Cryptography Everywhere
(IACR Distinguished Lecture)

Thomas A. Berson

Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94302, USA
Xerox Palo Alto Research Center
3333 Coyote Hill Rd, Palo Alto, CA 94304 USA
`berson@anagram.com`

1 Abstract

The past twenty years have seen cryptography move from arcane to commonplace, from difficult to easy, from expensive to cheap. Many influences are at work. These include: the professionalization of cryptographers, in which the IACR has played a significant role; the creation of textbooks and of courses; the steady growth of computational power delivered by the operation of Moore's Law; the algorithmic advances made by cryptographic researchers and engineers; the rise of e-commerce and wireless infrastructures which have a seemingly endless appetite for cryptographic services; the entry of many young people into the field; and the easing of government export controls. We envisage a near future where cryptographic operations will be as pervasive, cheap and unremarkable as IP protocol operations have become today.

Some things about this future are already clear. Cryptographic operations will disappear into the infrastructure. The complexities of cryptography and of cryptographic key management will be hidden from users. New sorts of protocols will become practical. New sorts of businesses will be possible. We will describe several such protocols and businesses. Other important aspects of this future are less clear, such as the social, economic, and political implications. We will hazard guesses at these and other impacts of cryptography everywhere.

2 Pointer to Further Detail

Further materials may be found at
http://www.anagram.com/berson/ac2000.html.

T. Okamoto (Ed.): ASIACRYPT 2000, LNCS 1976, pp. 72–72, 2000.