

Fair Cryptography

Çetin Kaya Koç

Oregon State University

Conflicting Interests

- Private industry wants secure communications
- Private citizens want privacy
- Law enforcement wants wiretapping ability

→ Encryption is a threat

Capstone Project

- U.S. Government cryptography standards
- Computer Security Act of 1987
- Contains
 - Digital signature: DSS
 - Hash function: SHS
 - Data encryption: Skipjack and Clipper
 - Key escrowing procedure
 - Key exchange: not specified

NIST National Institute of Standards
and Technology

selects and proposes official standards

NSA National Security Agency

designs cryptographic algorithms

Mykotronx Inc

produces Clipper and Capstone chips

Key Escrowing

According to Webster:

es•crow |es-,krō,es-|
(MF *escoue* scroll)

a deed, a bond, money, or a piece of property held in trust by a third party to be turned over to the grantee only upon the fulfillment of a condition

Key Escrowing

- Decryption key is stored with two escrow agencies
- Identities of the escrow agencies are not yet decided
- Escrow agencies give the key to a law enforcement agency which has the proper authorization
- Each escrow agency stores 80-bit strings, XOR to get the decryption key

Overview of Clipper Proposal

- Key is escrowed at time of manufacture
- Clipper is tamper-proof hardware
- Use is voluntary in private sector

Session Key K

- Encrypts the message
- Unique to each session

Unit Key U

- Encrypts the session key
- Embedded on chip, escrowed

Family Key F

- Encrypts “law enforcement block”
- Common to all users

Secure Communication

- Agree on a session key K
 - Protocol is unspecified
 - A public-key method, e.g., Diffie-Hellman key exchange algorithm can be used
- Message M is encrypted with K
 - Message block: $E(M, K)$
 - K is not escrowed

- Law enforcement block: LEAF
 - Session key is encrypted with unit key:
 $E(K, U)$
 - Serial number of sender: N
 - Authentication string: A
 - All encrypted with family key: F
 $E(\{E(K, U), N, A\}, F)$
 - LEAF is sent at least once during session

Receiver

- Decrypts LEAF to get authentication string
- Checks authentication string
- Decrypts message using session key K

Authentication string prevents users chopping off LEAF (Details are not specified)

Court-authorized Wiretapping

1. Uses family key to decrypt the law enforcement block
2. Now has serial number and encrypted session key
3. Obtains wiretap authorization from court
4. Presents authorization to escrow agencies
5. Obtains unit key to decrypt session key K
6. Uses session key to decrypt message

Skipjack Algorithm

- Block cipher
- 64-bit input, 64-bit output
- 80-bit key
- 32 rounds of a nonlinear function
- Same modes as DES
- DES: 64-bit IO, 56-bit key, 16 rounds

Skipjack is Classified

- Not in software
- Only from authorized manufacturers
- Not open to public scrutiny
- One-month review by a team of five independent cryptographers: **Secure**

E F Brickell	Sandia Labs
D E Denning	Georgetown University
S T Kent	BBN Corporation
D P Maher	AT&T
W Tuchman	Amperif Corporation

Unit Key Generation

- Details are not specified
- Programmed inside a vault at chip factory
- Two agents are involved
- Each agent generates random 80-bit string S_1 and S_2
- Serial number N padded to get three 64-bit strings N_1, N_3, N_3

- Triple encryption to get three 64-bit blocks:

$$R_1 = E(D(E(N_1, S_1), S_2), S_1)$$

$$R_2 = E(D(E(N_2, S_1), S_2), S_1)$$

$$R_3 = E(D(E(N_3, S_1), S_2), S_1)$$

- Concatenate: $R = R_1R_2R_3$
- 80-bit strings U_1 and U_2 are taken from R
- Unit key $U = U_1 \oplus U_2$
- Escrow agencies get U_1 and U_2

Analysis of Clipper System

- Points of attack (external or internal)
 - Escrow agencies
 - Chip factory
 - Courts
- Other Abuses
 - Wiretap beyond authorization period
 - Intentional trapdoor

- Advantages of key escrowing
 - Police can wiretap suspected criminals
 - Citizens obtain secure communication

- Disadvantages of key escrowing
 - Government invasion of privacy
 - Criminals will use unescrowed cryptography
 - Hinders economic competitiveness in security and communications

Clipper Politics

- Large opposition
- Distrust of government
- Industry sees restrictions
- Effective against criminals?

Two Levels of Debate

1. Policy

- Debate about key escrowing
Good or bad? How widespread?

