Acceptance speech

18 June 2026

Vincent Rijmen, awardee in the Information and Communication Technologies category (18th edition)

First of all, I would like to thank the BBVA Foundation for establishing this prize and for awarding it every year. Secondly, I thank the committee for awarding this prize to my colleague Joan Daemen and me. In a time when gut feelings and false appearances often seem to carry more weight than thoughts from experts, recognition like this carries twice as much weight.

Cryptology is a branch of science that has a long and glorious but also often tragic history. It was mainly linked to the diplomatic and military fields, and hence it was surrounded by secrecy, and in particular secret services. Until the 1980s, and even in the 1990s when I started my academic career, it was not uncommon that open research projects on cryptology were stopped or forbidden from starting, because it was felt that law-abiding citizens had no need for it.

This situation changed with the advent of the internet, when online payments and services such as e-Government, but also social media, dramatically increased the importance of secure communication for purely civilian purposes. Later came mobile phones and other forms of wireless communication, where eavesdropping or disruption can occur so easily that they can even happen accidentally. In fact, our modern society has become very much dependent on secure transmission of data and remote commands. Think of smart energy distribution systems where parts of the network are continuously being reconfigured depending on the increase or decrease of green energy production and variations in demand. Without cybersecurity it would be possible to bring down the electricity grid from behind a remote computer. There are numerous other examples of civilian critical infrastructure that must be protected against cyber attacks.

In open environments where products from different vendors need to be able to interoperate, and where all kinds of people have access to products and can investigate their inner workings, it is not possible to build strong security on trade secrets. Hence, the main instrument for protection against cyberattacks and privacy threats has to be cryptology. This observation has stimulated the use and need for open standards in cryptographic methods and for open research on cryptology and cybersecurity systems.

Cryptology includes both the design of algorithms, and the security evaluation of algorithms. People may wonder why it is so difficult to design secure systems, and why cryptographers don't develop once and for all a standard that can be used forever. This is because security evaluations, or security checks, just like a mathematical proof, start from basic assumptions. In the case of cryptology, these include assumptions about the actions that a cyberattacker might possibly take. Sadly, it turns out to be very difficult to fully predict the behavior, ingenuity and motivation of cyberattackers. Hence, progress in our field is characterized by an intense interaction between powerful design and intense security evaluation.

An equally important concern is the usability of security systems. Users have little patience with encryption programs that are either slow or complicated to use, or that require to memorize long and unpredictable passwords. While it is not so difficult to design systems that are secure or very fast, it remains a challenge to design systems that are secure, fast and user-friendly.

In order to get a well performing security system, both design and analysis have to be based on computer-aided analysis, statistics and deep mathematics. It requires patience, perseverance from the researchers, but also trust and sponsoring by public research agencies or by private organizations, for example the Fundamentos grants provided by the BBVA Foundation.

Since the mid 1970s open research in this domain has flourished and produced numerous cryptographic algorithms. However, most of these are broken shortly after publication. This is caused by the fact that designers typically have an overly positive mindset towards their own creation and a blind eye towards potential weaknesses. The trust in a cryptologic system is therefore necessarily based on open research and public cross-scrutiny of each other's designs. During the development of the Advanced Encryption Standard, we studied many other designs, invented new mechanisms, discarded them again and replaced them with other ideas.

Nowadays, the Advanced Encryption Standard is used to secure websites, electronic payments, computer disks, mobile phones, smart homes and many other systems from daily life. Even stronger, in applications such as GPS-like navigation systems for cars, ships and airplanes, the newest civilian systems use the Advanced Encryption Standard; and they are performing better than many military-grade systems. I see this as a triumph of open research.

Open research, careful testing, and public support keep our digital lives safe – thank you for helping make that possible.