VỀ MỘT THUẬT TOÁN MÃ HÓA XÁC THỰC HIỆU NĂNG CAO

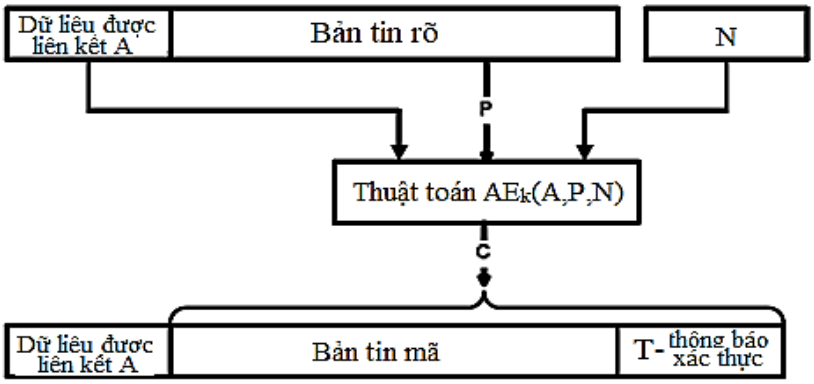
Nguyễn Thị Thu Nga*, Nguyễn Trường Thắng, Trần Mạnh Đông, Nguyễn Hoài Nam

Tóm tắt: *Trong thời đại công nghệ 4.0 đang phát triển mạnh mẽ, tội phạm mạng cũng trở nên tinh vi hơn. Tin tặc có thể dễ dàng phá vỡ các biện pháp bảo mật và truy cập được dữ liệu cá nhân nhạy cảm. Mặt khác, các cấu trúc mã hóa xác thực được sử dụng trong nhiều năm qua dựa trên các thuật toán mã khối đối xứng ngày càng bộc lộ nhiều hạn chế về hiệu năng, tốc độ xử lý do số lượng thông tin cần được xử lý và số lượng thông tin cần xác thực ngày càng nhiều. Bài báo trình bày một thuật toán mã hóa xác thực hiệu năng cao dựa trên thiết kế kiểu song công (duplex) với các tham số bảo mật thích hợp, sử dụng phép hoán vị có thể sử dụng để bảo vệ thông tin với các độ mật và thông tin có các mức độ nhạy cảm khác nhau.*

Từ khóa: Thuật toán mật mã; Mã hóa xác thực; Giải mã; Cấu trúc song công.

1. MỞ ĐẦU

Mã hóa xác thực (Eng. Authenticated Encryption) được thiết kế để đảm bảo tính bí mật, tính xác thực của một bản tin.Quá trình mã hóa xác thực (hình 1), bản rõ *P* kết hợp với khóa *K* được chuyển thành bản mã *C* có chứa mã xác thực *T*. Dữ liệu được liên kết *A* là dữ liệu bổ sung tùy chọn không được mã hóa mà chỉ được xác thực - mã xác thực *T* phụ thuộc vào các tham số trên. Nếu kết quả của quá trình giải mã có xác thực, dựa trên bản mã *C* sử dụng cùng một khóa *K*, hoặc chúng ta sẽ nhận được bản rõ *P* hoặc một thông báo: **"Lỗi"**, cho biết nguồn dữ liệu không chính xác và thiếu tính toàn vẹn.



Hình 1. *Sơ đồ hoạt động của thuật toán mã hóa xác thực AE.*

Bài toán mã hóa xác thực được quan tâm đầu tư nghiên cứu từ lâu. Sự phát triển của các lược đồ mã hóa xác thực liên quan chặt chẽ đến kết quả của cuộc thi NIST nhằm chọn ra chuẩn mã hóa AES mới. Quá trình lựa chọn thuật toán Rijndael và chấp thuận sử dụng thay thế cho DES đòi hỏi phải đánh giá các phương pháp mã khối hiện tại với các tham số của tiêu chuẩn mã hóa mới. Do đó, việc cập nhật các phương pháp hiện được sử dụng và phát triển các phương pháp mã hóa mới, bao gồm cả những phương pháp mã hóa có xác thực là một nhu cầu cấp thiết.

