RSA—Past, Present, Future

Adi Shamir

Weizmann Institute of Science, Israel
Adi.Shamir@weizmann.ac.il

In 2008 we are celebrating the 10-th anniversary of CHES and the 30-th anniversary of the publication of the RSA paper at CACM. In this talk I will survey some of the major RSA-related papers published at CHES during the last 10 years, describe my own research on security and implementation issues, introduce some new attacks, and make predictions about the future of RSA.

E. Oswald and P. Rohatgi (Eds.): CHES 2008, LNCS 5154, p. 443, 2008.