TCVN | **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN 7817-5:2026

ISO/IEC 11770-5:2020

Xuất bản lần 2

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN TOÀN - QUẢN LÝ KHÓA - PHẦN 5: QUẢN LÝ KHÓA NHÓM

Information technology – Security techniques – Key management

Part 5: Group key management

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN 7817-5:2025 hoàn toàn tương đương với ISO/IEC 11770-5:2020.

TCVN 7817-5:2025 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy Ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 7817 Công nghệ thông tin - Kỹ thuật an toàn - Quản lý khóa, gồm 07 phần:

- TCVN 7817-1 Phần 1: Khung tổng quan.

- TCVN 7817-2 Phần 2: Cơ chế sử dụng kỹ thuật đối xứng.

- TCVN 7817-3 Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.

- TCVN 7817-4 Phần 4: Cơ chế dựa trên bí mật yếu.

- TCVN 7817-5 Phần 5: Quản lý khóa nhóm.

- TCVN 7817-6 Phần 6: Dẫn xuất khóa.

- TCVN 7817-7 Phần 7: Xác thực trao đổi khóa dựa trên mật khẩu liên miền.

Lời giới thiệu

Trong một số ứng dụng, cần thiết phải chia sẻ khóa mật mã bí mật giữa một nhóm các thực thể. Hơn nữa, trong một số trường hợp, tập thành viên chính xác của nhóm các thực thể chia sẻ khóa có thể thay đổi theo thời gian.

Tiêu chuẩn này đề cập đến các kỹ thuật cho phép một khóa bí mật được chia sẻ bởi tất cả các thành viên của một nhóm xác định, với sự hỗ trợ của một bên thứ ba đáng tin cậy được gọi là trung tâm phân phối khóa. Các bước về việc thêm và xóa thành viên khỏi nhóm cũng được quy định.

TIÊU CHUẨN QUỐC GIA **TCVN 7817-5:2026**

Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý khóa - Phần 5: Quản lý khóa nhóm

Information technology – Security techniques – Key management - Part 5: Group key management

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các cơ chế để thiết lập các khóa đối xứng được chia sẻ ở trong các nhóm thực thể. Nó định nghĩa:

- Các cơ chế thiết lập khóa dựa trên mật mã khóa đối xứng cho nhiều thực thể sử dụng một trung tâm phân phối khóa (KDC); và

- Cơ chế thiết lập khóa đối xứng dựa trên cấu trúc khóa logic dạng cây tổng quát, bao gồm cả việc tạo lại khóa cá nhân và tạo lại khóa theo lô.

Tiêu chuẩn này cũng định nghĩa các cơ chế thiết lập khóa dựa trên chuỗi khóa, với an toàn về phía trước của nhóm, an toàn về phía sau của nhóm hoặc cả hai.

Tiêu chuẩn này cũng mô tả nội dung cần thiết của các thông điệp mang nguyên liệu khóa hoặc cần thiết để thiết lập các điều kiện mà theo đó nguyên liệu khóa có thể được thiết lập.

Tiêu chuẩn này không quy định thông tin không liên quan đến các cơ chế thiết lập khóa, cũng như không quy định các thông điệp khác như các thông báo lỗi. Định dạng rõ ràng của các thông điệp nằm ngoài phạm vi của tài liệu này.

Tiêu chuẩn này không quy định các phương pháp được sử dụng để thiết lập các khóa bí mật ban đầu cần được chia sẻ giữa mỗi thực thể và KDC, cũng như quản lý vòng đời khóa. Tài liệu này cũng không đề cập một cách rõ ràng đến vấn đề quản lý khóa liên miền.

2 Tài liệu viện dẫn

Các tài liệu tham chiếu dưới đây, toàn bộ hoặc một phần, được coi là yêu cầu cấu thành của tiêu chuẩn này. Đối với các tham chiếu có thời gian, chỉ phiên bản được chỉ định là có giá trị. Đối với các tham chiếu không có thời gian, phiên bản mới nhất của tài liệu được tham chiếu (bao gồm mọi sửa đổi) sẽ được áp dụng.

TCVN 12197(ISO/IEC 19772) Công nghệ thông tin - Các kỹ thuật an toàn - Mã hóa có sử dụng xác thực

TCVN 7817 (ISO/IEC 11770) Công nghệ thông tin - Kỹ thuật an toàn - Quản lý khóa - Phần 6: Dẫn xuất khóa

3 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này, áp dụng các thuật ngữ và định nghĩa sau đây:

3.1

Hoạt động (active)

Trạng thái của một thực thể mà trong đó thực thể có thể nhận được khóa bí mật dùng chung (3.24)

3.2

Khóa tổ tiên (ancestor key)

Khóa tổ tiên của thực thể x (ancestor key of an entity *x)*

Khóa mật mã trong một hệ thống phân cấp khóa logic (3.17) được gán cho một nút nằm trên đường dẫn trực tiếp từ nút lá (3.16) tương ứng với khóa cá nhân (3.11) của x đến nút gốc (3.23).

CHÚ THÍCH: Khóa tổ tiên là khóa bí mật dùng chung hoặc khóa mã hóa khóa.

3.3

An toàn phía sau với khoảng *T* (backward secrecy with interval *T*)

Trạng thái an toàn trong đó một thực thể tham gia vào một tập hợp các thực thể tại thời điểm $t = t_o$ không thể có được bất kỳ khóa bí mật nào đã được thiết lập giữa các thực thể này tại bất kỳ thời điểm nào trước t_o - T.

3.4

Tạo lại khóa theo lô với khoảng *T* (batch rekeying with interval *T*)

Phương pháp tạo lại khóa trong đó khóa bí mật dùng chung (3.24) và, theo tùy chọn, khóa mã hóa khóa (3.15) được cập nhật theo mỗi khoảng thời gian *T* (xem Điều 4).

3.5

Khóa con (child key)
Khóa con cho nút w (child key for a node *w*)

Khóa mã trong hệ thống phân cấp khóa logic (3.17) được gán cho một nút *w* không phải là nút gốc

CHÚ THÍCH: Khóa con phải là một khóa mã hóa khóa hoặc một khóa cá nhân.

3.6

Nút con (child node**)**
Nút con của nút *w* (child node of a node *w*)

Nút trong cây (3.25) liền kề với nút *w* và *w* nằm trên đường dẫn duy nhất giữa nút đó và nút gốc (3.23)

3.7

Cây d-ary (*d*-ary tree)

Một cây (3.25) trong đó mỗi nút có *d* nút con (3.6) ngoại trừ các nút lá (3.16) trong cây

3.8

An toàn về phía trước với khoảng *T* (forward secrecy with interval *T*)

Trạng thái an toàn trong đó một thực thể rời khỏi một tập hợp các thực thể tại thời điểm $t = t_o$ không thể có được bất kỳ khóa bí mật nào được thiết lập giữa các thực thể này tại bất kỳ thời điểm nào sau $t_o + T$.

3.9

An toàn về phía sau của nhóm (group backward secrecy)

Trạng thái an toàn trong đó một thực thể tham gia vào một nhóm các thực thể không thể có được bất kỳ khóa bí mật nào đã được thiết lập trước đó giữa các thực thể này.

3.10

An toàn về phía trước của nhóm (group forward secrecy)

Trạng thái an toàn trong đó một thực thể rời khỏi một nhóm các thực thể không thể có được bất kỳ khóa bí mật nào được thiết lập sau đó giữa các thực thể này.

3.11

Khóa cá nhân (individual key)

Khóa được chia sẻ giữa trung tâm phân phối khóa (3.14) và mỗi thực thể.

3.12

Tạo lại khóa cá nhân (individual rekeying)

Phương pháp tạo lại khóa trong đó khóa bí mật dùng chung (3.24) và, tùy chọn, các khóa mã hóa khóa (3.15) được tạo lại khi một thực thể tham gia hoặc rời đi.

3.13

Chuỗi khóa (key chain)

Tập các khóa mật mã không nhất thiết phải độc lập.

3.14

Trung tâm phân phối khóa (key distribution center)
KDC
Một thực thể được tin cậy để tạo mới hoặc thu thập, và phân phối khóa đến các thực thể

3.15

Khóa mã hóa khóa (key encryption key)

Khóa mật mã được sử dụng để mã hóa hoặc giải mã các khóa khác

[NGUỒN: TCVN 11295 (ISO/IEC 19790:2012)]

3.16

Nút lá (leaf node)

Nút trong cây (3.25) mà không có nút con (3.6).

