



Cryptography Research, Inc.

www.cryptography.com

LOCATIONS:

San Francisco, USA
London, UK

FOUNDED:

1995

FINANCIALS:

Private

INDUSTRIES:

- Financial Services
- Pay Television
- Wireless/Telecom
- Internet
- PC hardware/software
- Printer Supplies
- Smart Card
- Entertainment
- Defense

MANAGEMENT TEAM:

Paul Kocher, President and Chief Scientist
Benjamin Jun, VP of Technology
Kit Rodgers, VP of Business Development
and Licensing
Joseph Yang, VP and General Counsel

TECHNOLOGY ADVISORY BOARD:

Dr. Tom Berson
Founder and Owner, Anagram Laboratories
Dr. Dan Boneh
Associate Professor, Stanford University
Dr. Joan Feigenbaum
Professor, Yale University
Dr. Martin Hellman
Professor Emeritus, Stanford University
Dr. Peter G. Neumann
Principal Scientist, SRI International
Bruce Schneier
Founder and CTO, Counterpane Internet
Security

MEDIA CONTACTS:

United States (San Francisco)

Dan Borgasano
Schwartz Communications
+1 415 512-0770
DBorgasano@schwartz-pr.com

Europe (Paris)

Carol Leslie
Andrew Lloyd & Associates
+33 1 56 54 0700
carol@ala.com

COMPANY OVERVIEW

Cryptography Research, Inc. specializes in solving complex data security problems. The company licenses innovative technologies in areas including tamper resistance, content protection, and financial services. In addition, Cryptography Research performs security evaluations and provides specialized applied engineering services. Security systems designed by Cryptography Research engineers protect more than \$100 billion of commerce annually for the telecommunications, financial, digital television, entertainment and Internet industries.

ACHIEVEMENTS

The company is known for the strength of its cryptographic research and commercial data security solutions. Technologies designed by Cryptography Research are implemented in hundreds of millions of devices worldwide. Achievements include the design of SSL 3.0 (the dominant web security protocol). Research results also include creating practical renewable security technologies for high-definition optical disc formats, designing the DES Key Search machine, and discovering differential power analysis (DPA).

TECHNOLOGY LICENSING

The company actively licenses three main patented technology portfolios:

DPA Countermeasures

Fundamental techniques for securing tamper-resistant cryptographic devices (such as smart cards) against differential power analysis and other attacks.



Our certification logo program helps purchasers identify licensed products which have passed independent testing.

Pay TV Security

The CryptoFirewall™ is a silicon drop-in ASIC for securing pay-TV networks against signal piracy. The technology is complementary to conditional access systems and is successfully deployed in over 50 million set top boxes.

Anti-Counterfeiting

Silicon drop-in ASIC for preventing the counterfeiting of products used in disposable medical devices, printer consumables, and airplane parts.

Cryptography Research, Inc.

Leader in Advanced Cryptosystems

SERVICES AND TESTING EQUIPMENT

Cryptography Research offers unparalleled experience in solving security-related technical and business challenges. Services available to our licensees and consulting clients include:

Design Assistance

Hands-on expertise with protocols, software, and hardware enables the company to create efficient, robust standards-based security solutions, with a focus on testable high-assurance designs.

Product Evaluation

Experienced staff are expert at evaluating products in areas including:

- Architecture reviews (set-top boxes, PC-platforms, handheld devices, authentication tokens...)
- Device implementations
- Specification reviews
- Forensic analysis: Study of failure modes and recovery options
- Tamper resistance (e.g. DPA evaluations of smartcards and other devices)
- Component reviews: Random number generators, cryptographic cores
- Protocol reviews: Financial transactions, secure messaging, wireless applications
- Infrastructure reviews: Code update, secure renewability

Education & Training

We conduct specialized technical tutorials, hands-on workshops, and training seminars in areas including:

- Differential Power Analysis (basic concepts, advanced attacks, countermeasure utilization)
- Tamper resistance
- High assurance design practices
- Content protection methodologies (broadcast and physical media)
- Security validation and certification

DPA Workstation

Testing platform for evaluating smart cards and other devices:

- Includes custom hardware and software developed by Cryptography Research
- Is used by leading testing labs, chip manufacturers, smart card vendors, defense and government organizations

