Một số phân tích an toàn về đặc điểm thiết kế của chế độ EME2

Nguyễn Tuấn Anh

Bài báo này phân tích về đặc điểm thiết kế của EME2. Các phân tích được đưa ra dựa vào sự cần thiết của các thành phần: hàm biến đổi dữ liệu liên kết, phép cộng XOR liên kết sự phụ thuộc các biến và phép mã hóa thêm vào khi đầu vào không chẵn khối. Ngoài ra, bài báo cũng đưa ra chứng minh tính không phân biệt được của hàm biến đổi dữ liệu liên kết với một họ hàm giả ngẫu nhiên. Từ đó, kết hợp với các kết quả đã có [4], bài báo cung cấp cho người đọc cách nhìn khá đầy đủ về đặc điểm thiết kế của EME2.

1. Giới thiệu

Mã hóa trong thiết bị lưu trữ có những đặc tính mà các chế độ mã hóa thông thường không đáp ứng được. Vì vậy, để đáp ứng trong môi trường này, mã khối tinh chỉnh được và các lược đồ mã hóa tinh chỉnh được đã đề xuất trong [1, 2] sử dụng một giá trị tinh chỉnh (còn được gọi là dữ liệu liên kết khi ám chỉ độ dài thay đổi) là một đầu vào bổ sung trong thủ tục mã hóa/giải mã mà không cần giữ bí mật. Việc mong muốn các phép biến đổi này là một phép biến đổi bảo toàn độ dài đã đặt ra các định nghĩa an toàn phù hợp. Khái niệm mạnh nhất cho độ an toàn của một phép biến đổi bảo toàn độ dài là không phân biệt được với hoán vị ngẫu nhiên trước tấn công lựa chọn bản mã (pseudorandom permutation under chosen ciphertext attack - prp-cca) được định nghĩa bởi Luby và Rackoff [3]. Sau đó Liskov [1] đã mở rộng thành độ an toàn không phân biệt được với hoán vị ngẫu nhiên tinh chỉnh được trước tấn công lựa chọn bản mã (tweakable pseudorandom permutation under chosen ciphertext attack - tprp-cca) cho lược đồ mã hóa tinh chỉnh được.

Các công trình liên quan.

Gần đây, một vài chế độ hiệu quả đảm bảo độ an toàn prp-tcca đã được mô tả bởi Halevi và Rogaway [2, 4] để sử dụng trong ứng dụng mã hóa ở mức độ sector. Tuy nhiên, chế độ này tồn tại một số hạn chế như: chỉ mã hóa được với thông điệp đầu vào có độ dài là bội của kích cỡ mã khối cơ sở n. Ngoài ra, chế độ CMC [2] có tính tuần tự (chỉ được chứng minh an toàn trong mô hình mà tất cả các thông điệp cùng độ dài), trong khi chế độ EME [4] chỉ hạn chế cho các thông điệp có độ dài tối đa là n^2 bit. Các nghiên cứu gần đây hướng tới mục tiêu loại trừ những hạn chế trên. Năm 2004, nhà khoa học Shai Halevi đã dựa trên EME đề xuất chế độ EME* có thể áp dụng cho thông điệp có độ dài gần như bất kỳ và đạt được độ an toàn prp-

tcca. Chế độ EME2-AES là một trường hợp đặc biệt của EME*, được khuyến cáo sử dụng trong môi trường lưu trữ bởi IEEE P 1619.2 có thể vận dụng cho các khối có độ dài hầu như bất kỳ, nhưng không ngắn hơn kích cỡ của mã khối cơ sở. Cấu trúc của EME2-AES bao gồm 2 tầng mã hóa ECB và một tầng trộn nhẹ, có tính song song hóa và được chứng minh là không thể phân biệt được với hoán vị ngẫu nhiên trước tấn công lựa chọn bản mã.

Bài báo này phân tích các đặc điểm thiết kế của EME2 trên cơ sở các phản ví dụ (nếu như không có các thành phần này thì sẽ dẫn đến một chế độ không an toàn). Ngoài ra, bài báo đã chứng minh Bổ đề 3 đã được phát biểu [5] về tính không phân biệt được của hàm biến đổi dữ liệu liên kết.

Nội dung bài báo chia làm 3 phần: Sau phần giới thiệu, Phần 2 nhắc lại một số khái niệm cơ bản và tóm tắt các kết quả an toàn của EME2 đã có. Phần 3 đưa ra các phân tích đánh giá độ an toàn trong thiết kế của chế độ EME2.

