TCVN TIÊU CHUẨN QUỐC GIA

DỰ THẢO

TCVN XXXX:2024

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN - THUẬT TOÁN MẬT MÃ – MÃ KHỐI MKV

Information technology – Security techniques – Encryption algorithms – Block cipher MKV

HÀ NỘI - 2024

Mục lục

Lời nói đầu

Tiêu chuẩn TCVN XXXX MÃ KHỐI MKV do Ban cơ yếu Chính phủ xây dựng, đề nghị, Tổng cục Tiêu chuẩn Đo lường chất lượng thẩm định, Bộ Khoa học – Công nghệ công bố.

Nội dung của tiêu chuẩn này được xây dựng dựa trên việc thừa kế nội dung nghiên cứu của nhiệm vụ Khoa học – Công nghệ cấp Ban Cơ yếu Chính phủ, "Nghiên cứu xây dựng chuẩn mã khối sử dụng trong lĩnh vực dân sự" do TS. Nguyễn Bùi Cương, Viện Khoa học - Công nghệ mật mã, Ban Cơ yếu Chính phủ chủ nhiệm.

Lời giới thiệu

Mã khối có thể coi là "cốt lõi của cốt lõi", là trái tim của các sản phẩm bảo mật, an toàn thông tin, muốn làm chủ được công nghệ thiết kế các sản phẩm này phải làm chủ được thuật toán mật mã. Hiện nay, hầu hết các sản phẩm thương mại đều sử dụng chuẩn mã hoá tiên tiến (thuật toán mã hóa AES). Trên thế giới, không phải quốc gia nào cũng có chuẩn mã hoá của riêng mình, chỉ có một số ít các nước đã nghiên cứu ban hành chuẩn mã hoá cho lĩnh vực dân sự như Mỹ, Liên bang Nga, Trung Quốc, Hàn Quốc, Nhật Bản, Belarus, ...

Một số chuẩn mã hoá tiêu biểu của một số quốc gia trên thế giới			
STT	**Quốc Gia**	**Tên thuật toán**	**Tiêu chuẩn**
1.	Mỹ	AES	FIPS 197 ISO/IEC 18033-3:2010; RFC 3826
2.	Nga	Kuznyechik	GOST R 34.12-2015; RFC 7801
		Magma	GOST R 34.12-2015; RFC 8891
3.	Trung Quốc	SM4 (hoặc SMS4)	GB/T 32907-2016 ISO/IEC 18033-3:2010/Amd 1:2021 IEEE 802.11i
4.	Hàn Quốc	SEED	TTAS.KO-12.0004 ISO/IEC 18033-3:2010; RFC 4269
		LEA	KS X 3246; ISO/IEC 29192-2:2019
5.	Nhật Bản	CLEFIA	KS X 1213:2004, RFC 5794
		CAMELLIA	TTAS.KO-12.0040
6.	Belarus	Bel-T	СТБ 34.101.31-2011

Một nhà mật mã học nổi tiếng người Nga đã nói "*Một quốc gia được coi là vĩ đại nếu quốc gia đó sở hữu vũ khí hạt nhân, làm chủ không gian và có chuẩn mật mã của riêng mình*". Do vậy, việc sở hữu riêng chuẩn mật mã là một trong những yếu tố khẳng định tính tự chủ của Việt Nam trong công cuộc bảo vệ chủ quyền Quốc gia.

Một trong những mục tiêu của Chiến lược "Make in Vietnam" do Thủ tướng Chính phủ ban hành là phát triển kinh tế số chiếm 20% GDP, với việc xác định các bước tiến đột phá mang tính hệ thống, nhấn mạnh vào chuyển đổi chủ quyền công nghệ, có sự chuyển dịch mạnh mẽ từ lắp ráp, gia công sang sáng tạo, thiết kế một cách chủ động, tạo ra các sản phẩm công nghệ "Make in Vietnam". Trước bối cảnh lịch sử của sự chuyển mình trong xu thế phát triển của nền kinh tế số, bên cạnh việc thực hiện các nhiệm vụ chính trị quan trọng được Đảng và Nhà nước giao, với vai trò là Cơ quan mật mã quốc gia, Ban Cơ yếu Chính phủ đã chỉ đạo tổ chức nghiên cứu, xây dựng thuật toán mã khối để thiết kế, chế tạo các sản phẩm bảo mật, an toàn thông tin trong lĩnh vực dân sự phục vụ phát triển kinh tế số, xã hội số.

Ở một khía cạnh khác, khi mà bài toán bảo mật thông tin có sức nóng hơn bao giờ hết trước sự phát triển không ngừng của công nghệ lượng tử và các vấn đề đảm bảo an toàn thông tin trước những tấn công thám mã dựa trên tính toán lượng tử. Ban Cơ yếu Chính phủ đặt mục tiêu quan trọng là phải có một thuật toán mã hoá "Make in Vietnam", không chỉ an toàn lượng tử mà còn đảm bảo hiệu năng cần

thiết để đáp ứng nhu sử dụng trong thời đại số. Ngoài đảm bảo an toàn và hiệu quả sử dụng, mã khối phải có đặc trưng riêng, có cấu trúc riêng so với các chuẩn khác trên thế giới.

Đối với phạm vi dân sự trong nước, theo luật an toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015, trong chương 4 quy định về tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng, tại mục số 7 điều 38 về Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng có nội dung "Ban Cơ yếu Chính phủ với vai trò cơ quan mật mã quốc gia, có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự". Hiện nay, trong lĩnh vực dân sự, Ban Cơ yếu Chính phủ đã xây dựng và đề xuất Bộ Khoa học và Công nghệ công bố được 55 tiêu chuẩn quốc gia trong lĩnh vực mật mã. Các chuẩn được chấp thuận nguyên vẹn theo các chuẩn của ISO/IEC bởi vì Việt Nam là thành viên của tổ chức ISO/IEC. Tuy nhiên, để tạo sự thống nhất, thông suốt trong vấn đề bảo mật thông tin trong các hệ thống khác nhau, và khẳng định tính tự chủ về mật mã, việc xây dựng chuẩn riêng khẳng định tư tưởng và xu thế "Make in Vietnam" càng thật sự cần thiết. Với mục tiêu này, Ban Cơ yếu Chính phủ đã tiến hành xây dựng một mã khối với nhiều phiên bản về kích cỡ khối và độ dài khóa, có tên gọi là ViEncrypt trong quá trình phát triển xây dựng, sau đó được đổi tên thành MKV để tạo sự thống nhất về kí hiệu cho các tiêu chuẩn mật mã được xây dựng sau này dùng bảo vệ thông tin trong lĩnh vực dân sự. Trong đó có hai phiên bản kích cỡ khối, kích cỡ khối 256-bit với mong muốn đảm bảo độ an toàn cho hậu lượng tử còn 128-bit cho giai đoạn chuyển tiếp. Mỗi phiên bản mã khối đều có ba tùy chọn độ dài khóa với mức an toàn linh hoạt phù hợp cho các nhà làm ứng dụng. Mã khối MKV đã đạt được một số đặc điểm trong thiết kế như sau:

Về cấu trúc: MKV sử dụng cấu trúc dạng SPN dựa trên lược đồ FLC đạt được độ an toàn chứng minh được trong mô hình Luby-Rackoff, được xây dựng trong [2]. Bên cạnh đó, mã khối này có cấu trúc FLC-SDS đạt được độ an toàn thực tế trước thám mã vi sai và tuyến tính xem [3].

Về thành phần mật mã: Mã khối sử dụng hộp thế 8-bit cho khả năng xáo trộn và ma trận MDS cho khả năng khuếch tán cực đại. Các thành phần mật mã này đều có tính chất mật mã tốt và có xem xét đến khả năng tối ưu trong triển khai cài đặt phần mềm/phần cứng, xem [4, 6, 7].

Về lược đồ khóa: MKV có lược đồ khóa được thiết kế theo lược đồ lặp trong [5], có đảm bảo độ an toàn lý thuyết về cấu trúc và độ an toàn thực tế trước thám mã vi sai khóa quan hệ.

Về độ an toàn: Bên cạnh độ an toàn chứng minh được đối với hai thám mã phổ biến nhất là vi sai và tuyến tính, MKV đảm bảo kháng lại thám mã boomerang, thám mã tích phân, thám mã đại số, thám mã vi sai khóa quan hệ, thám mã vi sai không thể, ... Ngoài ra, MKV có được xem xét khả năng kháng lại một số thám mã lượng tử gần đây và thảo luận về mức an toàn trong thiết lập lượng tử có thể đạt được với kích thước khối, độ dài khóa được gia tăng.

Về hiệu năng: đảm bảo khả năng thực thi phù hợp với các ứng dụng thông dụng trong bảo mật thông tin thuộc lĩnh vực dân sự về phần cứng và phần mềm.

Công nghệ thông tin – Các kỹ thuật an toàn - Thuật toán mật mã – Mã khối MKV

Information technology - Security techniques – Encryption algorithms - Block cipher MKV

1 Phạm vi áp dụng

Tiêu chuẩn áp dụng cho việc mã hóa dữ liệu trong hoạt động giao dịch điện tử của các tổ chức, công dân Việt Nam và tổ chức, công dân nước ngoài có quan hệ kinh tế - xã hội với tổ chức, công dân Việt Nam.

Tiêu chuẩn này mô tả mã khối MKV được áp dụng trong các phương pháp mật mã và bảo mật thông tin, trong đó đảm bảo tính bí mật của thông tin khi truyền, xử lý và lưu trữ thông tin trong các hệ thống thông tin.

2 Thuật ngữ và định nghĩa

Đối với mục đích của tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau

2.1. Thuật toán mã hóa (encryption algorithm)

Là quá trình biến đổi bản rõ thành bản mã.

2.2. Thuật toán giải mã (decryption algorithm)

Là quá trình biến đổi bản mã thành bản rõ.

2.3. Mã khối (block cipher)

Là một hệ mã đối xứng có tính chất là thuật toán mã hóa hoạt động trên một khối bản rõ, nghĩa là một chuỗi bit có độ dài xác định, để thu được một khối bản mã.

Chú ý: ở đây ta có thể xem thuật ngữ "mã khối" và "thuật toán mã hóa khối" là như nhau.

2.4. Mã pháp (cipher)

Là một thuật ngữ khác của hệ mã (encipherment system). Là phương pháp mật mã được sử dụng để đảm bảo tính bí mật của dữ liệu, bao gồm thuật toán mã hóa và thuật toán giải mã.

2.5. Khối (block)

Là chuỗi các bit có độ dài xác định.

2.6. Mã hóa (encryption)

Là một thuật toán mật mã mà biến đổi (khả nghịch) dữ liệu để tạo thành bản mã, nghĩa là giấu nội dung thông tin của dữ liệu.

2.7. Khóa vòng (round key)

Là dãy ký tự được tính từ khóa (key) và điều khiển một biến đổi cho một vòng của mã khối.

2.8. Khóa (key)

Là dãy ký tự mà điều khiển hoạt động của biến đổi mật mã (cụ thể là quá trình mã hóa hoặc giải mã).

Chú ý: ở đây khóa phải là một dãy nhị phân.

2.9. Bản rõ (plaintext)

Thông tin chưa được mã hóa.

2.10. Lược đồ khóa (key schedule)

Là quá trình tính toán các khóa vòng từ khóa.

2.11. Giải mã (decryption)

Là phép biến đổi ngược của quá trình mã hóa tương ứng.

2.12. Bản mã (ciphertext)

Là dữ liệu sau phép biến đổi để giấu nội dung thông tin.

2.13. Véc tơ kiểm tra

Là tập hợp các đầu vào và đầu ra tương ứng của thuật toán mật mã, được sử dụng để kiểm tra tính đúng đắn của thuật toán.

3 Ký hiệu và thuật ngữ viết tắt

Các thuật ngữ viết tắt sau được sử dụng trong tất cả các phần của TCVN XXXX

0x	Tiền tố của các số được biểu diễn dưới dạng thập lục phân (hex);
$\mathbb{F}_2$	Trường hữu hạn chỉ có hai phần tử 0, 1, tức là $\mathbb{F}_2 = \{0,1\}$;
$\mathbb{F}_{2^8}$	Trường hữu hạn với đa thức sinh nguyên thủy $x^8 \oplus x^5 \oplus x^3 \oplus x \oplus 1$ trên $\mathbb{F}_2$;
V_n	Tập hợp xâu có độ dài n-bit;
$\oplus$	Phép toán logic XOR trên xâu bit, nghĩa là nếu A và B là hai xâu cùng độ dài thì $A \oplus B$ là xâu bit bao gồm các bit là kết quả phép toán logic XOR của A và B;
$x \| y$	Chuỗi kết quả của việc nối xâu y vào xâu x;
$\{0,1\}^d$	Xâu gồm d bit nhị phân;
$\bar{X}$	Xâu phủ định của xâu X;
$\langle r \rangle_w$	Dạng biểu diễn w-bit của số nguyên r;
l	Kích cỡ khối của mã khối, $l \in \{128,256\}$;
k	Độ dài khoá của mã khối, $k \in \{128,192,256,384,512\}$;
R	Số vòng của mã khối, $R \in \{6,7,8\}$;
w	Kích cỡ của trạng thái con;
t	Số lượng các byte trong trạng thái con;
X, x^i, x^i_j	Biểu diễn tương ứng trạng thái l-bit, trạng thái con w-bit và một byte trong trạng thái con của *quá trình mã hoá và giải mã;*

$\mathcal{K}, \mathcal{k}^i, \mathcal{k}_j^i$	Biểu diễn tương ứng trạng thái $2l$-bit, trạng thái con w-bit và một byte trong trạng thái con của quá trình *mở rộng khoá;*
s	Biến đổi thay thế từng byte trong trạng thái, còn được gọi là hộp thế;
SubCells (invSubCells)	Biến đổi trên trạng thái mã hoá (giải mã), dựa trên biến đổi s trên từng byte;
MixWords (invMixWords)	Biến đổi trên trạng thái mã hoá (giải mã), dựa trên biến đổi tuyến tính trên từng trạng thái con;
XWords	Biến đổi giữa các trạng thái con;
F_l, (invF_l)	Hàm vòng (nghịch đảo của hàm vòng) cho phiên bản có kích thước khối l;
UpdateKS$_l$	Biến đổi cập nhật trạng thái khoá của lược đồ khoá;
const$_i$	Hằng số phụ thuộc vào i cho biến đổi cập nhật UpdateKS$_l$;
P	Bản rõ l-bit, đầu vào của quá trình mã hoá và đầu ra của quá trình giải mã;
C	Bản mã l-bit, đầu vào của quá trình giải mã và đầu ra của quá trình mã hoá;
$\mathcal{K}_{\text{master}}$	Khoá chính k-bit;
$\mathcal{K}_i$	Khoá vòng $2l$-bit, được biểu diễn thành hai phần l-bit như sau $\mathcal{K}_i = \mathcal{K}_i^0 \| \mathcal{K}_i^1$ trong đó $\mathcal{K}_i^0, \mathcal{K}_i^1 \in V_l$;
$\mathcal{K}_{\text{post}}$	Khoá xoá trắng l-bit;
MKV$-l/k$	Phiên bản mã khối với kích cỡ khối l và độ dài khoá k;
Enc$_l$(.,.)	Hàm mã hoá cho phiên bản kích cỡ khối l-bit;
Dec$_l$(.,.)	Hàm giải mã cho phiên bản kích cỡ khối l-bit.

