Chương 4

XÁC THỰC & CHỮ KÝ SỐ

Vấn đề xác thực

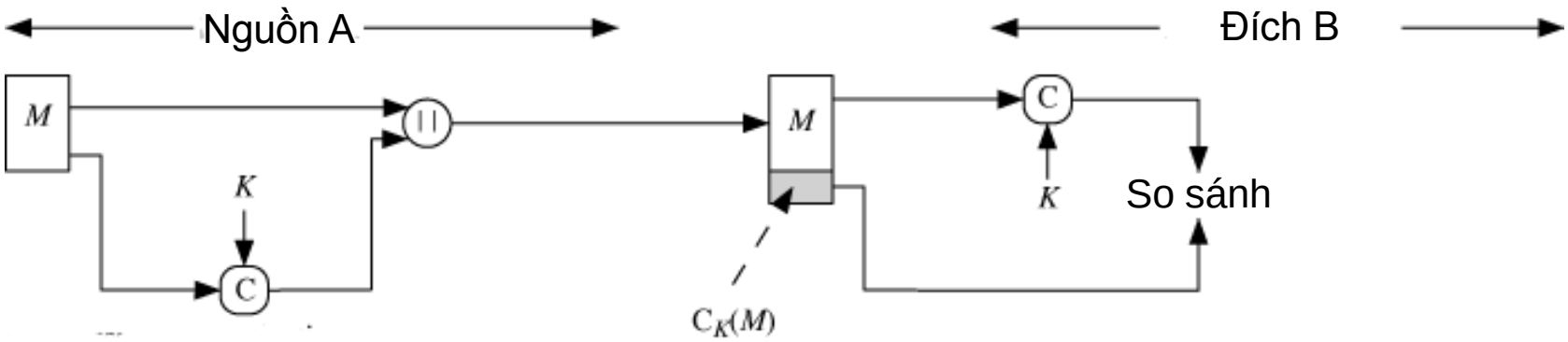
- Các tiêu chuẩn cần xác minh
  - Thông báo có nguồn gốc rõ ràng chính xác
  - Nội dung thông báo toàn vẹn không bị thay đổi
  - Thông báo được gửi đúng trình tự và thời điểm
- Mục đích để chống lại hình thức tấn công chủ động (xuyên tạc dữ liệu và giao tác)
- Các phương pháp xác thực thông báo
  - Mã hóa thông báo
  - Sử dụng mã xác thực thông báo (MAC)
  - Sử dụng hàm băm

Xác thực bằng cách mã hóa

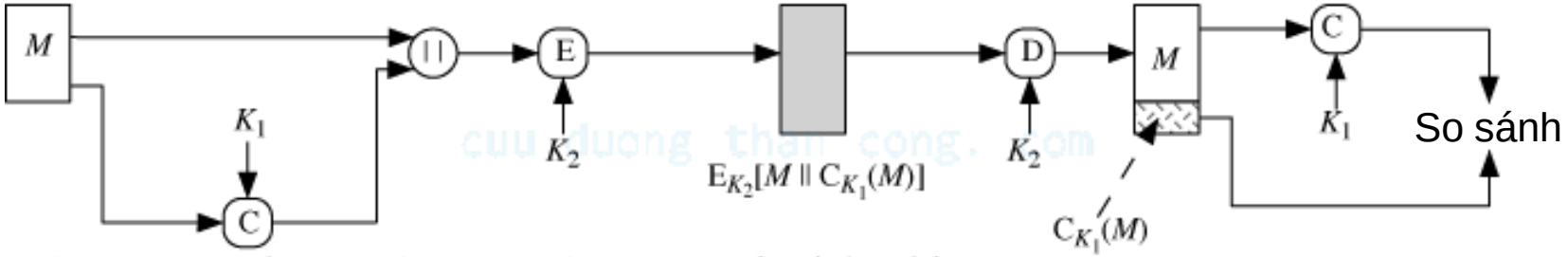
- Sử dụng mã hóa đối xứng
  - Thông báo gửi từ đúng nguồn vì chỉ có người gửi đó mới biết khóa bí mật dùng chung
  - Nội dung không thể bị thay đổi vì nguyên bản có cấu trúc nhất định
  - Các gói tin được đánh số thứ tự và mã hóa nên không thể thay đổi trình tự và thời điểm nhận được
- Sử dụng mã hóa khóa công khai
  - Không chỉ xác thực thông báo mà còn tạo chữ ký số
  - Phức tạp và mất thời gian hơn mã hóa đối xứng

