Untraceable electronic mail, return addresses, and digital pseudonyms

David Chaum

Communications of the ACM, 1981

Presented by Apu Kapadia
Sep. 8, 2009

Motivation:
Secrecy of Message not enough

- Crypto provides secrecy for message content
- Also need to provide anonymity
  - hide "who talks to whom"
  - but should not rely on a central TTP
- Several applications
  - Untraceable email, anonymous elections, etc.

Contributions:
First person to propose mixes

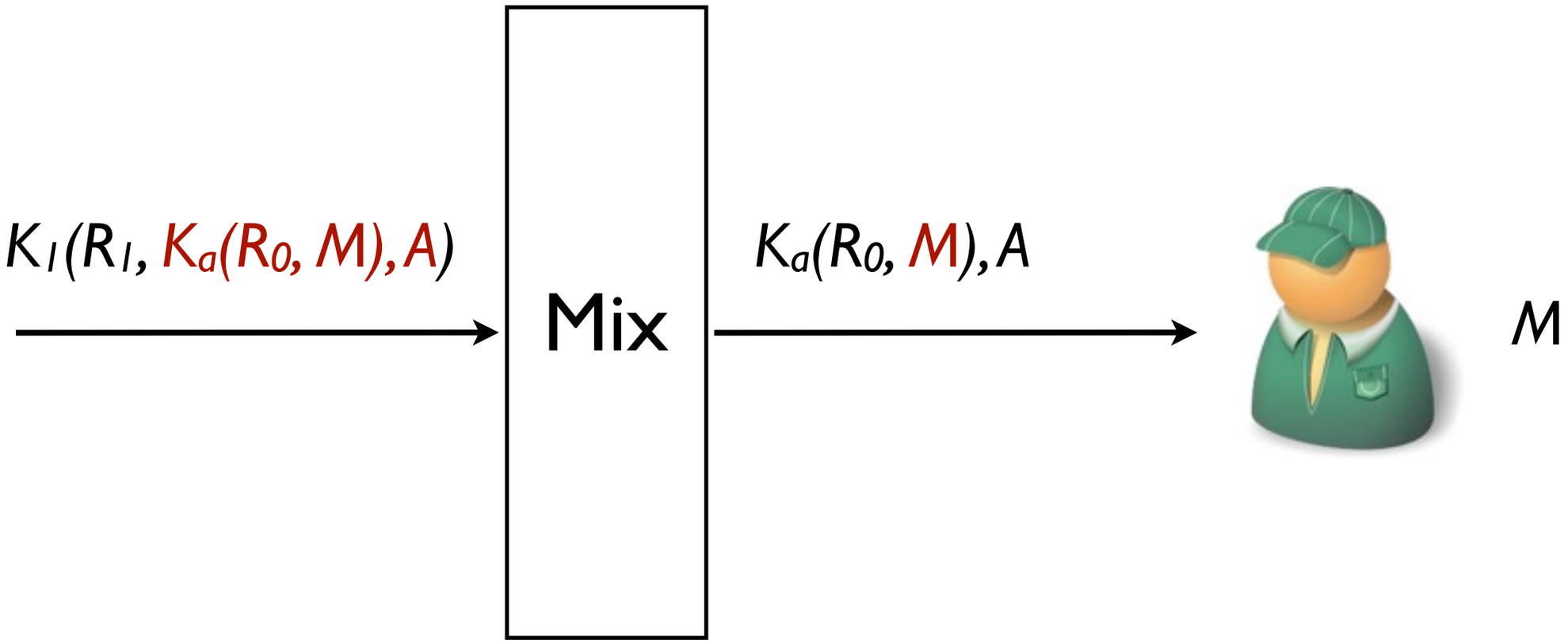
- Protocol to send anonymous email through a series of *mixes*
  - Provides sender anonymity
  - Mixes know only previous+next mixes in chain
  - A single honest mix provides anonymity
- Protocol supports anonymous return email

