

1996: The Cryptography Year in Review

*Yiqun Lisa Yin
RSA Laboratories*

*RSA Data Security Conference
January 28-31, 1997*



Outline

■ Research

- Recent attacks on cryptosystems and their impact
- Practice-oriented provable security
- New infrastructures for public-key cryptography

■ Standards

- IEEE P1363
- PKCS
- SET
- Other standards



Research

- **Recent cryptanalytic results**
 - attacks on smart card security
 - factorization of RSA-130
 - attacks on hash functions
- **Practice-oriented provable security**
 - HMAC: a new secure MAC
 - PSS: data formatting for RSA signature
 - DESX: its security against key search
- **New public-key infrastructure**
 - SD SI, SPKI, etc.



Attacks on Smart Card Security

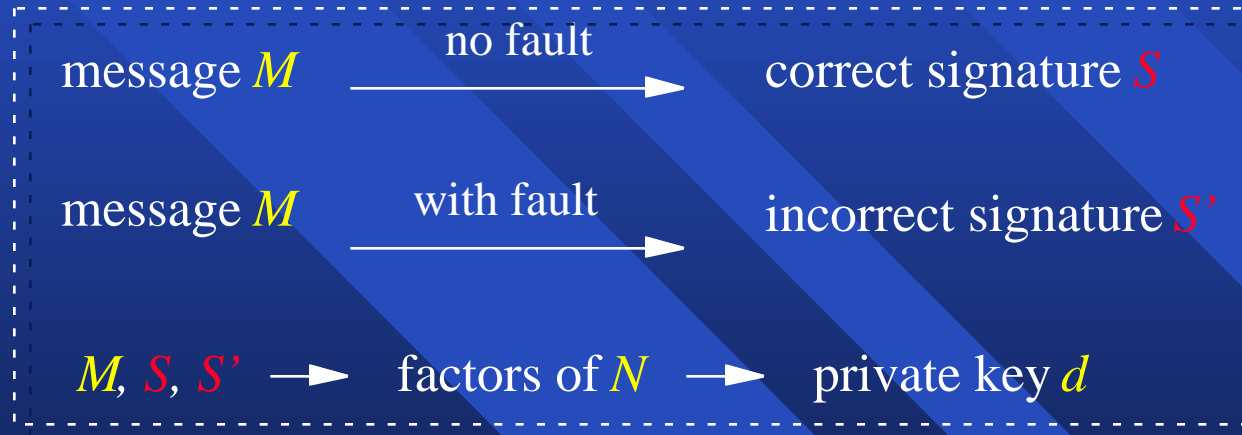
- **First announced by Bellcore in Sept. 1996**
 - Boneh, DeMillo, Lipton
 - Form of attack: recover keys in smart cards by introducing errors into key-dependent crypto operations through physical intrusions
 - apply the attack to certain public-key systems
- **Soon extended by several researchers**
 - Biham, Shamir
 - “differential fault analysis” on block ciphers
 - Anderson, Kuhn; ISS of Singapore



Example of an Attack

- Attacking RSA signature:

$$S = M^d \bmod N$$



- one or more S' may needed, depending on implementation of RSA
- the attack is independent of key size



Impact of the Attacks

- Basic idea of the attacks is applicable to many crypto devices
- At the current stage, the Bellcore attack is mainly of theoretical interest
 - no successful implementation of the attack on actual crypto devices has been reported
- Importance and relevance to secure hardware design should not be overlooked
 - security involves more than just good algorithms
 - good engineering is essential



How to Overcome the Attacks

- Do not produce an output if intrusion into the device is detected
- Verify the correctness of the result before outputting it
 - e.g., signature verification
 - may incur overhead; need further research
- Introduce randomness in the input
 - e.g., probabilistic signature scheme (PSS)
 - randomness needs to be concealed in the output