2. Một số khái niệm cơ bản

2.1. Lược đồ mã hóa tinh chỉnh được

Một lược đồ mã hóa tinh chỉnh được là một hàm $E: \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ trong đó $\mathcal{M} = \cup_{i \in I} \{0,1\}^i$ là không gian thông điệp (với tập chỉ số khác rỗng $I \in \mathbb{N}$) và $\mathcal{K} \neq \emptyset$ là không gian khóa và $\mathcal{T} \neq \emptyset$ là không gian giá trị tinh chỉnh. Yêu cầu đề ra: với mỗi $K \in \mathcal{K}$ và $T \in \mathcal{T}$ thì $E(K,T,\cdot) = E_K^T(\cdot)$ là một hoán vị bảo toàn độ dài trên $\mathcal{M}$. Hàm ngược của lược đồ mã hóa E là lược đồ giải mã $D = E^{-1}$, trong đó $X = D_K^T(Y)$ nếu và chỉ nếu $E_K^T(X) = Y$. Mã khối là trường hợp đặc biệt của lược đồ mã hóa tinh chỉnh được trong đó không gian thông điệp là $\mathcal{M} = \{0,1\}^n$ (với $n \geq 1$) và không gian giá trị tinh chỉnh là $\mathcal{T} = \{\mathcal{E}\}$ (chuỗi trống). Giá trị n được gọi là kích cỡ khối. Ký hiệu $\mathrm{Perm}(n)$ là tập các hoán vị trên $\{0,1\}^n$. Ký hiệu $\mathrm{Perm}^{\mathcal{T}}(\mathcal{M})$ là tập các hàm $\pi: \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ trong đó $\pi(T,\cdot)$ là một hoán vị bảo toàn độ dài.

2.2. Độ đo an toàn

Với một lược đồ mã hóa tinh chỉnh được $E: \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$, xét lợi thế của kẻ tấn công A (truy vấn (T,M) hoặc (T,C)) có trong việc phân biệt E và hàm ngược của nó với một hoán vị ngẫu nhiên tinh chỉnh được và hàm ngược:

$$\mathrm{Adv}_E^{\mathrm{prp-tcca}}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}: A^{E_K(\cdot,\cdot),E_K^{-1}(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\pi \xleftarrow{\$} Perm^{\mathcal{T}}(\mathcal{M}): A^{\pi(\cdot,\cdot),\pi^{-1}(\cdot,\cdot)}\right].$$

Ký hiệu $X \xleftarrow{\$} \mathcal{X}$ có nghĩa rằng chọn X ngẫu nhiên từ tập hữu hạn $\mathcal{X}$. Ký hiệu $\mathrm{Perm}^{\mathcal{T}}(\mathcal{M})$ là tập các hàm $\pi: \mathcal{T} \times \mathcal{M} \to \mathcal{M}$, trong đó $\pi(T,\cdot)$ là một hoán vị bảo toàn độ dài. $\mathrm{Perm}(n)$ là tập các hoán vị trên $\{0,1\}^n$.

Không mất tính tổng quát, giả sử rằng kẻ tấn công không bao giờ lặp lại các truy vấn mã hóa, không lặp lại các truy vấn giải mã, không truy vấn lại các giá trị đã trả về trước đó. Những truy vấn như vậy được xem là vô nghĩa, vì kẻ tấn công biết được đáp án mà anh ta sẽ nhận được.

Khi $\mathcal{R}$ là danh sách các năng lực và $\mathrm{Adv}^{\mathrm{xxx}}_{\Pi}(A)$ được định nghĩa, $\mathrm{Adv}^{\mathrm{xxx}}_{\Pi}(\mathcal{R})$ là giá trị lớn nhất của $\mathrm{Adv}^{\mathrm{xxx}}_{\Pi}(A)$ trên tất cả kẻ tấn công A mà sử dụng năng lực tối đa là $\mathcal{R}$. Năng lực là thời gian chạy t, số truy vấn lên bộ tiên tri q và độ phức tạp truy vấn (query complexity) σ_n (trong đó $n \geq 1$). Độ phức tạp truy vấn là tổng số khối n-bit trong tất cả truy vấn mà kẻ tấn công thực hiện (bao gồm cả dữ liệu và dữ liệu liên kết). Độ phức tạp truy vấn của truy vấn (T, P) là $\lceil |T|/n \rceil + \lceil |P|/n \rceil$ và độ phức tạp truy vấn của một tấn công là tổng các độ phức tạp của tất cả lần truy vấn. Tên gọi tóm tắt (t, q, σ_n) là rõ ràng để biết được năng lực muốn đề cập là gì.