2. XÂY DỰNG THUẬT TOÁN MÃ HÓA XÁC THỰC DỰA TRÊN THUẬT TOÁN MÃ KHỐI

Thông thường để thực hiện mã hóa xác thực thường chọn trước thuật toán mã hóa và thuật toán xác thực thích hợp, sau đó, kết hợp sử dụng chúng. Phương pháp mã hóa xác thực loại này, được gọi là phương pháp mã hóa xác thực tổng quát và phương pháp này không phải lúc nào cũng an toàn [12]. Hơn nữa, nguyên tắc xây dựng Phương pháp mã hóa xác thực tổng quát thì mỗi khối thông tin phải được xử lý hai lần: lần đầu thực hiện chức năng mã hóa và lần thứ hai

thực hiện chức năng xác thực, điều này làm cho các cấu trúc thực hiện phương pháp mã hóa xác thực tổng quát này thường bị chậm và đôi khi không xác định được rõ ràng thứ tự gọi các hàm trên cho thông điệp rõ *M* để có được một lược đồ mã hóa xác thực an toàn. Có thể chia ra ba phương pháp:

MtE: MAC then Encrypt (*Xác thực xong mới mã hóa*). Đầu tiên, thực hiện hàm MAC xác thực cho thông điệp rõ *M* bằng cách sử dụng khóa *K*1 nhận được mã thông báo xác thực $T = MAC_{K1}(M)$, và sau đó mã hóa cặp (*M.T*) bằng khóa *K*2, tạo ra bản mã *C*.

EtM: Encrypt then MAC*(Mã hóa xong mới xác thực)*. Đầu tiên, thực hiện mã hóa thông điệp *M* bằng khóa *K*2 thu được bản mã *C*, sau đó tính mã thông báo xác thực cho thông điệp được mã hóa $T = MAC_{K1}(C)$, kết quả nhận được là một cặp (*C, T*).

E&M: Encrypt-and-MAC *(Mã hóa và xác thực)*. Mã hóa thông điệp M bằng khóa *K*2 thu được bản mã C và tính mã thông báo xác thực cho thông điệp $T = MAC_{K1}(M)$, kết quả thu được là một cặp (*C, T*).

Tất cả các phương pháp trên đều được thực hiện trong thực tế. Giao thức SSL/TLS thực hiện theo phương pháp MtE, IPSec xử lý thông điệp theo thứ tự EtM và SSH theo cấu trúc E&M. Phương pháp được chọn chỉ rõ trình tự của quá trình giải mã và xác thực: trong trường hợp của MtE và E&M, việc giải mã diễn ra trước, sau đó, xác thực và trong trường hợp EtM - xác thực trước, sau đó giải mã.

Giải pháp thay thế cho phương pháp mã hóa xác thực tổng hợp là sử dụng mật mã khối chuyên dụng một lần (ví dụ OeB, IAPM, IAeBC) [10], đạt được mục đích mã hóa xác thực trong quá trình xử lý một tin nhắn. Điều này đã thúc đẩy các nhà thiết kế tìm kiếm các giải pháp thỏa hiệp mới có thể được sử dụng rộng rãi. Các chế độ mã hóa hai lần xong mới xác thực (ví dụ: GCM, ewe, INK) [2, 11] đã được phát triển, mặc dù không nhanh như các lược đồ mã hóa một lần được đề cập ở trên, nhưng vẫn cải tiến được hiệu suất một cách đáng kể. Đặc biệt là các chế độ mã hóa xác thực mới (không giống như các phương pháp mã hóa xác thực tổng quát) chỉ sử dụng một khóa để mã hóa và xác thực tin nhắn.

Cùng với sự phát triển của các lược đồ mã hóa xác thực, xuất hiện nhu cầu đính kèm thêm dữ liệu liên quan vào một thông điệp đã được mã hóa và xác thực. Nhưng dữ liệu đính kèm này không cần mã hóa và chỉ cần được xác thực. Nhu cầu này đã khiến nhiều nhà thiết kế lược đồ mã hóa xác thực (AE) đưa dữ liệu liên quan làm đầu vào vào lược đồ của họ. Các loại lược đồ này được gọi là Mã hóa xác thực với dữ liệu liên kết - AEAD (Eng. Authenticated Encryption with Associated Data), lần đầu tiên được chính thức hóa bởi Rogaway [13] và trở thành một thách thức khi thiết kế các lược đồ mã hóa xác thực AE chuyên dụng.

Các lược đồ mã hóa xác thực được dùng trong mã khối đối xứng có độ dài block thông tin 128 bit. Độ dài của mã thông báo xác thực dữ liệu trong lược đồ mã hóa xác thực bị giới hạn bởi thuật toán mã khối đối xứng được sử dụng. Độ dài tối đa của mã thông báo xác thực giới hạn ở 128 bit bằng độ dài của khối dữ liệu đang được xử lý. Trong các ứng dụng bảo mật thông tin cơ chế mật mã này không đủ mạnh [4].