Basic Operations

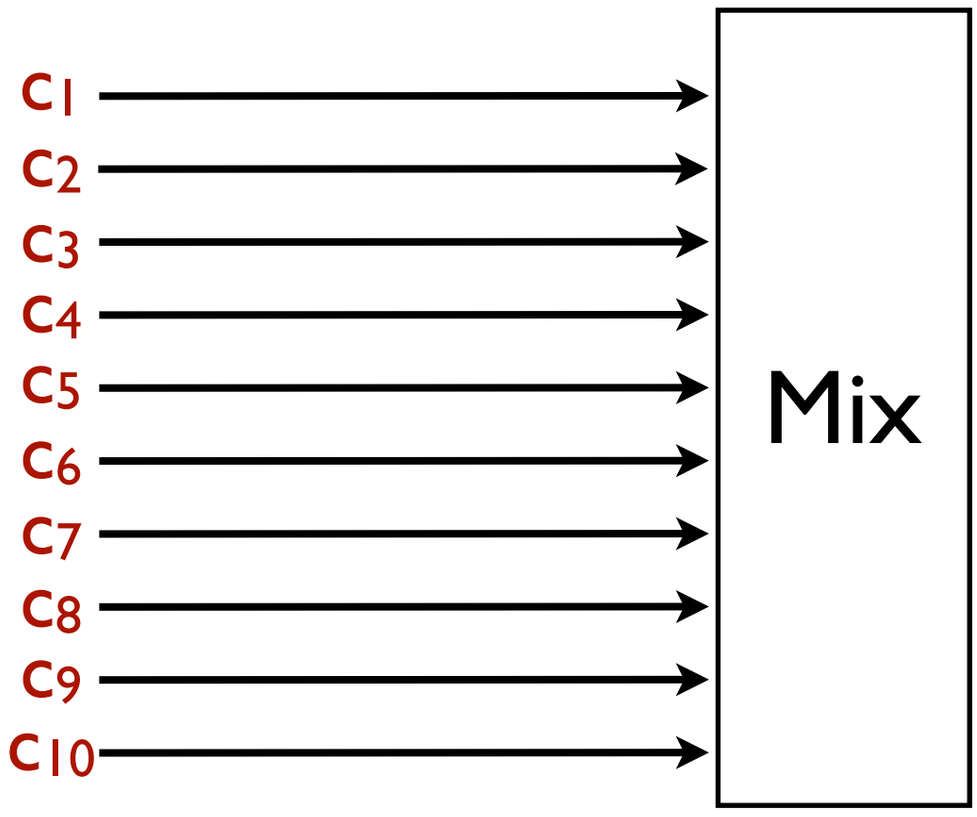
Context: DH 1976, RSA 1978

- Public and private keys *K and* K^{-1}
- Encrypt *x* and random *R* with key *K*
  - encryption, *c* = *K(R, x)*
  - *decryption, x* = $K^{-1}(c)$
- Sign message x and constant *C*
  - sign, *sig* = $K^{-1}(C, x)$
  - verify, given *m* and *sig*, check *K(sig)* = *C, m*

