www.frontiersofknowledgeawards-fbbva.es

Acceptance speech

18 June 2026

Joan Daemen, awardee in the Information and Communication Technologies category (18th edition)

First of all, I would like to thank the BBVA Foundation for awarding this prize to my colleague Vincent Rijmen and me for our work in cryptography. I would like to thank everyone that provided support, guidance and encouragement along the way. You know who you are.

Traditionally, cryptography is the craft of designing systems – ciphers – to safeguard the confidentiality and authenticity of communication. Well-designed ciphers can protect messages even against the most powerful outsiders, provided that short password-like strings, known as keys, remain secret. For millennia, cryptography and the art of breaking ciphers called cryptanalysis – together called cryptology – were well guarded and reserved for rulers, militaries, and diplomats, and often played a crucial role in warfare. As a result, progress was slow, and hard-won expertise often vanished with the passing of experts or the fall of empires.

This changed in the mid-seventies marked by the publication of the first open cryptographic standard by the US institute of standardization NIST: the Data Encryption Standard (DES). From that point on, cryptology became an open scientific discipline that gave rise to amazing progress in understanding. Since the turn of the century, with the rise of the internet and more generally the digitization of the world, cryptology has become a discipline of profound societal importance. Since the 1970s, open research has produced a vast array of cryptographic algorithms. Many of them were broken soon after publication. Designers, understandably proud of their creations, often overlook subtle weaknesses. A provably secure cipher that is practical has yet to be built, and many believe this is an unattainable ideal.

So how do we build trust in a cipher? Progress in cryptology arises from a disciplined process of trial and error within the academic community: ciphers

are proposed, analyzed, broken, repaired, and broken again, until the pace of new attacks slows. This cycle – sustained by peer-reviewed conferences, journals, and open collaboration – has proven remarkably fertile. Each attack yields new insights and design principles, leading to increasingly mathematical sophistication and the robust ciphers we have today.
When I started a PhD in cryptography in 1988, we were still a long way from solid ciphers. Research on symmetric cryptography was dominated by the DES standard and in practice governments, banks and industry were relying on a patched version of it called Triple-DES. And it looked like it would remain that way in the foreseeable future. Triple-DES was very efficient and seemed sufficiently secure, but it certainly could not be called elegant. So after some false starts, I decided to dedicate my PhD to trying to design ciphers that were efficient and secure but simpler and more elegant. The key to elegance was, and still is, symmetry, and this led to a number of rather academically oriented cipher designs that I am still very happy with. I knew I was on the right track when I got papers rejected by reviewers just saying "these ciphers look too simple to be secure" without any supporting evidence for weaknesses.

Then after my PhD, when I landed in a software consultant job in a multinational, I had an idea that I thought could lead to something big. But my job was no longer about cryptography and I did not have the energy to do it on my own after office hours. So then I contacted Vincent with whom I successfully collaborated at COSIC during my PhD. I proposed to work it out together and fortunately he said yes. Without my initiative and Vincent's positive answer both our lives would likely have gone quite differently, and we would not stand here before you today. Our collaboration led to a series of papers introducing a number of ciphers in the years 1996-1997.

Then the unexpected happened: we heard rumours of NIST plans to launch an open competition to find a successor of DES, and lo and behold, they actually did and they called it the Advanced Encryption Standard (AES) competition. NIST would host it but all the work (designs, cryptanalysis, comparison) would be done by the academic community, and submitters had to refrain from taking patents.

The ciphers we published in '96-'97 already addressed the requirements of NIST, so we just had to adapt a few details to have our submission. We looked for a name that contained parts of our names and ended up with Rijndael. We were competing with 14 other teams, several of them American, and much to our surprise NIST only used technical arguments in their selection. In October 2000 NIST announced Rijndael as AES winner.

The AES competition was a brilliant move by NIST, which up to that moment was distrusted by the academic community and framed as a subsidiary of the NSA. After the AES competition, NIST was seen as an essential contributor to the academic process and they went on to organize several similar open competitions.

We think we can say that our invention, Rijndael, and its underlying design principles, was a crucial step forward in the cryptologic process. In the 25 years after the standardization of Rijndael as AES by NIST, many published papers have reported cryptanalysis/interesting properties of Rijndael/AES, and

repeatedly the comment was made that it looks too simple to be secure. Still, no practical attacks have been published and over the years AES has become the most widely trusted cipher in the world, and has inspired tons of follow-up work.