2.1. Thuật toán OCB

Thuật toán OCB (Offeet CodeBook) là một lược đồ mã hóa xác thực một lần được phát triển bởi Rogaway, Bellare và Black [14]. OCB là cách có thể đạt được mã hóa xác thực mà không cần sử dụng hai thuật toán khác nhau và không phải hai lần xử lý bản tin riêng biệt. Phép toán xử lý lại từng khối tin để xác thực nó có thể thay thế bằng phép toán XOR các khối bản rõ và sau đó mã hóa kết quả thu được. Để tránh khả năng tiết lộ thông tin bản rõ, trước tiên cần phải "làm trắng" các khối được tổng hợp. "Làm trắng" bằng cách thực hiện phép toán XOR của các khối bản rõ với một chuỗi giả ngẫu nhiên. OCB định nghĩa việc sử dụng một cấu trúc tính toán theo cặp cụ thể của một chuỗi giả ngẫu nhiên độc lập bao gồm phép nhân với một phần tử không đổi trong trường nhị phân hữu hạn GF (2^{128}) và tính toán theo mã Gray. Phương pháp này cho phép tính toán một

số giá trị trước và lưu trữ chúng trong một bảng, cho phép giảm thời gian tính toán trong quá trình hoạt động OCB. Thiết kế được đề xuất cũng làm cho OCB trở thành một chế độ một khóa (khác với các chế độ IACBC và IAPM trước đây). Các ưu điểm của chế độ OCB bao gồm:

• Mã hóa xác thực một lần;

• Chỉ sử dụng một khóa;

• Có khả năng tính toán song song, nhờ vào cấu trúc dựa trên chế độ sổ mã điện tử;

• Hiệu suất cao nhờ cứng hóa và lập trình.

Điểm yếu của phiên bản cơ bản của OCB là các header chỉ được xác thực nhưng không được mã hóa. Chế độ OCB đã được cấp bằng sáng chế, tuy nhiên, việc sử dụng còn bị hạn chế.

2.2. Phương pháp GCM

GCM (Galois/Counter Mode) [11] là phương pháp mã hóa xác thực hai lần được NIST khuyến nghị sử dụng. Phương pháp GCM đảm bảo tính bảo mật của các tin nhắn bằng cách sử dụng chế độ đếm CTR để mã hóa và xác thực tin nhắn và dữ liệu bổ sung bằng hàm băm phổ quát được xác định trên trường nhị phân hữu hạn Galois GF(2^{128}). Bản tin ở chế độ GCM được xử lý theo quy tắc "Mã hóa trước xác thực sau" (Encrypt-then-MAC). Điều này cho phép xác minh tính xác thực của dữ liệu ở phía nhận mà không cần phải giải mã trước. Các ưu điểm của GCM bao gồm:

• Đảm bảo tính bảo mật và xác thực của các thông điệp chỉ cần sử dụng một khóa;

• Minh bạch, dễ phân tích và triển khai xây dựng;

• Có khả năng xử lý dữ liệu trực tuyến;

• Hiệu suất phần cứng và phần mềm cao;

Trong triển khai phần cứng, thiết kế GCM cho phép tận dụng những ưu điểm của cấu trúc AES pipeline. Điều này làm cho GCM trở thành một trong những giải pháp tốt nhất cho các mạng có tốc độ IO Gbit/s và cao hơn. Hiệu suất của phần mềm thực hiện chức năng xác thực cũng rất cao nhờ sử dụng phương pháp bảng.

2.3. Phương pháp INK

Phương pháp mã hóa xác thực INK [15] là phương pháp hoạt động hai lần vừa đảm bảo tính bảo mật và xác thực của các thông điệp và cho phép xác thực dữ liệu thêm vào liên quan mà chưa được mã hóa. Phương pháp INK kết hợp các ưu điểm của lược đồ xác thực tin nhắn Carter-Wegman với mã hóa trong chế độ bộ đếm CTR. Những lợi thế chính của INK bao gồm:

• Thực hiện cả mã hóa và xác thực thông điệp rõ chỉ cần sử dụng thuật toán mã khối đối xứng, không cần hàm mã hóa tóm lược Hash;

• Có thể thực hiện tính toán song song;

• Chỉ sử dụng một khóa;