3.17

Hệ thống phân cấp khóa logic (logical key hierarchy)

Một cây (3.25) được sử dụng để quản lý khóa bí mật dùng chung và các khóa mã hóa khóa (3.15).

3.18

Cấu trúc khóa logic (logical key structure)

Cấu trúc logic để quản lý khóa

CHÚ THÍCH: Việc lựa chọn hệ thống phân cấp khóa logic không phụ thuộc vào cấu trúc liên kết mạng.

3.19

Hàm một chiều (one-way function)

Hàm có tính chất là dễ dàng tính được đầu ra đối với một đầu vào cho trước, nhưng việc tìm một đầu vào tương ứng với một đầu ra cho trước lại là bất khả thi về mặt tính toán

3.20

Hàm dẫn xuất khóa một bước (one-step key derivation function)
OKDF
Đây là một hàm dẫn xuất khóa (KDF) chỉ hoạt động trong một giai đoạn duy nhất, trái ngược với các KDF khác yêu cầu hai giai đoạn tách biệt là trích xuất khóa và mở rộng khóa

[ISO/IEC 11770-6:2016]

3.21

Số ngẫu nhiên (random number)

Tham số biến thiên thời gian có giá trị không thể đoán trước.

[ISO/IEC 11770-1:2010]

3.22

Tạo lại khóa (rekeying)

Quá trình cập nhật và phân phối lại khóa bí mật dùng chung (3.24) và, tùy chọn, các khóa mã hóa khóa (3.15)

CHÚ THÍCH: Quá trình này được thực hiện bởi trung tâm phân phối khóa.

3.23

Nút gốc (root node)

Nút đặc biệt được xác định duy nhất trong cây

3.24

Khóa bí mật dùng chung (shared secret key)

Khóa được chia sẻ với tất cả các thực thể hoạt động thông qua một cơ chế thiết lập khóa cho nhiều thực thể

3.25

Cây (tree)

Đồ thị liên thông, không có chu trình với một nút đặc biệt được xác định là nút gốc (3.23)

4 Ký hiệu và thuật ngữ viết tắt

COM(X,Y)	hàm tạo ra một khóa từ các mục dữ liệu X và Y, được thiết kế để sử dụng làm khóa cho thuật toán mã hóa đang được dùng
CUT(k,S)	hàm tạo ra một chuỗi con có độ dài k bằng với các bit có trọng số thấp nhất của một chuỗi bit S
d	số lượng nút con của một nút không phải nút lá (xem thuật ngữ cây d-ary)
$e(K,Z)$	kết quả của việc mã hóa dữ liệu Z bằng một thuật toán mã hóa đối xứng, sử dụng khóa bí mật K
h	số lượng nút trên đường đi trực tiếp từ một nút lá đến nút gốc
$K_{A,i}(x)$	khóa tổ tiên cho thực thể x tại tầng thứ i, tính từ nút gốc
$K_{BW,i}$	khóa về phía sau cho thời điểm i
$K_{C,w}$	khóa con được gán cho nút w
$K_{FW,i}$	khóa về phía trước cho thời điểm i
K_I	khóa cá nhân
$K_I(x)$	khóa cá nhân được chia sẻ giữa thực thể X và trung tâm phân phối khóa
$K_{KE,w}$	khóa mã hóa khóa được gán cho nút w
K_{SS}	khóa bí mật dùng chung
KDC	trung tâm phân phối khóa
m	số lượng thực thể kết nối với trung tâm trong cấu trúc hình sao
OKDF1	hàm dẫn xuất khóa một bước nhận một đầu vào duy nhất đã được định nghĩa trong TCVN 7817-6 (ISO/IEC 11770-6)
OKDF6	hàm dẫn xuất khóa một bước nhận một khóa và dữ liệu đầu vào như đã được định nghĩa trong TCVN 7817-6 (ISO/IEC 11770-6)
OWF	hàm một chiều được sử dụng trong việc tính toán một chuỗi khóa
$r_{BW,init}$	số ngẫu nhiên dùng để khởi tạo chuỗi khóa phía sau
$r_{FW,init}$	số ngẫu nhiên dùng để khởi tạo chuỗi khóa phía trước
T	độ dài của khoảng thời gian được sử dụng trong việc tạo lại khóa theo lô
||	toán tử nhị phân biểu thị sự ghép các mục dữ liệu

5 Các yêu cầu

Các cơ chế thiết lập khóa được chỉ ra trong tài liệu này cho phép thiết lập các khóa bí mật dùng chung trong một nhóm các thực thể được xác định bằng cách sử dụng truyền tin đa hướng. Để đảm bảo an

toàn, các cơ chế này tích hợp một quy trình cập nhật khóa được sử dụng khi một thực thể mới tham gia hoặc một thực thể hiện có rời khỏi nhóm.

a) Các cơ chế được quy định trong tài liệu này cung cấp hoặc an toàn về phía sau của nhóm và an toàn về phía trước của nhóm, hoặc an toàn về phía sau và an toàn về phía trước với các khoảng thời gian. Loại an toàn về phía sau/về phía trước của nhóm nên được lựa chọn tùy thuộc vào các yêu cầu an toàn của ứng dụng cụ thể. Loại thuộc tính an toàn về phía sau/về phía trước của nhóm được xác định bởi lựa chọn của phương pháp tạo lại khóa: tạo lại khóa cá nhân cung cấp an toàn về phía sau/về phía trước của nhóm, và tạo lại khóa theo lô cung cấp an toàn về phía sau/về phía trước với các khoảng thời gian. Việc sử dụng tạo lại khóa theo lô yêu cầu lựa chọn tham số khoảng thời gian *T*. Phương pháp tạo lại khóa và thiết lập tham số có ảnh hưởng mạnh mẽ đến yêu cầu an toàn. Do đó, chúng phải được xác định theo chính sách bảo mật của ứng dụng.
b) Các kỹ thuật mã hóa đối xứng, như được yêu cầu cho các cơ chế được quy định tại Điều 6, phải được lựa chọn trong số đã được chuẩn hóa trong TCVN 12197(ISO/IEC 19772).
c) Khóa bí mật dùng chung được thiết lập bằng cách sử dụng kênh liên lạc an toàn hoặc không an toàn. Mỗi khóa cá nhân sẽ được trao đổi giữa KDC và mỗi thực thể bằng kênh an toàn để cho phép liên lạc an toàn. Kênh liên lạc an toàn là kênh mà kẻ tấn công không thể nghe lén hoặc can thiệp vào các thông điệp trong kênh.
d) Các cơ chế thiết lập khóa chính trong tài liệu này yêu cầu sử dụng các số ngẫu nhiên để tạo ra khóa bí mật dùng chung, và theo tùy chọn, các khóa mã hóa khóa. Để biết cách tạo các số ngẫu nhiên, xem tiêu chuẩn TCVN 12853 (ISO/IEC 18031).
e) Phụ lục A định nghĩa các mã định danh đối tượng theo TCVN 10583 (ISO/IEC 9834, tất cả các phần) được sử dụng để định danh các cơ chế được quy định trong tài liệu này. Bất kỳ thay đổi nào đối với đặc tả của các cơ chế mà dẫn đến thay đổi về hành vi chức năng đều dẫn đến thay đổi mã định danh đối tượng được gán cho các cơ chế đó.

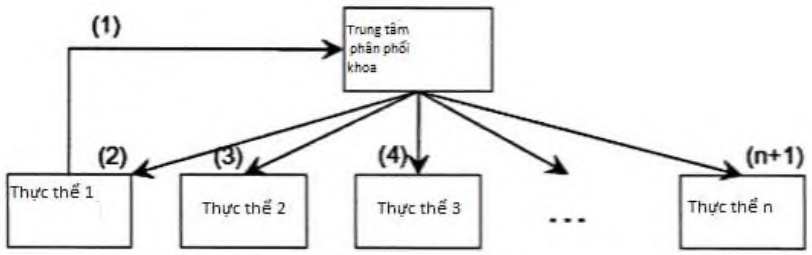
6 Cơ chế thiết lập khóa dựa trên cây

6.1 Mô hình tổng quát

Việc sử dụng các cơ chế được quy định trong tài liệu này cho phép thiết lập một khóa bí mật được chia sẻ bởi tất cả các thực thể trong một nhóm được xác định. Điều này cho phép bất kỳ thành viên nào của nhóm gửi một thông điệp được mã hóa đến tất cả các thành viên khác trong nhóm sao cho chỉ các thành viên trong nhóm (và trung tâm phân phối khóa) mới có thể giải mã được thông điệp đó. Các cơ chế này cũng cho phép trung tâm phân phối khóa cập nhật khóa bí mật đã được thiết lập để đảm bảo rằng một thông điệp được mã hóa chỉ có thể được giải mã bởi các thực thể là thành viên của nhóm tại thời điểm thông điệp đó được mã hóa.