RSA-130 is Factored

- What is RSA-130?
 - a composite number of 130 decimal digits, listed as part of the RSADSI Factoring Challenge
 - factored in Apr. 1996 by a group of researchers
- Some big numbers factored in past years

| Number | Month | MIPS-years | algorithm |
|---------|-------|------------|-----------|
| RSA-100 | 4/91 | 7 | q.s. |
| RSA-110 | 4/92 | 75 | q.s. |
| RSA-120 | 6/93 | 830 | q.s. |
| RSA-129 | 4/94 | 5000 | q.s. |
| RSA-130 | 4/96 | 500 | g.n.f.s. |

q.s.: quadratic sieve, g.n.f.s.: generalized number field sieve



Impact of the Factorization of RSA-130

- Confirmed that for very large general-purpose factorizations, g.n.f.s. is the algorithm of choice
- 512-bit RSA modulus (less than 160 digits) can be anticipated to offer marginal security
- Factoring a 768-bit RSA modulus would require about 10^8 MIPS-years with current techniques
 - this is the minimum length of modulus currently recommended by RSA Labs



Attacks on Hash Functions

- **General design approach for hash functions**
 - iterative structure based on a *compression function*
 - in particular, MD4 has been used as the basis for the design of many other hash functions
- **Recent attacks**
 - Mostly done by Dobbertin (1995, 1996)
 - collisions of the reduced-round RIPEMD
 - collisions of MD4
 - collisions of the MD5 compression function



Status of Hash Functions

- **MD4**

- collisions found; should not be used

- **MD5, MD2**

- collisions for the compression function found
 - existing signatures formed by them are not at risk
 - remain suitable for use as one-way hash functions
 - should not be used for future applications requiring collision-resistant property

- **Alternative hash functions**

- SHA1, RIPEMD-128, RIPEMD-160



Practice-Oriented Provable Security

Motivation

- What do we have?
 - concrete primitives (math operations)

- DES:
 $(P, K) \rightarrow C$

- MD5:
 $M \rightarrow h(M)$

- RSA:
 $x \rightarrow x^e \bmod n$

- Usually, input and output have fixed lengths

- What do we need?
 - **secure and practical** schemes and protocols

- encryption

- MAC

- digital signature

- session key distribution

-



Practice-Oriented Provable Security

General Approach

- **Formalize definitions**
 - primitives (e.g., a hash function)
 - schemes (e.g., a MAC)
- **Construct schemes based on primitives**
- **Prove security**
 - assumption: primitives are good
(e.g., RSA is a good trapdoor one-way function)
 - reduction in the proof:
if there is an attack on the scheme, then there is
an attack on the primitive



HMAC: A Secure MAC

- Bellare, Canetti, Krawczyk (Crypto'96)
- Construction is based a hash function ***H***

$HMAC(\textit{text}, \textit{key})$

$= \textit{H}(\textit{key} \oplus \textit{opad}, \textit{H}(\textit{key} \oplus \textit{ipad}, \textit{text}))$

- *opad*, *ipad* are two fixed 64-byte strings
- HMAC was recently chosen by the IPSEC workgroup of IETF



PSS: Probabilistic Signature Scheme

- Bellare, Rogaway (Eurocrypt'96)
- Data formatting for RSA signature: $S = M^d \bmod N$

$$w = H(M \parallel r)$$

$$\text{formatted block} = w \parallel (M \parallel 00\dots 00) \oplus G(w)$$

- r is a random number; G is based on a hash function

- counterpart to OAEP for RSA encryption
- under consideration by IEEE P1363 standard
- for PKCS #1:

$$\text{formatted block} = 0001 \parallel \text{FF}\dots\text{FF} \parallel 00 \parallel H(M)$$



DESX: Its Security against Key Search

- DESX (designed by Rivest)

- $DESX_{k, k1, k2}(x) = DES_k(x \oplus k1) \oplus k2$
- a DESX key has $56+64+64 = 184$ bits

- Security analysis of DESX

- Killian, Rogaway (Crypto' 96)
- effective key length of DESX at least $118 - \lg m$ bits
 - assume that the attacker sees m plaintext blocks and their encryption under DESX
- DESX has proven stronger than DES against key search



New Public-Key Infrastructures

■ Motivations

- slow development of PK infrastructure
- existing proposals are
 - too complex (ASN.1 encoding, for example)
 - inadequate for developing secure distributed systems

■ Some new proposals in the area

- SDSI (Rivest, Lampson)
- SPKI (Ellison, Frantz, Thomas)
- PolicyMaker (Blaze, Feigenbaum, Lacy)
- W3C's work; evolution of X.509