Mã xác thực thông báo (MAC)

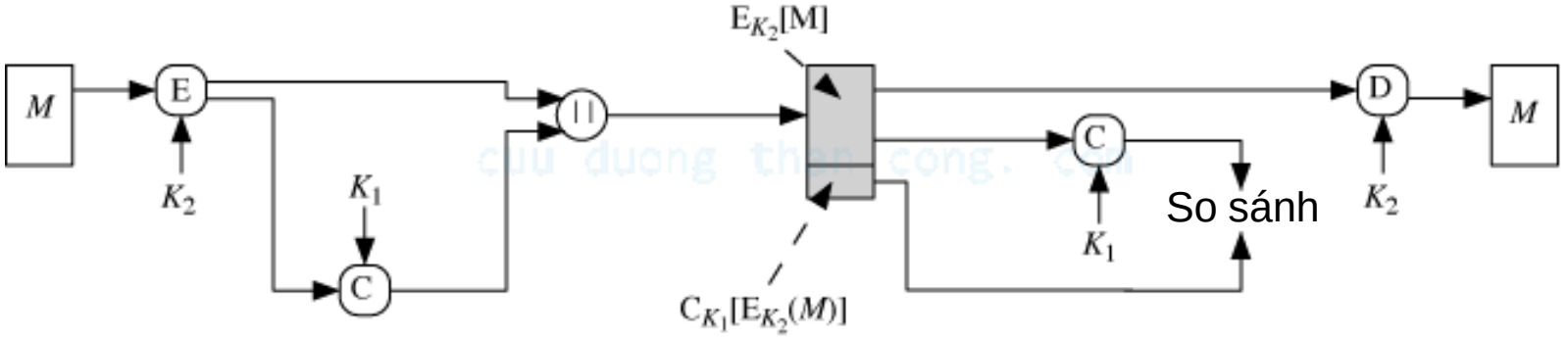
- Khối kích thước nhỏ cố định gắn vào thông báo tạo ra từ thông báo đó và khóa bí mật chung
- Bên nhận thực hiện cùng giải thuật trên thông báo và khóa để so xem MAC có chính xác không
- Giải thuật tạo MAC giống như giải thuật mã hóa nhưng không cần nghịch được
- Có thể nhiều thông báo cùng có chung MAC
  - Nhưng nếu biết một thông báo và MAC của nó, rất khó tìm ra một thông báo khác có cùng MAC
  - Các thông báo có cùng xác suất tạo ra MAC
- Đáp ứng 3 tiêu chuẩn xác thực



