CHES: Past, Present, and Future

Jean-Jacques Quisquater

UCL Crypto Group
Universite Catholique de Louvain
Louvain-La-Neuve, Belgium
quisquater@dice.ucl.ac.be

CHES is (coming to be) a very interesting conference thanks to the excellent submitted papers, the new results about embedded systems, the coprocessors, and the new use of FPGAs.

But my talk will be about the nice locations for the CHES conference:

- First, it was Worcester and I'll speak about Vernam.
- Next, it was Paris and I'll speak about the Rose-Sainte-Croix company and, more importantly, the principle of Kerckhoffs (with a curious story about Napoleon).
- And now it is Redwood City: here is the whole of the public-key crypto is near or just there (Diffie, Hellman, Merkle, El Gamal, RSA Data Security, the RSA conferences at this hotel, ...). And a surprise: a big and secure embedded system: from Lockheed and it is the SeaShadow; it is time to think about James Bond, ..., and, finally, smart cards).
- the travel in the time and the space is finished and I'll propose some ideas for next location.

B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523, p. 1, 2003.