Hình 1 thể hiện mô hình tổng quát về thiết lập khóa cho nhiều thực thể, trong đó trung tâm phân phối khóa có thể liên lạc với tất cả các thực thể. Việc liên lạc giữa trung tâm phân phối khóa và các thực thể không cần phải bảo mật. Trung tâm phân phối khóa và mỗi thực thể sẽ chia sẻ một khóa riêng biệt khác nhau. Trung tâm phân phối khóa chịu trách nhiệm phân phối khóa bí mật được chia sẻ cho tất cả các thực thể đang hoạt động. Yêu cầu tham gia/rời khỏi được thể hiện là (1) và việc phân phối khóa cho các thực thể là (2), (3), ..., (*n* + 1). Từ (2) trở đi, thứ tự theo đó các cập nhật xảy ra không quan trọng.

CHÚ THÍCH: Nếu một trong các thực thể nắm giữ khóa bí mật dùng chung không thể liên lạc được trong một khoảng thời gian, thực thể đó có thể bỏ lỡ thông báo cập nhật khóa và do đó sẽ không thể tính toán được khóa bí mật chung đã cập nhật.



Hình 1- Mô hình tổng quát của thiết lập khóa cho nhiều thực thể

6.2 Quá trình tham gia

Một thực thể gửi yêu cầu tham gia đến trung tâm phân phối khóa để bắt đầu quá trình nhận khóa bí mật dùng chung. Nếu tạo lại khóa cá nhân được sử dụng, như cần thiết để hỗ trợ an toàn về phía sau/về phía trước của nhóm, thì trung tâm phân phối khóa sẽ thực hiện quá trình tạo lại khóa sau khi yêu cầu tham gia được chấp nhận. Tuy nhiên, nếu sử dụng tạo lại khóa theo lô, hỗ trợ an toàn về phía sau/về phía trước với các khoảng thời gian, thì quá trình tạo lại khóa sẽ không được tự động thực hiện tại thời điểm này.

6.3 Quá trình rời đi

Một thực thể gửi yêu cầu rời nhóm đến trung tâm phân phối khóa để ngừng nhận khóa bí mật dùng chung. Nếu sử dụng tạo lại khóa cá nhân, thì trung tâm phân phối khóa sẽ thực hiện các quy trình tạo lại khóa sau khi thực thể đó rời nhóm. Tuy nhiên, nếu sử dụng tạo lại khóa theo lô, thì trung tâm phân phối khóa sẽ ghi lại các thực thể rời nhóm cho khoảng thời gian tạo lại khóa tiếp theo.

CHÚ THÍCH: Khi sử dụng tạo lại khóa theo lô, thực thể rời nhóm vẫn có thể giải mã các thông tin liên lạc được gửi trong nhóm cho đến khi quá trình tạo lại khóa theo lô tiếp theo diễn ra.

6.4 Quá trình tạo lại khóa

Qúa trình này bao gồm việc trung tâm phân phối khóa cập nhật khóa bí mật dùng chung với các thực thể trong một nhóm; nó cũng có thể bao gồm việc cập nhật các khóa mã hóa khóa. Nếu sử dụng tạo lại khóa cá nhân, thì quy trình này sẽ được thực hiện như một phần của các quy trình gia nhập và rời nhóm. Nếu sử dụng tạo lại khóa theo lô, thì quy trình này sẽ được thực hiện theo các khoảng thời gian đều đặn.

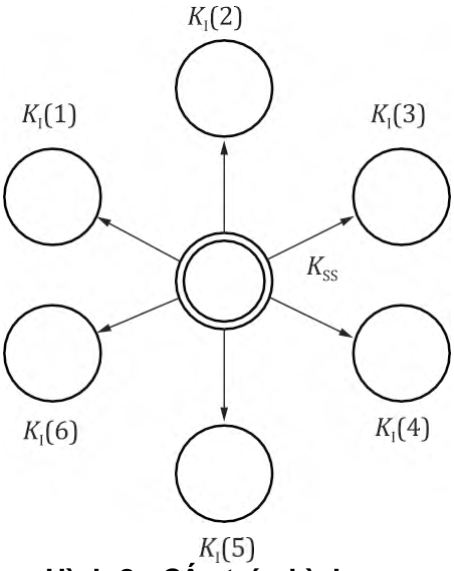
6.5 Cấu trúc khóa logic

6.5.1 Tổng quát

Các cơ chế thiết lập khóa có thể được phân loại theo cấu trúc logic được xác định bởi cách thức được sử dụng để phân phối khóa bí mật dùng chung từ trung tâm phân phối khóa đến các thực thể hoạt động trong nhóm. Ba cấu trúc khóa logic cụ thể được định nghĩa trong Điều 6.5.2 đến 6.5.4.

6.5.2 Cấu trúc hình sao

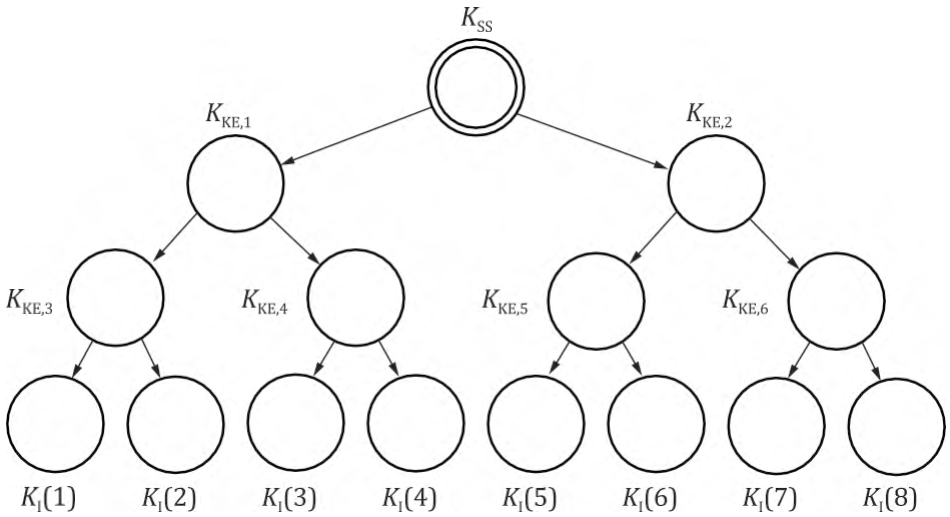
Trong cấu trúc hình sao, khóa bí mật dùng chung được mã hóa trực tiếp để phân phối bằng cách sử dụng các khóa cá nhân được gán cho các thực thể. Một ví dụ của cấu trúc hình sao với 6 khóa mã hóa khóa được chỉ ra trong Hình 2, trong đó vòng tròn kép ký hiệu trung tâm phân phối khóa.



Hình 2 - Cấu trúc hình sao

6.5.3 Cấu trúc hình cây *d*-ary

Trong cấu trúc dạng cây, số lượng khóa mã hóa khóa mà các thực thể nắm giữ có thể được giảm bớt. Hình 3 cho thấy cấu trúc cây nhị phân với *d* = 2. Một khóa bí mật chung được gán cho nút gốc của cây. Mỗi khóa cá nhân được gán cho các nút lá của cây. Ngoài ra, các khóa mã hóa khóa được gán cho các nút khác. Các khóa mã hóa khóa này được chia sẻ bởi nhiều thực thể có khóa cá nhân được gán cho các nút con cháu của nút mà khóa mã hóa khóa được gán. Chi phí liên lạc của quá trình rời đi có thể được giảm bằng cách sử dụng các khóa mã hóa khóa. Mỗi thực thể có tất cả các khóa được gán cho các nút trên đường đi từ nút gốc đến nút lá mà khóa cá nhân của thực thể đó được gán. Do đó, số lượng khóa mà một thực thể có tỷ lệ thuận với logarit của tổng số thực thể đang hoạt động.