a) Xác thực thông báo



b) Xác thực thông báo và bảo mật; MAC gắn vào nguyên bản

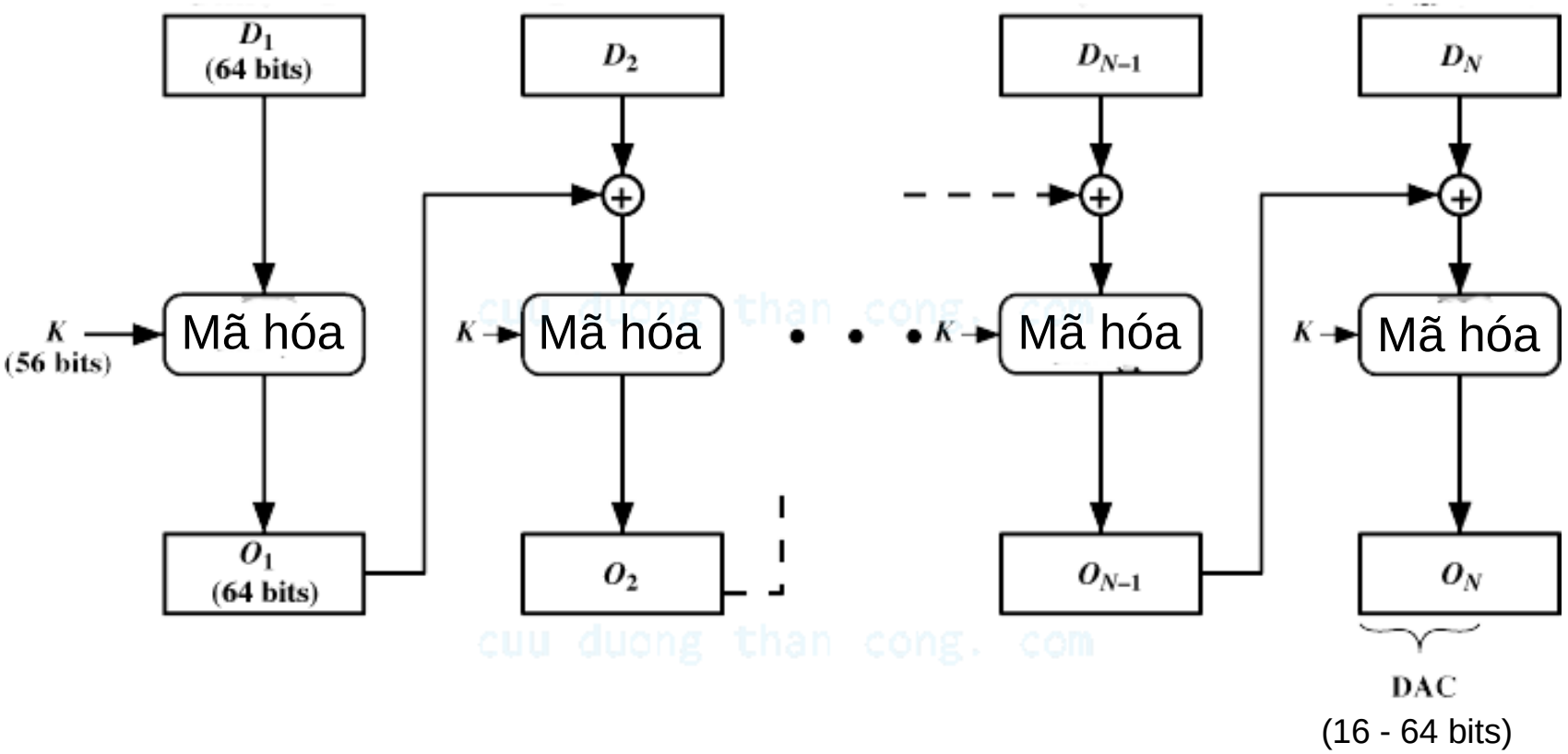


c) Xác thực thông báo và bảo mật; MAC gắn vào bản mã

Vì sao dùng MAC

- Nhiều trường hợp chỉ cần xác thực, không cần mã hóa tốn thời gian và tài nguyên
  - Thông báo hệ thống
  - Chương trình máy tính
- Tách riêng các chức năng bảo mật và xác thực sẽ khiến việc tổ chức linh hoạt hơn
  - Chẳng hạn mỗi chức năng thực hiện ở một tầng riêng
- Cần đảm bảo tính toàn vẹn của thông báo trong suốt thời gian tồn tại không chỉ khi lưu chuyển
  - Vì thông báo có thể bị thay đổi sau khi giải mã

MAC dựa trên DES (DAC)

