ĐỀ XUẤT CÁC GIAO THỨC DH-KE AN TOÀN VÀ HIỆU QUẢ

Nguyễn Thanh Sơn[1], Lều Đức Tân[2*], Đặng Vũ Sơn[3]

Tóm tắt: *Trong bài báo, các tác giả đã phân tích, đánh giá về mức độ an toàn và hiệu quả của một số giao thức thỏa thuận khóa theo giao thức Diffie-Hellman như: giao thức Arazi, giao thức Harn, giao thức Phan, giao thức Liu-Li và một số sửa đổi cho các giao thức Harn và giao thức Phan để đạt được tính an toàn quá khứ hoàn toàn. Bài báo cũng đề xuất cải tiến giao thức Arazi, giao thức Liu-Li để tăng tính an toàn và hiệu quả.*

Từ khóa: Giao thức DH-KE; HFS; PFS; Giao thức Arazi; Giao thức Phan; Giao thức Harn; Giao thức Liu-Li,...

1. ĐẶT VẤN ĐỀ

Một trong những tiêu chuẩn an toàn quan trọng nhất cho giao thức thỏa thuận khóa đó là "tiêu chuẩn an toàn phía trước" được cho bởi định nghĩa sau:

Định nghĩa 1. (tiêu chuẩn an toàn phía trước)

- Nếu khóa bí mật dài hạn của một bên bị lộ thì các khóa phiên được tạo ra trước đó cũng không tìm ra được thì giao thức được gọi là "*an toàn quá khứ một phía*" (HFS: Half Forward Secrecy).
- Nếu khóa bí mật dài hạn của cả hai bên bên bị lộ thì các khóa phiên được tạo ra trước đó cũng không tìm ra được thì giao thức được gọi là "an toàn quá khứ hoàn toàn" (PFS: Perfect Forward Secrecy).

1.1. Đối tượng và nội dung khảo sát

Đối tượng được xem xét gồm 4 giao thức thỏa thuận khóa theo giao thức Diffie-Hellman kết hợp với lược đồ chữ ký số DSA, bao gồm giao thức Arazi [1], giao thức Harn [2], giao thức Phan [4] và giao thức của Jie Liu và Jianhua Li [3].

Về mặt an toàn: Đầu tiên, chúng tôi xem xét lại các đánh giá của các tác giả trên về giao thức của mình và của người khác. Kết quả thu được trong lĩnh vực này là kết luận: "Tự đánh giá của Phan là chưa đúng". Thực chất giao thức Phan chỉ là HFS chứ không phải PFS. Tiếp theo chúng tôi đưa ra một sửa đổi đơn giản cho hai giao thức Harn (vốn không là HFS) và Phan (chỉ là HFS) để đạt được tính PFS. Chúng tôi cũng nghiên cứu đề xuất một giao thức cải tiến dựa trên giao thức Azari để đạt được tính an toàn và hiệu quả.

Về mặt hiệu quả: Xuất phát từ thực tế là: "***Các phần việc trong một giao thức luôn được thực hiện trên hai thiết bị tính toán độc lập***" chính vì thế mà nhiều phần việc có thể thực hiện đồng thời trên những thiết bị tính toán khác nhau đó. Công việc tiếp theo của chúng tôi là "giao việc" cho các bên tham gia giao thức một cách hợp lý để thu được các giao thức mới hiệu quả hơn.

1.2. Một số ký hiệu và kết quả đơn giản

$t_m(n)$ là chi phí trung bình cho một phép nhân rút gọn theo modulo n.

t_{exp} là chi phí trung bình cho một phép tính $a^e \bmod p$ với $e < q$.

$t_{inv}(n)$ là chi phí trung bình cho một phép tính $a^{-1} \bmod n$.

t_H là chi phí trung bình cho một phép tính hàm $H: \{0,1\}^\infty \to \{0,1\}^h$.

t_{DSAVer} là chi phí cho một phép kiểm tra (r, s) có là chữ ký hợp lệ của người có tham số công khi y lên thông báo M theo lược đồ DSA.