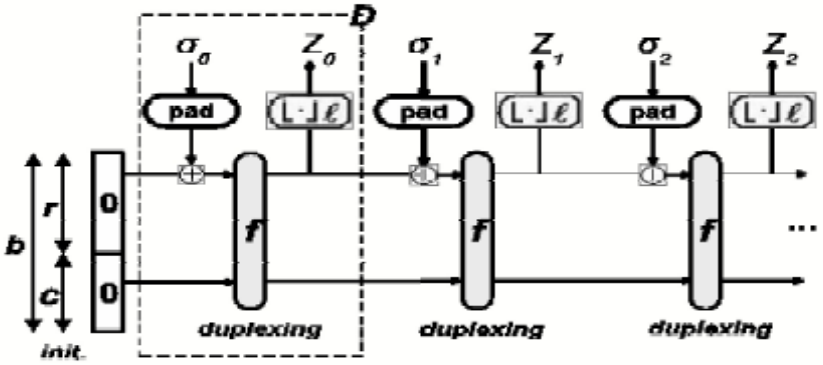
• Hiệu suất phần cứng và phần mềm cao.

Phương pháp INK thì mỗi một block thông tin được xử lý 2 lần theo kiểu đầu tiên xác thực và sau đó mã hóa, nhờ đó làm tăng độ an toàn và bí mật thông tin vì đối phương chặn thu chỉ thu được bản mã mà thôi.

3. CẤU TRÚC SONG CÔNG

Cấu trúc song công (hình 2), giống như cấu trúc sponge [4], sử dụng phép biến đổi với độ dài cố định hoặc hoán vị f hoạt động trên một số bit cố định b và quy tắc đệm "pad" để xây dựng lược đồ mật mã. Cấu trúc song công hoạt động dựa trên trạng thái $b = r + c$ bit. Giá trị b được gọi là độ rộng, giá trị r được gọi là tốc độ bit và giá trị c là dung lượng.

Các giá trị khác nhau của tốc độ bit và dung lượng mang lại sự cân bằng giữa tốc độ và bảo mật. Tốc độ bit cao hơn cho phép mã hóa nhanh hơn nhưng kém an toàn hơn. Quan trọng là c bit cuối cùng của trạng thái (b bit) không bao giờ bị tác động trực tiếp bởi các khối đầu vào và trong quá trình tạo ra đầu ra. Dung lượng c, tham số bảo mật quan trọng nhất, xác định mức độ bảo mật có thể đạt được của các cấu trúc. Cấu trúc song công tạo nên một object nhận một chuỗi bit đầu vào và tạo một chuỗi bit đầu ra phụ thuộc vào tất cả các đầu vào nhận được trước đó. Một dạng của cấu trúc song công (duplex object) ký hiệu là D như sau:



Hình 2. *Cấu trúc song công.*

Cấu trúc song công D có b bit trạng thái. Khi khởi tạo, tất cả các bit trạng thái được đặt về không (0). Khi đó, có thể gửi các kết nối D.duplexing(σ, ℓ), với σ là chuỗi bit đầu vào và ℓ xác định số lượng bit đầu ra nhất định. Số bit tối đa ℓ mà người ta có thể yêu cầu là r và chuỗi đầu vào phải đủ ngắn để sau khi thực hiện có được một khối r-bit duy nhất đầu ra duy nhất.

Cấu trúc song công có thể sử dụng để:

• Mã hóa xác thực một lần

• Bảo vệ an toàn khóa mã

Các cuộc tấn công phân tích mã vào các cấu trúc song công có thể được chia thành hai nhóm:

• Nhóm 1 là các cuộc tấn công vào tính không ngẫu nhiên, điểm yếu của hoán vị bên trong hoặc biến đổi ngẫu nhiên. Tấn công thám mã như vậy được xây dựng dựa trên các hàm (hoán vị hoặc biến đổi).

• Nhóm 2 là các cuộc tấn công vào thuật toán mật mã dựa trên cấu trúc sponge hoặc cấu trúc song công.

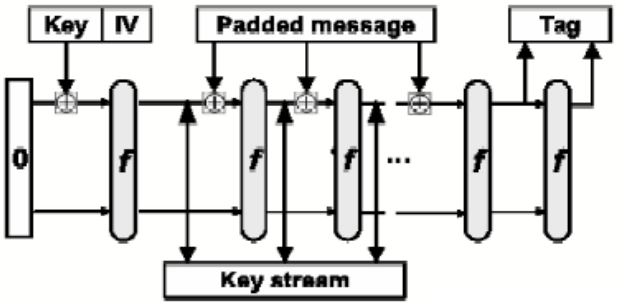
4. THUẬT TOÁN MÃ HÓA XÁC THỰC (AE) DỰA TRÊN CẤU TRÚC SONG CÔNG

Độ an toàn chứng minh được là một tính năng quan trọng của các thuật toán mật mã hiện đại. Các cấu trúc song công được [3] trình bày với các tham số an toàn thích hợp, sử dụng phép hoán vị tạo nên các thuật toán với độ an toàn chứng minh được.