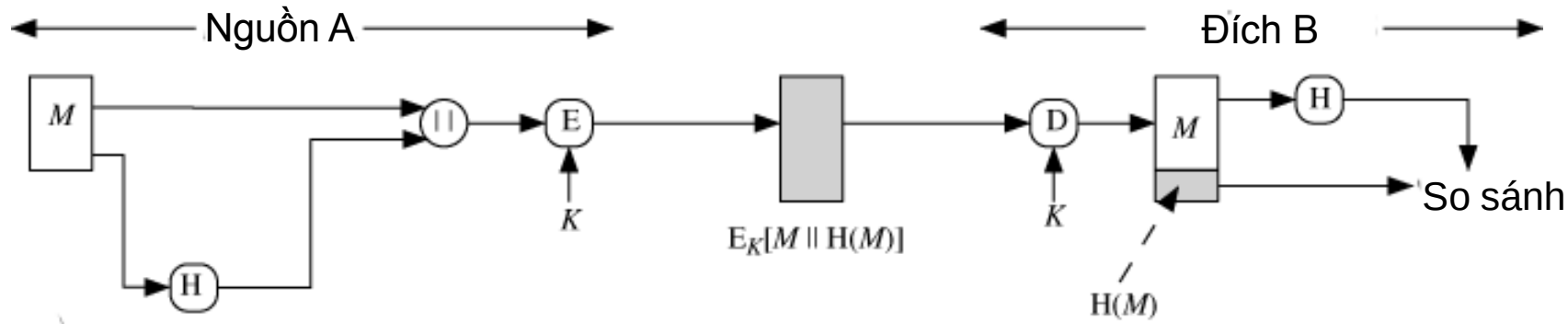


Hàm băm

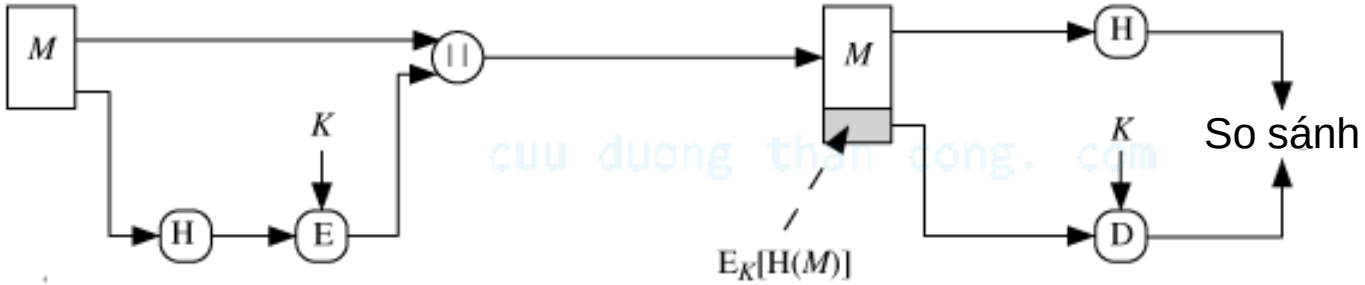
- Tạo ra một giá trị băm có kích thước cố định từ thông báo đầu vào (không dùng khóa)

$$h = H(M)$$

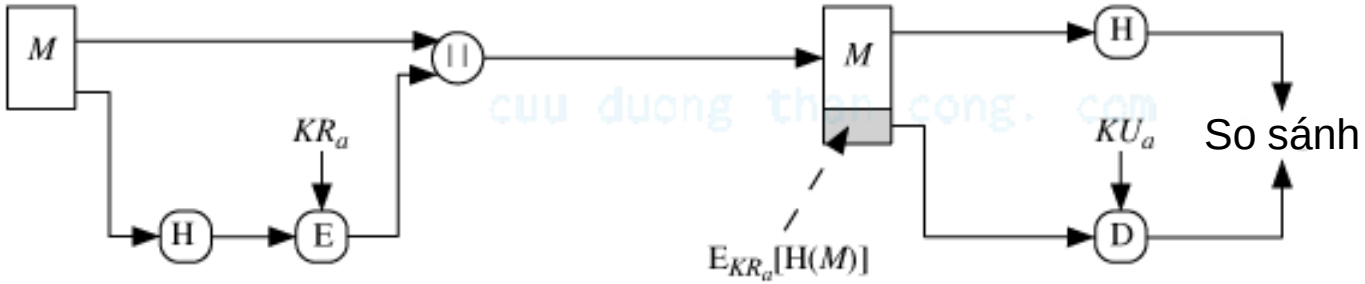
- Hàm băm không cần giữ bí mật
- Giá trị băm gắn kèm với thông báo dùng để kiểm tra tính toàn vẹn của thông báo
- Bất kỳ sự thay đổi M nào dù nhỏ cũng tạo ra một giá trị h khác



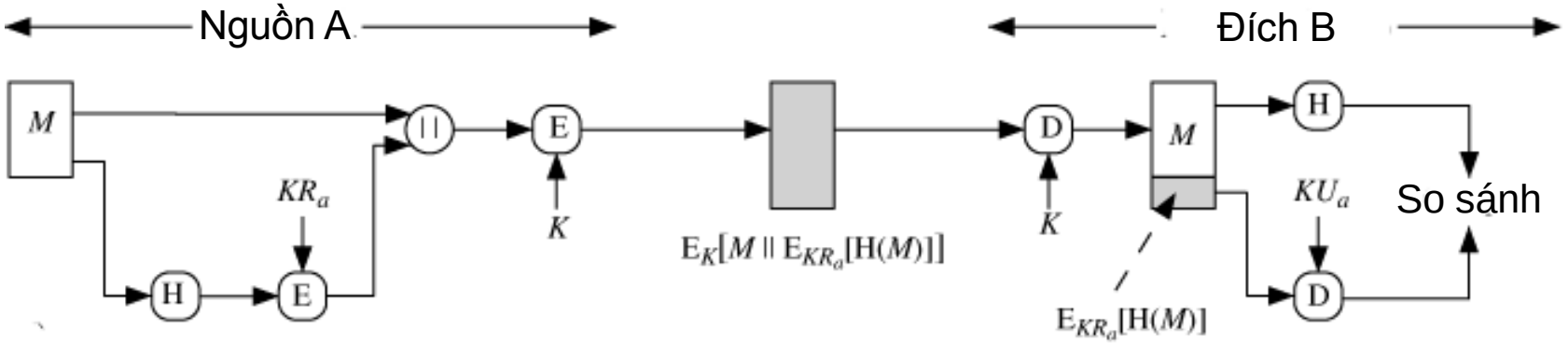
a) Xác thực thông báo và bảo mật; mã băm gắn vào nguyên bản