Một số quy đổi: Dựa vào các phương pháp karatsuba và bình phương-nhân, ta có các qui đổi sau: $t_m(2n) = 3 \times t_m(n)$; $t_{exp} = 1.5 \times \log_2(q) \times t_m(p)$.

1.3. Lược đồ chữ ký DSA

Tham số miền (p, q, g), trong đó, p, q là hai số nguyên tố với $q \mid p - 1$ và $g \in GF^*(p)$ thỏa mãn ord(g) = q; Tập các thông báo: $\{0,1\}^\infty$;

Hàm tóm lược thông báo: H: $\{0,1\}^{\infty} \to \{0,1\}^{l}$, *l* được gọi là độ dài tóm lược;

Tham số mật của người ký: x ∈ (0, q);

Tham số công khai của người ký: $y = g^x \bmod p$.

Chữ ký lên thông báo M của người có tham số mật x là cặp $(r,s) \in (0,q)^2$, ký hiệu là *DSASig*(M, x), như một hàm được xác định theo thuật toán sau:

Thuật toán 1. (Tạo chữ ký DSA)

Input: M, x. Output: *DSASig*(M, x). 1. $k \in_R (0,q)$. 2. $r \leftarrow (g^k \bmod p) \bmod q$; if (r = 0) then goto 1.	3. $h \leftarrow H(M)$. 4. $s \leftarrow k^{-1}(h + xr) \bmod q$; if $(s = 0)$ then goto 1. 5. Return (r, s).

Việc chấp nhận (r, s) là chữ ký lên thông báo M của người có tham số công khai y là thông báo thuộc tập {"*Accept*", "*Reject*"}, ký hiệu là *DSAVer*(M, (r, s), y), như một hàm được xác định theo thuật toán sau:

Thuật toán 2. (Kiểm tra chữ ký DSA)

Input: M, (r, s), y. Output: *DSAVer*(M, (r, s), y). 1. If $(r,s) \notin (0,q)^2$ tren return "*Reject*". 2. $w \leftarrow s^{-1} \bmod q$. 3. $h \leftarrow H(M)$.	4. $u \leftarrow h.w \bmod q$. 5. $v \leftarrow r.w \bmod q$. 6. $r' \leftarrow (g^u.y^v \bmod p) \bmod q$. 7. If (r' = r) then return "*Accept*". 8. Else return "*Reject*".

Từ thuật toán 2 ta có: $t_{DSAVer} = t_{inv}(q) + t_H + 2t_m(q) + t_m(p) + 2t_{exp}$ (1)

2. ĐÁNH GIÁ MỨC ĐỘ AN TOÀN CHO MỘT SỐ GIAO THỨC

2.1. Giao thức Arazi và các phân tích

2.1.1. Giao thức Arazi

Năm 1993 Arazi là người đầu tiên đề xuất giao thức trao đổi khóa bằng cách tích hợp giao thức DH-KE với lược đồ DSA (xem [1]). Việc mô tả giao thức cho trong hình sau:

Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$	
A giữ tham số mật x_A.	B giữ tham số mật x_B.
Bước 1. *A tạo thông tin thỏa thuận, ký lên đó rồi truyền cho B.*	
A.1 $v \in_R (0,q)$. A.2 $R_A = g^v \bmod p$. A.3 $r_A = R_A \bmod q$. A.4 $e_A = H(R_A)$. A.5 $s_A = v^{-1}(e_A + x_A r_A) \bmod q$. A.6 Send (R_A, s_A) to B.	
Bước 2. *B xác thực (R_A, s_A) là của A. Nếu chấp nhận A, B tạo thông tin thỏa thuận, ký lên đó rồi truyền cho A.*	
	B.1 $r_A = R_A \bmod q$. B.2 If $DSA_{Ver}(R_A, (r_A, s_A), y_A) = "Reject"$ then break protocol. B.3 $w \in_R (0,q)$. B.4 $R_B = g^w \bmod p$.