4 Mã khối MKV

4.1. Thông tin chung

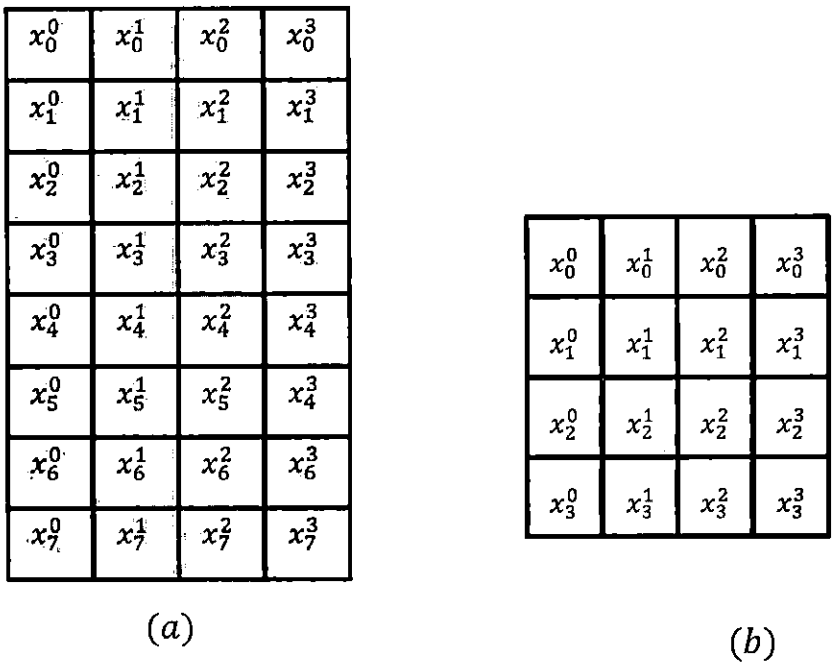
Mã khối này xử lý khối dữ liệu có kích cỡ 128-bit hoặc 256-bit, được kí hiệu MKV-l với l biểu thị kích thước khối. Trong đó, MKV-128 có ba phiên bản khóa có độ dài 128-bit, 192-bit và 256-bit tương ứng với số vòng là 6, 7, 8; còn MKV-256 có ba phiên bản khóa có độ dài 256-bit, 384-bit, 512-bit tương ứng với số vòng là 6, 7, 8. Khi đã rõ kích thước khóa và số vòng, kí hiệu MKV-l/k với số vòng R nhằm đặc tả rõ hơn thuật toán trong phần sau. Khi đó, chúng ta có tổng cộng 6 phiên bản với kích thước khối/độ dài khóa/số vòng khác nhau được mô tả trong Bảng 1.

Bảng 1 - Các phiên bản trong MKV.

STT	Phiên bản	l	k	R
1.	MKV-128	128	128	6
2.			192	7
3.			256	8
4.	MKV -256	256	256	6
5.			384	7
6.			512	8

4.2. Các khái niệm và biến đổi cơ bản

4.2.1. Các trạng thái



Hình 1 - Mô tả trạng thái cho quá trình mã hóa và giải mã của hai phiên bản MKV-256 (a) và MKV-128 (b)

4.2.1.1. Trạng thái mã hóa và giải mã

Trong quá trình mã hóa và giải mã, các phép biến đổi cơ bản sẽ cập nhật xâu bit X có độ dài l-bit, xâu này được gọi là trạng thái bên trong của mã khối. Trạng thái X này được chia thành bốn xâu w-bit x^0, x^1, x^2, x^3, được gọi là trạng thái con, như sau $X = x^0 \| x^1 \| x^2 \| x^3$. Mỗi trạng thái con x^i $(0 \leq i < 4)$ được biểu diễn dưới dạng byte như sau $x^i = x_0^i \| x_1^i \| \dots \| x_{t-1}^i, x_j^i \in V_8$ với mọi $0 \leq i < 4, 0 \leq j < t$; trong có $t = 4$ đối với MKV-128 còn $t = 8$ đối với MKV-256. Do đó, trạng thái này có thể được biểu diễn dưới dạng bảng kích thước $t \times 4$ với phần tử có giá trị một byte. Mỗi cột của bảng trạng thái chính là biểu diễn một trạng thái con của X. Cụ thể, trạng thái được biểu diễn trong Hình 1. Để biểu diễn ngắn gọn cho trạng thái mã hóa và giải mã của hai phiên bản này, trong chuẩn dùng dạng tổng quát sau:

x_0^0	x_0^1	x_0^2	x_0^3
x_1^0	x_1^1	x_1^2	x_1^3
... ...			
x_{t-1}^0	x_{t-1}^1	x_{t-1}^2	x_{t-1}^3

4.2.1.2. Trạng thái lược đồ khóa

Trong lược đồ khóa, các khóa vòng được lấy ra từ các trạng thái $2l$ bit, gấp đôi với trạng thái mã hóa và giải mã ở trên. Khi đó, trạng thái trong $\mathcal{K}$ sẽ được xử lý thành 8 từ w-bit $\mathcal{k}^0, \mathcal{k}^1, \mathcal{k}^2, \mathcal{k}^3, \mathcal{k}^4, \mathcal{k}^5, \mathcal{k}^6, \mathcal{k}^7$ như sau:

$$\mathcal{K} = \mathcal{k}^0 \| \dots \| \mathcal{k}^7$$

trong đó $\mathcal{k}^i$ là các xâu w-bit được chia thành t byte có dạng $\mathcal{k}_0^i \| \dots \| \mathcal{k}_{t-1}^i, \mathcal{k}_j^i \in V_8$ với mọi $0 \le i < 8, 0 \le j < t$. Trạng thái này biểu diễn thành một bảng $t \times 8$ với các phần tử w bit, được mô tả bởi Hình 2. Trong đó, mỗi trạng thái $\mathcal{K}$ cũng sẽ được biểu diễn thành hai phần $\mathcal{K} = \mathcal{K}^{\text{Left}} \| \mathcal{K}^{\text{Right}} \in V_{2l}$, trong đó $\mathcal{K}^{\text{Left}} = \mathcal{k}^0 \| \mathcal{k}^1 \| \mathcal{k}^2 \| \mathcal{k}^3 \in V_l, \mathcal{K}^{\text{Right}} = \mathcal{k}^4 \| \mathcal{k}^5 \| \mathcal{k}^6 \| \mathcal{k}^7 \in V_l$.

MKV-128

$\mathcal{k}_0^0$	$\mathcal{k}_0^1$	$\mathcal{k}_0^2$	$\mathcal{k}_0^3$	$\mathcal{k}_0^4$	$\mathcal{k}_0^5$	$\mathcal{k}_0^6$	$\mathcal{k}_0^7$
$\mathcal{k}_1^0$	$\mathcal{k}_1^1$	$\mathcal{k}_1^2$	$\mathcal{k}_1^3$	$\mathcal{k}_1^4$	$\mathcal{k}_1^5$	$\mathcal{k}_1^6$	$\mathcal{k}_1^7$
$\mathcal{k}_2^0$	$\mathcal{k}_2^1$	$\mathcal{k}_2^2$	$\mathcal{k}_2^3$	$\mathcal{k}_2^4$	$\mathcal{k}_2^5$	$\mathcal{k}_2^6$	$\mathcal{k}_2^7$
$\mathcal{k}_3^0$	$\mathcal{k}_3^1$	$\mathcal{k}_3^2$	$\mathcal{k}_3^3$	$\mathcal{k}_3^4$	$\mathcal{k}_3^5$	$\mathcal{k}_3^6$	$\mathcal{k}_3^7$

MKV-256

$\mathcal{k}_0^0$	$\mathcal{k}_0^1$	$\mathcal{k}_0^2$	$\mathcal{k}_0^3$	$\mathcal{k}_0^4$	$\mathcal{k}_0^5$	$\mathcal{k}_0^6$	$\mathcal{k}_0^7$
$\mathcal{k}_1^0$	$\mathcal{k}_1^1$	$\mathcal{k}_1^2$	$\mathcal{k}_1^3$	$\mathcal{k}_1^4$	$\mathcal{k}_1^5$	$\mathcal{k}_1^6$	$\mathcal{k}_1^7$
$\mathcal{k}_2^0$	$\mathcal{k}_2^1$	$\mathcal{k}_2^2$	$\mathcal{k}_2^3$	$\mathcal{k}_2^4$	$\mathcal{k}_2^5$	$\mathcal{k}_2^6$	$\mathcal{k}_2^7$
$\mathcal{k}_3^0$	$\mathcal{k}_3^1$	$\mathcal{k}_3^2$	$\mathcal{k}_3^3$	$\mathcal{k}_3^4$	$\mathcal{k}_3^5$	$\mathcal{k}_3^6$	$\mathcal{k}_3^7$
$\mathcal{k}_4^0$	$\mathcal{k}_4^1$	$\mathcal{k}_4^2$	$\mathcal{k}_4^3$	$\mathcal{k}_4^4$	$\mathcal{k}_4^5$	k_4^6	$\mathcal{k}_4^7$
$\mathcal{k}_5^0$	$\mathcal{k}_5^1$	$\mathcal{k}_5^2$	$\mathcal{k}_4^3$	$\mathcal{k}_5^4$	$\mathcal{k}_5^5$	k_5^6	$\mathcal{k}_4^7$
$\mathcal{k}_6^0$	$\mathcal{k}_6^1$	$\mathcal{k}_6^2$	$\mathcal{k}_6^3$	$\mathcal{k}_6^4$	$\mathcal{k}_6^5$	k_6^6	$\mathcal{k}_6^7$
$\mathcal{k}_7^0$	$\mathcal{k}_7^1$	$\mathcal{k}_7^2$	$\mathcal{k}_7^3$	$\mathcal{k}_7^4$	$\mathcal{k}_7^5$	k_7^6	$\mathcal{k}_7^7$

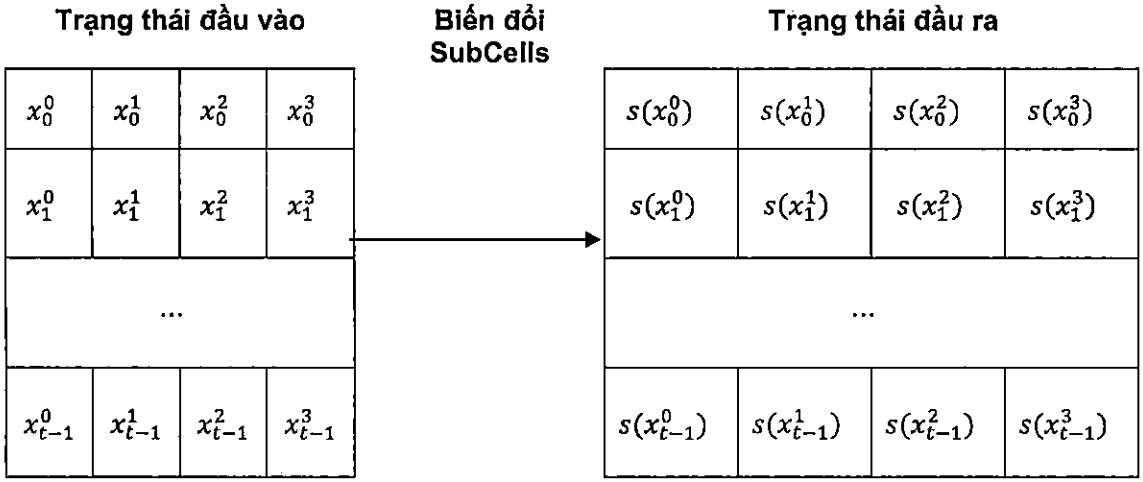
Hình 2 - Minh họa cho trạng thái khóa của MKV-l

4.2.2. Các biến đổi cơ sở của trạng thái

4.2.2.1. Biến đổi SubCells và invSubCells

Biến đổi SubCells xử lý trên toàn bộ trạng thái $X \in V_l$ bằng cách áp dụng hộp thế s vào từng byte x_j^i, được minh họa trong Hình 3. Nghịch đảo của biến đổi này được kí hiệu là invSubCells, dựa trên hộp thế nghịch đảo s^{-1} của s.