Thuật toán mã hóa xác thực DuplexAE trình bày trong hình 3 sử dụng cấu trúc song công và là thuật toán một lần. Sau khi khởi tạo, thuật toán tích hợp khóa bảo mật K. Từ thời điểm này, có thể ứng dụng thuật toán mã hóa xác thực để bảo mật khóa mã hoặc để mở khóa. Chuỗi các khối đã được tạo dùng để mã hóa và đánh dấu mã xác thực (T) tùy thuộc vào khóa K và dữ liệu được tạo nên trước đó. Khóa sử dụng để mã hóa không tiết lộ bất kỳ thông tin nào liên quan đến mã đánh dấu xác thực. Mã xác thực và mã thông báo xác thực không tiết lộ trình tự mã hóa, vì trình tự mã hóa được thực hiện với các đối tượng song công (duplex) khác nhau.

Mã hóa xác thực là ví dụ về hàm song công được chuyển đổi thành hàm có khóa với khóa bí mật ở đầu vào của thuật toán mã hóa xác thực (AE). Hàm song công hoạt động giống như một

hàm ngẫu nhiên đối với bất kỳ ai không biết khóa bí mật nhưng có quyền truy cập vào hàm song công. Độ an toàn của hàm song công với khóa bí mật được trình bày trong hình 3.



Hình 3. *Thuật toán mã hóa xác thực dựa trên cấu trúc song công (Duplex AE).*

Các biểu thức toán học sau đây dùng cho thuật toán bảo vệ khóa dựa trên cấu trúc song công [3].

$$max\left\{\left(\frac{M^2}{2}+2M.N\right)2^{-c}, N.2^{-|K|}\right\} \quad (1)$$

Trong đó, tham số M là độ phức tạp của dữ liệu được xử lý, tức là số lần gọi thuật toán khóa, tham số N là số lần biến đổi được thực hiện bởi phép biến đổi (hoặc phép hoán vị) và $|K|$ là độ dài của khóa trong trường hợp điển hình, nếu $M \ll 2^{c/2}$ thì độ phức tạp tính toán bé hơn và bằng

$$min\left(\frac{2^{c-1}}{M}, 2^{|K|}\right) \quad (2)$$

Khóa bảo mật liên quan đến thông số dung lượng theo biểu thức sau:

$$|K| + 1 + log_2 M \leq c \quad (3)$$

Biểu thức trên cho thấy có thể giảm dung lượng c (số hoán vị được sử dụng) với một mức bảo mật nhất định hoặc để đạt được độ bảo mật cao hơn với một dung lượng cố định. Biểu thức cũng cho thấy với các thuật toán trên cho phép sử dụng các thuật toán nhanh, đơn giản (nghĩa là xây dựng thuật toán sử dụng các hoán vị với số lượng nhỏ hơn), đặc biệt ứng dụng cho các thiết bị (phần cứng) có tài nguyên hạn chế.

Thuật toán mã hóa xác thực một lần dựa trên cấu trúc song công đáp ứng các yêu cầu bảo mật để khôi phục khóa (xác suất khôi phục khóa K trong N lần thử nghiệm không lớn hơn$(N.2^{-|K|})$. Sử dụng cấu trúc song công rất an toàn vì khả năng giả mạo mã thông báo xác thực$\left(2^{-|T|}\right)$và khôi phục bản rõ $\left(N.2^{-|K|}\right)$ rất bé.

Mã hóa xác thực dựa trên cấu trúc song công mang lại những ưu điểm sau:

• Thực hiện thuật toán một lần;

• Chỉ yêu cầu một hoán vị hoàn hảo với độ lớn xác định không đổi;

• Mã hóa xác thực cho văn bản-text (chuỗi bit) cần thiết và chỉ xác thực các văn bản yêu cầu phải xác thực;

• Rất linh hoạt, vì có thể được lựa chọn độ dài của khối thông tin cần xử lý, miễn là tham số dung lượng c lớn hơn giới hạn an toàn xác định;

• Độ dài mã thông báo xác thực được giới hạn ở $c/2$ bit, dài hơn đáng kể so với các thuật toán mã hóa xác thực (AE) dựa trên mã khối.