	B.5 $r_B = R_B \bmod q$. B.6 $e_B = H(R_B)$. B.7 $s_B = w^{-1}(e_B + x_B r_B) \bmod q$. B.8 Send (R_B, s_B) to A. B.9 return $K_B = (R_A)^w \bmod p$.
Bước 3. *A xác thực (R_B, s_B) là của B. Nếu chấp nhận A tính khóa chung.*	
A.7 $r_B = R_B \bmod q$. A.8 If $DSA_{Ver}(R_B, (r_B, s_B), y_B) = "Reject"$ then break protocol. A.9 Else return $K_A = (R_B)^v \bmod p$.	

Hình 1. *Giao thức Arazi.*

2.1.2. Các phân tích

Giao thức trên có hai nhược điểm cơ bản, đó là:

- Thứ nhất, thông báo được ký là công khai, do đó, nếu lộ khóa bí mật chẳng hạn x_A thì sẽ tính được ***v*** *và từ đó tính được khóa chung. Nói một cách khác thì giao thức này không HFS.*

- Thứ hai, g*iao thức không xác thực khóa được thỏa thuận. Tức là sau khi thực hiện giao thức thành công thì cả A lẫn B cũng không rõ đối tác của mình có khóa chung với mình hay không. Để thấy rõ nhược điểm này, ta xem xét việc một người C nào đó muốn mạo danh B để thực hiện giao thức với A. Người này chỉ cần có được một cặp (R_B, s_B) do B tính và truyền trong một giao dịch với D bất kỳ rồi dùng nó để truyền cho A trong bước 2. Khi này, A sẽ thực hiện nốt các bước A.7, A.8 và A.9 để được K_A tưởng là khóa chung với B.*

2.2. Giao thức Harn và các phân tích

Năm 1995, L. Harn và các cộng sự đề xuất sửa đổi giao thức của Arazi nhằm khắc phục nhược điểm thứ nhất của giao thức này trên ý tưởng dùng nhiều khóa phiên nhằm đạt được nhiều khóa thỏa thuận. Điều quan trọng là trong giao thức của họ thì khóa phiên dùng trong lược đồ chữ ký được lấy là tổng của các khóa phiên dùng để tạo khóa thỏa thuận và việc làm này nhược điểm thứ nhất của giao thức Arazi đã được khắc phục. Giao thức của Harn được mô tả trong [2], trong đó Harn và các cộng sự sử dụng 2 khóa phiên để thu được 3 khóa thỏa thuận.

- ***Các phân tích đối với giao thức Harn***

Cải tiến của Harn tưởng chừng như khắc phục được nhược điểm thứ nhất của giao thức Arazi. Tuy nhiên, một vấn đề mới được nảy sinh ở đây đó là giao thức Harn cung cấp nhiều hơn 1 khóa phiên cho nên dẫn đến bài toán an toàn phía trước cần phải bổ xung điều kiện cho phù hợp. Cụ thể định nghĩa 1 phải được hiểu một cách đầy đủ là

Định nghĩa 2. (tiêu chuẩn an toàn phía trước cho giao thức thỏa thuận nhiều khóa)

- Nếu khóa bí mật dài hạn của một bên bị lộ, trong các giao dịch được thực hiện trước đó nếu biết 1 khóa thỏa thuận nào đó vẫn không tìm được một khóa thỏa thuận khác thì giao thức được gọi là HFS.

- Nếu khóa bí mật dài hạn của cả hai bên bên bị lộ, trong các giao dịch được thực hiện trước đó nếu biết 1 khóa thỏa thuận nào đó vẫn không tìm được một khóa thỏa thuận khác thì giao thức được gọi là PFS.

