Univ.-Prof. Dr. Vincent Rijmen
Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
E-Mail: vincent.rijmen@iaik.tugraz.at
Tel.: 0316 873 5529

Vincent Rijmen

Since 01. 10. 2004 Professor of `Applied Cryptography' at the Institute for Applied Information Processing and Communications (IAIK)

The field of information security forms a bridge between mathematics and computer sciences. Cryptography is an important aspect of information security: it is the science of codes: breaking old codes, constructing new codes and finding new applications in which to employ them.

For a long time, cryptography was only practiced by diplomats and the military. Nowadays, cryptographic codes are essential building blocks for secure emails and access control systems, cash machines and on-line banking, digital signatures and e-Government applications. The easier it becomes to collect and access all kinds of information, the greater the need becomes for means to guarantee the correctness of data and to limit access to confidential or private data.

The challenge in cryptographic research is to construct mathematical transformations that have desirable security properties on the one hand, but, on the other hand, should also be efficiently realizable in hardware and/or software. In this respect, the most interesting event of the end of the 1990's was doubtlessly the selection process for a new encryption standard organized by the National Institute of Standards and Technology (NIST) of the US Federal Administration. For the last 30 years, the information security standards of NIST have been followed by all banking organizations, Internet security developers and software companies. Hence, the selection of a new standard by NIST is of importance outside the US as well.

The Advanced Encryption Standard (AES) competition received submissions, evaluations and other contributions from all over the world. Even after the selection of the AES, research continues. The development of new cryptanalysis techniques necessitates continuous re-evaluation of security. The introduction of new applications puts new demands on implementations and requires the rethinking of the possibilities for optimization of performance, energy consumption, cost, … Here, at the Institute for Applied Information Processing and Communications (IAIK), the AES has also been, and still is, studied extensively, both from the security viewpoint and the implementation viewpoint (http://www.iaik.tu-graz.at/research).

Whereas encryption algorithms protect the secrecy of documents, digital signatures aim to protect the correctness of electronic documents and contracts. They are an essential security component of Internet banking systems and e-Government applications. For these types of applications, correctness of data is much more important than secrecy. The newly founded crypto group at the IAIK focuses mainly on the security evaluation of hash functions, which are an essential component of digital signature schemes. The topic is approached with a multi-disciplinary approach, combining techniques from error correction coding, non-linear equation solving and discrete probability theory.

Recent observations illustrate that besides the purely mathematical properties of a cryptographic code, also its implementation needs to be evaluated for its security. For instance, it has been shown that a very precise measurement of the electro-magnetic radiation field of a chip during the time it executes cryptographic operations, may yield enough information to recover secret values from the chip. The design of secure hardware is a research topic of the SCA lab at the IAIK (http://www.iaik.tu-graz.ac.at/research/sca-lab/).

The working of a cryptographic algorithm

Resume

1970	Born in Leuven, Belgium
1993	Obtained the degree of Electronics engineer at the University of Leuven (KULeuven)
1997	Obtained the degree of doctor in the applied sciences; start of the design of Rijndael
2000	Rijndael selected as the AES
2001	Chief Cryptographer of Cryptomathic A/S
2004	Professor `Applied Cryptography' at the TU Graz