Các hộp thế này được biểu diễn dưới dạng Bảng 1, Bảng 2. Chú ý, các giá trị của các bảng này được biểu diễn dưới dạng thập lục phân (hex), trong đó giá trị đầu ra của hộp thế là giá trị giao nhau giữa cột được xác định bởi 4-bit trọng số thấp và hàng được xác định bởi 4-bit trọng số cao của đầu vào. Ví dụ, $s(0x24) = 0x1C$ và $s^{-1}(0x82) = 0xB4$.



Hình 3 - Mô tả phép biến đổi SubCells

Bảng 1 – Biểu diễn dạng tra bảng của hộp thế *s*

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	01	11	91	E1	D1	B1	71	61	F1	21	C1	51	A1	41	31	81
10	00	10	E3	92	B5	D4	77	66	89	38	AB	4A	CD	5C	2F	FE
20	08	5F	3B	B0	[illegible]	C2	83	DD	E8	F6	47	79	95	2B	AA	64
30	0F	48	D0	29	A3	1A	F2	BB	65	CC	E4	3D	57	7E	86	9F
40	0C	2A	F4	1F	5B	90	EE	C5	36	6D	73	88	BC	A7	49	D2
50	0A	3C	18	85	E0	4D	99	A4	B3	5E	DA	C7	72	FF	6B	26
60	06	76	CF	A8	4E	59	60	17	DC	9B	32	F5	23	84	ED	BA
70	07	67	2D	3B	FA	8C	16	70	54	A2	98	BE	EF	D9	C3	45
80	0E	A9	62	5A	27	BF	34	9C	FD	D5	8E	E6	1B	43	78	C0
90	03	B2	87	C4	9D	6E	4B	F8	7A	E9	2C	AF	D6	15	50	33
A0	0D	FB	56	EC	3F	75	B8	42	1E	24	C9	93	80	6A	D7	AD
B0	04	E5	B9	7D	82	A6	CA	2E	97	13	6F	DB	44	30	FC	58
C0	0B	8D	9A	46	74	28	DF	53	CB	B7	F0	6C	AE	E2	35	19
D0	05	94	7B	DE	C6	F3	AC	39	4F	8A	55	20	68	BD	12	E7
E0	02	D3	A5	F7	69	EB	5D	8F	22	40	B6	14	3A	C8	9E	7C
F0	09	CE	4C	63	D8	37	25	EA	A0	7F	1D	52	F9	96	B4	8B

Bảng 2 – Biểu diễn dạng tra bảng của hộp thế s^{-1}

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	10	00	E0	90	B0	D0	60	70	20	F0	50	C0	40	A0	80	30
10	11	01	DE	B9	EB	9D	76	67	52	CF	35	8C	24	FA	A8	43
20	DB	09	E8	6C	A9	F6	5F	84	C5	33	41	2D	9A	72	B7	1E
30	BD	0E	6A	9F	86	CE	48	F5	19	D7	EC	73	51	3B	22	A4
40	E9	0D	A7	8D	BC	7F	C3	2A	31	4E	1B	96	F2	55	64	D8
50	9E	0B	FB	C7	78	DA	A2	3C	BF	65	83	44	1D	E6	59	21
60	66	07	82	F3	2F	38	17	71	DC	E4	AD	5E	CB	49	95	BA
70	77	06	5C	4A	C4	A5	61	16	8E	2B	98	D2	EF	B3	3D	F9
80	AC	0F	B4	26	6D	53	3E	92	4B	1B	D9	FF	75	C1	8A	E7
90	45	02	13	AB	D1	2C	FD	B8	7A	56	C2	69	87	94	EE	3F
A0	F8	0C	79	34	57	E2	B5	4D	63	81	2E	1A	D6	AF	CC	9B
B0	23	05	91	58	FE	14	EA	C9	A6	B2	6F	37	4C	DD	7B	85
C0	8F	0A	25	7E	93	47	D4	5B	ED	AA	B6	C8	39	1C	F1	62
D0	32	04	4F	E1	15	89	9C	AE	F4	7D	5A	BB	68	27	D3	C6
E0	54	03	CD	12	3A	B1	8B	DF	28	99	F7	E5	A3	6E	46	7C
F0	CA	08	36	D5	42	6B	29	E3	97	FC	74	A1	BE	88	1F	5D

4.2.2.2. Biến đổi MixWords và invMixWords

Với mỗi trạng thái đầu vào $X = x^0 \| x^1 \| x^2 \| x^3$, phép biến đổi MixWords cập nhật từng trạng thái con x^i qua một biến đổi tuyến tính dựa trên ma trận có kích thước $t \times t$ trên trường $\mathbb{F}_{2^8}$, được minh họa trong Hình 4. Cụ thể, các giá trị byte trong từng xâu $y^i (0 \leq i < 4)$ của đầu ra $Y = y^0 \| y^1 \| y^2 \| y^3$ được xác định thông qua véc tơ cột $\begin{pmatrix} y_0^i \\ \vdots \\ y_{t-1}^i \end{pmatrix}$ tạo bởi phép nhân ma trận $M = (m_{i,j})_{t \times t}$ với véc tơ cột $\begin{pmatrix} x_0^i \\ \vdots \\ x_{t-1}^i \end{pmatrix}$ xác định từ đầu vào x^i như sau:

$$\begin{pmatrix} y_0^i \\ \vdots \\ y_{t-1}^i \end{pmatrix} = \begin{pmatrix} m_{0,0} & \cdots & m_{0,(t-1)} \\ \vdots & \ddots & \vdots \\ m_{(t-1),0} & \cdots & m_{(t-1),(t-1)} \end{pmatrix} \begin{pmatrix} x_0^i \\ \vdots \\ x_{t-1}^i \end{pmatrix}$$

với các byte $y_j^i, x_j^i, m_{i',j'}$ được coi là các phần tử trên trường $\mathbb{F}_{2^8}$ với mọi $0 \leq j, i', j' < (t-1)$. Chú ý, các phép toán được thực hiện trên trường $\mathbb{F}_{2^8}$ đã được lựa chọn. Nghịch đảo của biến đổi này được kí hiệu là invMixWords. Trong đó,

Đối với MKV-128, MixWords và invMixWords sử dụng ma trận 4×4 trên $\mathbb{F}_{2^8}$ tương ứng như sau:

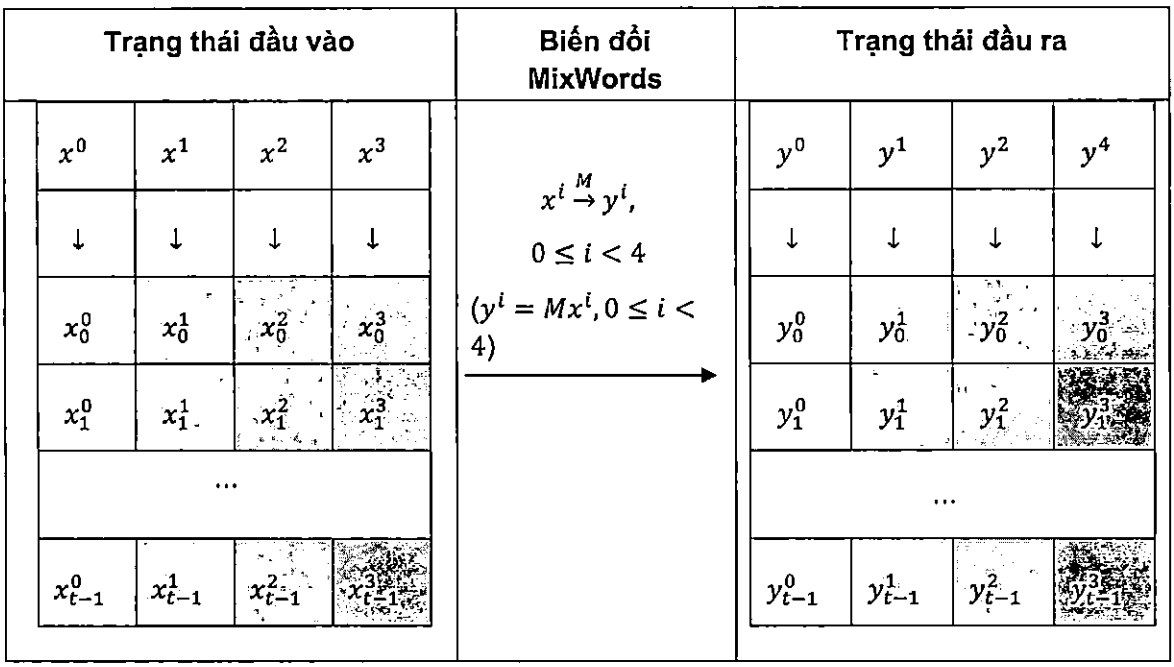
$$M_4 = \begin{pmatrix} 0x01 & 0x02 & 0x01 & 0x03 \\ 0x03 & 0x07 & 0x01 & 0x04 \\ 0x04 & 0x0B & 0x03 & 0x0C \\ 0x0C & 0x1E & 0x06 & 0x14 \end{pmatrix},$$

$$M_4^{-1} = \begin{pmatrix} 0x14 & 0x06 & 0x18 & 0x0B \\ 0x0B & 0x02 & 0x0D & 0x05 \\ 0x05 & 0x01 & 0x07 & 0x02 \\ 0x02 & 0x01 & 0x03 & 0x01 \end{pmatrix}$$

Đối với MKV-256, MixWords và invMixWords sử dụng ma trận 8×8 trên $\mathbb{F}_{2^8}$ tương ứng như sau:

$$M_8 = \begin{pmatrix} 0x01 & 0x04 & 0xDB & 0x0C & 0x14 & 0x0C & 0xDB & 0x04 \\ 0x04 & 0x11 & 0x15 & 0xEB & 0x5C & 0x24 & 0x1D & 0xCB \\ 0xCB & 0x55 & 0x38 & 0xE6 & 0xD5 & 0xAF & 0x0D & 0x4C \\ 0x4C & 0xD0 & 0x5D & 0x15 & 0x91 & 0xF8 & 0xA7 & 0x16 \\ 0x16 & 0x14 & 0x18 & 0xB5 & 0x06 & 0x79 & 0x30 & 0xFF \\ 0xFF & 0x97 & 0xE0 & 0xB0 & 0x66 & 0xAE & 0x8D & 0xB1 \\ 0xB1 & 0x6D & 0xF6 & 0x7D & 0x3C & 0xFB & 0xCF & 0x1F \\ 0x1F & 0xCD & 0x5C & 0x72 & 0xDA & 0xB8 & 0xCA & 0xB3 \end{pmatrix}$$

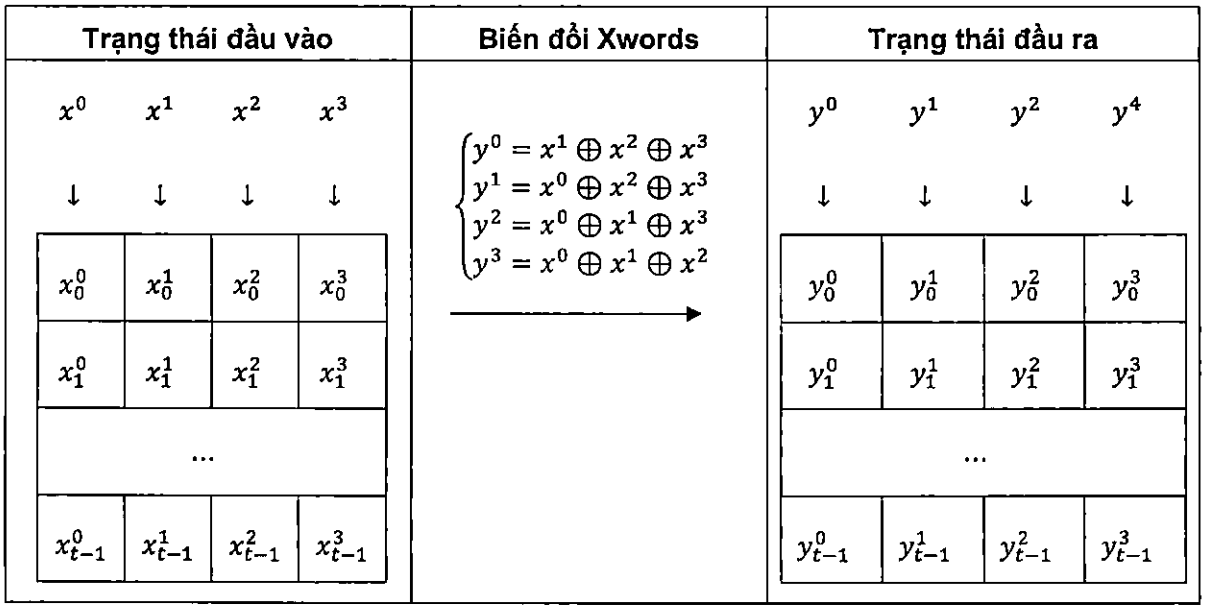
$$M_8^{-1} = \begin{pmatrix} 0xB3 & 0xCA & 0xB8 & 0xDA & 0x72 & 0x5C & 0xCD & 0x1F \\ 0x1F & 0xCF & 0xFB & 0x3C & 0x7D & 0xF6 & 0x6D & 0xB1 \\ 0xB1 & 0x8D & 0xAE & 0x66 & 0xB0 & 0xE0 & 0x97 & 0xFF \\ 0xFF & 0x30 & 0x79 & 0x06 & 0xB5 & 0x18 & 0x14 & 0x16 \\ 0x16 & 0xA7 & 0xF8 & 0x91 & 0x15 & 0x5D & 0xD0 & 0x4C \\ 0x4C & 0x0D & 0xAF & 0xD5 & 0xE6 & 0x38 & 0x55 & 0xCB \\ 0xCB & 0x1D & 0x24 & 0x5C & 0xEB & 0x15 & 0x11 & 0x04 \\ 0x04 & 0xDB & 0x0C & 0x14 & 0x0C & 0xDB & 0x04 & 0x01 \end{pmatrix}$$



Hình 4 - Mô tả phép biến đổi MixWords

4.2.2.3. Biến đổi Xwords

Biến đổi này cập nhật trạng thái đầu vào $X = x^0||x^1||x^2||x^3$ bằng cách cộng XOR các trạng thái con với nhau để nhận giá trị cho trạng thái tiếp theo $Y = y^0||y^1||y^2||y^3$ được xác định trong Hình 5.