2.3. Chế độ EME2

Chế độ EME2-AES chính là một trường hợp đặc biệt sử dụng mã khối cơ sở là AES của EME*, được đề xuất bởi Shai Halevi [5] dành cho mã khối cơ sở bất kỳ vào năm 2004. Mô tả của EME* có thêm một số biến trung gian so với EME2-AES, sự xuất hiện của các biến này sẽ làm cho việc chứng minh an toàn thuận lợi hơn (để thống nhất ta sẽ gọi chung là EME2). Xét một mã khối $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Khi đó EME2$[E]$:$(\mathcal{K} \times \{0,1\}^{2n}) \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ là một chế độ mã hóa với dữ liệu liên kết, trong đó $\mathcal{K}$ có kích thước như của mã khối cơ sở E, $\mathcal{T} = \{0,1\}^{0..n(2^n-3)}$ và $\mathcal{M} = \{0,1\}^{n..n(2^n-2)}$. Nói cách khác, khóa cho EME2$[E]$ bao gồm một khóa K của mã khối cơ sở E và hai khối n-bit, L và R. EME2$[E]$ chấp nhận các thông điệp có độ dài bất kỳ lớn hơn hoặc bằng n (nhưng không lớn hơn $n(2^n - 2)$) và dữ liệu liên kết có độ dài bất kỳ (nhưng không lớn hơn $n(2^n - 3)$). Rõ ràng, trong thực tế các giới hạn trên xem như không có giới hạn nào cả.

Hàm $H_{K,R}(T_1 \cdots T_{l-1}, T_l)$: // $|T_1| = \cdots = |T_{l-1}| = n, 0 < |T_l| \leq n$

1 **if** T là chuỗi trống **return** $E_K(R)$

2 **for** $i \in [1..l-1]$ **do** $TTT_i \leftarrow E_K(2^i R \oplus T_i) \oplus 2^i R$
3 **if** $|T_l| = n$ **then** $TTT_l \leftarrow E_K(2^l R \oplus T_l) \oplus 2^l R$
4 **else** $|TTT_l| \leftarrow E_K\big(2^{l+1} R \oplus (T_l 10..0)\big) \oplus 2^{l+1} R$

5 **return** $TTT_1 \oplus \cdots \oplus TTT_l$	
Thuật toán $\boldsymbol{E}_{K,L,R}(T; P_1 \cdots P_m)$	**Thuật toán** $\boldsymbol{D}_{K,L,R}(T; C_1 \cdots C_m)$
// $\lvert P_1\rvert = \cdots = \lvert P_{m-1}\rvert = n, 0 < \lvert P_m\rvert \le n$	// $\lvert C_1\rvert = \cdots = \lvert C_{m-1}\rvert = n, 0 < \lvert C_m\rvert \le n$
01 **if** $\lvert P_m\rvert = n$ **then** $lastFull \leftarrow m$ 02 **else** $lastFull \leftarrow m - 1$ 03 $PPP_m \leftarrow P_m$ đệm với 10..0	01 **if** $\lvert C_m\rvert = n$ **then** $lastFull \leftarrow m$ 02 **else** $lastFull \leftarrow m - 1$ 03 $CCC_m \leftarrow C_m$ đệm với 10..0
04 **for** $i \leftarrow 1$ **to** $lastFull$ **do** 05 $PP_i \leftarrow 2^{i-1}L \oplus P_i$ 06 $PPP_i \leftarrow E_K(PP_i)$ 07 $SP \leftarrow PPP_2 \oplus \cdots \oplus PPP_m$ 08 $MP_1 \leftarrow PPP_1 \oplus SP \oplus H_{K,R}(T)$ 09 **if** $\lvert P_m\rvert = n$ **then** $MC_1 \leftarrow E_K(MP_1)$ 10 **else** $MM \leftarrow E_K(MP_1)$ 11 $MC_1 \leftarrow E_K(MM)$ 12 $C_m \leftarrow P_m \oplus$ (chặt cụt MM) 13 $CCC_m \leftarrow P_m$ đệm với 10..0 14 $M_1 \leftarrow MP_1 \oplus MC_1$	04 **for** $i \leftarrow 1$ **to** $lastFull$ **do** 05 $CC_i \leftarrow 2^{i-1}L \oplus C_i$ 06 $CCC_i \leftarrow E_K^{-1}(CC_i)$ 07 $SC \leftarrow CCC_2 \oplus \cdots \oplus CCC_m$ 08 $MC_1 \leftarrow CCC_1 \oplus SC \oplus H_{K,R}(T)$ 09 **if** $\lvert C_m\rvert = n$ **then** $MP_1 \leftarrow E_K^{-1}(MC_1)$ 10 **else** $MM \leftarrow E_K^{-1}(MC_1)$ 11 $MP_1 \leftarrow E_K^{-1}(MM)$ 12 $P_m \leftarrow C_m \oplus$ (chặt cụt MM) 13 $PPP_m \leftarrow P_m$ đệm với 10..0 14 $M_1 \leftarrow MP_1 \oplus MC_1$
15 **for** $i = 2$ **to** $lastFull$ **do** 16 $j = \lceil i/n \rceil, k = (i-1) \bmod n$ 17 **if** $k = 0$ **then** 18 $MP_j \leftarrow PPP_i \oplus M_1$ 19 $MC_j \leftarrow E_K(MP_j)$ 20 $M_j \leftarrow MP_j \oplus MC_j$ 21 $CCC_i \leftarrow MC_j \oplus M_1$ 22 **else** $CCC_i \leftarrow PPP_i \oplus 2^k M_j$	15 **for** $i = 2$ **to** $lastFull$ **do** 16 $j = \lceil i/n \rceil, k = (i-1) \bmod n$ 17 **if** $k = 0$ **then** 18 $MC_j \leftarrow CCC_i \oplus M_1$ 19 $MP_j \leftarrow E_K^{-1}(MC_j)$ 20 $M_j \leftarrow MP_j \oplus MC_j$ 21 $PPP_i \leftarrow MP_j \oplus M_1$ 22 **else** $PPP_i \leftarrow CCC_i \oplus 2^k M_j$
23 $SC \leftarrow CCC_2 \oplus \cdots \oplus CCC_m$ 24 $CCC_1 \leftarrow MC_1 \oplus SC \oplus H_{K,R}(T)$ 25 **for** $i \leftarrow 1$ **to** $lastFull$ **do** 26 $CC_i \leftarrow E_K(CCC_i)$ 27 $C_i \leftarrow CC_i \oplus 2^{i-1}L$	23 $SP \leftarrow PPP_2 \oplus \cdots \oplus PPP_m$ 24 $PPP_1 \leftarrow MP_1 \oplus SP \oplus H_{K,R}(T)$ 25 **for** $i \leftarrow 1$ **to** $lastFull$ **do** 26 $PP_i \leftarrow E_K^{-1}(PPP_i)$ 27 $P_i \leftarrow PP_i \oplus 2^{i-1}L$
28 **return** $C_1 \cdots C_m$	28 **return** $P_1 \cdots P_m$

