



THE 1997 RSA DATA SECURITY CONFERENCE

SPEAKER BIOGRAPHY

DEVELOPERS' TRACK

Panel: Securing Broadcast Transmissions

Speaker: **Dror Lapidot**

Algorithmic Research Ltd.

15 Gush Etzion

Givat Shmuel, Israel

Phone: 972-3-5322799

Fax: 972-3-5322650

Email: dror@arx.com

Part 2 Company Background:

Algorithmic Research Ltd. (AR), founded in 1988, is headquartered in Givat Shmuel, Israel with 35 employees worldwide. AR has always been profitable with significant annual growth rates over past few years. Marketing subsidiaries are based in Frankfurt, London, and Singapore. The company is privately held by founders, employees, with Koor Industries as a significant minority shareholder. AR owns intellectual property, such as, Batch RSA, Broadcast Encryption, Security processor architectures, etc. Clients include about 40 of the world's largest financial institutions. AR markets thus far have been primarily in Europe and the Far East. Long term strategic partnerships/alliances include those with Canal+ (pay TV).

Presentation Overview:

This presentation will deal with pay TV and broadcast encryption. We will present a scheme that allows a center to efficiently broadcast a secret message to any subset of privileged subscribers out of some universe so that coalitions of subscribers of some prespecified size, not in the privileged set, cannot learn the secret. We will also present a cryptographic scheme that helps trace the source of leaks when sensitive data is made available to a large set of users. These two cryptographic schemes can be easily combined and they complement each other.

Speaker Background:

Dror Lapidot received a B.Sc. in mathematics and computer science at the Hebrew University, Jerusalem in 1988, and completed his Ph.D. in computer science and served as an advisor through The Weizman Institute, Adi Shamir in 1992-93. Dr. Lapidot did his postdoc work at the Lab for Computer Science at MIT during 1995-96. He is currently a Cryptographic Consultant at Algorithmic Research Ltd.

PRESENTATION