Center," said CISAC co-director David Relman. "Both of them think broadly and deeply far outside the bounds of their formal training and the areas of accomplishment for which they are now being recognized by this prize."

Persis Drell, dean of Stanford's School of Engineering, said the award, and the work behind it, exemplified the caliber and tone of research for which the school's faculty are noted.

"Engineers want to have a positive impact on our world, and we are enormously proud to have Marty Hellman as an emeritus member of the Stanford Engineering faculty," Drell said.

Boneh, whose main area of research is applied cryptography, said Diffie and Hellman's work continued to inspire a new generation of cryptographers.

"Beyond the practical implications of the work, their groundbreaking 1976 paper 'New Directions in Cryptography' introduced new concepts and opened up new directions that were previously thought to be impossible," Boneh said.

"It introduced number theory into the realm of cryptography and launched an entire academic discipline to further develop the area of public-key cryptography. By now there are thousands of researchers and tens of thousands of research papers building on their work. The field of cryptography would be a pale image of what it is today without the work of Diffie and Hellman."

See more news ›

Instagram

Facebook

Twitter

Stanford | ENGINEERING

475 Via Ortega, Stanford, CA 94305

Stanford Engineering Magazine

Departments

Open Faculty Positions

Sign up for our email

Your source for engineering research and ideas

email address Sign up