Hình 1. Lược đồ mã hóa và giải mã của E=EME2[E]

Hình 1 mô tả Lược đồ mã hóa và giải mã của E=EME2[E]. Trong đó $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ là một mã khối. Dữ liệu liên kết có độ dài bất kỳ $T \in \{0,1\}^*$, bản rõ là $P = P_1 \cdots P_m$ và bản mã là $C = C_1 \cdots C_m$.

2.4. Độ an toàn của chế độ EME2

Năm 2004, tính không phân biệt của EME2 đã được Shai Halevi làm rõ.

Định lý 1 [5]. Mọi kẻ tấn công phân biệt EME2[Perm(n)] với một hoán vị ngẫu nhiên tinh chỉnh được bảo toàn độ dài, sử dụng nhiều nhất q truy vấn với không quá σ_n khối (một số trong đó có thể là không chẵn khối) có lợi thế nhiều nhất là $(3\sigma_n + 3q)^2/2^{n+1}$. Sử dụng ký hiệu trong Phần 1, ta có:

$$\mathrm{Adv}^{\mathrm{prp-tcca}}_{\mathrm{EME2[Perm(n)]}}(q, \sigma_n) \leq \frac{(2.5\sigma_n + 3q)^2}{2^{n+1}}.$$

Hệ quả 1 ([5]). Cố định $n, t, q, \sigma_n \in \mathbb{N}$ và một mã khối $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Khi đó

$$\mathrm{Adv}^{\mathrm{prp-tcca}}_{\mathrm{EME2}[E]}(t, q, \sigma_n) \leq \frac{(2.5\sigma_n + 3q)^2}{2^{n+1}} + 2\mathrm{Adv}^{\mathrm{prp-cca}}_{E}\left(t', 2q + \left(2 + \frac{1}{n}\right)\sigma_n\right)$$

trong đó $t' = t + O(n\sigma_n)$.