SDSI: Simple distributed Secure Infrastructure

- **Keys are “*Principals*”**
 - a principal is the private key that signs statements, and it is identified with the corresponding public key
- **Names are always *local***
 - a principal can use *arbitrary* local names
 - a principal can *export* bindings of names to values (e.g., principals or group definitions) by issuing corresponding certificates

■ Simple syntax



SDSI Certificates

- Certificates are signed statements
- Certificates may bind names to values, describe the owner of public key, or serve other functions

```
( Cert:
  ( Local-Name: "Lisa Yin" )
  ( Value: (Principal: ... ) )
  ( Signed:
    ( Object-Hash: (SHA-1: #54321 ) )
    ( Date: 1997-01-30T8:30 )
    ( Expiration-Date: 1997-01-30T9:30 )
    ( Signer: (Principal: ... ) )
    ( Signature: #12345 ) ) )
```



SPKI: Simple Public Key Infrastructure

- **Certificates have two primary characteristics**
 - authorization and delegation of authority are explicit, never assumed as they traditionally are with identity certificates
 - designed to be simple to implement
- **SPKI supports SDSI fully**
 - in particular, it supports SDSI names



SPKI Certificates

- An SPKI certificate body consists of a 5-tuple: $\langle I, S, D, A, V \rangle$
 - I : Issuer (a principal which can speak)
 - S : Subject (a principal or object being spoken about)
 - D : An integer (the permission to delegate A)
 - A : A specific authorization (possibly parameterized)
 - V : Validity period or other conditions
- Every certificate format currently known can be mapped to these 5-tuples



Standards Activities

- **IEEE P1363**
 - a comprehensive standard for public-key cryptography
- **RSA Labs' PKCS series**
 - preview of the next generation
- **SET**
 - a standard for securing payment card transactions over open networks



What is P1363?

- **Emerging IEEE standard for public-key cryptography**
 - discrete logarithm systems
 - elliptic curve systems
 - integer factorization systems
- **A set of tools from which implementations, other standards can be built**



Highlights of P1363

- **Comprehensive**
 - key generation and representation
 - key agreement, encryption, and digital signatures
- **Separation of primitives and schemes**
 - implementation can be compliant to either
- **Incorporating new developments**
 - “unified” model of key agreement
 - authenticated public-key encryption
 - encryption of arbitrary-length messages with one operation
 - “provably secure” schemes



Status of P1363

- **First meeting Jan. 1994**
- **Most recent meeting Nov. 1996**
 - **version 1**
 - more established techniques
 - draft available for review
 - **version 2**
 - more advanced techniques
 - contributions available, more solicited
- **Balloting of version 1 in 1997**



What is PKCS ?

- **RSA Labs' Public-Key Crypto Standards**
 - a series of standards first published in 1993
 - basis for many other standards
 - very widely used
- **Events after the genesis of PKCS**
 - new crypto algorithms
 - “provably secure” schemes
 - emerging standards
 - problems with some existing algorithms



PKCS: The Next Generation

- **Changes and additions in consideration**
 - #1 (RSA), #3 (DH), #7 (Crypto Message Syntax)
 - add P1363 support (e.g., OAEP, elliptic curve methods)
 - #5 (Password-Based Encryption)
 - add triple-DES, RC5, SHA-1
 - #6 (Extended Certificate Syntax)
 - superseded by X.509 version 3
 - #12 (Personal Information Exchange Syntax)
 - a possible new document



