



# THE 1997 RSA DATA SECURITY CONFERENCE

## SPEAKER BIOGRAPHY

### **CRYPTOGRAPHERS' Track**

The Exact Security of Digital Signatures:

How to Sign with RSA and Rabin

Speaker: **Mihir Bellare**

Assistant Professor

University of California at San Diego

Dept. of Computer Science & Engineering,

Mail Code 0114

9500 Gilman Drive, La Jolla, CA 92093

Phone: 619-534-4544 Fax: 619-534-7029

Email: [mihir@cs.ucsd.edu](mailto:mihir@cs.ucsd.edu)

### **Company Background:**

The Computer Science and Engineering Department at University of California at San Diego is one of the top ones in the country. It offers both Ph.D. and Masters degrees and the faculty conduct research in many areas including systems, high performance computing, software, architecture, security, theory, databases, and VLSI.

### **Presentation Overview:**

We point to weaknesses in the current methods of signing with RSA, including some standardized ones. We then propose a new scheme, the PSS (Probabilistic Signature Scheme). It fits within the hash-then-decrypt paradigm used by current schemes, and in particular has the same cost as these. However, unlike current schemes, it can be proven secure based on standard assumptions about RSA and the ideality of the underlying hash functions, and the security translation is "tight." A variant of PSS, called PSS-R (PSS with recovery) permits message recovery, effectively reducing signature size by appreciable amounts. Joint work with Phillip Rogaway, UC Davis.

### **Speaker Background:**

Mihir Bellare received his BS (in mathematics) from the California Institute of Technology in 1986, and his Ph.D. (in computer science) from the Massachusetts Institute of Technology in 1991. From 1991 to 1995, he was at the IBM T.J. Watson Research Center, Hawthorne, New York, working in network security and complexity theory. He joined the Computer Science and Engineering Department of the University of California at San Diego in October 1995. His research interest is cryptography, with an emphasis on applying the ideas of provable security to the design of practical protocols.

**PRESENTATION**