Hình 5 - Mô tả phép biến đổi MixWords

Chú ý. Biến đổi này có tính chất tự nghịch đảo. Thật vậy, từ công thức của XWords, chúng ta cũng có:

$$\begin{cases} x^0 = y^1 \oplus y^2 \oplus y^3 \\ x^1 = y^0 \oplus y^2 \oplus y^3 \\ x^2 = y^0 \oplus y^1 \oplus y^3 \\ x^3 = y^0 \oplus y^1 \oplus y^2 \end{cases}$$

4.3. Hàm vòng

Biến đổi hàm vòng F_l biến đổi trạng thái đầu vào $X \in V_l$ thành trạng thái đầu ra $Y \in V_l$ dựa trên các biến đổi SubCells, MixWords, XWords và cộng XOR khóa vòng $\mathcal{K} = \mathcal{K}^0 \| \mathcal{K}^1 \in V_{2l}$ với $\mathcal{K}^0, \mathcal{K}^1 \in V_l$, như sau:

$$F_l: V_{2l} \times V_l \longrightarrow V_l$$

$$(\mathcal{K}^0 \| \mathcal{K}^1, X) \mapsto Y$$

trong đó,

$$Y = \mathrm{XWords}\Big(\mathrm{SubCells}\big(\mathrm{MixWords}\big(\mathrm{SubCells}(X \oplus \mathcal{K}^0)\big) \oplus \mathcal{K}^1\big)\Big)$$

Hàm $\mathbf{inv}F_l$. Được thực hiện dựa trên các biến đổi invSubCells, invMixWords, XWords và cộng XOR khóa vòng $= \mathcal{K}^0 \| \mathcal{K}^1 \in V_{2l}$ với $\mathcal{K}^0, \mathcal{K}^1 \in V_l$, như sau:

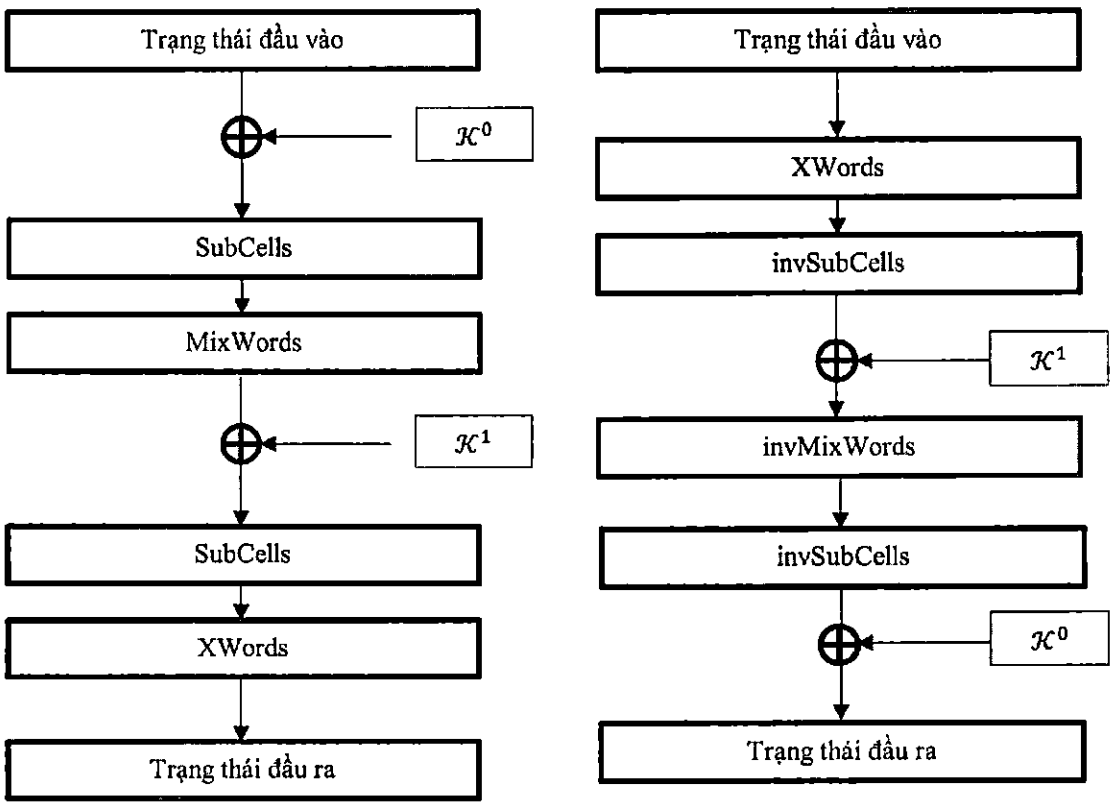
$$\mathrm{inv}F_l: V_{2l} \times V_l \longrightarrow V_l$$

$$(\mathcal{K}^0 \| \mathcal{K}^1, X) \mapsto Y$$

trong đó,

$$Y = \mathrm{invSubCells}\Big(\mathrm{invMixWords}\big(\mathrm{inSubCells}\big(\mathrm{XWords}(X)\big) \oplus \mathcal{K}^1\big)\Big) \oplus \mathcal{K}^0$$

Hai quá trình này được minh họa trong Hình 6.

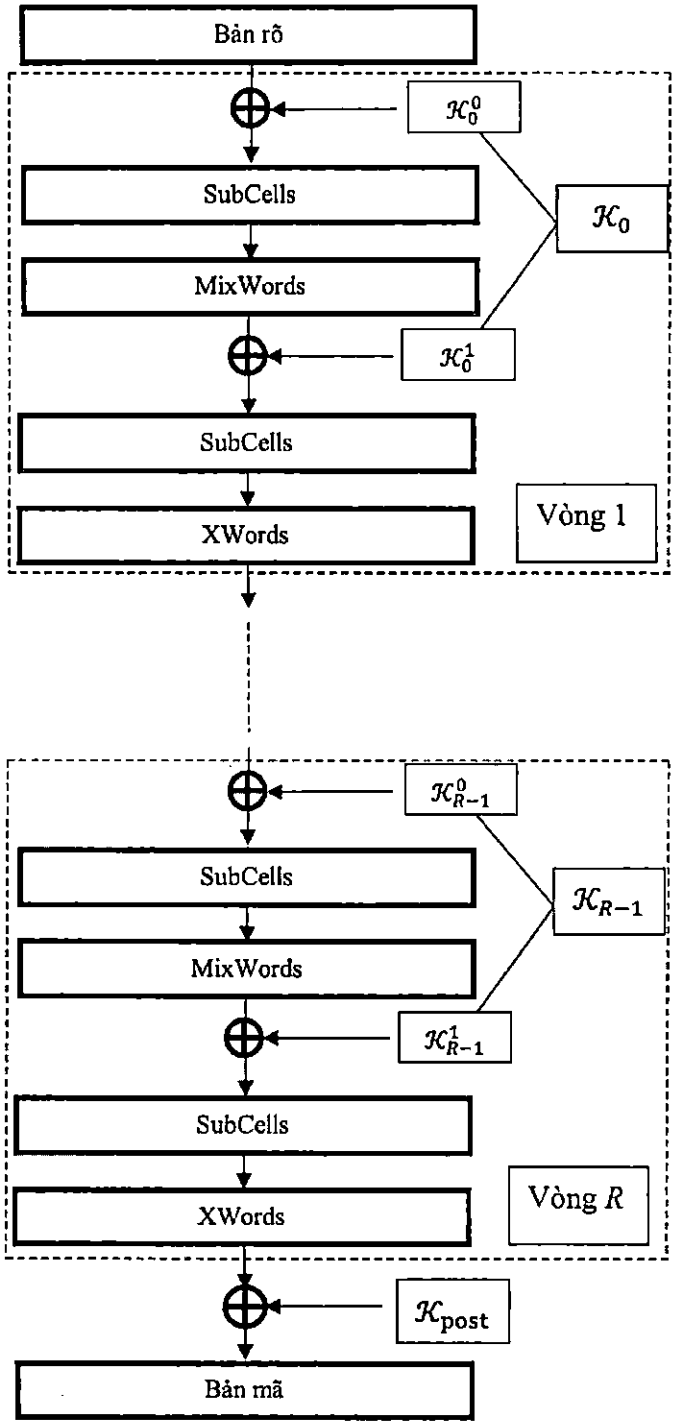


Hình 6 - Mô tả hàm vòng và nghịch đảo qua các biến đổi trạng thái

4.4. Quá trình mã hóa

Để mã hóa một bản rõ l-bit P thành một bản mã l-bit C, quá trình mã hóa của mã khối MKV-l thực hiện R lần lặp hàm vòng F_l kết hợp cộng xóa trắng sau khi thực hiện lặp các hàm vòng. Cụ thể, quá trình này sử dụng R khóa vòng có độ dài $2l$-bit, $\mathcal{K}_i \in V_{2l} (0 \leq i < R)$, và một khóa làm trắng $\mathcal{K}_{\text{post}} \in V_l$ được sinh bởi lược đồ khóa từ khóa chính $\mathcal{K}_{\text{master}}$. Khi đó, quá trình này được xác định bởi công thức sau:

$$C = \text{Enc}_l(\mathcal{K}_{\text{master}}, P) = F_l\left(\mathcal{K}_{R-1}, F_l\left(\mathcal{K}_{R-2}, \left(\ldots, F_l(\mathcal{K}_0, P)\right)\right)\right) \oplus \mathcal{K}_{\text{post}}$$

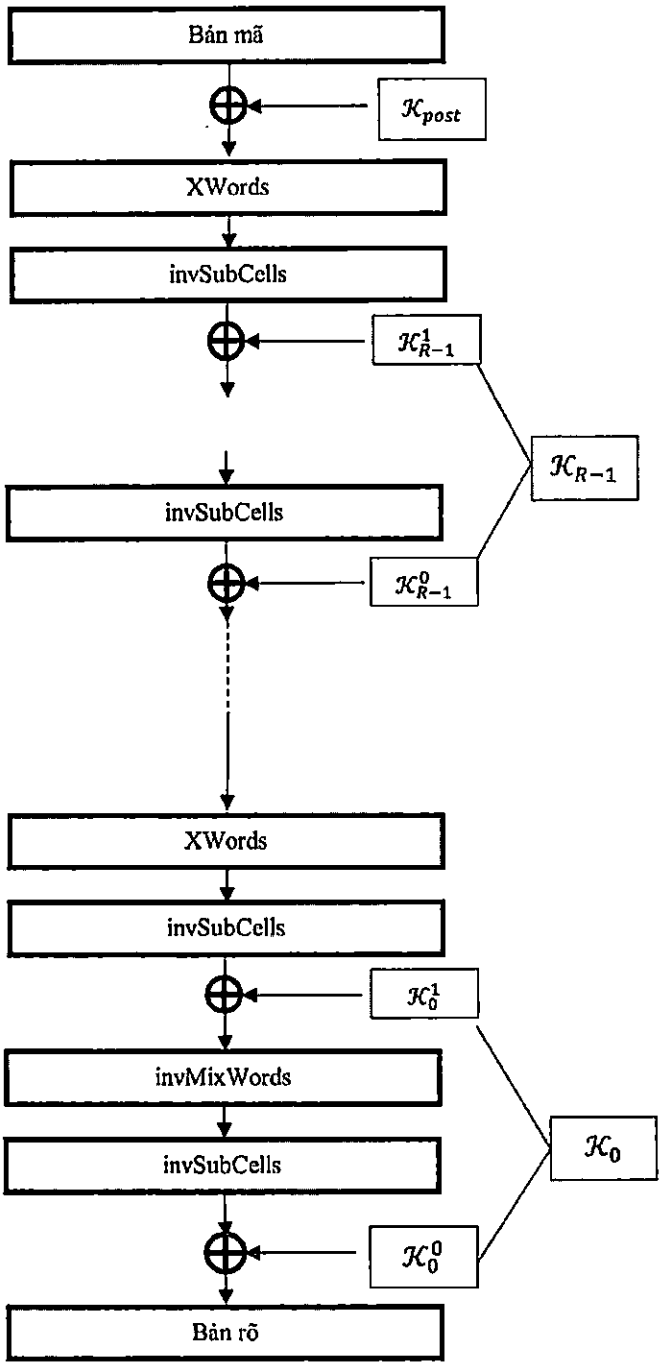


Hình 7 - Mô tả quá trình mã hóa qua các biến đổi trạng thái

4.5. Quá trình giải mã

Để giải mã một bản mã l-bit C thành một bản rõ l-bit P, quá trình giải mã của mã khối MKV-l lặp lại R lần hàm vòng $\text{inv}F_l$ cũng sử dụng R khóa vòng $\mathcal{K}_i \in V_{2l} (0 \leq i < R)$ và khóa làm trắng $\mathcal{K}_{\text{post}} \in V_l$ giống như quá trình mã hóa. Khi đó, quá trình này được xác định bởi công thức sau:

$$P = \text{Dec}_l(\mathcal{K}_{\text{master}}, C) = \text{inv}F_l\left(\mathcal{K}_0, \text{inv}F_l\left(\mathcal{K}_1, \left(\ldots, \text{inv}F_l(\mathcal{K}_{R-1}, C \oplus \mathcal{K}_{\text{post}})\right)\right)\right).$$