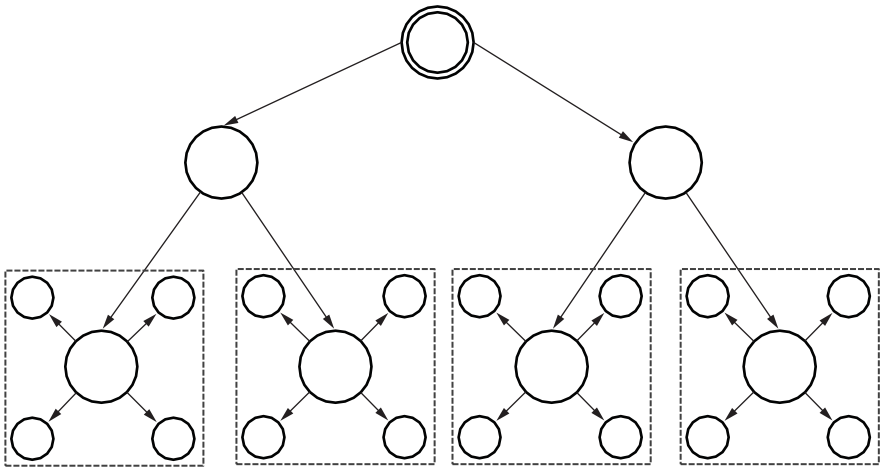


Hình 3 - Cấu trúc hình cây *d*-ary

6.5.4 Cấu trúc hình cây tổng quát

Cấu trúc hình cây tổng quát có thể được sử dụng làm cấu trúc khóa logic. Cấu trúc hình cây tổng quát này sử dụng một cấu trúc hình cây *d*-ary, trong đó *m* thực thể tạo thành một cụm. Cấu trúc này có thể được xem là sự kết hợp giữa cấu trúc hình sao với *m* điểm và cấu trúc hình cây *d*-ary. Cấu trúc này có thể được dùng để tối ưu hóa hiệu quả của các cơ chế thiết lập khóa (xem Phụ lục B). Hình 4 minh họa cấu trúc hình cây với *d* = 2 và *m* = 4. Cấu trúc hình cây tổng quát bao gồm một cấu trúc hình cây *d*-ary,

tuy nhiên, điều ngược lại thì không thể. Ví dụ, cấu trúc hình cây trong Hình 4 không phải là một cấu trúc hình cây *d*-ary.



Hình 4 - Cấu trúc hình cây tổng quát

6.6 Cơ chế thiết lập khóa dựa trên khóa đối xứng

6.6.1 Tổng quát

Tiêu chuẩn này định nghĩa hai cơ chế thiết lập khóa dựa trên mật mã khóa đối xứng cho nhiều thực thể, dựa trên cấu trúc hình cây tổng quát: 1) cơ chế tạo lại khóa cá nhân và 2) cơ chế tạo lại khóa theo lô. Trong cơ chế tạo lại khóa cá nhân, quá trình tạo lại khóa được thực hiện mỗi khi một thực thể tham gia hoặc rời đi.

6.6.2 Cơ chế 1 - Cơ chế thiết lập khóa bằng tạo lại khóa cá nhân

Cơ chế này dựa trên cấu trúc cây với tạo lại khóa cá nhân.

a) Quá trình tham gia

Giả định rằng có một tập hợp n thực thể đang hoạt động $\{u_1, u_2, ..., u_n\}$, và một thực thể mới u_{n+1} tham gia. Gọi $K_{A,l}(u_i)$ là khóa tổ tiên của thực thể u_i được gán cho lớp thứ l tính từ nút gốc của hệ thống phân cấp khóa logic. Gọi h là chiều cao của hệ thống phân cấp khóa logic.

1) Thực thể u_{n+1} gửi yêu cầu tham gia đến trung tâm phân phối khóa.
2) Trung tâm phân phối khóa gán khóa cá nhân u_{n+1} (tức là $K_l(u_{n+1})$) đến nút lá của hệ thống phân cấp khóa logic.
3) Trung tâm phân phối khóa tạo các số ngẫu nhiên và cập nhật khóa tổ tiên của khóa cá nhân của u_{n+1} bằng cách sử ụng các số này. K_{SS}, $K_{A,1}(u_{n+1})$, $K_{A,2}(u_{n+1})$, ..., $K_{A,h}(u_{n+1})$ được cập nhật thành K'_{SS}, $K'_{A,1}(u_{n+1})$, $K'_{A,2}(u_{n+1})$, ..., $K'_{A,h}(u_{n+1})$ tương ứng.
4) Trung tâm phân phối khóa mã hóa mỗi khóa được cập nhật bằng khóa cũ, và phát quảng bá nó. Tức là $e(K_{SS}, K'_{SS})$, $e(K_{A,1}(u_{n+1}), K'_{A,1}(u_{n+1}))$, $e(K_{A,2}(u_{n+1}), K'_{A,2}(u_{n+1}))$, ..., và $e(K_{A,h}(u_{n+1}), K'_{A,h}(u_{n+1}))$ được phát quảng bá.
5) Mỗi thực thể có được các khóa đã cập nhật bằng cách sử dụng các khóa cũ.
6) Trung tâm phân phối khóa mã hóa các khóa đã được cập nhật $K'_{SS}||\ K'_{A,1}(u_{n+1})||\ K'_{A,2}(u_{n+1})||...||\ K'_{A,h}(u_{n+1})$ bằng khóa cá nhân u_{n+1} và gửi $e(K_l(u_{n+1}),\ K'_{SS}||\ K'_{A,1}(u_{n+1})||\ K'_{A,2}(u_{n+1})||...||\ K'_{A,h}(u_{n+1}))$ đến u_{n+1}.

7) Thực thể u_{n+1} nhận được các khóa.

b) Quá trình rời đi

Giả định có n thực thể đang hoạt động $\{u_1, u_2, ..., u_n\}$, và thực thể u_j ($1 \le j \le n$) rời khỏi nhóm.

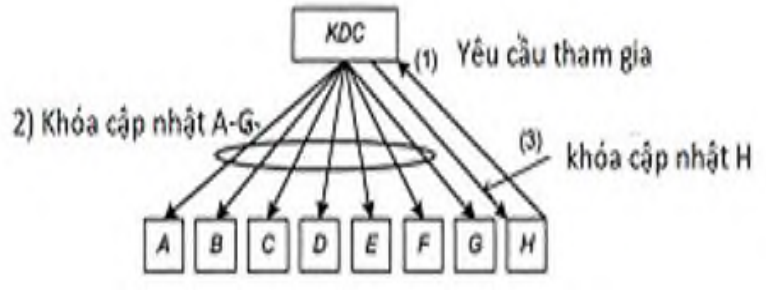
1) Trung tâm phân phối khóa tạo các số ngẫu nhiên và cập nhật các khóa tổ tiên của khóa cá nhân u_j bằng cách sử dụng các số này. K_{SS}, $K_{A,1}(u_j)$, $K_{A,2}(u_j)$, ..., $K_{A,h}(u_j)$ lần lượt được cập nhật thành K'_{SS}, $K'_{A,1}(u_j)$, $K'_{A,2}(u_j)$, ..., $K'_{A,h}(u_j)$ tương ứng.
2) Trung tâm phân phối khóa mã hóa từng khóa đã được cập nhật bằng các khóa con ngoại trừ khóa cá nhân của u_j và phát quảng bá chúng. Ví dụ K'_{SS} được mã hóa bằng các khóa con $K_{C,1}$, $K_{C,2}$, ..., $K_{C,d}$, và $e(K_{C,1}, K'_{SS})$, $e(K_{C,2}, K'_{SS})$, ...,và $e(K_{C,d}, K'_{SS})$ được quảng bá;

CHÚ THÍCH Trong trường hợp các khóa con được cập nhật, thì các khóa con đã được cập nhật được sử dụng.