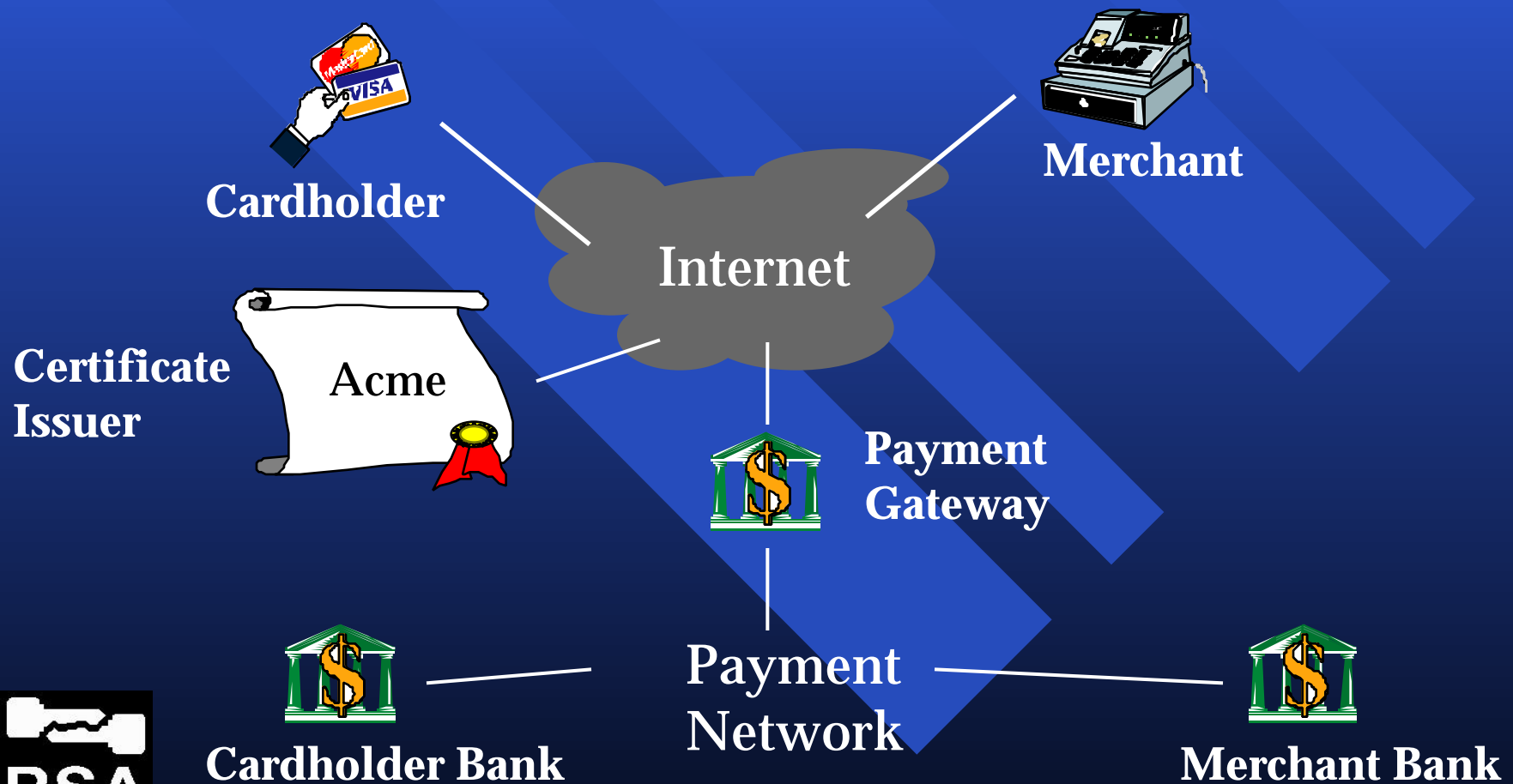
PKCS #11 and PICA

- **PKCS #11: Cryptographic Token API**
 - emerging de facto standard for programming interface to tokens
 - v1.0 published in April 1995
 - v1.1 final spec under construction
- **PICA**
 - platform-independent cryptographic API
 - initiated by a consortium of companies
 - currently soliciting suggestions



SET: Secure Electronic Transaction

- A new and secure way of getting the most from the electronic commerce market



Status of SET

- Announced by Visa and MasterCard, with others in the industry, in Feb. 1996
- June 1996 SET spec includes
 - business description
 - protocol description
 - programmer's guide
- Ongoing implementation effort
- Updated spec is expected by the end of 1996



1997 Outlook

- DES replacement research continues
- More provable security
- Smart card security
- System cryptography
- TRUST



The Growth of RSA Laboratories

- RSA Labs is the research and consulting division of RSADSI / Security Dynamics
- As of Sept. 1996, two locations
 - Redwood City, CA and Boston, MA
- Complementary and collaborative efforts
 - cryptographic technology
 - security technology
 - security assurance
- Contacting RSA Labs
 - rsa-labs@rsa.com, <http://www.rsa.com/rsalabs>

