Prof. Dr. Çetin Kaya Koç

Çetin Kaya Koç received his Ph.D. in Electrical & Computer Engineering from University of California Santa Barbara in 1988. His research interests are in electronic voting, cyber-physical security, cryptographic hardware and embedded systems, elliptic curve cryptography and finite fields, and deterministic, hybrid and true random number generators.

Koç is the co-founder of the Conference on Cryptographic Hardware and Embedded Systems. The CHES Conference is the second largest cryptography conference and the premier forum for presenting scientific advances in all aspects of cryptographic hardware and security of embedded systems. More than 400 engineers and scientists from over 30 countries participate in CHES, submitting nearly 150 papers every year, with acceptance rate less than 20%. Koç was the program co-chair and proceedings editor of the CHES Conference in 1999-2003. Koç has been a permanent member of the CHES steering committee, in addition to serving as the publicity chair, the general chair, and the program committee member since its founding in 1999. In 2010, 2013, and 2016, Crypto and CHES conferences were held together at University of California Santa Barbara, and Koç was the general chair.

Koç is the founding Editor-in-Chief of the Journal of Cryptographic Engineering (JCEN), which covers all aspects of design and implementation of cryptographic hardware and software, including the research areas of the CHES Conference. The JCEN is a quarterly journal, started in January 2011. The first issue of every year is a special issue devoted to selected and expanded papers of the CHES Conference of the previous year. Koç is also co-founder of two other conferences: International Workshop on the Arithmetic of Finite Fields (WAIFI) and Security Proofs for Embedded Systems (PROOFS). WAIFI is a forum of engineers and mathematicians interested in efficient software and hardware realizations of finite fields. On the other hand, the goal of the PROOFS workshop is to promote methodologies that increase the confidence level in the security of embedded systems, especially those that contain cryptographic mechanisms. Koç is in the steering committee of both WAIFI and PROOFS, and he was the program co-chair of WAIFI 2008 and the general co-chair of WAIFI 2010. He was the general chair of PROOFS in 2013, which took place at UCSB following the CHES Conference. Koç also chaired the Open Problems in Mathematical and Computational Sciences Conference, held in Istanbul in September 18-20, 2013, and Cyber-Physical Security Education Workshop, held in July 17-19, 2017 in Paris, France.

Koç has been in the editorial boards of IEEE Transactions on Computers (2003-2008 and 2015-now) and IEEE Transactions on Mobile Computing (2003-2007). He was a guest co-editor of April 2003 & November 2008 issues of the IEEE Transactions on Computers on cryptographic and cryptanalytic hardware and embedded systems. In 2007, Koç was elected as IEEE Fellow for his contributions to cryptographic engineering. Furthermore, Koç is an Associate Editor of the prestigious International Journal of Foundations of Computer Science since March 2016.

Koç is the co-author of the three books Cryptographic Algorithms on Reconfigurable Hardware, Cryptographic Engineering, and Open Problems in Mathematics and Computational Science, published by Springer in 2007, 2009, and 2014, respectively. In addition to contributing to 6 conference proceedings as co-editor, he has also authored or co-authored more than 150 scientific papers, and 13 US patents. Koç graduated 15 Ph.D. students and 37 M.S. students, and also directed research theses of 6 undergraduate students. 11 of his Ph.D. students are currently professors (3 in the US, 1 in Mexico, and 7 in other countries); the remaining work for global high-tech companies in the US.

Koç was an Assistant Professor at University of Houston (1988-1992), Assistant, Associate and Full Professor at Oregon State University (1992-2007). He established Information Security Laboratory at Oregon State University, and received Award for Outstanding and Sustained Research Leadership in September 2001. Currently, Koç has appointments at İstinye University (İstanbul, Turkey), Nanjing University of Aeronautics and Astronautics (Nanjing, China), and University of California Santa Barbara. His research at UC Santa Barbara is funded privately and also by NSF, on aspects of electronic voting machines, cryptographic engineering, and cyber-physical security, performed within Koç Lab composed of postdoctoral researchers, PhD and MS candidates, and undergraduate students.