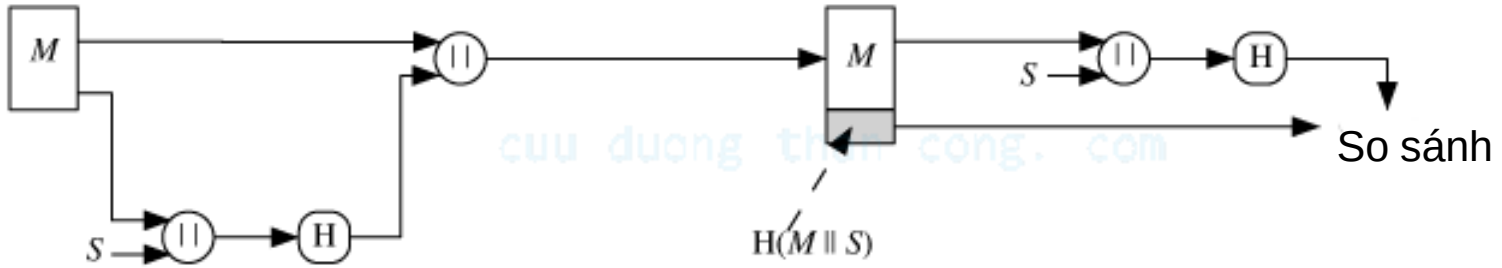
b) Xác thực thông báo; mã băm được mã hóa sử dụng phương pháp đối xứng



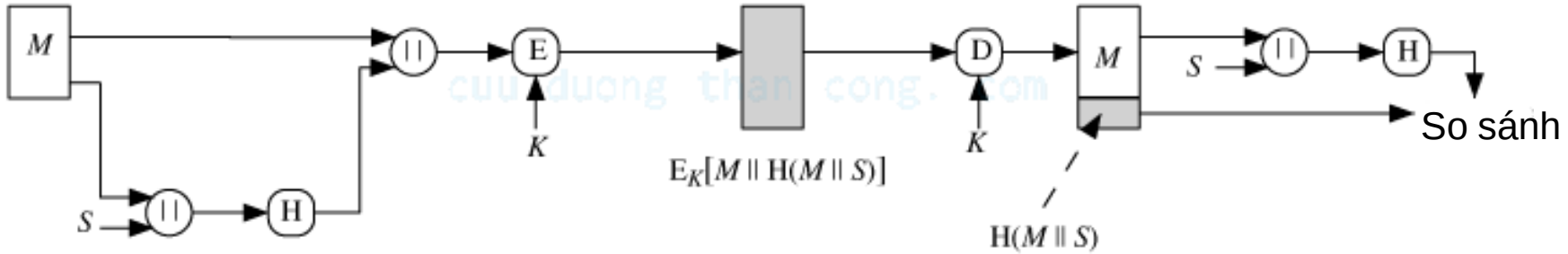
c) Xác thực thông báo; mã băm được mã hóa sử dụng phương pháp khóa công khai