Bảng 1 trình bày tổng hợp các thuộc tính của các lược đồ mã hóa xác thực được thực hiện dựa trên mật mã khối và thuật toán mã hóa xác thực AE dựa trên cấu trúc song công (duplex). Trong đó: độ an toàn của xác thực và độ bảo mật của thuật toán AE dựa trên thiết kế song công (duplex)

là lớn nhất. Dễ dàng lựa chọn các tham số cho thuật toán mã hóa xác thực dựa trên cấu trúc song công. Thuật toán mã hóa xác thực dựa trên cấu trúc song công có thể được sử dụng để bảo mật thông tin có độ mật cao, cũng như bảo mật thông tin với các mức độ nhạy cảm khác nhau.

Bảng 1. *So sánh các lược đồ mã hóa xác thực chọn lọc [15].*

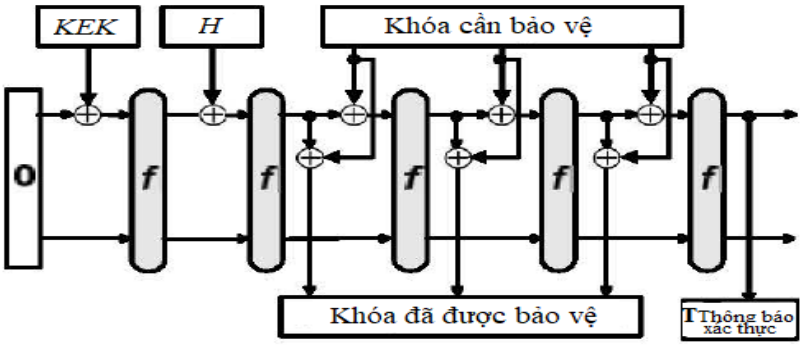
Thuật toán AE	OCB	GCM	INK	DuplexAE
Phương thức thực hiện	1. $A+E$	1. E 2. A	1.A 2.E	1. $A + E$
Độ an toàn Xác thực cực đại	2^{128}	2^{128}	2^{128}	$2^{c/2}$ $(2^{160}$-$2^{512})$
Độ bí mật cực đại	$(2^{128}$-$2^{255})$	$(2^{128}$-$2^{255})$	$(2^{128}$-$2^{255})$	$min(2^{c-60}, 2^{\|K\|})$ $(2^{160}$-$2^{512})$
Phương thức biến đổi	AES	AES	AES	Duplex r = {1152,1088,832,576} c = {448,512,768,1024}

5. BẢO MẬT KHÓA MẬT MÃ

Bảo mật của khóa mật mã (*Eng: Key wrapping*) là một ví dụ về việc sử dụng mã hóa xác thực. Một thuật toán như vậy đảm bảo tính bí mật và toàn vẹn của dữ liệu, đặc biệt cho các khóa mật mã hoặc các dữ liệu quan trọng. Thuật toán bảo mật khóa mã có độ dài bất kỳ nhờ sử dụng một khóa cụ thể để mã hóa khóa (*Eng: Key Encrypting Key - KEK*). Các thuật toán này là thành phần quan trọng của hệ thống quản lý khóa [8], đảm bảo tính bí mật và tính toàn vẹn của các khóa mật mã trong suốt thời gian vận chuyển và lưu trữ. Các thuật toán bảo mật khóa được xây dựng theo các chuẩn mật mã đã được phê duyệt.

Độ an toàn và độ an toàn chưa được chứng minh được trình bày trong ANSI X9.102, các thuật toán bảo vệ khóa (ví dụ: TDKW, AESKW) dựa trên mật mã khối thúc đẩy sự phát triển của thuật toán SIV (*Eng. the Synthetic Initialization Vector mode*), cũng dựa trên mật mã khối. Thuật toán này đã được chuẩn hóa trong *RFC 5297* như một phương thức hoạt động mới của thuật toán AES.

Thuật toán mã hóa xác thực dựa trên cấu trúc kiểu song công là một thuật toán bảo mật được chứng minh an toàn, không có các mối đe dọa. Ví dụ về sử dụng thuật toán mã hóa xác thực được trình bày trong hình 3 là thuật toán bảo mật khóa song công - DuplexKW được trình bày trong hình 4.