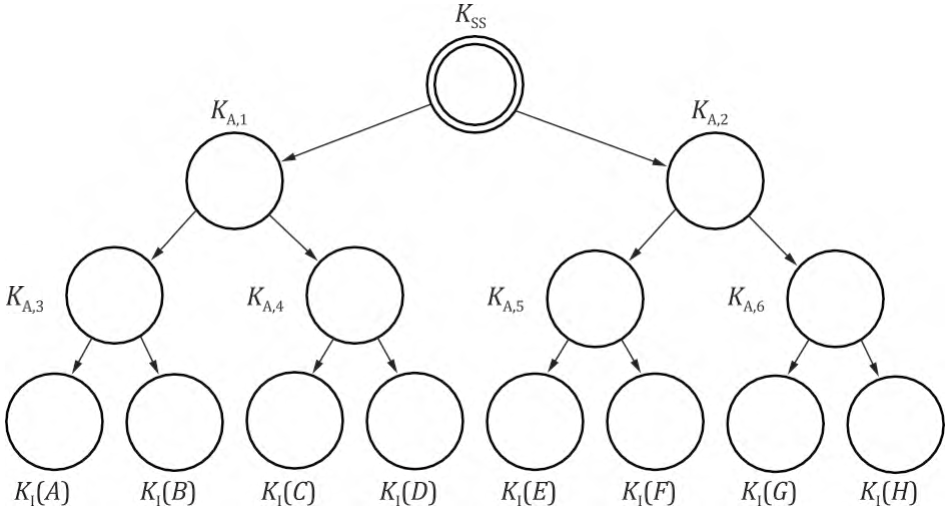
3) Mỗi thực thể nhận được các khóa được cập nhật bằng cách sử dụng các khóa con.

Ví dụ ứng dụng 1

Ví dụ này minh họa quá trình tham gia của Cơ chế 1 trong kịch bản được thể hiện ở Hình 5. Giả định rằng trung tâm phân phối khóa sử dụng hệ thống phân cấp khóa logic trong Hình 6 và thực thể H bắt đầu tham gia vào. Nhắc lại rằng, mỗi thực thể đang hoạt động có tất cả các khóa được gán cho các nút trên đường dẫn của hệ thống phân cấp khóa logic, từ nút lá tương ứng với khóa cá nhân của thực thể đó đến nút gốc. Ví dụ, thực thể A có các khóa $K_I(A)$, $K_{A,3}$, $K_{A,1}$, và K_{SS}.



Hình 5 - Quá trình tham gia của cơ chế 1 – cơ chế tạo lại khóa cá nhân



Hình 6 - Quy trình khóa logic

Các khóa được cập nhật *(UpdatedKey$_{A\text{-}G}$),* được phát quảng bá bởi trung tâm phân phối khóa đến *A, B, C, D, E, F*, và *G* là:

$$UpdatedKey_{A\text{-}G} = e(K_{SS}, K'_{SS})||e(K_{A,2}, K'_{A,2})||e(K_{A,6}, K'_{A,6})$$

Các khóa được cập nhật *(UpdatedKey$_H$),* được gửi bởi trung tâm phân phối khóa đến *H* là:

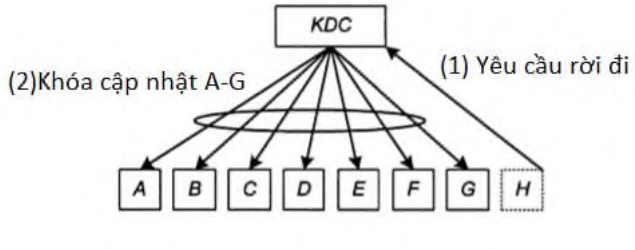
$$UpdatedKey_H = e(K_I(H), K'_{SS}||K'_{A,2}||K'_{A,6})$$

(1) *H* gửi yêu cầu tham gia đến trung tâm phân phối khóa.
(2) Trung tâm phân phối khóa tạo và phát quảng bá *UpdatedKey$_{A\text{-}G}$ đến A, B, C, D, E, F, và G.*
(3) Trung tâm phân phối khóa tạo và gửi *UpdatedKey$_{A\text{-}G}$ đến H.*

CHÚ THÍCH Trung tâm phân phối khóa và thực thể *H* đã chia sẻ khóa cá nhân của *H* trước đó.

Ví dụ ứng dụng 2

Ví dụ này minh họa quá trình rời đi của Cơ chế 1 trong kịch bản được thể hiện ở Hình 7. Giả định rằng trung tâm phân phối khóa sử dụng hệ thống phân cấp khóa logic trong Hình 6 và thực thể *H* muốn rời đi.



Hình 7 - Quá trình rời đi của cơ chế 1 – cơ chế với tạo lại khóa cá nhân

Dạng của các khóa cập nhật *(UpdatedKey$_{A\text{-}G}$)* được phát quảng bá bởi trung tâm phân phối khóa đến *A, B, C, D, E, F, và G* là:

$$UpdatedKey_{A\text{-}G} = e(K_{A,1},K'_{SS})||e(K'_{A,2},K'_{SS})||e(K_{A,5},K'_{A,2})||e(K'_{A,6},K'_{A,2})||e(K_I(G),K'_{A,6})$$

(1) *H* gửi yêu cầu rời đi đến trung tâm phân phối khóa.
(2) Trung tâm phân phối khóa tạo và phát quảng bá *UpdatedKey$_{A\text{-}G}$* đến *A, B, C, D, E, F, và G.*

6.6.3 Cơ chế 2 – Cơ chế thiết lập khóa bằng tạo lại khóa theo lô

Trong cơ chế tạo lại khóa theo lô với khoảng *T*, quá trình tạo lại khóa được thực hiện định kỳ sau mỗi khoảng thời gian *T*.

a) Quá trình tham gia

Giả định rằng có *n* thực thể đang hoạt động {u_1, u_2, ..., u_n}, và thực thể u_{n+1} tham gia vào nhóm.

1) Thực thể u_{n+1} gửi yêu cầu tham gia đến trung tâm phân phối khóa.

2) Trung tâm phân phối khóa gán khóa cá nhân của u_{n+1} (tức là $K_I(u_{n+1})$) cho nút lá của hệ thống phân cấp khóa logic.
3) Trung tâm phân phối khóa mã hóa các khóa tổ tiên của khóa cá nhân của u_{n+1} bằng chính khóa cá nhân của u_{n+1}. Sau đó, trung tâm phân phối khóa gửi $e(K_I(u_{n+1}), K_{SS}||K_{A,1}(u_{n+1})||K_{A,2}(u_{n+1})|| \ ... \ ||K_{A,h}(u_{n+1}))$ đến u_{n+1}.
4) Thực thể u_{n+1} nhận được K_{SS} và $K_{A,1}(u_{n+1})$, $K_{A,2}(u_{n+1})$, …, $K_{A,h}(u_{n+1})$.

b) Quá trình rời đi

Thực thể rời đi gửi yêu cầu rời đi đến trung tâm phân phối khóa.

CHÚ THÍCH Việc tạo lại khóa không được thực hiện trong quá trình rời đi của cơ chế tạo lại khóa theo lô.

c) Quá trình tạo lại khóa

Quá trình này được thực hiện theo một khoảng thời gian đều đặn T. Giả định có một tập hợp n thực thể đang hoạt động $\{u_1, u_2, \ldots u_n\}$ và các thực thể của tập hợp $\{u_{i,1}, u_{i,2}, \ldots, u_{i,k}\}$ rời đi trong một khoảng thời gian tạo lại khóa. k là số lượng các thực thể rời đi trong khoảng thời gian tạo lại khóa i.

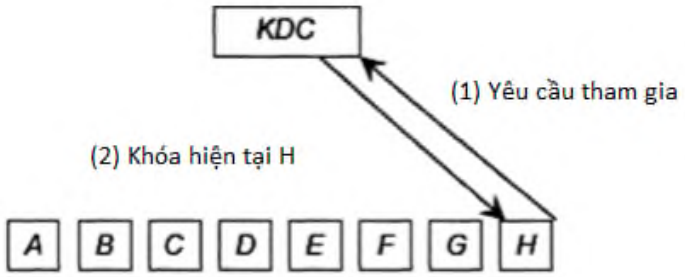
1) Trung tâm phân phối khóa tạo ra các số ngẫu nhiên và cập nhật các khóa tổ tiên của các khóa cá nhân $u_{i,1}$, $u_{i,2}$, ..., $u_{i,k}$ sử dụng các số ngẫu nhiên. K_{SS}, $K_{A,1}(u_{i,1})$, $K_{A,1}(u_{i,2})$, …, $K_{A,1}(u_{i,k})$, $K_{A,2}(u_{i,1})$, $K_{A,2}(u_{i,2})$, …, $K_{A,2}(u_{i,k})$, …, $K_{A,h}(u_{i,1})$, $K_{A,h}(u_{i,2})$, …, $K_{A,h}(u_{i,k})$ được cập nhật theo thứ tự tương ứng thành K'_{SS}, $K'_{A,1}(u_{i,1})$, $K'_{A,1}(u_{i,2})$, …, $K'_{A,1}(u_{i,k})$, $K'_{A,2}(u_{i,1})$, $K'_{A,2}(u_{i,2})$, …, $K'_{A,2}(u_{i,k})$, …, $K'_{A,h}(u_{i,1})$, $K'_h(u_{i,2})$, …,$K'_{A,h}(u_{i,k})$.
2) Trung tâm phân phối khóa mã hóa từng khóa đã được cập nhật bằng tất cả các khóa con của nó trừ các khóa cá nhân của $u_{i,1}$, $u_{i,2}$, …, $u_{i,k}$ và phát quảng bá chúng. Ví dụ K'_{SS} được mã hóa với các khóa con $K_{C,1}$, $K_{C,2}$, ..., $K_{C,d}$ *và* $e(K_{C,1}, K'_{SS})$, $e(K_{C,2}, K'_{SS})$, ...,*và* $e(K_{C,d}, K'_{SS})$ được quảng bá.