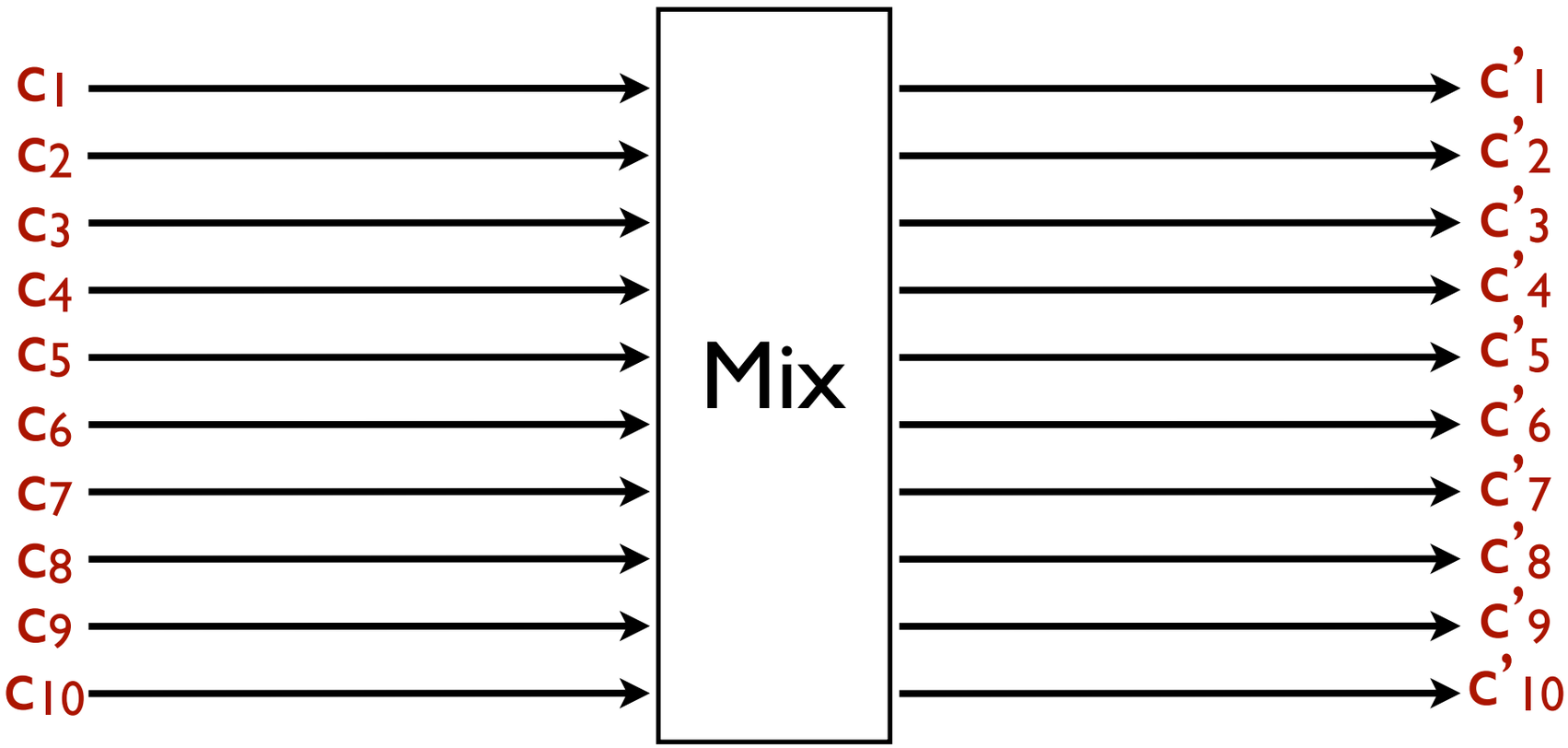
Protocol for sending email



Actually, mix shuffles batches of messages



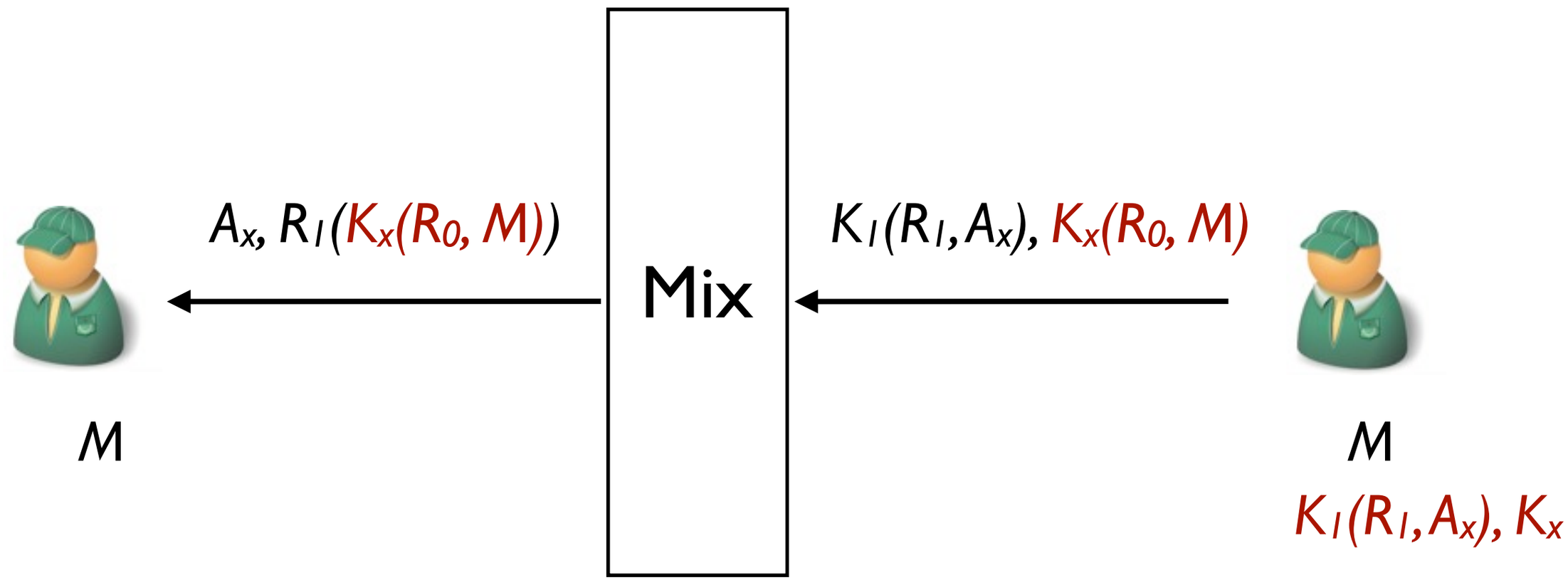
Actually, mix shuffles batches of messages



Protocol for multiple mixes

- $\boldsymbol{K_n(}R_n, K_{n-1}(R_{n-1}, ..., K_2(R_2, K_1(R_1, K_a(R_0, M), A))..)\boldsymbol{)}$
  - Each mix in the *cascade* "peels off" a layer of encryption
  - Final step as before

Return addresses supported



Protocol for multiple mixes

- $K_1(R_1, K_2(R_2, ..., K_{n-1}(R_{n-1}, K_n(R_n, A_x))..)),\ K_x(R_0, M)$
  - $K_2(R_2, K_3(R_3, ..., K_{n-1}(R_{n-1}, K_n(R_n, A_x))..)),\ R_1(K_x(R_0, M))$
  - Each mix in the *cascade* "peels off" a layer of encryption, and re-encrypts the message

- Alice receives $R_n\ (R_{n-1}...(R_2\ (K_x(R_0, M))...)$
  - Alice peels off layers because she picked the R's herself

Additional protections

- Hide number of messages sent/received
  - senders output fixed batches
  - receivers search output of mixes to hide number of received messages
- Load balancing by picking a subset of mixes
  - hide the number of mixes
  - replies indistinguishable from regular email

Improved protocol

- Chop message into fixed size blocks
  - all messages have the same number of blocks
- Each mix
  - decrypt first block, obtain encryption key *R*
  - re-encrypt remaining blocks with *R*
  - add dummy block

Discussion Questions

- Why hide the number of mixes?
- Why hide distinction between forward and reverse email?

- Analysis and experimentation were missing. Did you find yourself skeptical of some of the claims?
- Sending a random number of messages for efficiency? What if you want to send more messages than the random value?