Hình 8 - Mô tả quá trình giải mã qua các biến đổi trạng thái

4.6. Lược đồ khóa

Lược đồ khóa của mã khối MKV-l sử dụng một biến đổi trạng thái của khóa, được gọi là biến đổi $\mathrm{UpdateKS}_l$. Biến đổi trạng thái này thực hiện cập nhật đối với trạng thái khóa có kích cỡ $2l$-bit $K = K^{\mathrm{Left}} \| K^{\mathrm{Right}} \in V_{2l}$ của vòng này để lấy ra khóa của vòng tiếp theo theo các bước như sau:

- **Bước 1:**(Khởi tạo) Trạng thái khóa ban đầu K_0 sẽ được khởi tạo từ khóa chính $\mathcal{K}_{\mathrm{master}}$ đối với trường hợp khóa $2l$-bit và từ khóa được bổ sung đối với trường hợp còn lại như sau:

$$K_0 = \begin{cases} \mathcal{k}^0 \| \dots \| \mathcal{k}^7 & \text{trường hợp } \mathcal{K}_{\mathrm{master}} = \mathcal{k}^0 \| \dots \| \mathcal{k}^7 \in V_{2l} \\ \mathcal{k}^0 \| \dots \| k^4 \| \mathcal{k}^5 \| \overline{\mathcal{k}^2} \| \overline{\mathcal{k}^3} & \text{trường hợp } \mathcal{K}_{\mathrm{master}} = \mathcal{k}^0 \| \dots \| k^5 \in V_{3l/2} \\ \mathcal{k}^0 \| \dots \| \mathcal{k}^3 \| \overline{\mathcal{k}^0} \| \dots \| \overline{\mathcal{k}^3} & \text{trường hợp } \mathcal{K}_{\mathrm{master}} = \mathcal{k}^0 \| \dots \| \mathcal{k}^3 \in V_l \end{cases}$$

- **Bước 2:** (Sinh các khóa vòng) Chúng ta nhận được các khóa vòng $\mathcal{K}_i, i = 0, 1, \dots, R-1$ và $\mathcal{K}_{\mathrm{post}}$ từ khóa được sinh ra trong quá trình cập nhật trạng thái khóa bởi hàm $\mathrm{UpdateKS}_l$ dựa trên các hằng số vòng $\mathrm{Const}_i^{\mathrm{Left}}, \mathrm{Const}_i^{\mathrm{Right}}$ có giá trị $2l$ bit có phụ thuộc các chỉ số vòng i, được xác định như sau:

$$\begin{cases} \mathrm{Const}_i^{\mathrm{Left}} = \langle 2i \rangle_{2l} \\ \mathrm{Const}_i^{\mathrm{Right}} = \langle 2i+1 \rangle_{2l} \end{cases}$$

Biến đổi này cập nhật trạng thái khóa $2l$-bit tại vòng i với đầu vào là trạng thái tại vòng trước đó $K_{i-1} = K_{i-1}^{\mathrm{Left}} \| K_{i-1}^{\mathrm{Right}} \in V_{2l}$ cho ra trạng thái mới tiếp theo $K_i = K_i^{\mathrm{Left}} \| K_i^{\mathrm{Right}}$ dựa trên hằng số $2l$-bit Const_i theo công thức sau:

$$\mathrm{UpdateKS}_l[\mathrm{Const}_i]: V_{2l} \longrightarrow V_{2l}$$

$$\left(K_{i-1}^{\mathrm{Left}} \| K_{i-1}^{\mathrm{Right}}\right) \longmapsto \left(K_i^{\mathrm{Left}} \| K_i^{\mathrm{Right}}\right)$$

trong đó

$$\begin{cases} K_i^{\mathrm{Left}} = F_l\left(0, F_l\left(\mathrm{Const}_{i-1}^{\mathrm{Right}}, K_{i-1}^{\mathrm{Right}}\right)\right) \\ K_i^{\mathrm{Right}} = K_i^{\mathrm{Left}} \oplus F_l\left(0, F_l\left(\mathrm{Const}_{i-1}^{\mathrm{Left}}, K_{i-1}^{\mathrm{Left}}\right)\right) \end{cases}$$

với F_l là hàm vòng. Xem mô tả Hình 9.

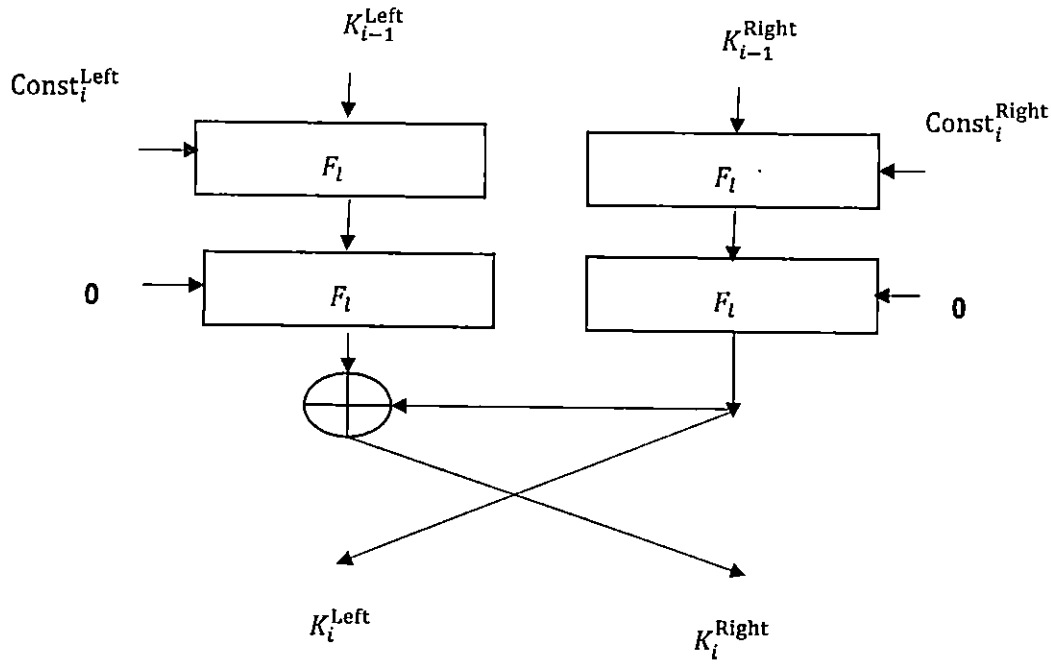
Thực hiện R lần cập nhật ta có các giá trị trạng thái khóa $K_0, K_1, \dots, K_R$. Khi đó, các khóa cho quá trình mã và giải mã $\mathcal{K}_0, \dots, \mathcal{K}_{R-1} \in V_{2l}, \mathcal{K}_{\mathrm{post}} \in V_l$ được xác định như sau:

$$\mathcal{K}_0 = (\mathcal{K}_0^0 \| \mathcal{K}_0^1) = (K_0^{\mathrm{Left}} \| K_1^{\mathrm{Left}})$$

$$\mathcal{K}_1 = (\mathcal{K}_1^0 \| \mathcal{K}_1^1) = (K_1^{\mathrm{Right}} \| K_2^{\mathrm{Left}})$$

$$\mathcal{K}_i = \left(\mathcal{K}_i^0 \| \mathcal{K}_i^1\right) = \left(K_l^{\mathrm{Right}} \| K_{i+1}^{\mathrm{Left}}\right), 2 \le i < R$$

$$\mathcal{K}_{\mathrm{post}} = K_R^{\mathrm{Right}}$$



Hình 9 - Biến đổi $\text{UpdateKS}_1[C]$ trên trạng thái khóa

PHỤ LỤC A Véc tơ kiểm tra cho MKV

A.1. Phiên bản kích cỡ khối 128-bit

A.1.1. Trường hợp khóa 128-bit:

Bản rõ :
u8 X[6] = {
0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
};

Khóa chính:
u8 MasterKey[ ] = {
0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11
};

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11
K01: 0D 96 E3 D1 96 32 6A C6 83 15 EF 29 34 37 AB 0A
K02: 05 6F 4B 9A 95 33 CA 5B 6D DC 9B 6A 7E CE 62 A7
K03: D6 26 AD 46 28 C7 1B B9 14 E5 A9 5B 4B 64 40 E1
K04: BB BE 38 EF FA E9 03 80 B8 B8 9E B0 0A B5 93 42
K05: 6C B1 7B 9E 1F 7C C4 AF 12 3B 73 D3 E4 36 13 CF
K06: AE BF 06 AC 43 F1 15 1E A1 F4 E5 27 DB 99 69 FD
K07: 1A 6D 25 63 A6 32 39 02 94 D0 C6 23 61 6B A9 CC
K08: B9 E5 40 FC F1 0F 0D E0 CF F7 D7 02 0D 64 DF 79
K09: 3E 45 29 0E F0 47 E0 B7 C2 C0 6D 48 56 FB 76 74
K10: BA 7F 68 9F 56 12 F6 C4 49 98 27 AB 9A 63 FE 29
K11: 2B 4D FA 61 28 CC 1D 7E A8 BA 0C E2 FE DC F7 AE
K_post: 5B 40 A6 BF 12 50 B1 E8 9A 89 4F 39 F4 F4 5B 9D
```

Trạng thái 128-bit cập nhật qua các vòng:

```
Vòng 1
1.AddRoundKey:  10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 11
2.SubCells:     00 08 0F 0C 0A 06 07 0E 03 0D 04 0B 05 02 09 10
3.MixWords:     0B 07 15 22 13 33 5D FC 00 0E 00 05 38 48 C9 58
4.AddRoundKey:  06 91 F6 F3 85 01 37 3A 83 1B EF 2C 0C 7F 62 52
5.SubCells:     71 B2 25 63 BF 11 BB E4 5A 4A 7C 95 A1 45 CF 18
6.XWord:        44 1E 08 69 8A BD 96 EE 6F E6 51 9F 94 E9 E2 12

Vòng 2
1.AddRoundKey:  41 71 43 F3 1F 8E 5C B5 02 3A CA F5 EA 27 80 B5
2.SubCells:     2A 67 1F 63 FE 78 72 A6 91 E4 F0 37 B6 DD 0E A6
3.MixWords:     5E D8 C4 60 BD D6 F9 01 DB 5E A7 36 E8 74 1D 0E
4.AddRoundKey:  88 FE 69 26 95 11 E2 B8 CF BB 0E 6D A3 10 5D EF
5.SubCells:     FD B4 9B 83 6E 10 A5 97 19 DB 31 84 EC 00 FF 7C
6.XWord:        9B CB 6B 6F 08 6F 55 7B 7F A4 C1 68 8A 7F 0F 90

Vòng 3
1.AddRoundKey:  20 75 53 80 F2 86 56 FB C7 1C 5F D8 80 CA 9C D2
2.SubCells:     08 8C 85 0E 4C 34 99 52 53 CD 26 4F 0E F0 D6 7B
3.MixWords:     AC 7C B1 F9 4B A2 BB 80 15 F1 95 00 9E 85 1A C7
```

```
4.AddRoundKey:  C0 CD CA 67 54 DE 7F 2F 07 CA E6 D3 7A B3 09 08
5.SubCells:     0B E2 F0 17 E0 12 45 64 61 F0 5D DE 98 7D 21 F1
6.XWord:        19 9F 39 4B F2 6F 8C 38 73 8D 94 82 8A 00 E8 AD

Vòng 4
1.AddRoundKey:  B7 20 3F E7 B1 9E 99 26 D2 79 71 A5 51 99 81 50
2.SubCells:     2E 08 9F 8F E5 50 E9 83 7B A2 67 75 3C E9 A9 0A
3.MixWords:     1B BF 5B EB 02 2C B2 56 EC 06 6B 3D 72 0C DB A4
4.AddRoundKey:  01 D2 7E 88 A4 1E 8B 54 78 D6 AD 1E 13 67 72 68
5.SubCells:     11 7B C3 FD 3F 2F E6 E0 54 AC 6A 2F 92 17 2D DC
6.XWord:        F9 94 A1 13 D7 C0 84 0E BC 43 08 C1 7A F8 4F 32

Vòng 5
1.AddRoundKey:  40 71 E1 EF 26 CF 89 EE 73 B4 DF C3 77 9C 90 4B
2.SubCells:     0C 67 D3 7C 83 19 D5 9E 3B 82 E7 46 70 D6 03 88
3.MixWords:     95 02 B8 9C ED 1A 01 76 39 6A EC 41 47 91 E7 95
4.AddRoundKey:  AB 47 91 92 1D 5D E1 C1 FB AA 81 09 11 6A 91 E1
5.SubCells:     93 C5 B2 87 5C FF D3 8D 52 C9 A9 21 10 32 B2 D3
6.XWord:        1E 04 C8 7F D1 3E A9 75 DF 08 D3 D9 9D F3 C8 2B

Vòng 6
1.AddRoundKey:  A4 7B A0 E0 87 2C 5F B1 96 90 F4 72 07 90 36 02
2.SubCells:     3F BE 0D 02 9C 95 26 E5 4B 03 D8 2D 61 03 F2 91
3.MixWords:     63 03 6F 76 BF D6 29 1D E2 B8 83 D4 0D 4A 28 B9
4.AddRoundKey:  48 4E 95 17 97 1A 34 63 4A 02 8F 36 F3 96 DF 17
5.SubCells:     36 49 6E 66 F8 AB A3 A8 73 91 C0 F2 63 4B E7 66
6.XWord:        E8 71 84 3C 26 93 49 F2 AD A9 2A A8 BD 73 0D 3C
AddRoundKey:    B3 31 22 83 34 C3 F8 1A 37 20 65 91 49 87 56 A1

Bản mã: B3 31 22 83 34 C3 F8 1A 37 20 65 91 49 87 56 A1
```

A.1.2. Trường hợp khóa 192-bit

128-bit bản rõ:

```
u8 X[16] = {
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
      };
```

Khóa chính:

```
u8 MasterKey[] = {
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19
      };
```

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11
K01: 7B 3A 4E 09 7B A0 DC 30 DE 75 FE 23 3F 07 75 E3
K02: 73 C3 E6 42 78 A1 7C AD 30 BC 8A 60 75 FE BC 4E
K03: 76 96 76 6B F7 D5 B7 CE 8E FB 2D 0C F5 84 71 2A
K04: A0 AD 2D A4 B6 EA EB 64 42 63 33 88 28 39 6B A4
K05: 50 09 D3 C2 4B 0B B1 00 0A 4C D2 84 DE 14 84 66
K06: 1D 20 13 F8 E0 B2 AD 3B 8B 72 DA 16 ED EE FE 1F
```

K07: DE 80 0A A5 D3 12 88 22 4E A8 C8 31 9B 4C 7B 4D
K08: 04 52 0D 51 10 1C 4F 09 28 58 50 48 65 1B 99 86
K09: 12 6C B6 39 53 B2 B4 8E 25 07 15 C1 A6 34 A9 A1
K10: 87 C1 86 C2 C2 66 35 7C 7A DE B4 99 DE 97 B1 0D
K11: 6B 70 A7 45 F9 17 7B 7E 99 89 CC C7 6B D8 EF 23
K12; B0 7C 4C 82 09 CA E7 0F 65 88 D8 9B 52 2C B4 4D
K13: 7E 71 EB B8 DA 06 7C B0 F9 37 F8 91 7A B5 8B F8
K_post: 8A EA 8B A1 0E 51 22 6E 2D B4 65 A1 48 5B D1 F8

Trạng thái 128-bit cập nhật qua các vòng:

Vòng 1
1.AddRoundKey: 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 11
2.SubCells: 00 08 0F 0C 0A 06 07 0E 03 0D 04 0B 05 02 09 10
3.MixWords: 0B 07 15 22 13 33 5D FC 00 0E 00 05 38 48 C9 58
4.AddRoundKey: 70 3D 5B 2B 68 93 81 CC DE 7B FE 26 07 4F BC BB
5.SubCells: 07 7E C7 79 DC C4 A9 AE 12 BE B4 83 61 D2 44 DB
6.XWord: AF A8 59 F6 74 12 37 21 BA 68 2A 0C C9 04 DA 54

Vòng 2
1.AddRoundKey: DC 6B BF B4 0C B3 4B 8C 8A D4 A0 6C BC FA 66 1A
2.SubCells: 68 F5 58 82 A1 7D 88 1B 8E C6 0D 23 44 1D 60 AB
3.MixWords: 5C 23 4E CB FE 74 DC F7 41 3C 4E 4F C8 05 DA 50
4.AddRoundKey: 2A B5 38 A0 09 A1 6B 39 CF C7 63 43 3D 81 AB 7A
5.SubCells: 47 A6 65 0D 21 FB F5 CC 19 53 A8 1F 7E A9 93 98
6.XWord: 46 01 CE 4B 20 5C 5E 8A 18 F4 03 59 7F 0E 38 DE

Vòng 3
1.AddRoundKey: E6 AC E3 EF 96 B6 B5 EE 5A 97 30 D1 57 37 53 7A
2.SubCells: 5D 80 F7 7C 4B CA A6 9E DA F8 0F 94 A4 BB 85 98
3.MixWords: 05 36 50 B0 DB 75 F5 42 99 F2 A8 AC FF 28 19 4E
4.AddRoundKey: 55 3F 83 72 90 7E 44 42 93 BE 7A 28 21 3C 9D 28
5.SubCells: 4D 9F 5A 2D 03 C3 5B F4 C4 FC 98 E8 5F 57 15 E8
6.XWord: 98 68 D6 F4 D6 34 D7 2D 11 0B 14 31 8A A0 99 31

Vòng 4
1.AddRoundKey: 85 48 C5 0C 36 86 7A 16 9A 79 CE 27 67 4E 67 2E
2.SubCells: BF 36 28 A1 F2 34 98 77 2C A2 35 DD 17 49 17 AA
3.MixWords: 33 92 EF 4F 9B DE A4 73 3A 5B 73 67 47 04 23 45
4.AddRoundKey: ED 12 E5 EA 48 CC 2C 51 74 F3 BB 56 DC 48 58 08
5.SubCells: C8 E3 EB B6 36 AE 95 3C FA 63 DB 99 68 36 B3 F1
6.XWord: A4 FB FD 54 5A B6 83 DE 96 7B CD 7B 04 2E A5 13

Vòng 5
1.AddRoundKey: A0 A9 F0 05 4A AA CC D7 BE 23 9D 33 61 35 3C 95
2.SubCells: 0D 24 09 B1 73 C9 AE 39 FC B0 15 29 76 1A 57 6E
3.MixWords: B4 70 64 2E 2F F6 C2 FC D9 F3 A0 88 A7 18 04 1F
4.AddRoundKey: A6 1C D2 17 7C 44 76 72 FC F4 B5 49 01 2C AD BE
5.SubCells: B8 CD 7B 66 EF 5B 16 2D F9 D8 A6 6D 11 95 6A FC
6.XWord: 07 16 DA BC 50 80 B7 F7 46 03 07 B7 AE 4E CB 26

Vòng 6
1.AddRoundKey: 80 D7 5C 7E 92 E6 82 8B 3C DD B3 2E 70 D9 7A 2B
2.SubCells: 0E 39 72 C3 87 5D 62 E6 57 BD 7D AA 07 8A 98 79
3.MixWords: 60 BE 56 47 5E 9D 57 3E AE 34 F0 D2 2B 95 D5 EE
4.AddRoundKey: 0B CE F1 02 A7 8A 2C 40 37 BD 3C 15 40 4D 3A CD
5.SubCells: 51 35 CE 91 42 8E 95 0C BB 30 57 D4 0C A7 E4 E2

```
6.XWord:        F5 19 26 3A E6 A2 7D A7 1F 1C BF 7F A8 8B 0C 49

Vòng 7
1.AddRoundKey:  45 65 6A B8 EF 68 9A A8 7A 94 67 E4 FA A7 B8 04
2.SubCells:     90 59 32 97 7C DC 2C 1E 98 9D 17 69 1D 42 97 D1
3.MixWords:     82 07 BC 50 E1 92 6C D1 25 B5 14 AA 56 6C FC 3E
4.AddRoundKey:  FC 76 57 E8 3B 94 10 61 DC 82 EC 3B 2C D9 77 C6
5.SubCells:     F9 16 A4 22 3D 9D 00 76 68 62 3A 3D 95 8A 70 DF
6.XWord:        C0 75 4A 94 04 FE EE C0 51 01 D4 8B AC E9 9E 69

AddRoundKey:    4A 9F C1 35 0A AF CC AE 7C B5 B1 2A E4 B2 4F 91
Bản mã:     4A 9F C1 35 0A AF CC AE 7C B5 B1 2A E4 B2 4F 91
```

A.1.3. Trường hợp khóa 256-bit

128-bit bản rõ:

```
u8 X[16] = {
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
      };
```

Khóa chính:

```
u8 MasterKey[ ] = {
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19,
            0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x22, 0x23
      };
```

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11
K01: 1E 5E F1 98 8B A6 29 B7 4D 70 AA 1B D7 CD CF DE
K02: 16 A7 59 D3 88 A7 89 2A A3 B9 DE 58 9D 34 06 73
K03: 47 B9 AE 3A 79 D6 32 26 9D 71 CC 30 56 C7 15 C7
K04: 5E E7 ED A3 89 0A 36 C1 8E 0C B3 43 81 DE FA 91
K05: 93 1C BC AF 68 66 CD BE 5B CC C7 64 15 BC 95 89
K06: CD 7D 1D AD 6D 24 98 0A 14 6B 63 09 82 4A 16 5B
K07: 6D 71 1F E3 9B 9A E8 49 C9 2E EA E5 C1 EB 32 62
K08: D7 2F 9F F3 2A 5F 63 DA 4B 2F C7 24 4D A8 49 B0
K09: 4F D5 B7 17 1A D6 82 02 D5 EB 13 95 92 75 04 E1
K10: FD D6 E3 93 B0 72 05 9C 16 AF 32 E5 12 92 F5 07
K11: 24 B9 A9 0A 33 15 57 25 94 4E B6 25 AD 55 0E 42
K12: 7E 0B 4A 70 99 8D 25 30 66 75 31 AD 0F 68 C7 2F
K13: B0 0A E0 DD 45 BE 53 5D 4A D6 E4 F3 BC D1 48 36
K14: 47 D3 B9 82 12 0C AB EA BA C0 9C 68 A2 21 55 9C
K15: 9F 1D 7C 45 5B EC 4A 14 61 02 6B BD BB D7 E6 6B
K_post: 91 73 60 DD 13 66 4E 1F 9B 42 D3 03 8B 9D FF 81


==============
Trạng thái 128-bit cập nhật qua các vòng:
Vòng 1
1.AddRoundKey:  10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 11
2.SubCells:     00 08 0F 0C 0A 06 07 0E 03 0D 04 0B 05 02 09 10
```

```
3.MixWords:     0B 07 15 22 13 33 5D FC 00 0E 00 05 38 48 C9 58
4.AddRoundKey:  15 59 E4 BA 98 95 74 4B 4D 7E AA 1E EF 85 06 86
5.SubCells:     D4 5E 69 6F 7A 6E FA 88 A7 C3 C9 2F 7C BF 71 34
6.XWord:        A1 12 42 93 0F 22 D1 74 D2 8F E2 D3 09 F3 5A C8

Vòng 2
1.AddRoundKey:  B7 B5 1B 40 87 85 58 5E 71 36 3C 8B 94 C7 5C BB
2.SubCells:     2E A6 4A 0C 9C BF B3 6B 67 F2 57 E6 9D 53 72 DB
3.MixWords:     17 07 4C F1 C7 FB 84 92 FE 93 D0 F9 0F 7D 67 11
4.AddRoundKey:  50 BE E2 CB BE 2D B6 B4 63 E2 1C C9 59 BA 72 D6
5.SubCells:     0A FC A5 6C FC 2B CA 82 A8 A5 CD B7 5E 6F 2D AC
6.XWord:        0A E1 2A 99 FC 36 45 77 A8 B8 42 42 5E 72 A2 59

Vòng 3
1.AddRoundKey:  54 06 C7 3A 75 3C 73 B6 26 B4 F1 01 DF AC 58 C8
2.SubCells:     E0 71 53 E4 8C 57 3B CA 83 82 CE 11 E7 80 B3 CB
3.MixWords:     56 C9 96 10 6C 5F 09 56 51 D7 EF 7E 09 1D 20 A4
4.AddRoundKey:  C5 D5 2A BF 04 39 C4 E8 0A 1B 28 1A 1C A1 B5 2D
5.SubCells:     28 F3 47 58 D1 CC 74 22 C1 4A E8 AB CD FB A6 2B
6.XWord:        DD 7D 3A A2 24 42 09 D8 34 C4 95 51 38 75 DB D1

Vòng 4
1.AddRoundKey:  10 00 27 0F 49 66 91 D2 20 AF F6 58 BA 3F CD 8A
2.SubCells:     00 01 DD 81 6D 60 B2 7B 08 AD 25 B3 6F 9F E2 8E
3.MixWords:     77 88 30 B7 92 C9 A6 7C A2 99 4A 9B 21 9D 78 D9
4.AddRoundKey:  1A F9 2F 54 09 53 4E 35 6B B7 A0 7E E0 76 4A BB
5.SubCells:     AB 7F 64 E0 21 85 49 1A F5 2E 0D C3 02 16 73 DB
6.XWord:        D6 BD 37 02 5C 47 1A F8 88 EC 5E 21 7F D4 20 39

Vòng 5
1.AddRoundKey:  01 92 A8 F1 76 18 79 22 C3 C3 99 05 32 7C 69 89
2.SubCells:     11 87 1E CE 16 89 A2 3E 46 46 E9 B1 D0 EF 9B D5
3.MixWords:     53 80 51 1B CF A2 DC 66 DB 48 A3 AA EA 32 A6 D9
4.AddRoundKey:  1C 55 E6 0C D5 74 5E 64 0E A3 B0 3F 78 47 A2 38
5.SubCells:     CD 4D 5D A1 F3 FA 6B 4E 31 EC 04 9F 54 C5 56 65
6.XWord:        96 D3 39 B4 A8 64 0F 5B 6A 72 60 8A 0F 5B 32 70

Vòng 6
1.AddRoundKey:  6B 05 DA 27 18 16 0A C7 7C DD 52 6F 1D C9 C7 77
2.SubCells:     F5 B1 55 DD 89 77 C1 53 EF BD 18 BA 5C B7 53 70
3.MixWords:     A5 02 67 17 53 78 BC 62 43 F2 39 85 DA 24 05 C4
4.AddRoundKey:  81 BB CE 1D 60 6D EB 47 D7 BC 8F A0 77 71 0B 86
5.SubCells:     A9 DB 35 5C 06 84 14 C5 39 44 C0 0D 70 67 51 34
6.XWord:        4F A7 85 FC E0 F8 A4 65 DF 38 70 AD 96 1B E1 94

Vòng 7
1.AddRoundKey:  31 AC CF 8C 79 75 81 55 B9 4D 41 00 99 73 26 BB
2.SubCells:     48 80 19 1B A2 8C A9 4D 13 A7 2A 01 E9 3B 83 DB
3.MixWords:     57 50 88 56 EF A2 11 29 5F 13 42 6A 5A 23 21 2F
4.AddRoundKey:  E7 5A 68 8B AA 1C 42 74 15 C5 A6 99 E6 F2 69 19
5.SubCells:     8F DA DC E6 C9 CD F4 FA D4 28 B8 E9 5D 4C 9B 38
6.XWord:        40 A9 D7 2B 06 BE FF 37 1B 5B B3 24 92 3F 90 F5