CHÚ THÍCH 2 Trong trường hợp mà các khóa con được cập nhật, thì các khóa con đã được cập nhật được sử dụng.

3) Mỗi thực thể nhận được các khóa được cập nhật bằng cách sử dụng các khóa con.

Ví dụ ứng dụng 3

Ví dụ này minh họa quá trình tham gia của Cơ chế 2 trong kịch bản được thể hiện ở Hình 8. Giả định rằng trung tâm phân phối khóa sử dụng hệ thống phân cấp khóa logic trong Hình 6 và thực thể H tham gia vào. Nhắc lại rằng mỗi thực thể có tất cả các khóa được gán cho các nút trên đường dẫn của hệ thống phân cấp khóa logic, từ nút lá tương ứng với khóa cá nhân của thực thể đó đến nút gốc. Ví dụ, thực thể A có $K_I(A)$, $K_{A,3}$, $K_{A,1}$, và K_{SS}.



Hình 8 - Quá trình tham gia của cơ chế 2 – cơ chế Tạo lại khóa theo lô

Dạng của các khóa cập nhật $CurrentKey_H$ được gửi bởi trung tâm phân phối khóa đến *H* như sau:

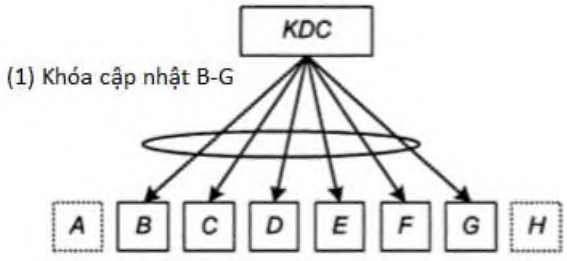
$$CurrentKey_H = e(K_I(H), K_{SS}||K_{A,2}||K_{A,6})$$

(1) *H* gửi yêu cầu tham gia đến trung tâm phân phối khóa.

(2) Trung tâm phân phối khóa tạo và gửi $CurrentKey_H$ đến *H.*

Ví dụ ứng dụng 4

Ví dụ này minh họa quá trình rời đi của Cơ chế 2 trong kịch bản được thể hiện ở Hình 9. Giả định rằng trung tâm phân phối khóa sử dụng hệ thống phân cấp khóa logic trong Hình 6 và các thực thể *A* và *H* phải rời đi.



Hình 9 – Quá trình Tạo lại khóa của cơ chế 2 – cơ chế với tạo lại khóa theo lô

Các khóa cập nhật ($UpdatedKey_{B\text{-}G}$) được phát quảng bá bởi trung tâm phân phối khóa đến *B, C, D, E, F* và *G* như sau:

$$UpdatedKey_{B\text{-}G} = e(K'_{A,1},K'_{SS})||e(K'_{A,2},K'_{SS})||e(K'_{A,3},K'_{A,1})||e(K_{A,4},K'_{A,1})||$$

$$e(K_{A,5},K'_{A,2})||e(K'_{A,6},K'_{A,2})||e(K_I(B),K'_{A,3})||e(K_I(G),K'_{A,6})$$

Trung tâm phân phối khóa tạo và phát quảng bá $UpdatedKey_{B\text{-}G}$ *đến B, C, D, E, F, và G.*

7 Quản lý khóa nhóm dựa trên chuỗi khóa với chuỗi khóa về phía trước bị giới hạn

7.1 Mô hình tổng quát

Để giới hạn thời gian hiệu lực của các khóa trong phạm vi (trong giới hạn) số hội viên nhóm tĩnh, các chuỗi khóa rất hữu ích. Chuỗi khóa có thể giới hạn quyền truy cập vào thông tin đã được mã hóa trong các phiên làm việc tương lai, các phiên làm việc trong quá khứ, hoặc cả hai. Trong một chuỗi khóa, các khóa riêng lẻ/cá nhân phụ thuộc vào nhau. Sử dụng một giá trị khởi tạo, khóa đầu tiên sẽ được tính toán. Khóa thứ hai được tính toán dựa trên khóa thứ nhất, khóa thứ ba dựa trên khóa thứ hai, và cứ thế tiếp tục. Nếu thực thể phi tập trung có khả năng thực hiện phép tính này, nó sẽ cho phép việc tạo khóa phi tập trung một cách hiệu quả. Độ dài của chuỗi khóa được giới hạn bởi một số lượng khóa được xác định trước. Bất kỳ một khóa cụ thể nào trong chuỗi khóa, cùng với khoảng thời gian mà nó có hiệu lực, sẽ xác định khoảng thời gian mà thông tin được mã hóa có thể được giải mã bằng chính khóa đó.

Trong tiêu chuẩn này, hai loại chuỗi khóa được xem xét. Chuỗi khóa về phía trước giới hạn quyền truy cập vào thông tin đã mã hóa trong quá khứ (tức là an toàn phía trước của nhóm), trong khi chuỗi khóa về phía sau giới hạn quyền truy cập vào thông tin đã mã hóa trong tương lai (tức là an toàn phía sau của nhóm). Bởi vì số lượng khóa trong một chuỗi khóa phía trước và phía sau là hữu hạn, số lượng khóa trong các chuỗi này phải được lựa chọn cẩn thận khi triển khai hệ thống.

Việc tính toán các khóa trong chuỗi dựa trên các hàm một chiều. Các hàm một chiều chỉ cho phép tính toán theo một hướng duy nhất. Điều này có nghĩa là, bắt đầu từ kết quả của một hàm một chiều, không thể tính toán ngược lại để tìm ra giá trị khởi đầu. Hàm dẫn xuất khóa từ TCVN 7817-6 (ISO/IEC 11770-6) sẽ được chọn cho hàm một chiều này.

Các biện pháp đặc biệt sẽ được thực hiện để ngăn chặn các cuộc tấn công thông đồng, trong đó một hoặc nhiều người tham gia cố ý cung cấp thông tin cho kẻ tấn công. Nếu một thực thể có quyền truy cập vào một phần của chuỗi khóa, và một thực thể khác có quyền truy cập vào một phần khác của cùng chuỗi khóa đó, họ có thể tái tạo lại chuỗi khóa từ điểm khởi đầu thấp nhất của cả hai phần cho đến điểm kết thúc cao nhất của cả hai phần.

Các khóa của một chuỗi khóa sẽ phải được xử lý như các khóa bí mật, và việc chuyển tiếp chúng tới các thực thể khác cần phải được ngăn cấm.

7.2 Tính toán của trung tâm phân phối khóa

7.2.1 Các chuỗi khóa

Thực thể phân phối khóa cần thiết lập các chuỗi khóa trước khi hoạt động bình thường. Điều này có nghĩa là, tùy thuộc vào nhu cầu, chuỗi khóa về phía trước và/hoặc chuỗi khóa về phía sau sẽ phải được xác định. Khi đó, kết quả cho chuỗi khóa về phía trước là:

$$K_{FW} = \{K_{FW,0}, K_{FW,1}, \ldots, K_{FW,n-1}, K_{FW,n}\}$$

Và cho chuỗi khóa về phía sau:

$$K_{BW} = \{K_{BW,0}, K_{BW,1}, \ldots, K_{BW,T-1}, K_{BW,T}, \ldots\}$$

Cả hai chuỗi khóa đều được tính toán bằng cách sử dụng các hàm một chiều.