d) Xác thực bằng mã hóa khóa công khai và bảo mật bằng mã hóa đối xứng



e) Xác thực không cần mã hóa nhờ hai bên chia sẻ một giá trị bí mật chung

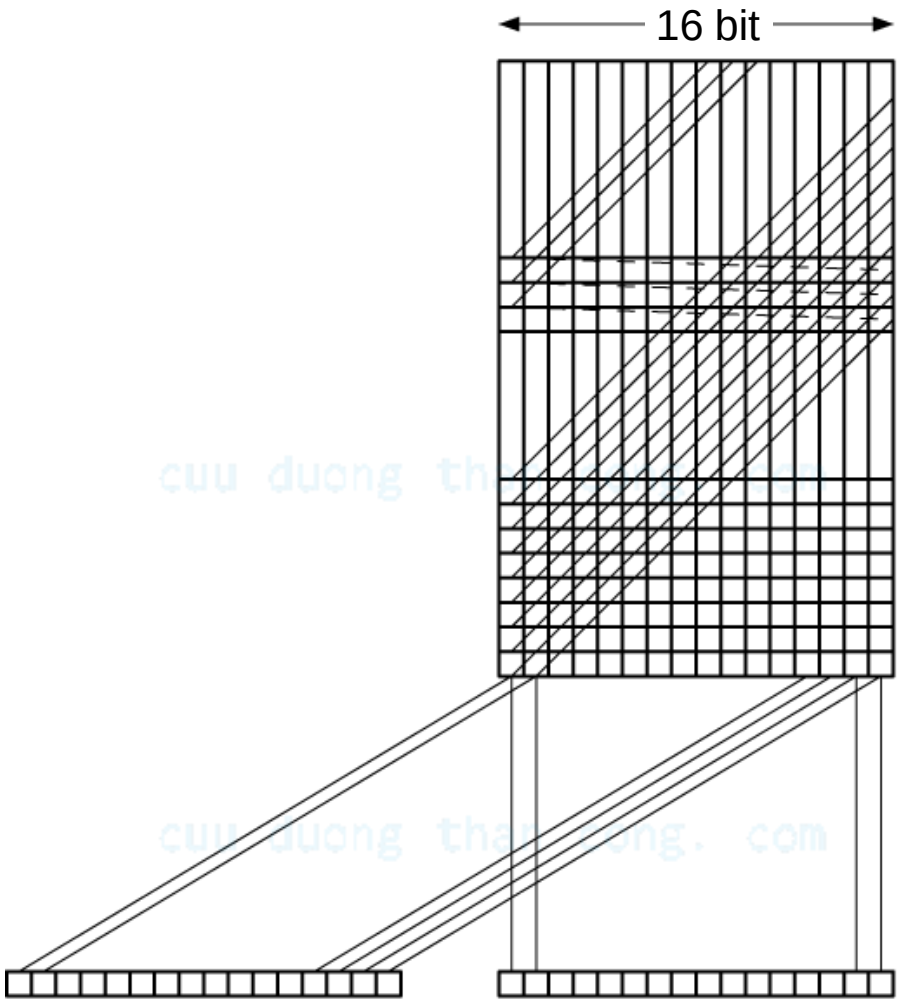


f) Xác thực nhờ một giá trị bí mật chung; bảo mật bằng phương pháp đối xứng

Yêu cầu đối với hàm băm

- Có thể áp dụng với thông báo M có độ dài bất kỳ
- Tạo ra giá trị băm h có độ dài cố định
- H(M) dễ dàng tính được với bất kỳ M nào
- Từ h rất khó tìm được M sao cho H(M) = h
  - Tính một chiều
- Từ M_1 rất khó tìm được M_2 sao cho $H(M_2) = H(M_1)$
  - Tính chống xung đột yếu
- Rất khó tìm được (M_1, M_2) sao cho $H(M_1) = H(M_2)$
  - Tính chống xung đột mạnh

Các hàm băm đơn giản



XOR dịch vòng trái 1 bit XOR mỗi khối 16 bit

Kiểu tấn công ngày sinh

- Nghịch lý ngày sinh
  - Trong 23 người, xác suất tìm ra 1 người khác có cùng ngày sinh với A là ≈ 6%
  - Xác suất 2 trong 23 người có cùng ngày sinh là ≈ 50%
- Cách thức tấn công mã băm m bit
  - Tạo ra $2^{m/2}$ biến thể đồng nghĩa của thông báo hợp lệ
  - Tạo ra $2^{m/2}$ biến thể của thông báo giả mạo
  - So sánh 2 tập thông báo với nhau tìm ra 1 cặp có cùng mã băm (xác suất > 0,5 theo nghịch lý ngày sinh)
  - Để người gửi ký biến thể hợp lệ, rồi dùng chữ ký gắn vào biến thể giả mạo