Vòng 8
1.AddRoundKey:  07 7A 6E A9 14 B2 54 DD A1 9B 2F 4C 30 1E C5 69
2.SubCells:     61 98 ED 24 B5 B9 E0 BD FB AF 64 BC 0F 2F 28 9B
```

```
3.MixWords:      FB 6B E3 9C E0 E4 56 48 05 D4 65 CD FF CE B3 7E
4.AddRoundKey:   64 76 9F D9 BB 08 1C 5C 64 D6 0E 70 44 19 55 15
5.SubCells:      4E 16 33 8A DB F1 CD 72 4E AC 31 07 5B 38 4D D4
6.XWord:         CE 65 B1 A1 5B 82 4F 59 CE DF B3 2C DB 4B CF FF
AddRoundKey:     5F 16 D1 7C 48 E4 01 46 55 9D 60 2F 50 D6 30 7E

Bản mã:      5F 16 D1 7C 48 E4 01 46 55 9D 60 2F 50 D6 30 7E
```

A.2. Phiên bản kích cỡ khối 256-bit

A.2.1. Trường hợp khóa 256-bit

256-bit bản rõ:

```
u8 X[32] = {
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00,
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
      };
```

Khóa chính:

```
u8 MasterKey[] = {
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19,
            0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x22, 0x23,
      };
```

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 0102030405060708090A0B0C0D0E0F1112131415161718191A1B1C1D1E1F2223
K01: 76368C1BC3DDC4F2BCF2A54A3C85118A97D64BB3CF850B8515981001CA34B469
K02: F32BE9C6475D22B2ABE501737966F40B002F89CCB4DCA01A1CB7F556C57C71B0
K03: 0C80CE24AB11D29C98C111711F2CBE1A28DAC73F740672043954D9C85CD9B195
K04: 3EF30A853F19CDA61BDA23FECF5D7580F954305623CA4514A669D1F27509881C
K05: 89BD87E8F6AA9F7A29D0D39505510FDDD35BD355094250154ADD5D348575EC82
K06: F84B92DD2CB4B952D036B5906DF690FBD01FCBCD24871DF6E021D5A70F43AD30
K07: AF50D62B5D2DFD0580A20B34F6573F85978A8367D0ECD62C4D447B39FA984C86
K08: 8FFA10E8FBB876119C943352CB28C29ECCCA0F1183D8C2D48CB4E240A74D6C0D
K09: ED6736E666CF9A4B730832133114D2C18997E45CB31D3880CF8FD7D0D96DE0A5
K10: F491BBB533F98DED821E128BAA65ADE0D075B3269D7119EAF24DDEA519D8B0AE
K11: C6A15E895EDD3A088E0352ECD36606038E34C5219B93CF45012B9C7E9CEE241E
K_post: 0604FB69603202363D4DEAEC1E7DA30CB865E2557A210EF064ED3ECA3CFC65C3
==============
256-bit trạng thái được cập nhật qua các vòng:
Vòng 1
1.AddRoundKey:   10203040506070809 0A0B0C0D0E0F011033127514371 6F9183B1A7D1C3F1DD23
2.SubCells:      00080F0C0A06070E030D040B05020910E148DD3C1F67BAB25AE5429446CEBDB0
3.MixWords:      CAD8632769B0D425B7CF228040572FDDFE4C43764014C861EB6CEB186F86CC57
4.AddRoundKey:   BCEEEF3CAA6D10D70B3D87CA7CD23E57699A08C58F91C3E4FEF4FB19A5B2783E
5.SubCells:      449E7C57C9840039517E9CF0EF7B86A49B2CF128C0B24669B4D8523875B95486
6.XWord:         7E8A3FE05A70944B6B6ADF477C8F12D6A138B29F5346D21B8ECC118FE64DC0F4

Vòng 2
1.AddRoundKey:   8DA1D6261D2DB6F9C08FDE3405E9E6DDA1173B53E79A7201927BE4D92331B144
2.SubCells:      43FBAC835C2BCA7F0BC012A3B1405DBDFB663D858F2C2D1187BE698AB048E55B
```

```
3.MixWords:     17ABF4EE275C844C2E21B3BD37673BE89CF8E5FC23FC2BCA2CF55B928E120B48
4.AddRoundKey:  1B2B3ACA8C4D56D0B6E0A2CC284B85F2B42222C357FA59CE15A1825AD2CBBADD
5.SubCells:     4A79E4F01BA79905CA0256AEE888BF4C823E3E46A41D5E35D4FB62DA7B6C6FBD
6.XWord:        9CC70A3237F98EC41CBCB86CC4D6A88D5480D084884349F402458C185732787C

Vòng 3
1.AddRoundKey:  A23400B708E043620766 9B920B8BDD0DADD4E0D2AB890CE0A42C5DEA223BF060
2.SubCells:     56A3012EF1021FCF6160AF8751E6BD416AC6027B93D5A1023F95FFB63E3D0906
3.MixWords:     D7D4EC565C68A1B01E438548FADD5A93D413610D96868C9DC3C9EA8C72E238F4
4.AddRoundKey:  5E696BBEAAC23ECA379356DDFF8C554E0748B2589FC4DC888914B7B8F797D476
5.SubCells:     6B9BF5FCC99A86F0BBC499BD8B1B4D496136B9B3337468FDD5B52E97EAF8C616
6.XWord:        0F470E995297E3A2DF1862D81016281B05EA42D6A8790DAFB169D5F271F5A344

Vòng 4
1.AddRoundKey:  F70C9C447E235AF00F2ED7487DE0B8E0D5F5891B8CFE1059514800557EB60E74
2.SubCells:     EAA1D65BC3B0DA0981AA3936D9029702F337D54A1BB4005E3C36014DC3CA31FA
3.MixWords:     E98B60E28761A734018A964F93725E81ECFAC182B078143FFD88C88751ACC9AC
4.AddRoundKey:  46DBB6C9DA4C5A3181289D7B652561047B7042E56094C213B0CCB3BEAB34852A
5.SubCells:     EE20CAB755BCDA48A9E815BE59C276D1BE07F4EB069D9A9204AE7DFC93A3BF47
6.XWord:        13419CA9CCFC5304548943A0C082FF9D4366A2F59FDD13DEF9CF2BE20AE3360B

Vòng 5
1.AddRoundKey:  9CBB8C4137442515C81D70F20BAA3D038FACADE41C05D10A757BC9A2ADAE5A06
2.SubCells:     D6DB1B2ABB5BC2D4CB5C074C51C97EE1C0806A69CDB194C18CBEB7566AD7DA71
3.MixWords:     0482160E19295E9159E0EA68F4C9AE48A15006C74089E799B96D2C8C9C3E89CC
4.AddRoundKey:  E9E520E87FE6C4DA2AE8D87BC5DD7C8928C7E29BF394DF1976E2FB5C45536969
5.SubCells:     40EB0822455D745547224FBE28BDEFD5E853A5AF639DE73816A5527290859B9B
6.XWord:        B9D4B863DBA59376BE1DFFFFB64508F6116C15EEFD65001BEF9AE2330E7D7CB8

Vòng 6
1.AddRoundKey:  4D4503D6E85C1E9B3C03ED741C20A516C119A6C8601419F11DD73C9617A5CC16
2.SubCells:     A790E1AC22722FAF57E1C8FACD0875778D38B8CB06B538CE5C39574B6675AE77
3.MixWords:     496E42B1B04F0693B9C1EE430921F206787024C3C11371913DDC757843EDD668
4.AddRoundKey:  8FCF1C38EE923C9B37C2BCAFDA47F405F644E1E25A80BED43CF7E906DF03F276
5.SubCells:     C019CD659E8757AFBB9A44AD55C5D8B1255BD3A5DA0EFCC657EA4071E7E14C16
6.XWord:        C92BD779682A6861B2A85EB1A368E77F2C69C9B92CA3C3085ED85A6D114C73D8

AddRoundKey:    CF2F2C1008186A578FE5B45DBD154473940C2BEC5682CDF83A3564A72DB0161B

Bản mã:        CF2F2C1008186A578FE5B45DBD154473940C2BEC5682CDF83A3564A72DB0161B
```

A.2.2. Trường hợp khóa 384-bit

256-bit bản rõ:

```
u8 X[ 32] = {
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00,
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
      };
```

Khóa chính:

```
u8 MasterKey[ ] = {
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19,
```

```
            0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x22, 0x23,
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11
        };
```

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 0102030405060708090A0B0C0D0E0F111213141516171819 1A1B1C1D1E1F2223
K01: 35F234E762094BEF7F90057BA12E56DB20433885F9B4AD6F4C21BE29EF6F297D
K02: B0EF513AE689ADAF6887A142E4CDB35AB7BAFAFA82ED06F0450E5B7EE027ECA4
K03: 2C4C07A264BE2819A215173CF2CE25E75089327A607CE3FB2A0ABAAAAC3D3BDC
K04: A0B4380ABD7E8AEECB1B822E89F5A29E2C120E5D73846E855425AC84617F4E11
K05: 5A0B2120D46402B490F893E0DFB9C510CA5DD633E336BF798292CC653F96AD40
K06: 072C7AC69A1E9F1F060A5104EE5F6B92FC3FF8DF0A2E895A8CFD616B8BE38DD5
K07: E95745D944897593CCD2A65A38CE7E717475CDE189A2B24B253DDC387BAF2955
K08: 440362C7663017E46BC67A10F0AE315A42555EFBA21ED097EAB6A18BB97DBD41
K09: 91D39F3EA84C23EA105A504B3A99542D5221A1478562401A75C4D374C615A2C9
K10: 1F99B21A7E4E43DE1EB130A4764C1D57B62D2A5C4E4549CA8FC1138993AD0052
K11: 30B1180C9FB294B5011CBBB5725847AFC90EFA5A1C13A52AE3998A369EF0B31A
K12: 44176BBC496077BFFB06FFEBDCA009C85CBE4FE3478982430F13FEC2D8BAF0FD
K13: 71B03957A4C3FC8E51A59BE7572AA8BA004BEC9EB81588496C270FC7E7A96F8F
K_post: 33DAA26C488F2C679F520A4ABE8D86AB7CB1237403703C5B5338C97EBE42F97F
```

==========

256-bit trạng thái được cập nhật qua các vòng:

```
Vòng 1
1.AddRoundKey:  102030405060708090A0B0C0D0E0F011033127514371 6F9183B1A7D1C3F1DD23
2.SubCells:     00080F0C0A06070E030D040B05020910E148DD3C1F67BAB25AE5429446CEBDB0
3.MixWords:     CAD8632769B0D425B7CF228040572FDDFE4C43764014C861EB6CEB186F86CC57
4.AddRoundKey:  FF2A57C00BB99FCAC85F27FBE1797906DE0F7BF3B9A0650EA74D553180E9E52A
5.SubCells:     8B47A40B511333F0CB26DD52D3A2A2711281BE63130D593142A74D480E40EB47
6.XWord:        9B002E79CEEF1007DB6157204C5E818602C634118CF17AC652E0C73A91BCC8B0

Vòng 2
1.AddRoundKey:  2BEF7F432866BDA8B3E6F662A89332DCB57CCEEB0E1C7C3617EE9C44719B2414
2.SubCells:     797C451FE860301E7D5D25CF1EC4D068A6EF351431CDEFF2669ED65B67AF1CB5
3.MixWords:     61417A501052793E25C95D21A6952D5EE6DEA97BFF2A650BD994A0F577771057
4.AddRoundKey:  4D0D7DF274EC512787DC4A1D545B08B9B6579B019F5686F0F39E1A5FDB4A2B8B
5.SubCells:     A741D94CFA3A3CDD9C68735CE0C7F113CAA4AF1133993409635 0AB26207379E6
6.XWord:        359C776BF32DBCFC0EB5DD7BE9D0713258790136 3A8EB428F18D05012964F9C7

Vòng 3
1.AddRoundKey:  95284F614E533612C5AE5F556025D3AC746B0F6B490ADAADA5A8A985481BB7D6
2.SubCells:     6EE8D2764985F2E328D7264D06C2DE80FAF581F56DC1556A751E24BF364A2EAC
3.MixWords:     01A5338DBE47B14A3AAF587C88F2056626C593BAD0C182C4410C1411C0AC24E5
4.AddRoundKey:  5BAE12AD6A23B3FEAA57CB9C574BC076EC98458933F73DBDC39ED874FF3A89A5
5.SubCells:     C7D7E36A32B07DB4C9A46CD6A4880B163A7A90D529EA7E3046504FFA8BE4D575
6.XWord:        B58EB3F90686A053BBFD3C4590BED6F14823C0461DDCA3D734091F69BFD20892

Vòng 4
1.AddRoundKey:  B2A2C93F9C983F4CBDF76D417EE1BD63B41C389917F22A8DB8F47E0234318547
2.SubCells:     B956B79FD67A9FBC30EA842AC3D330A882CD65E9664C474397D8C391A348BFC5
3.MixWords:     6706C9C343940B94A684CC7FE7771BE4BD4151F2644EFE71C301942FD12C42AC
4.AddRoundKey:  8E518C1A071D7E076A566A25DFB96595C9349C13EDEC4C3AE63C4817AA836BF9
5.SubCells:     783C1BAB615CC361329932C2E713596EB7A3D692C83ABCE45D573666C95AF57F
6.XWord:        D86DD236E67310F592C8FB5F603C8AFA17F21F0F4F156F70FD06FFFB4E7526EB
```