Chế độ EME2 là sự phát triển của EME, kế thừa những đặc tính tốt và loại bỏ những hạn chế mà chế độ cũ còn tồn tại. Việc vẫn sử dụng phép mã hóa trong tầng trộn giữa như của EME (biến $MC_1 = E_K(MP_1)$ - bước 09) là cần thiết cho độ an toàn của thuật toán EME2. Điều này được chỉ ra tương tự như phân tích của trường hợp thuật toán EME [4] (trang 6-7). Hơn nữa, EME2 thêm phép mã hóa đối với các khối P_{in+1} (dòng 16-21) là để áp dụng cho các bản rõ có độ dài khối lớn hơn $n + 2$. Nếu không sử dụng cách thức này thì EME2 sẽ trở thành EME và khi đó độ dài thông điệp sẽ bị hạn chế. Trong [4] đã đưa ra tấn công phân biệt cho EME2 khi độ dài khối lớn hơn $n + 2$ (trang 7-8). Tuy nhiên vẫn còn một số thành phần khác được bổ sung trong EME2 chưa được phân tích cụ thể.

3. Một số phân tích an toàn về đặc điểm thiết kế của chế độ EME2

Phần này lý giải một số lựa chọn thiết kế được sử dụng EME2 bằng cách đưa ra chứng minh an toàn hoặc chỉ ra rằng nếu thiếu chúng thì sẽ dẫn đến một chế độ không an toàn.

3.1. Sự cần thiết của hàm $H_{K,R}$

Chế độ EME2 xây dựng một hàm $H_{K,R}$ từ mã khối E để băm dữ liệu liên kết, từ giá trị đầu vào T có độ dài bất kỳ ta thu được một chuỗi n-bit T^*. Đầu tiên là một số phân tích ban đầu về hàm $H_{K,R}$.

Nếu kẻ tấn công có thể điều khiển được giá trị T^*, khi đó thực hiện 2 truy vấn (T^1, P) và (T^2, P) sao cho $T^{1^*} = T^{2^*}$ thu được C^1 và C^2. Trong trường hợp kẻ tấn công được sử dụng bộ tiên tri là EME2 thì luôn có $C^1 = C^2$. Trong trường hợp kẻ tấn công được sử dụng bộ tiên tri là một hoán vị ngẫu nhiên tinh chỉnh được thì $C^1 = C^2$ với xác suất $1/2^{|P|}$. Hàm $H_{K,R}$ trong thuật toán là cần thiết để không cho kẻ tấn công có thể kiểm soát được giá trị T^*. Dưới đây thực hiện phân tích hàm $H_{K,R}$ để thấy rõ hơn điều này, chú ý rằng $H_{K,R}$ sử dụng phép mã hóa chính là $E_K(2^i R \oplus T_i) \oplus 2^i R$ đối với khối thứ i.

- Nếu trong phép mã hóa trên không có khóa R thì $T^* = \bigoplus_i E_K(T_i)$. Khi đó kẻ tấn công dễ dàng chọn $T^1 \neq T^2$ sao cho các khối trong mỗi giá trị này là giống nhau sẽ tạo ra được $T^{1^*} = T^{2^*} = 0$.
- Nếu không có sự tham gia của khóa R bên trong hàm mã hay cụ thể hơn là: $TTT_i = E_K(T_i) \oplus 2^i R$. Khi đó, kẻ tấn công sẽ chọn $T^1 = TT$ và $T^2 = T'T'$ thì $T^{1^*} = T^{2^*} = 2R \oplus 4R$.
- Nếu không có sự tham gia của khóa R bên ngoài hàm mã hay cụ thể hơn là: $TTT_i = E_K(2^i R \oplus T_i)$. Trong trường hợp kẻ tấn công được truy vấn giải mã thì sẽ bị lộ khóa R và điều khiển được T^*.

Hơn nữa, khi thay thế phép tính $E_K(T \oplus jR) \oplus jR$ bằng phép tính $f_j(T)$, trong đó với mỗi j có một hàm ngẫu nhiên độc lập $f_j: \{0,1\}^n \to \{0,1\}^n$ thì có sai khác không đáng kể đối với cách nhìn của kẻ tấn công. Cụ thể, với $n, q_p, q_f \in \mathbb{N}$ cố định và một kẻ tấn công truy cập vào ba bộ tiên tri $A^{E(\cdot),D(\cdot),F(\cdot,\cdot)}$, xét hai thí nghiệm sau đây:

- Trong thí nghiệm thứ nhất (Expr1), chọn ngẫu nhiên một hoán vị π trên $\{0,1\}^n$ và một chuỗi $R \in \{0,1\}^n$. Sau đó, với $x, y, j \in \{0,1\}^n$ và $j \neq 0$, bộ tiên tri $E(x)$ trả lời $\pi(x)$, bộ tiên tri $D(y)$ trả lời $\pi^{-1}(y)$ và bộ tiên tri $F(j, x)$ trả lời $\pi(x \oplus jR) \oplus jR$ (trong đó phép nhân jR trên trường $GF(2^n)$).
- Trong thí nghiệm thứ hai (Expr2), ta chọn ngẫu nhiên một hoán vị π trên $\{0,1\}^n$ và 2^n hàm $\{f_j: \{0,1\}^n \to \{0,1\}^n\}_{j \in \{0,1\}^n}$. Sau đó, với $x, y, j \in \{0,1\}^n$ và $j \neq 0$, bộ tiên tri $E(x), D(y)$ trả lời lần lượt là $\pi(x), \pi^{-1}(y)$, bộ tiên tri $F(j, x)$ trả lời $f_j(x)$.