An ninh hàm băm và MAC

- Kiểu tấn công vét cạn
  - Với hàm băm, nỗ lực phụ thuộc độ dài m của mã băm
    - Độ phức tạp của tính một chiều và tính chống xung đột yếu là 2^m; của tính chống xung đột mạnh là $2^{m/2}$
    - 128 bit có thể phá được, thường dùng 160 bit
  - Với MAC, nỗ lực phụ thuộc vào độ dài k của khóa và độ dài n của MAC
    - Độ phức tạp là $\min(2^k, 2^n)$
    - Ít nhất phải là 128 bit
- Kiểu thám mã
  - Hàm băm thường gồm nhiều vòng như mã hóa khối nên có thể tập trung khai thác điểm yếu hàm vòng

Chữ ký số

- Xác thực thông báo không có tác dụng khi bên gửi và bên nhận muốn gây hại cho nhau
  - Bên nhận giả mạo thông báo của bên gửi
  - Bên gửi chối là đã gửi thông báo đến bên nhận
- Chữ ký số không những giúp xác thực thông báo mà còn bảo vệ mỗi bên khỏi bên kia
- Chức năng chữ ký số
  - Xác minh tác giả và thời điểm ký thông báo
  - Xác thực nội dung thông báo
  - Là căn cứ để giải quyết tranh chấp

Yêu cầu đối với chữ ký số

- Phụ thuộc vào thông báo được ký
- Có sử dụng thông tin riêng của người gửi
  - Để tránh giả mạo và chối bỏ
- Tương đối dễ tạo ra
- Tương đối dễ nhận biết và kiểm tra
- Rất khó giả mạo
  - Bằng cách tạo thông báo khác có cùng chữ ký số
  - Bằng cách tạo chữ ký số theo ý muốn cho thông báo
- Thuận tiện trong việc lưu trữ

Chữ ký số trực tiếp

- Chỉ liên quan đến bên gửi và bên nhận
- Với mật mã khóa công khai
  - Dùng khóa riêng ký toàn bộ thông báo hoặc giá trị băm
  - Có thể mã hóa sử dụng khóa công khai của bên nhận
  - Quan trọng là ký trước mã hóa sau
- Chỉ có tác dụng khi khóa riêng của bên gửi được đảm bảo an ninh
  - Bên gửi có thể giả vờ mất khóa riêng
    - Cần bổ xung thông tin thời gian và báo mất khóa kịp thời
  - Khóa riêng có thể bị mất thật
    - Kẻ cắp có thể gửi thông báo với thông tin thời gian sai lệch

Chữ ký số gián tiếp

- Có sự tham gia của một bên trọng tài
  - Nhận thông báo có chữ ký số từ bên gửi, kiểm tra tính hợp lệ của nó
  - Bổ xung thông tin thời gian và gửi đến bên nhận
- An ninh phụ thuộc chủ yếu vào bên trọng tài
  - Cần được bên gửi và bên nhận tin tưởng
- Có thể cài đặt với mã hóa đối xứng hoặc mã hóa khóa công khai
- Bên trọng tài có thể được phép nhìn thấy hoặc không nội dung thông báo

Các kỹ thuật chữ ký số gián tiếp

(a) Mã hóa đối xứng, trọng tài thấy thông báo

(1) X [redacted]: $M \| E_{K_{XA}}[ID_X \| H(M)]$

(2) A [redacted]: $E_{K_{AY}}[ID_X \| M \| E_{K_{XA}}[ID_X \| H(M)] \| T]$

(b) Mã hóa đối xứng, trọng tài không thấy thông báo

(1) X [redacted]: $ID_X \| E_{K_{XY}}[M] \| E_{K_{XA}}[ID_X \| H(E_{K_{XY}}[M])]$

(2) A [redacted]: $E_{K_{AY}}[ID_X \| E_{K_{XY}}[M] \| E_{K_{XA}}[ID_X \| H(E_{K_{XY}}[M])] \| T]$

(c) Mã hóa khóa công khai, trọng tài không thấy thông báo

(1) X [redacted]: $ID_X \| E_{KR_X}[ID_X \| E_{KU_Y}[E_{KR_X}[M]]]$

(2) A [redacted]: $E_{KR_A}[ID_X \| E_{KU_Y}[E_{KR_X}[M]] \| T]$

Ký hiệu : X = Bên gửi M = Thông báo

Y = Bên nhận T = Nhãn thời gian

A = Trọng tài