2. Implementation

- Debate about a given system
e.g., Clipper

The two levels have not been distinguished in the recent controversy

Fair Public-Key Cryptography

Public-key cryptosystems with escrowed keys

Proposed by Silvio Micali of MIT

- Software implementation
- Users generate their own keys
- Users choose their cryptosystem

Fair cryptography does NOT require

- Tamper-proof hardware
- Secret algorithm

Desired Properties

- Secure communication for ordinary user
- Access to message by authorized agency
- Audit trail: No undetectable or unauthorized wiretaps
- Law enforcement knows it can access messages with authorization
- Time-limited access

Overview of Fair Cryptography

- Choose public-key cryptosystem
- Distribute pieces of private key to escrow agencies
- Escrow agencies can verify that they have pieces of private key corresponding to user's public key without disclosing pieces of key

Diffie-Hellman

- Prime p and element g common to all users
- Alice:
private key x , public key $A = g^x \pmod{p}$
- Bob:
private key y , public key $B = g^y \pmod{p}$
- Alice and Bob both calculate the shared key:

$$K = g^{xy} \pmod{p}$$

Fair Diffie-Hellman

- Assume 5 trustees (esrow agencies)

- Alice chooses 5 secret numbers

$$x_1, x_2, x_3, x_4, x_5 \in [1, p - 1]$$

- Let $x = \sum x_i \pmod{p - 1}$

- Private key: x , Public key: $A = g^x \pmod{p}$

- x_i s are private pieces of key

- Public pieces of key: $t_i = g^{x_i} \pmod{p}$

- Trustee i gets x_i and t_i
- Trustees together verify that $\prod t_i = A$
$$\prod t_i = \prod g^{x_i} = g^{x_1+x_2+x_3+x_4+x_5} = g^x = A$$
- This ensures that $\sum x_i$ is Alice's private key
- Four of the trustees cannot find Alice's private key
- Alice and Bob communicate as usual

RSA Cryptosystem

- Pick two primes: p and q
- The modulus is the product: $n = pq$
- Euler's function $\phi(n) = (p - 1)(q - 1)$
- Select $e \in (1, \phi(n))$ with $\gcd(e, \phi(n)) = 1$
- Compute $d = e^{-1} \bmod \phi(n)$
- Public key: e , Private key: d
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

Towards Fair RSA

- Let p be a prime and $t = x^2 \pmod p$
- The equation $x^2 = t \pmod p$ has two solutions: $\pm x$
- If $p = 3 \pmod 4$, then x can be found easily
$$x = t^{(p+1)/4} \pmod p$$
- If $n = pq$, then the equation $x^2 = t \pmod n$ has four solutions: $\pm x$ and $\pm y$
- Solving $x^2 = t \pmod n$ is hard; If you can find both roots x and y , then you can factor n

- Since $x^2 = t$ and $y^2 = t$ modulo n , we have

$$\begin{aligned}x^2 - y^2 &= 0 \pmod{n} \\(x - y)(x + y) &= 0 \pmod{n}\end{aligned}$$

Thus, either $\gcd(n, x - y)$ or $\gcd(n, x + y)$ is one of the prime factors p or q

- Jacobi symbol: $J(a, n) = +1$ or -1

- Jacobi symbol is multiplicative

$$J(ab, n) = J(a, n)J(b, n)$$

- Of the four square roots modulo n , two are Jacobi $+1$ and two are Jacobi -1
- If you know a Jacobi $+1$ root **and** a Jacobi -1 root of $t \in (1, n)$, then **you can factor** n and find the private key d

Fair RSA

- Alice chooses primes p and q
- $n = pq$ and $p, q = 3 \pmod{4}$
- Alice chooses 5 Jacobi $+1$ integers

$$x_1, x_2, x_3, x_4, x_5 \in Z_n^*$$

where Z_n^* is set of integers modulo n , which are relatively prime to n

- Let $x = \prod x_i \pmod{n}$ and $s = \prod x_i^2 \pmod{n}$

- Alice computes y , a Jacobi -1 root of s
- $y^2 = s = \prod x_i^2 = (\prod x_i)^2 = x^2$
- x and y are Jacobi $+1$ and Jacobi -1 roots of s , respectively
- Anyone who knows x and y can factor n
- Alice sends x_i and y to trustee i
- Trustee i checks that x_i is Jacobi $+1$ and that y is Jacobi -1

- By sharing the x_i^2 s, trustees can verify that

$$\prod x_i^2 = y^2$$

and thus that $\prod x_i$ is a Jacobi $+1$ root of $s = y^2$

- Trustees together can produce a Jacobi $+1$ and a Jacobi -1 root of s
- Therefore, trustees can factor n , and recover private key
- Cooperation of all 5 trustees is necessary to factor n

Clipper versus Fair PKC

Clipper:

- Requires users to trust key generation center
- Requires secure hardware
- No software implementations
- Automatic key registration
- Process is invisible to users
- Possible abuse by authorities, not users

Clipper versus Fair PKC

Fair PKC:

- Users generate own keys
- No secure hardware is needed
- Software implementations are possible
- Key registration is more complicated
- Users have more responsibility
- Abuse by users more of a concern

Additional Features in Fair PKC

- A subset of trustees can reconstruct private key in case a trustee loses data

Example: 4 out of 5

- Time-limited access
 - Keys with expiration periods

Open Questions

- How can cryptography best meet the needs of society?
- Will ordinary cryptography become illegal?
 - Key escrowing is ineffective against criminals unless ordinary cryptography is illegal
 - “... Privacy will be the first roadkill along the information superhighway”
(Brock N. Meeks, *Wired*, April 1994)
 - Ordinary cryptography would be legal but unusual and unsupported
- Criminals may use unescrowed keys even if it is illegal to do so