Trong [5] đã phát biểu mối quan hệ giữa cách nhìn trong hai thí nghiệm trên với sự sai khác là $\frac{q_f(q_f+2q_p)}{2^n}$ (xem Lemma 3 [5]). Tuy nhiên, tác giả lại không đưa ra chứng minh hay chỉ dẫn nào cho khẳng định này. Sau khi nghiên cứu các tài liệu có liên quan, chúng tôi phát biểu và chứng minh bổ đề sau.

Bổ đề 1. Với $n, q_p, q_f \in \mathbb{N}$ cố định. Với mọi kẻ tấn công $A^{E(\cdot),D(\cdot),F(\cdot,\cdot)}$ như trên thực hiện nhiều nhất q_p truy vấn lên E và D, nhiều nhất q_f truy vấn lên F, thì ta có:

$$\left|\Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1] - \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1]\right| \leq \frac{q_f(q_f + 4q_p)}{2^n}.$$

Chứng minh. Giả sử rằng kẻ tấn công sẽ không thực hiện các truy vấn vô nghĩa (lặp lại truy vấn, mã hóa rồi giải mã và ngược lại). Hình 2 mô tả game để chứng minh Bổ đề 1. Trong đó, game C1 bao gồm phần in đậm mô tả cho thí nghiệm Expr1, game C2 không có phần in đậm mô tả cho thí nghiệm Expr2.

Khởi tạo
1. $R \xleftarrow{\$} \{0,1\}^n$, $S \leftarrow \{0,1\}^n$, $T \leftarrow \{0,1\}^n$, for $x \in \{0,1\}^n$ do $\pi(x) \leftarrow$undefined

Trả lời truy vấn

Với truy vấn lên bộ tiên tri E
2. If $x \in$Domain(π) then bad$\leftarrow$true, **return** $\boldsymbol{\pi(x)}$
3. $y \leftarrow S$
4. If $y \in$Range(π) then bad$\leftarrow$true, $\boldsymbol{y \leftarrow \overline{\mathbf{Range}}(\pi)}$
5. $\pi(x) \leftarrow y$, $S \leftarrow S - \{y\}$,$T \leftarrow T - \{x\}$, return y

Với truy vấn lên bộ tiên tri D
6. If $y \in$ Range(π) then bad$\leftarrow$true, **return** $\boldsymbol{\pi^{-1}(y)}$
7. $x \leftarrow T$
8. If $x \in$ Domain(π) then bad$\leftarrow$true, $\boldsymbol{x \leftarrow \overline{\mathbf{Domain}}(\pi)}$
9. $\pi^{-1}(y) \leftarrow x, T \leftarrow T - \{x\}, S \leftarrow S - \{y\}$, return x

Với truy vấn lên bộ tiên tri F
10. If $x \oplus jR \in$ Domain(π) then bad$\leftarrow$true, **return** $\boldsymbol{\pi(x \oplus jR) \oplus jR}$
11. $z \leftarrow \{0,1\}^n$
12. If $z - jR \in$Range(π) then bad$\leftarrow$true, $\boldsymbol{z - jR \leftarrow \overline{\mathbf{Range}}(\pi)}$
14. $\pi(x \oplus jR) \leftarrow z - jR$, return z.

Hình 2. Game sử dụng trong chứng minh Bổ đề 1

Xét với Game C1: trong thủ tục trả lời truy vấn cho bộ tiên tri E thực hiện kiểm tra xem có phải x trong tập xác định của π hay không. Nhắc lại rằng, giả sử kẻ tấn công không thực hiện các truy vấn vô nghĩa, nhưng việc kiểm tra là cần thiết bởi vì