```
Vòng 5
1.AddRoundKey:  9C6EB0F180430711F90E814F9092BBA055A741F4ED0BBFE717B05E70F7089BAA
2.SubCells:     D6ED04CE0E1F61107F31A9D20387DB0D4D422AD8C851588F66046B07EAF1AFC9
3.MixWords:     B5ED57810CCD2D56589A6EEBBAE4C9D9FA9527E5E3F686264B2DD2D76A168844
4.AddRoundKey:  243EC8BFA4810EBC48C03EA0807D9DF4A8B486A26694C63C3EE901A3AC032A8D
5.SubCells:     1C86CB583FA93144360B860D0ED915D81E82456609DDF57864011EC80E14743
6.XWord:        AEC9A3B7EEA58DCC8444EEE2DFD5A950ACCD5CB9B19163DF340F790351EDFBCB

Vòng 6
1.AddRoundKey:  B15011AD90EBCE129AF5DE46A999B4071AE076E5FFD42A15BBCE6A8AC240FB99
2.SubCells:     E50A106A031435E32C3712EE24E98261AB0216EB8BC647D4DB35328E9A0C52E9
3.MixWords:     1CCDDA0CAB634412CF84A78BBBB496CB64553B2F61EA3A974121616BD3DC6964
4.AddRoundKey:  2C7CC20034D1D0A7CE981C3EC9ECD164AD5BC1757DF99FBDA2B8EB5D4D2CDA7E
5.SubCells:     95EF9A01A3940542357ACD86B73A944E6AC78D8CD97F3330569714FFA79555C3
6.XWord:        092A54F5C9D0F2BDA9BF0372DD7E63B1F6024378B33BC4CFCA52DA0BCDD1A23C

Vòng 7
1.AddRoundKey:  4D3D3F4980B0850252B9FC9901DE6A79AABC0C9BF4B2468CC54124C9156B52C1
2.SubCells:     A77E9F6D0E04BF911813F9E9111232A2C944A1AFD8B9EE1B282A1CB7D4F5188D
3.MixWords:     8C4DA67CBA8D63474412D951D1010413513DD5DEBCCE5F4F0F9974C4AC29ED17
4.AddRoundKey:  FDFD9F2B1E4E9FC915B742B6862BACA95176394004DBD70663BE7B034B808298
5.SubCells:     969633792F4933B7D42EF4CA347980243C16CC0CD1203971A8FCBEE1880E627A
6.XWord:        40C486276D57DB2F027C4194766768BCEA447952933ED1E97EAE0BBFCA108AE2

AddRoundKey:    731E244B25D8F7489D2E4BDEC8EAEE1796F55A26904EEDB22D96C2C17452739D

Bản mã: 731E244B25D8F7489D2E4BDEC8EAEE1796F55A26904EEDB22D96C2C17452739D
```

A.2.3. Trường hợp khóa 512-bit

256-bit bản rõ:

```
u8 X[32] = {
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00,
            0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88,
            0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x00
      };
```

Khóa chính:

```
u8 MasterKey[ ] = {
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19,
            0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x22, 0x23,
            0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08,
            0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x11,
            0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19,
            0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x22, 0x23
      };
```

Khóa vòng nhận được qua lược đồ khóa:

```
K00: 0102030405060708090A0B0C0D0E0F1112131415161718191A1B1C1D1E1F2223
K01: 0DFA1AFCF24D9EA6B8474CEF0CE50882B04E558844923E7AA7345C12635F0FDA
K02: 88E77F2176CD78E6AF50E8D64906ED0327B797F73FCB95E5AE1BB9456C17CA03
K03: FADF391182528BDA63D44334982F1C8F1662CBD79C2E80604988D1EAC0883849
```

```
K04: 82F06BA656B8E8BFBD4872135B02FCBA87220A3D363DE740F0479A7995945A84
K05: 25836B891DF51DD69E785DD16F94755D6C218481E5BBD08F198171C762DCDE7F
K06: AF71C99CAD941146323BC475F55F60DFBB0F3E64BD2CC2C30EBDBDDF04903C15
K07: 3CEF690AF2854AB37A3DC5555FD46D2F5F0317E4CCA38F3430B422F765069B41
K08: 0193618B0F9951A56F606764733FF303E7782E20AB39386FE69EC472B8518398
K09: 7F1BF79313C8D09ACBB887D89F7E089A5BD630C3AE236155C7B085BD647AAC3A
K10: 1E1EFEA70626C728C704C66A16093572CF3A0DFED543E93DF76DA4860C77D161
K11: 14C16E06F4B2201E95C46CC5109FD24F59B1A0AFB2F9151196EC27ECB80F1309
K12: BC10EB16E662D7D75B9D7558AD3512B898E08432289B258CCED26E04E85A9CF4
K13: 5357BB918766EE5DD44EB514C5A982031FEA67AFB2BFE9B005F07F9E0CDCE853
K14: C47B3ABD145394EDF720AD2B74636F1F8033C7D5B59A0B1394280D4BFC871F82
K15: 2CA2C80D745DBF608D6A1C0B50B978498718FCFA35A128301E94DFDEF182EEDC
K_post: 780C0C2578E27FE79523DFD66CC414DA21A81FB050A370C9E4F2E4364DE3D644
==============
256-bit trạng thái được cập nhật qua các vòng:
Vòng 1
1.AddRoundKey:  102030405060708090A0B0C0D0E0F011033127514371 6F9183B1A7D1C3F1DD23
2.SubCells:     00080F0C0A06070E030D040B05020910E148DD3C1F67BAB25AE5429446CEBDB0
3.MixWords:     CAD8632769B0D425B7CF228040572FDDFE4C43764014C861EB6CEB186F86CC57
4.AddRoundKey:  C72279DB9BFD4A830F886E6F4CB2275F4E0216FE0486F61B4C58B70A0CD9C38D
5.SubCells:     533EA220AF96735A81FDEDBABCB9DD26499177B4D134254ABCB32EC1A18A4643
6.XWord:        74DFB4CFCC07BE2FA61CFB55DF2810536E70615BB2A5E83F9B52382EC21B8B36

Vòng 2
1.AddRoundKey:  FC38CBEEBACAC6C9094C1383962EFD5049C7F6AC8D6E7DDA3549816BAE0C4135
2.SubCells:     F9656C9E6FF0DFB721BC925A4BAA960A6D53258043EDD9551A6DA9F5D7A12A1A
3.MixWords:     33CD1BC938C59FDA49B2B53271A98441F67368F7AE0DF4D8F5D197C9A69BC337
4.AddRoundKey:  C91222D8BA9714002A66F606E98698CEE011A320322374B8BC5946236613FB7E
5.SubCells:     B7E33E4F6FF8B5014760257140347A350210EC08D0B0FA97445EEEB0609252C3
6.XWord:        012E27C9F016D261F1AD3CF7DFDA1D55B4DDF58E4F5E9DF7F293F736FF7C35A3

Vòng 3
1.AddRoundKey:  83DE4C6FA6AE3ADE4CE54EE484D8E1EF33FFFFB379637AB702D46D4F6AE86F27
2.SubCells:     5A12BCBAB8D7E412BCEB4969274FD37C298B8B7DA2A8982E91C684D23222BADD
3.MixWords:     B5A2AB397E56D75302F5A7BBD2671C85498783415591F3A4E674EAFC793A7AAF
4.AddRoundKey:  9021C0B063A3CA859C8DFA6ABDF369D825A607C0B02A232BFFF59B3B1BE6A4D0
5.SubCells:     035F0B04A8ECF0BFD6431D3230639B4FC2B8610B0447B0798B37AF3D4A5D3F05
6.XWord:        9FCCD3047E7914334AD0C532E6F67FC35E2BB90BD2D254F517A4773D9CC8DB89

Vòng 4
1.AddRoundKey:  30BD1A98D3ED057578EB014713A91F1CE524876F6FFE96361919CAE29858E79C
2.SubCells:     0F30AB7ADEC8B18C541411C59224FECDEB1C9CBABAB44BF23838F0A57AB38FD6
3.MixWords:     CA02F497E08CCF92BBC8D31B364884A028AB3924613A634725D41642824221DD
4.AddRoundKey:  F6ED9D9D12098521C1F5164E699CE98F77A82EC0AD99EC73156034B5E744BA9C
5.SubCells:     25C81515E321BF5F8D3777499BD640C0701EAA0B6AE93A3BD406A3A68F5B6FD6
6.XWord:        292F7EE47E64152D81D01CB80693EAB27CF9C1FAF7AC9049D8E1C857121EC5A4

Vòng 5
1.AddRoundKey:  28BC1F6F71FD4488EEB07BDC75AC19B19B81EFDA5C95A8263E7F0C25AA4F463C
2.SubCells:     E844FEBA67965BFD9E04BE688C8038E5AFA97C55726E1E838645A1C2C9D2EE57
3.MixWords:     A856D95AB77C159204A040A6D09E482D2468B886034BC01856721A7CB4424934
4.AddRoundKey:  D74D2EC9A4B4C508CF18C77E4FE040B77FBE8845AD68A14D91C29FC1D038E50E
5.SubCells:     39A7AAB73F8228F1198953C3D2020C2E45FCFD906ADCFBA7B29A338D0565EB31
6.XWord:        EEEF9DDEBDBB1CB8CEC164AA503B386792B4CAF9E8E5CFEE65D204E4875CDF78
```

```
Vòng 6
1.AddRoundKey:  F0F16379BB9DDB9009C5A2C046320D155D8EC7073DA626D392BFA0628B2B0E19
2.SubCells:     09CEA8A2DB1520032128560BEED041D4FF7853617EB883DE87580DCFE6793138
3.MixWords:     F407A9D34E0211DD207BFD9EB74CF9C5F1E1E1D2F7D028D966E40F487E076686
4.AddRoundKey:  E0C6C7D5BAB031C3B5BF915BA7D32B8AA850417D45293DC8F00828A4C608758F
5.SubCells:     02DF53F36F044846A658B2C742DE798E1E0A2AD990F67ECB09F1E83FDFF18CC0
6.XWord:        B1A370210DD98B85152491152003BA4DAD76090BF22BBD08BA8DCBEDBD2C4F03

Vòng 7
1.AddRoundKey:  0DB39B37EBBB5C524EB9E44D8D36A8F535968D39DAB09884745FA5E95576D3F7
2.SubCells:     417DAFBB14DB7218491369A743F21E371A4B43CC55047A27FA2675404D16DEEA
3.MixWords:     F23119C44FE4A2D7435FFC2B0F34D344FBE3A2B3C00028FFDBB4CBADD96E9788
4.AddRoundKey:  A166A255C8824C8A9711493FCA9D5147E409C51C72BFC14FDE44B433D5B27FDB
5.SubCells:     FB60564DCB62BC8EF8106D9FF0153CC5692128CD2D588DD2125B8229F3B94520
6.XWord:        836AC77B2EF4F437801AFCA91583747C112BB9FBC8CEC56B6A51131F162F0D99

Vòng 8
1.AddRoundKey:  4711FDC63AA760DA773A518261E01B6391187E2E7D54CE78FE791E54EAA8121B
2.SubCells:     C51096DFE442065570E43C6276024AA8B289C3AAD9E03554B4A22FE0B61EE34A
3.MixWords:     8A32DEC2C642AF1C84B33F9094A8C0D8CE9A48D4A38C61B7530A30659342A1B6
4.AddRoundKey:  A69016CFB21F107C09D9239BC411B8914982B42E962D49874D9EEFBB62C04F6A
5.SubCells:     B8037719B9FE00EF218AB0AF741097B26D6282AA4B2B6D9CA7507CDBCF0BD232
6.XWord:        EBB84EDEF030281C723189683DDEBF413ED9BB6D02E5456FF4EB451C86C5FAC1

AddRoundKey:    93B442FB88D257FBE71256BE511AAB9B1F71A4DD524635A61019A12ACB262C85

Bản mã: 93B442FB88D257FBE71256BE511AAB9B1F71A4DD524635A61019A12ACB262C85
```

Thư mục tài liệu tham khảo

[1] Tiêu chuẩn quốc gia TCVN 11367-1:2016: Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 1: Tổng quan

[2] Cuong Nguyen, Anh Nguyen, Phong Trieu, Long Nguyen, and Lai Tran. *Analysis of a new practically secure SPN-based scheme in the Luby-Rackoff model*. in *The 9th International Conference on Future Data and Security Engineering*. 2022. Springer.

[3] Cuong Nguyen, Nam Tran, and Long Nguyen. *FLC: A New Secure and Efficient SPN-Based Scheme for Block Ciphers*. in *2022 9th NAFOSTED Conference on Information and Computer Science (NICS)*. 2022. IEEE.

[4] Tran Sy Nam, Nguyen Van Long, and Nguyen Bui Cuong. *An Optimized Bit-Slice Implementation of Secure 8-Bit Sbox Based on Butterfly Structure*. in *2023 15th International Conference on Knowledge and Systems Engineering (KSE)*. 2023. IEEE.

[5]. Bui Cuong Nguyen and Tuan Anh Nguyen, *Evaluating pseudorandomness and superpseudorandomness of the iterative scheme to build SPN block cipher*. Journal of Science and Technology on Information security, 2017. **40**(2): p. 40.

[6]. Trần Sỹ Nam, Nguyễn Văn Long, and Nguyễn Bùi Cương, *Xây dựng tầng tuyến tính có cài đặt hiệu quả cho mã khối 128-bit có cấu trúc FLC*, *Hội thảo nghiên cứu ứng dụng mật mã và an toàn thông tin*, Học viện Kỹ thuật mật mã, Hà nội, năm 2022.

[7]. Tran Sy Nam, Nguyen Van Long, and Nguyen Bui Cuong, *Đề xuất tầng tuyến tính và đánh giá khả năng cài đặt trong xây dựng mã khối 256-bit có cấu trúc FLC*. Tạp chí Khoa học và Công nghệ trong lĩnh vực An toàn thông tin, 2(16) 2023, 31-38. https://doi.org/10.54654/isj.v1i16.920.