Với định nghĩa trên, cùng với kết quả do Phan chỉ ra trong [4], ta có kết quả sau:

Mệnh đề 1. *Giao thức của Harn là không HFS.*

Chứng minh làm rõ mệnh đề 1

Giả sử bị lộ x_A thì trong một phiên giao dịch bất kỳ nào đó dùng đến khóa này ta luôn tính

được $v_1 + v_2 \equiv v^{-1} \pmod q$ từ $s_A = v.(h_A + x_A r_A) \bmod q$. Biết rằng, các khóa thỏa thuận trong phiên này do A tính sẽ là

$$K_{A1} = (n_1)^{v_1} \bmod p,\ K_{A2} = (n_2)^{v_2} \bmod p \text{ và } K_{A3} = (n_2)^{v_1} \bmod p.$$

Nên ta có quan hệ sau: $K_{A2}.K_{A3} \equiv (n_2)^{v_1+v_2} \pmod p$. Như vậy, nếu lộ K_{A2} thì sẽ tính được $K_{A3} = (n_2)^{v_1+v_2}.(K_{A2})^{-1} \bmod p$ (và tương tự ngược lại).

Mệnh đề đã được chứng minh.■

Đánh giá chung: *Giao thức của Harn vẫn còn nguyên các nhược điểm như của Arazi*.

2.3. Giao thức Phan

Năm 2005, Raphael C.-W. Phan đã đưa ra một giao thức mới khắc phục toàn bộ những nhược điểm của gaio thức Harn. Hơn thế nữa, Raphael C.-W. Phan còn chỉ ra giao thức của mình là PFS, giao thức được mô tả chi tiết trong [4].

- ***Các phân tích đối với giao thức Phan***

Do giao thức của Phan lược đồ DSA được dùng để ký lên thông báo $M = m_1||K_{A1}||K_{A2}$ đối với A và thông báo $M = n_1||K_{B1}||K_{B2}$ đối với B nên việc các chữ ký này được chấp nhận đồng nghĩa với các khóa thỏa thuận $(K_{A1}, K_{A2}) = (K_{B2}, K_{B1})$ tức là giao thức này có tính chất sau:

Tính chất 2. *Giao thức Phan là xác thực khóa hiện*.

Ngoài ra, mệnh đề dưới đây cho thấy giao thức của Phan là HFS và không như nhận định của ông, nó không là PFS.

Mệnh đề 3. *Giao thức của Phan là HFS nhưng không PFS*.

Chứng minh

Giả sử bị lộ x_A thì trong một phiên giao dịch bất kỳ nào đó dùng đến khóa này ta không thể tìm được v từ thành phần thứ hai trong chữ ký của A vì tham số $h = H(m_1||K_{A1}||K_{A2})$ là không tính được cho dù biết thêm một trong hai giá trị K_{A1} hoặc K_{A2}. Điều trên chứng tỏ giao thức là HFS.

Tuy nhiên, nếu biết cả x_A và x_B thì do

$$K_{A1} = (n_1)^{v.x_A} \bmod p = g^{v.w.x_A} \bmod p.$$
$$K_{A2} = (n_2)^{v} \bmod p = g^{v.w.x_B} \bmod p.$$

Nên $K_{A1} = (K_{A2})^{x_A (x_B)^{-1} \bmod q} \bmod p$ và

$$K_{A2} = (K_{A1})^{x_B (x_{AB})^{-1} \bmod q} \bmod p.$$

Điều trên dẫn đến nếu biết thêm một trong hai khóa thỏa thuận sẽ tính được nốt khóa còn lại trong phiên giao dịch. Nói một cách khác giao thức không là PFS và mệnh đề đã được chứng minh.■

2.4. Giao thức Liu-Li

Năm 2007, các tác giả Jie Liu và Jianhua Li đã chỉ ra giao thức của Phan bộc lộ quan hệ giữa hai khóa được thỏa thuận trong mỗi phiên giao dịch, đó là: $(K_A)^{x_A} \equiv (K_{A2})^{x_B} \pmod p$ và khắc phục nhược điểm trên bằng giao thức của mình được mô tả trong [3].

- ***Các phân tích***

Từ nguyên lý hoạt động của giao thức do Jie Liu và Jianhua Li mô tả và theo đánh giá của các tác giả tại [3], ta thấy giao thức Liu-Li có các tính chất của giao thức Phan và có thêm tính chất sau:

Tính chất 4. *Giao thức của Liu-Li là PFS*.