giá trị của x có thể đã xuất hiện trước đó trong các truy vấn lên bộ tiên tri F với chuỗi $x \oplus jR$. Nếu truy vấn của kẻ tấn công không nằm trong tập xác định của π thì sẽ chọn ngẫu nhiên một phần tử y trong tập S. Tuy nhiên có thể giá trị của y đã thuộc vào miền giá trị của π. Mặc dù, luôn loại bỏ khỏi S bất kỳ giá trị trả về nào trong thủ tục trả lời truy vấn bộ tiên tri E hoặc các giá trị truy vấn lên bộ tiên tri D, nhưng điều này vẫn có thể xảy ra vì miền giá trị của π còn được bổ sung khi truy vấn lên bộ tiên tri F. Tương tự ta có với bộ tiên tri D. Với bộ tiên tri F, đầu tiên kiểm tra xem $x \oplus jR$ có thuộc tập xác định của π hay không. Nếu đúng thì trả về $\pi(x \oplus jR) \oplus jR$, ngược lại chọn ngẫu nhiên z từ tập $\{0,1\}^n$. Tuy nhiên, giá trị $z - jR$ này có thể đã thuộc miền giá trị của π. Nếu điều này xảy ra ta chọn $z - jR$ ngẫu nhiên từ $\overline{\text{Range}}(\pi)$. Nhận thấy rằng, Game C1 mô tả đúng quá trình trả lời truy vấn trong Expr1. Vì vậy $\Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1] = \Pr[A^{C1} \Rightarrow 1]$.

Xét đến Game C2: thực hiện xóa các phần bôi đen của Game C1. Chứng minh rằng Game C2 mô tả chính xác quá trình trả lời truy vấn trong Expr2. Với truy vấn lên bộ tiên tri E và D, Game C2 trả về giá trị được chọn ngẫu nhiên từ $\{0,1\}^n$ những đã được loại trừ các truy vấn cũng như các câu trả lời trước đó của hai bộ tiên tri này. Với truy vấn lên bộ tiên tri F, khi được truy vấn (x, j), thì luôn trả về một giá trị được chọn ngẫu nhiên từ tập $\{0,1\}^n$. Do đó, $\Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1] = \Pr[A^{C2} \Rightarrow 1]$.

Gọi sự kiện *bad* xảy ra là B. Chú ý rằng Game C1 và Game C2 là giống nhau cho đến khi sự kiện *bad* xảy ra. Khi đó: $\Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1|\overline{\text{B}}] = \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1|\overline{\text{B}}]$ và $\Pr_{\text{Expr1}}[\text{B}] = \Pr_{\text{Expr2}}[\text{B}]$.

$$\left| \Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1] - \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1] \right|$$

$$= \Big| \Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1|\overline{\text{B}}] \cdot \Pr_{\text{Expr1}}[\overline{\text{B}}] + \Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1|\text{B}] \cdot \Pr_{\text{Expr1}}[\text{B}]$$
$$- \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1|\overline{\text{B}}] \cdot \Pr_{\text{Expr2}}[\overline{\text{B}}] - \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1|\text{B}] \cdot \Pr_{\text{Expr2}}[\text{B}] \Big|$$

$$= \left| \Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1|\text{B}] \cdot \Pr_{\text{Expr1}}[\text{B}] - \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1|\text{B}] \cdot \Pr_{\text{Expr2}}[\text{B}] \right|$$

$$\leq \left| \Pr_{\text{Expr2}}[\text{B}] \left(\Pr_{\text{Expr1}}[A^{E,D,F} \Rightarrow 1|\text{B}] - \Pr_{\text{Expr2}}[A^{E,D,F} \Rightarrow 1|\text{B}] \right) \right| \leq \Pr_{\text{Expr2}}[\text{B}]$$

Để chặn xác suất $\Pr_{\text{Expr2}}[\text{B}]$, giả sử rằng q'_p và q''_p là số truy vấn lần lượt lên bộ tiên tri E và D, khi đó $q_p = q'_p + q''_p$.

Đầu tiên xét xác suất xảy ra *bad* của dòng 2. Lưu ý rằng *bad* chỉ xảy ra ở dòng 2 khi một truy vấn x của kẻ tấn công lên bộ tiên tri E trùng với một truy vấn $x' + j'R$ nào đó lên bộ tiên tri F. Tuy nhiên, điều này chỉ xảy ra với xác suất không vượt quá $q'_p q_f / 2^n$. Xác suất xảy ra *bad* của dòng 4 khi giá trị y trả về trùng với một giá trị trả về $z' - j'R$ nào đó mà kẻ tấn công đã truy vấn lên bộ tiên tri F. Xác suất xảy ra điều này cũng không quá $q'_p q_f / 2^n$. Đối với xác suất xảy ra *bad* của dòng 6 và dòng 8 đều là $q''_p q_f / 2^n$. Cuối cùng, xét sự kiện *bad* tại bộ tiên tri F. Ở dòng 10 xác suất xảy ra *bad* khi $x + jR$ trùng với $x' + j'R$ hoặc x'' nào đó trong tập xác định của π được định nghĩa trong hai bộ tiên tri trước. Khi đó, xác suất xảy ra *bad* là không vượt quá $\frac{q_f^2}{2^{n+1}} + \frac{q_f q_p}{2^n}$. Đối với dòng 12, sự kiện *bad* xảy ra khi $z - jR$ trùng với $z' - j'R$ nào đó đã được truy vấn trước hoặc $z - jR$ thuộc tập S. Khi đó xác suất xảy ra *bad* sẽ không vượt quá $\frac{q_f q_p}{2^n} + \frac{q_f^2}{2^{n+1}}$.