Trong trường hợp này, các giá trị khởi đầu là $K_{FW,n}$ và $K_{BW,0}$. Chỉ số n của giá trị khởi tạo $K_{FW,n}$ phải được chọn một cách thích hợp dựa trên các khía cạnh ứng dụng và triển khai, vì nó đánh dấu điểm kết thúc của chuỗi khóa về phía trước.

7.2.2 An toàn về phía trước của nhóm

Trung tâm phân phối khóa xây dựng chuỗi khóa về phía trước bằng cách sử dụng giá trị khởi đầu đã cho $K_{FW,n}$. Bất kỳ khóa nào có trong chuỗi giới hạn đều có thể được tính toán bằng cách:

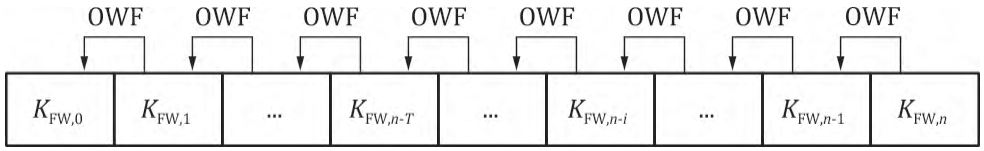
$$K_{FW,n-i-1} = OWF(K_{FW,n-i}),\ i = 0,1,2,\ldots,n\text{-}1$$

trong đó OWF là một hàm một chiều. Mối quan hệ tương tác có thể được biểu thị như sau:

$$K_{FW,n-T} = OWF^{T}\left(K_{FW,n}\right) := \underbrace{OWF\left(OWF\left(\ldots OWF\left(K_{FW,n}\right)\right)\right)}_{T \text{ times}},\ T = 1,2,3,\ldots,n$$

Hình 10 cũng trình bày việc tính toán chuỗi khóa phía trước $K_{FW,n}$ … $K_{FW,0}$.

Chuỗi này đạt được tính an toàn về phía trước với khoảng T, vì việc biết khóa $K_{FW,T}$ không cho phép tính toán bất kỳ khóa $K_{FW,t}$ nào với $t>T$.



Hình 10 - Xây dựng chuỗi khóa phía trước bằng cách sử dụng hàm một chiều

Ví dụ ứng dụng 5

Trong ví dụ này, việc xây dựng chuỗi khóa về phía trước của trung tâm phân phối khóa sử dụng hàm OKDF1 từ TCVN 7817-6 (ISO/IEC 11770-6) làm hàm một chiều và thực hiện các bước sau.

1) Trung tâm phân phối khóa tạo ra một số ngẫu nhiên an toàn làm giá trị khởi đầu $r_{FW,init}$.
2) Trung tâm phân phối khóa sử dụng hàm OKDF1 để băm giá trị khởi đầu ngẫu nhiên thành một kích thước cố định có độ dài phù hợp. Đầu ra được dùng làm khóa đầu tiên, $K_{FW,n}$. Tức là, $K_{FW,n}$ $K_{FW,n}$ = OKDF1($r_{FW,init}$) được tính toán.
3) Phần tử tiếp theo của chuỗi được xây dựng bằng cách sử dụng $K_{FW,n}$ làm đầu vào cho OKDF1 và sử dụng đầu ra của hàm là $K_{FW,n-1}$: $K_{FW,n-1}$ = OKDF1($K_{FW,n}$).
4) Các khóa mới của chuỗi được tạo ra bằng phương pháp dẫn xuất khóa đã được phê duyệt. Đầu vào luôn là khóa cuối cùng hiện tại của chuỗi, $K_{FW,n-i+1}$, và đầu ra là $K_{FW,n-i}$: $K_{FW,n-i}$ = OKDF1($K_{FW,n-i+1}$).
5) Việc tính toán kết thúc ngay khi trung tâm phân phối khóa tuyên bố một giá trị cuối cùng $K_{FW,0.}$

7.2.3 An toàn về phía sau của nhóm

An toàn về phía sau của nhóm có thể được thực hiện bằng cách xác định chuỗi khóa phía sau. Bất kỳ khóa nào có trong chuỗi đều có thể được tính toán như sau:

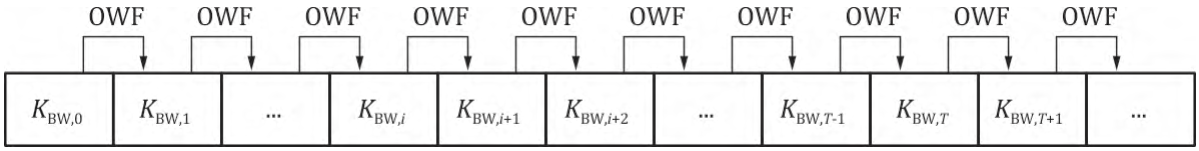
$$K_{BW,i+1} = OWF(K_{BW,i}),\ i = 0,1,2,\ldots$$

Trong đó OWF là một hàm một chiều. Mối quan hệ tương quan có thể được biểu thị như sau:

$$K_{BW,T} = \mathrm{OWF}^{T}\left(K_{BW,0}\right) := \underbrace{\mathrm{OWF}\left(\mathrm{OWF}\left(\ldots \mathrm{OWF}\left(K_{BW,0}\right)\right)\right)}_{T \text{ times}}, T = 1,2,3,\ldots$$

Trung tâm phân phối khóa có khả năng tính toán liên tục chuỗi khóa phía sau $K_{BW,0}$ … $K_{BW,T}$ … như được trình bày trong Hình 11.

Chuỗi này đạt được tính an toàn về phía sau với khoảng T, vì nó không cho phép truy cập vào thông tin đã mã hóa tại thời điểm $t<T$ trong trường hợp thực thể người dùng biết khóa $K_{BW,T}$. Bất kỳ chuỗi khóa nào $K_{BW,i}$ … $K_{BW,T}$,… đều đưa ra hạn chế cho bất kỳ thời gian nào $t < t_i$.



Hình 11 - Xây dựng chuỗi khóa phía sau bằng việc sử dụng hàm một chiều

Ví dụ ứng dụng 6

Trong ví dụ này, việc xây dựng chuỗi khóa phía sau của trung tâm phân phối khóa sử dụng hàm dẫn xuất khóa OKDF1 từ TCVN 7817-6 (ISO/IEC 11770-6) làm hàm một chiều và thực hiện các bước sau.

1) Trung tâm phân phối khóa tạo ra một số ngẫu nhiên an toàn có tên là $r_{BW,init}$ làm giá trị khởi tạo.
2) Trung tâm phân phối khóa sử dụng hàm băm OKDF1 để băm giá trị khởi tạo ngẫu nhiên thành một kích thước cố định theo yêu cầu. Đầu ra của hàm băm này được sử dụng làm khóa đầu tiên, $K_{BW,0}$. Nói cách khác, khóa đầu tiên $K_{BW,0}$ được tính toán bằng công thức: $K_{BW,0}$ = OKDF1($r_{BW,init}$).
3) Phần tử tiếp theo của chuỗi được xây dựng bằng cách sử dụng $K_{BW,0}$ làm đầu vào cho OKDF1, và đầu ra của hàm này được dùng làm $K_{BW,1}$: $K_{BW,1}$ = OKDF1($K_{BW,0}$).
4) Các khóa mới trong chuỗi được tạo ra bằng cách sử dụng hàm OKDF1. Ứng với mỗi lần lặp, đầu vào luôn là khóa cuối cùng hiện tại của chuỗi, được ký hiệu là $K_{BW,i}$, và đầu ra là khóa tiếp theo $K_{BW,i+1}$: $K_{BW,i+1}$ = OKDF1($K_{BW,i}$).

7.2.4 An toàn về phía trước và về phía sau

Để kết hợp giữa an toàn về phía trước và về phía sau, các chuỗi khóa riêng lẻ được kết nối với nhau để cho phép truy cập có giới hạn theo cả hai hướng. Việc này được thực hiện bằng một hàm khác tên là COM, dùng để kết hợp các khóa riêng lẻ $K_{FW,i}$ và $K_{BW,i}$. Hàm COM có thể phụ thuộc vào một khóa K được chia sẻ giữa trung tâm phân phối khóa và các thực thể người dùng. Kết quả kết hợp này tạo ra khóa

$$K_i = \mathrm{COM}(K_{FW,i}, K_{BW,i}),\ i = 1,2,\ldots$$

Điều này sẽ được kiểm tra xem bất kỳ khóa nào được tạo ra K_i có đáp ứng các yêu cầu bảo mật của thuật toán mã hóa, vốn sẽ sử dụng K_i làm khóa bí mật hay không. Mặc dù rất khó để tạo ra các khóa yếu, nhưng cần phải có các biện pháp đối phó, và rất có thể việc tạo lại khóa sẽ là cần thiết trong trường hợp như vậy.