3. ĐỀ XUẤT GIAO THỨC AN TOÀN VÀ HIỆU QUẢ

3.1. Hướng cải tiến Harn hoặc Phan để đạt tính PFS

3.1.1. Ý tưởng cải tiến

Ý tưởng cải tiến xuất phát từ nhận xét sau: *Nếu giao thức của Harn và của Phan chỉ lấy 1 khóa chung cho mỗi phiên giao dịch thì sẽ không tồn tại kiểu tấn công tìm khóa còn lại, do đó, giao thức mới tương ứng sẽ đạt PFS.*

3.1.2. Phân tích hiệu quả của việc cải tiến theo ý tưởng trên

Theo mô tả nguyên lý hoạt động thì chi phí của giao thức Liu-Li chỉ nhiều hơn của Phan đúng 4 phép nhân trên GF(q), trong khi đó, giao thức Liu-Li cung cấp gấp đôi số khóa và cùng đạt tính chất PFS. Như vậy, việc cải tiến giao thức của Phan là không có ý nghĩa thực tiễn. Đối với giao thức của Harn, ngoài việc chỉ lấy 1 khóa thỏa thuận cần thêm phần xác thực khóa hiện nên việc làm này sẽ làm cho chi phí thực hiện của giao thức không khác nhiều so với giao thức của Liu-Li, chính vì vậy, đây cũng là hướng không có ý nghĩa thực tiễn.

3.2. Cải tiến giao thức của Arazi để đạt PFS

Học theo cách khắc phục nhược điểm thứ nhất (trong giao thức nguyên thủy) do Phan thực hiện, bố trí lại trình tự công việc để khâu sử dụng lược đồ chữ ký xảy ra sau khi có khóa thỏa thuận nhằm:

- Xác thực khóa hiện.
- Công việc của hai đối tác trong giao thức được thực hiện đồng thời.

Chúng tôi đề xuất một giao thức cải tiến cho Arazi như sau:

3.2.1. Mô tả giao thức Arazi cải tiến

Giao thức Arazi cải tiến được mô tả theo hình 3 dưới đây.

Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$	
A giữ tham số mật x_A.	B giữ tham số mật x_B.
Bước 1. *A, B tạo và truyền các thông tin thỏa thuận khóa cho nhau.*	
A.1 $v \in_R (0, q)$. A.2 $R_A = g^v \bmod p$. A.3 Send R_A to B.	B.1 $w \in_R (0, q)$. B.2 $R_B = g^w \bmod p$. B.3 Send R_B to A.
Bước 2. *A tính khóa chung, ký lên thông báo $M_A = K_A \|\| R_A \|\| R_B$ rồi gửi chữ ký cho B.* *B tính khóa chung, ký lên thông báo $M_B = K_B \|\| R_B \|\| R_A$ rồi gửi chữ ký cho A.*	
A.4 $K_A = (R_B)^v \bmod p$. A.5 $r_A = R_A \bmod q$. A.6 $h_A = H(K_A \|\| R_A \|\| R_B)$. A.7 $s_A = v^{-1}(h_A + x_A r_A) \bmod q$. A.8 Send s_A to B.	B.4 $K_B = (R_A)^w \bmod p$. B.5 $r_B = R_B \bmod q$. B.6 $h_B = H(K_B \|\| R_B \|\| R_A)$. B.7 $s_B = w^{-1}(h_B + x_B r_B) \bmod q$. B.8 Send s_B to A.
Bước 3. *A xác thực B và xác thực khóa chung.*	
A.9 $r_B = R_B \bmod q$. A.10 $M_B = K_A \|\| R_B \|\| R_A$. A.11 If $Ver_{DSA}(M_B, (r_B, s_B), y_B) = "Reject"$ then break protocol. A.12 Else return K_A.	B.9 $r_A = R_A \bmod q$. B.10 $M_A = K_B \|\| R_A \|\| R_B$. B.11 If $Ver_{DSA}(M_A, (r_A, s_A), y_A) = "Reject"$ then break protocol. B.12 Else return K_B.

Hình 2. *Giao thức Arazi cải tiến.*

3.2.2. Phân tích giao thức

Giao thức Arazi cải tiến có các đặc tính sau.

Tính chất 5. *Chi phí cho một lần giao dịch thành công theo giao thức Arazi cải tiến cho bởi công thức sau.*

$$T_A = 4t_{exp} + 2t_{inv} + 2t_H + 4t_m(q) + t_m(p). \quad (2)$$

Tính chất 6. *Giao thức Arazi cải tiến là xác thực khóa hiện và nếu H là an toàn thì giao thức là PFS.*

Chứng minh

Từ giả thiết H là an toàn nên một khi chữ ký được chấp nhận là tương đương với hai thông báo $M_A = K_B||R_A||R_B$ do B tính và $M_A = K_A||R_A||R_B$ trùng nhau hay cả hai đều đã có khóa chung là $K_A = K_B$. nên giao thức là xác thực khóa.

Giả sử biết x_A và x_B. Từ H là an toàn đồng nghĩa với việc không tìm được K_A từ $h_A = H(K_A||R_A||R_B)$ và sẽ không tìm được v từ $s_A = v^{-1}(h_A + x_A r_A) \bmod q$; tương tự đối với K_B và w. Điều trên có nghĩa giao thức là PFS. Tính chất đã được chứng minh.■

3.3. Cải tiến giao thức của Liu-Li để tăng tính hiệu quả

Thực hiện ý tưởng giao việc cho các bên tham gia giao thức một cách hợp lý, chúng tôi đề xuất giao thức cải tiến của giao thức Liu-Li để đạt tính hiệu quả như sau:

Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$	
A giữ tham số mật x_A.	B giữ tham số mật x_B.
Bước 1. *A, B tạo và truyền các thông tin thỏa thuận khóa.*	
A.1 $v_{1,}v_2 \in_R (0, q)$.	B.1 $w_{1,}w_2 \in_R (0, q)$.
A.2 $m_A = g^{v_1} \bmod p$.	B.2 $m_B = g^{w_1} \bmod p$.
A.3 $n_A = (y_A)^{v_2} \bmod p$.	B.3 $n_B = (y_B)^{w_2} \bmod p$.
A.4 Send (m_A, n_A) to B.	B.4 Send (m_B, n_B) to A.
Bước 2. *A, B tính cặp khóa chung (K_1, K_2), ký lên thông báo chứa thông tin thỏa thuận và khóa chung tìm được của mình rồi truyền cho đối tác.*	
A.5 $K_{A1} = (m_B)^{v_2.x_A \bmod q} \bmod p$.	B.5 $K_{B1} = (m_A)^{w_2.x_B \bmod q} \bmod p$.
A.6 $K_{A2} = (n_B)^{v_1} \bmod p$.	B.6 $K_{B2} = (n_A)^{w_1} \bmod p$.
A.7 $h = H(m_A||n_A||K_{A1}||K_{A2})$.	B.7 $h = H(m_B||n_B||K_{B1}||K_{B2})$.
A.8 $r_A = m_A \bmod q$.	B.8 $r_B = m_B \bmod q$
A.9 $s_A = {v_1}^{-1}(h + x_A r_A) \bmod q$.	B.9 $s_B = {w_1}^{-1}(h + x_B r_B) \bmod q$.
A.10 Send s_A to B.	B.10 Send s_B to A.
Bước 3. *A, B kiểm chữ ký. Nếu chấp nhận thì lấy khóa chung .*	
A.11 $r_B = m_B \bmod q$.	B.11 $r_A = m_A \bmod q$.
A.12 $M = m_B||n_B||K_{A2}||K_{A1}$.	B.12 $M = m_A||n_A||K_{B2}||K_{B1}$.
A.13 If $Ver_{DSA}(M, (r_B, s_B))$" = "$Acept$ then return (K_{A1}, K_{A2}).	B.13 If $Ver_{DSA}(M, (r_A, s_A))$ = "$Acept$ then return (K_{B2}, K_{B1}).
A.14 Else break protocol.	B.14 Else break protocol.

Hình 3. *Giao thức Liu-Li cải tiến.*

Giao thức Liu-Li cải tiến có các đặc tính giống hệt như của Arazi cải tiến nhưng mỗi lần giao dịch sẽ được hai khóa thỏa thuận với chi phí cho trong kết quả sau:

Tính chất 7. *Chi phí cho một lần giao dịch thành công theo giao thức Liu-Li cải tiến cho bởi công thức sau.*

$$T_A = 6t_{exp} + 2t_{inv} + 2t_H + 5t_m(q) + t_m(p). \quad (3)$$

Nhận xét. Từ (2) và (3) chúng ta thấy rằng:

- *Giao thức Arazi cải tiến là hiệu quả hơn so với Liu-Li cải tiến về chi phí cho một giao dịch thỏa thuận.*
- *Giao thức Liu-Li cải tiến là hiệu quả hơn so với Arazi cải tiến về chi phí trung bình cho một khóa được thỏa thuận.*
- *Như vậy, tùy theo môi trường ứng dụng mà chúng ta lựa chọn giao thức cho phù hợp.*

Chẳng hạn trong một định kỳ (có tính bắt buộc như đầu mỗi ngày) cần thực hiện việc thiết lập khóa, nếu ít xảy ra tình huống phải đổi khóa giữa chừng thì ta sẽ dùng Arazi còn ngược lại ta dùng Liu-Li.

4. KẾT LUẬN

Bài báo đã trình bày các phân tích, đánh giá về mặt an toàn và hiệu quả của một số giao thức trao đổi khóa dựa trên giao thức Diffie-Hellman như giao thức Arazi, giao thức Harn, giao thức Phan, giao thức Liu-Li. Bài báo cũng đưa ra một số sửa đổi cho các giao thức Harn và giao thức Phan để đạt được tính an toàn quá khứ hoàn toàn. Bài báo cũng đề xuất cải tiến giao thức Arazi, giao thức Liu-Li để tăng tính an toàn và hiệu quả.

TÀI LIỆU THAM KHẢO

[1]. B. Arazi *Integrating a Key Distribution Procedure into the Digital Signature Standard*, Electrolics Letters, 29(11), (1993). pp. 966-967.

[2]. L. Harn. *Modified Key Agreement Protocol Base on the Digital Signature Standard*, Electronics Letters, Vol.31(6), (1995), pp. 448-449.

[3]. Jie Liu and Jianhua Li. *A Better Improvement on the Integreated Diffie-Hellman – DSA Key Agreement Protocol*, IEEE Communications Letters (2010); 11: 114-117.

[4]. Phan, CRW, *Fixing the Integratied Diffie-Hellman DSA Key Exchange Protocol*, IEEE Communications Letters (2005); 9: pp. 570-572.

ABSTRACT

PROPOSING SOME SECURE AND EFFECTIVE PROTOCOLS DH-KE

In the paper, the authors analyzed and evaluated the safety and effectiveness of some key agreement protocols based on Diffie-Hellman protocol such as Arazi, Harn, and Phan protocol, Liu-Li protocol and some modifications to the Harn protocol and the Phan protocol to perfect forward secretcy. In the paper, the Arazi and Liu-Li protocols to increase safety and efficiency had been also proposed improving.

Keywords: Protocol DH-KE; HFS; PFS; Protocol Arazi; Protocol Phan; Protocol Harn; Protocol Liu-Li,...

Nhận bài ngày 28 tháng 7 năm 2020
Hoàn thiện ngày 06 tháng 8 năm 2020
Chấp nhận đăng ngày 14 tháng 12 năm 2020

Địa chỉ: [1]Cục Quản lý mật mã dân sự và kiểm định sản phẩm mật mã;
[2]Học viện Kỹ thuật mật mã, Ban Cơ yếu Chính phủ;
[3]Ban Cơ yếu Chính phủ.
[*]Email: leutan70@gmail.com.