Từ các lập luận trên ta có $\Pr_{\text{Expr2}}[\text{B}] \leq \frac{2q'_p q_f}{2^n} + \frac{2q''_p q_f}{2^n} + \frac{q_f^2}{2^{n+1}} + \frac{q_f q_p}{2^n} + \frac{q_f q_p}{2^n} + \frac{q_f^2}{2^{n+1}} = \frac{q_f(q_f + 4q_p)}{2^n}$. ■

3.2. Sự cần thiết của phép cộng XOR trong biến trung gian SP, SC

Trong thuật toán mã hóa EME2 (tương tự cho giải mã) biến $SP = \sum_{i=2} PPP_i$ hay $SC = \sum_{i=2} CCC_i$ để làm cho giá trị bản mã phụ thuộc tất cả bản rõ. Không mất tính tổng quát, giả sử rằng $SP = \sum_{i=3} PPP_i$, điều này có nghĩa là SP không phụ thuộc vào P_2 hay M_1 không phụ thuộc vào P_2. Nếu kẻ tấn công thực hiện hai truy vấn (T, P^1) và (T, P^2) với P^1 giống P^2 ngoại trừ khối thứ 2, thì sẽ thu được bản mã là C^1 và C^2 với C^1 giống với C^2 ngoại trừ khối thứ hai trong trường hợp sử dụng bộ tiên tri EME2.

3.3. Phân tích trường hợp không chẵn khối

Có một lưu ý rằng $C_m = P_m \oplus (\text{chặt cụt } MM)$, nếu không có MM thì giả sử MM được thay thế bởi MP_1 (đối với MC_1 chứng minh tương tự nhưng cho chiều giải mã), khi đó $C_m = P_m \oplus (\text{chặt cụt } MP_1)$. Do P_m và C_m công khai nên kẻ tấn công có thể dễ dàng biết được $MP_1 = \sum_i PPP_i \oplus T^*$ (thêm một vài phép thử). Ta có kịch bản như sau: đầu tiên kẻ tấn công truy vấn (T^1, P) và (T^2, P) và thu được

MP_1^1 và MP_1^2. Sau đó, kẻ tấn công tiếp tục thực hiện truy vấn (T^1, P') và (T^2, P') thu được $MP_1'^1$ và $MP_1'^2$. Trong trường hợp sử dụng bộ tiên tri EME2, thì $MP_1^1 \oplus MP_1^2 = T^{1^*} \oplus T^{2^*} = MP_1'^1 \oplus MP_1'^2$. Như vậy, đối với các bản rõ không chẵn khối thì cần phải thực hiện thêm một bước mã hóa (biến $MM = E_K(MP_1)$).

4. Kết luận. Bài báo đã thực hiện phân tích sự cần thiết của các thành phần trong thiết kế của EME2 như: hàm xử lý giá trị liên kết $H_{K,R}$, sự phụ thuộc của các biến trung gian SP, SC, bước mã hóa thêm vào trong trường hợp đầu vào không chẵn khối. Ngoài ra, bài báo còn đưa ra chứng minh cho Bổ đề 1 (Lemma 3 [5]) liên quan đến tính không phân biệt được của hàm $H_{K,R}$ với một họ hàm được lựa chọn ngẫu nhiên.

Tài liệu tham khảo

1. Liskov, M., R.L. Rivest, and D. Wagner, *Tweakable block ciphers*, in *Advances in Cryptology - CRYPTO 2002*. 2002, Springer. pp. 31-46.
2. Halevi, S. and P. Rogaway, *A tweakable enciphering mode*, in *Advances in Cryptology-CRYPTO 2003*. 2003, Springer. pp. 482-499.
3. Luby, M. and C. Rackoff, *How to construct pseudorandom permutations from pseudorandom functions.* SIAM Journal on Computing, 1988. 17(2): pp. 373-386.
4. Halevi, S. and P. Rogaway. *A parallelizable enciphering mode*. in *Cryptographers' Track at the RSA Conference*. 2004. Springer.
5. Halevi, S. *EME*: Extending EME to handle arbitrary-length messages with associated data*. in *International Conference on Cryptology in India*. 2004. Springer.