Hình 4. *Thuật toán đảm bảo an toàn gói khóa dựa trên cấu trúc kiểu duplex (DuplexKW).*

Trong thuật toán này, khóa được bảo mật có độ dài tùy ý được mã hóa bằng cách sử dụng khóa bảo vệ khóa (*Eng. KEK*). Nếu mỗi khóa cần bảo mật được liên kết với một số nhận dạng duy nhất thì chỉ cần thêm số nhận dạng đó vào khóa được bảo mật và sau đó mỗi khóa sẽ được mã hóa bằng một chuỗi mã khác, mặc dù sử dụng cùng một khóa bảo vệ khóa (*KEK*).

Đầu vào cho thuật toán bảo vệ khóa, được thể hiện trong hình 4, là khóa bảo vệ các khóa - KEK, mã định danh duy nhất của khóa H và bản rõ (khóa cần được bảo mật) có độ dài bất kỳ. Thực hiện thuật toán DuplexKW, ta có khóa bảo mật và mã xác thực của nó T. Trong quá trình giải mã khóa, đầu vào cho thuật toán DuplexKW là khóa dùng để bảo mật các khóa - *KEK*, mã định danh duy nhất H ở dạng mã hóa của khóa bảo mật trước đó và mã xác thực T. Trong quá trình giải mã, khóa được bảo mật được giải mã và kiểm tra tính toàn vẹn. Nếu mã thông báo xác thực nhận được và mã nhận dạng không khớp thì thông báo lỗi. Trường hợp ngược lại là khóa được giải mã và số nhận dạng H.

Bảng 2 trình bày thuộc tính của một số lược đồ bảo mật khóa được chọn dựa trên mật mã khối và thuật toán bảo mật khóa (hình 4) được thực hiện dựa trên phép biến đổi kiểu song công (duplex). Dễ dàng nhận thấy rằng độ an toàn của xác thực chỉ dựa trên các thuật toán mã khối là chưa đủ.

Bảng 2. *So sánh một số thuật toán được lựa chọn đảm bảo an toàn khóa mã [15].*

Thuật toán KW	TDKW	AESKW	SIV	duplexKW
Độ an toàn xác thực cực đại	2^{48}	2^{63}	2^{128}	$2^{c/2}$ (2^{160}-2^{512})
Độ mật cực đại	2^{112}	(2^{128}-2^{255})	(2^{128}-2^{255})	$min(2^{c-60}, 2^{\|K\|})$ c = {448,512,768,1024}
Phương pháp biến đổi	3DES	AES	AES	Duplex r = {1152,1088,832,576}, c = {448,512,768,1024}

Thuật toán bảo mật khóa dựa trên cấu trúc kiểu song công có tính linh hoạt trong việc lựa chọn các tham số. Có thể xác định mức độ an toàn có thể chứng minh được bằng cách chọn các thông số thích hợp của cấu trúc song công. Thuật toán này có thể được sử dụng để bảo vệ thông tin có độ mật cao, cũng như bảo vệ thông tin khác có mức độ nhạy cảm khác nhau.

6. KẾT LUẬN

Mã hóa xác thực thường được sử dụng trong các giao thức mật mã đảm bảo bí mật trong thương mại điện tử và các giao thức để bảo mật mạng không dây. Tuy nhiên, khi triển khai thực hiện các lược đồ mã hóa xác thực hiện có đòi hỏi có tốc độ thực hiện nhanh và lượng thông tin được xử lý, công suất mã hóa xác thực ngày càng cao. Vì vậy, cần có một lược đồ mã hóa xác thực mới, có thể trở thành một chuẩn, tương tự như các thuật toán AES hoặc SHA-3.

Cuộc thi CAESAR (*Competition for Authenticated Encryption: Security, Applicability and Robustness*) cho lược đồ mã hóa xác thực đã được tổ chức bởi cộng đồng các nhà nghiên cứu mật mã (đây không phải là một cuộc thi chính thức của NIST). Ban Giám khảo cuộc thi 22 thành viên, gồm các nhà mật mã học nổi tiếng như Joan Daemen, Lars R. Knudsen, Kaisa Nyberg và Vincent Rijmen. Cuộc thi nhằm chọn ra một hoặc nhóm các thuật toán mã hóa xác thực tốt nhất và các thuật toán đủ điều kiện tham gia các giai đoạn tiếp theo của cuộc thi trên cơ sở kết quả được xem xét công khai. Không chỉ ước tính độ an toàn của các thuật toán mã hóa xác thực chống lại các cuộc tấn công thám mã mà còn phải chứng minh về độ an toàn của chúng.

Các thuật toán mã hóa xác thực dựa trên cấu trúc song công với các tham số phù hợp được chứng minh là an toàn, hiệu quả. Cuộc thi CAESAR tạo nên một một sự thay thế việc xây dựng mã hóa xác thực dựa trên các thuật toán khối đối xứng.

Bảo mật khóa mật mã là một ví dụ thực tế của việc sử dụng mã hóa xác thực. Các thuật toán bảo mật được xây dựng bằng cách sử dụng cấu trúc song công với các lược đồ dựa trên mật mã khối, có độ xác thực cao hơn và linh hoạt hơn trong lựa chọn các tham số biến đổi.

Lời cảm ơn: *Bài báo này được hỗ trợ một phần bởi đề tài cơ sở (mã số CS20.10) Viện công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam.*

TÀI LIỆU THAM KHẢO

[1]. D. Stinson, Cryptography, *"Theory and Practice"*. CRC Press, LLC, 1995.

[2]. M. Bellare, C. Namprempre, "*Authenticated encryption: Relations among notions and analysis of thegeneńc composition paradigm, Journal of Cryptology*", vol. 21, no. 4, 2008.

[3]. G. Bertoni, J. Deamen, M. Peeters, G. Van Assche, "*Cryptographic sponge functions*", January 2015,http://sponge.noekeon.org.

[4]. M.Borowski, *"The sponge construction as a source of secure cryptographic primitives*", Military Cornmunication Conference, France, 2018.

[5]. M.Borowski, M. Leśniewicz, R. Wicik, MGrzonkowski, "*Generation of random keys for cryptographic systerns*", Annales UMCS lnformatica, AIXII, 3 (2016).

[6]. I. Dinur, O. Dunkelman, A Shamir, "*Self differential crypt analysis ofup to 5 rounds of SHA-3*",http://eprintiacr.org/2012/672.pdf.

[7]. M. Kutyłowski, WB. Strothmann, "*Lý thuyết mật mã và thực hành đảm bảo an toàn các hệ thống máy tính*", Nhà xuất bản Read Me, Warsawa 1998.

[8]. D. KKhovratovich, "*Keywrappingwith fixedpermutation*", http://eprint.iacr.org/2013/145.pdf.

[9]. V. Gligor, P. Donescu, "*Fast encryption and authentication: XCBC encryption and XECB authentication modes*", FSE 2012, LNCS 2355, Springer-V er lag, 2012.

[10]. M. Duan, X. Lai, "*Improved zero-sum distinguisher for full round K.eccak-fpermutation*", 2012,http://eprintiacr.org/ 2012/ 023.pdf.

[11]. NIST, "*Special Publication 800-38D, Recornmendationfor Błock Cipher Modes of Operation:Galois/Counter Mode (GCM) and GMAC*", 2009.

[12]. Jovanovic P., Luykx A., Mennink B, *"Beyond 2c/2 security in sponge-based authenticated encryption modes"*, http://eprint.iacr.org/2016/373.pdf.

[13]. P. Rogaway, "*Authenticated-encryption with associated-data*", ACM Conference on Computer and Cornmunications Security (CCS-9), ACM Press, 2005.

[14]. P. Rogaway, M. Bellare, J. Black, *"OCB: A block cipher mode of operation for efficient authenticated encryption*", ACM Transactions on lnformation and System Security, 2006.

[15]. R. Gliwa, "*Uwierzytelnione szyfrowanie wspecjalnych sieciach telekomunikacyjnych*", Rozprawadoktorska, Wojskowa Akademia Techniczna, WydziałElektroniki, 2016.

ABSTRACT

ABOUT A HIGH PERFORMANCE AUTHENTICATED ENCRYPTION ALGORITHM

In the rapidly growing era of technology 4.0, cybercrime is also becoming more sophisticated. Hackers can easily circumvent security measures and gain access to sensitive personal data. On the other hand, the authentication cipher structures used over the years based on symmetric block ciphers have increasingly revealed many limitations in performance, processing speed due to the amount of information that needs to be processed, and the amount of information be verified increasing. The paper presents a high-performance authentication encryption algorithm based on a duplex design with appropriate security parameters using permutations that can be used to protect information with a degree of confidentiality and information that has varying degrees of sensitivity.

Keywords: Encryption algorithm; Authenticated Encryption AE; Decryption; Duplex construction.

Nhận bài ngày 04 tháng 02 năm 2021
Hoàn thiện ngày 10 tháng 3 năm 2021
Chấp nhận đăng ngày 10 tháng 6 năm 2021

Địa chỉ: Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam.
*Email: thungalnt@gmail.com.