Ví dụ ứng dụng 7

Ví dụ về hàm COM(*X, Y*) để tạo khóa mã hóa K_i có độ dài *k*, trong trường hợp khóa này không phụ thuộc vào khóa chung *K*:

$$COM(K_{FW,i}, K_{BW,i}) = CUT(k, OKDF1(K_{FW,i} || K_{BW,i}))$$

Ví dụ này sử dụng hàm dẫn xuất khóa OKDF1 từ TCVN 7817-6 (ISO/IEC 11770-6) và thực hiện các bước sau:

1) $K_{FW,i}$ và $K_{BW,i}$ được nối lại với nhau.

2) Giá trị của ($K_{FW,i}$ || $K_{BW,i}$) được dùng làm đầu vào cho hàm OKDF1.

3) Một chuỗi con gồm *k* bit có trọng số thấp nhất từ đầu ra của hàm OKDF1 được chọn.

4) Kết quả được sử dụng làm khóa K_i để giải mã dữ liệu đã được mã hóa.

Một ví dụ thay thế về hàm COM(*X, Y*) trong trường hợp khóa K_i có phụ thuộc vào khóa *K*:

$$COM(K_{FW,i}, K_{BW,i}) = CUT(k, OKDF6(K_{FW,i} || K_{BW,i}, K))$$

Ví dụ này sử dụng hàm dẫn xuất khóa OKDF1 từ TCVN 7817-6 (ISO/IEC 11770-6) và thực hiện các bước sau:

1) $K_{FW,i}$ và $K_{BW,i}$ được nối lại với nhau để tạo ra chuỗi $s = (K_{FW,i} || K_{BW,i})$.

2) Giá trị *s* được sử dụng làm thông tin bí mật, và $t' = K$ được sử dụng làm giá trị ngẫu nhiên cho đầu vào của hàm OKDF6.

3) Một chuỗi con gồm *k* bit có trọng số thấp nhất từ đầu ra của hàm OKDF6(*s*, *t'*) được chọn.

4) Kết quả được sử dụng làm khóa K_i để giải mã dữ liệu đã được mã hóa.

7.3 Tính toán bởi thực thể client

Để truy cập thông tin được mã hóa, bên nhận phải có cùng các khóa với trung tâm phân phối khóa (KDC) trong suốt thời gian đó. Việc truyền toàn bộ chuỗi khóa từ KDC đến bên nhận là không hiệu quả. Do đó, bên nhận được phép tính các chuỗi khóa. Để duy trì sự giới hạn truy cập, bên nhận sẽ không được giữ các giá trị khởi tạo của các chuỗi khóa.

Nhìn chung, bên nhận được cung cấp các giá trị $K_{FW,i+k}$ ($i+k \leq n$) cho chuỗi khóa về phía trước và $K_{BW,i}$ cho chuỗi khóa về phía sau. Với các khóa này, việc truy cập vào các dữ liệu có thời gian $t < t_i$ hoặc $t > t_{i+k}$ là không thể.

Bên nhận cũng được cung cấp các hàm cần thiết để tính toán chuỗi khóa. Chuỗi phía trước và chuỗi phía sau không nhất thiết phải sử dụng cùng một hàm một chiều OWF.

Việc tính toán chuỗi khóa về phía trước, chuỗi khóa về phía sau và chuỗi khóa kết hợp được thực hiện theo cùng một cách đã được mô tả trong 7.2.2 đến 7.2.4.

PHỤ LỤC A
(Quy định)
Định danh đối tượng

```
KeyManagementGroupKeyManagement {
iso(1) standard(0) key-management(11770) part5(5) asn1-
module(0) key-management-mechanisms(0) }

DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --
-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias

-- Synonyms --

is11770-5 OID ::= { iso(1) standard(0) key-management(11770) part5(5) }
mechanism OID ::= { is11770-5 mechanisms(1) }

-- Symmetric Key-based Key Establishment Mechanisms --

ke-mechanism-ind-re    OID    ::=    {
mechanism 1 } ke-mechanism-bat-re OID
::= { mechanism 2 }

-- Key Chain-based Group Key Management --

ke-chain-with-limited-for-key-chains OID ::= { mechanism 4 }

-- Key Chains with Tree-based Key Distribution --

ke-chain-with-tree-based-key-dist OID ::= { mechanism

5 } END -- KeyManagementGroupKeyManagement --
```

PHỤ LỤC B
(Tham khảo)
Cơ chế cân bằng tải cho cấu trúc cây tổng quát

Phụ lục này mô tả ảnh hưởng của việc sử dụng cơ chế cân bằng tải đối với cấu trúc cây tổng quát, như đã được định nghĩa trong Điều 6. Tổng chi phí liên lạc hoặc tổng chi phí tính toán được áp đặt lên một trung tâm phân phối khóa (KDC) và các thực thể có thể được cân bằng bằng cách thay đổi cấu trúc của hệ thống phân cấp khóa logic. Tổng chi phí liên lạc được xác định bởi số lượng khóa cần được cập nhật. Ngoài ra, tổng chi phí tính toán được áp đặt lên một KDC và các thực thể được xác định lần lượt bởi tổng số quy trình mã hóa và giải mã. Chúng được định nghĩa bằng các tham số *d* và *m*. Chi phí liên lạc và tính toán cho hai ví dụ về bộ tham số được cho trong Bảng B.1 và Bảng B.2.

Nói chung, có sự đánh đổi giữa chi phí liên lạc tối đa và chi phí tính toán tối đa. Trong cấu trúc cây *d*-ary, sự đánh đổi này được kiểm soát bởi bậc *d* của cây. Chi phí liên lạc cao nhất và chi phí tính toán cao nhất áp đặt lên các thực thể sẽ tăng, trong khi chi phí tính toán cao nhất áp đặt lên trung tâm phân phối khóa (KDC) sẽ giảm khi tham số *d* giảm. Chi phí liên lạc/tính toán tối đa có nghĩa là tổng chi phí liên lạc/tính toán cao hơn trong quá trình tham gia và quá trình rời đi. Cấu trúc hình cây tổng quát cho phép cân bằng tải chi tiết bằng cách thay đổi hai tham số: bậc *d* của hệ thống phân cấp khóa logic và số lượng thực thể trong một cụm *m*.

Bảng B.1 - Chi phí liên lạc và tính toán tổng thể khi người dùng thứ 64 tham gia hoặc rời khỏi một cây với 63 người dùng và bậc cây *d*=2.

	Tổng chi phí liên lạc	**Tổng chi phí tính toán tác động lên trung tâm phân phối khóa**	**Tổng chi phí tính toán tác động lên thực thể**
Quá trình tham gia	6	7	121
Quá trình rời đi	6	11	120

Bảng B.2 – Tổng chi phí liên lạc và tính toán khi người dùng thứ 64 tham gia hoặc rời khỏi một cây với 64 người dùng và bậc cây *d*=4.

	Tổng chi phí liên lạc	**Tổng chi phí tính toán tác động lên trung tâm phân phối khóa**	**Tổng chi phí tính toán tác động lên thực thể**
Quá trình tham gia	3	4	82
Quá trình rời đi	3	11	81

Thư mục tài liệu tham khảo

[1] TCVN 11495-1 (ISO/IEC 9797-1) Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC) - Phần 1: Cơ chế sử dụng mã khối.

[2] TCVN 11495-2 (ISO/IEC 9797-2) Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC) - Phần 2: Cơ chế sử dụng hàm băm chuyên dụng.

[3] TCVN 11816-3 (ISO/IEC 10118-3) Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng.

[4] TCVN 7817-1 (ISO/IEC 11770-1) Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khoá - Phần 1: Khung tổng quát.

[5] TCVN 7817-3 (ISO/IEC 11770-3) Công nghệ thông tin - Kỹ thuật mật mã quản lý khoá - Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng.

[6] TCVN 12853:2020 (ISO/IEC 18031:2011) Công nghệ thông tin - Các kỹ thuật an toàn - Bộ tạo bit ngẫu nhiên

[7] TCVN 11295 (ISO 19790) Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã.