Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ 26 (2010) 44-48

Mã hoá đồng cấu và ứng dụng

Trịnh Nhật Tiến*, Đặng Thu Hiền, Trương Thị Thu Hiền, Lương Việt Nguyên

Khoa Công nghệ Thông tin, Trường Đại học Công nghệ, ĐHQGHN, 144 Xuân Thủy, Hà Nội, Việt Nam

Nhận ngày 8 tháng 10 năm 2009

Tóm tắt: Hệ mã hoá Elgamal có tính chất đồng cấu, nhờ nó có thể tính được kết quả trong cuộc bỏ phiếu "chọn một trong hai", mà không cần giải mã từng lá phiếu. Sơ đồ chia sẻ bí mật Shamir phối hợp với hệ mã hoá Elgamal còn có tính chất đặc biệt hơn nữa, nhờ nó có thể chia lá phiếu thành nhiều mảnh, cử tri gửi mỗi mảnh cho một thành viên ban kiểm phiếu, khi khớp các mảnh phiếu lại sẽ được nội dung đầy đủ của lá phiếu. Bài báo này trình bày các tính chất trên và chỉ ra ứng dụng của chúng trong bỏ phiếu từ xa.

1. Tính chất đồng cấu của hệ mã hóa Elgamal

1.1. Hệ mã hóa Elgamal

Chọn số nguyên tố lớn p sao cho bài toán logarit rời rạc trong $\mathbf{Z_p}$ là khó giải, **g** là phần tử sinh trong $\mathbf{Z_p^*}$. Chọn tập bản rõ $\mathbf{P = Z_p}$, chọn tập bản mã $\mathbf{C} = \{(a, b) / a, b \in \mathbf{Z_p}\}$.

Chọn khóa bí mật là $\mathbf{a} \in \mathbf{Z_p^*}$, khóa công khai là $\mathbf{h = g^a}$.

Để mã hóa **m**, ta chọn số ngẫu nhiên bí mật **k**, bản mã là $(\mathbf{x}, \mathbf{y}) = \mathbf{E_k}(\mathbf{m}) = (\mathbf{g^k}, \mathbf{h^k m})$.

Tài liệu được giải mã là $\mathbf{m = y / x^a}$.

1.2. Khái niệm mã hoá đồng cấu

Cho tập bản rõ P tạo thành nhóm với phép tính $\oplus$, tập bản mã C tạo thành nhóm với phép tính $\otimes$.

$\mathbf{E_k}(\mathbf{m})$ là hàm mã hoá bản rõ **m** theo tham số ngẫu nhiên bí mật **k**.

Hệ mã hóa **E** được gọi là có ***tính chất*** $(\oplus, \otimes)$- ***đồng cấu***, nếu với tham số $\mathbf{k}=\mathbf{k_1}+\mathbf{k_2}$, thỏa mãn công thức đồng cấu:

$\mathbf{E_{k1}}(\mathbf{m_1}) \otimes \mathbf{E_{k2}}(\mathbf{m_2}) = \mathbf{E_k}(\mathbf{m_1} \oplus \mathbf{m_2})$, trong đó $\mathbf{m_1}$, $\mathbf{m_2}$ là 2 bản rõ, $\mathbf{k_1}$, $\mathbf{k_2}$ là 2 tham số ngẫu nhiên bí mật.

1.3. Hệ mã hóa Elgamal có tính chất đồng cấu

a) Hệ mã hoá Elgamal có tính chất đồng cấu, vì với $k = k_1 + k_2$, *ta có:*

$E_{k1}(m_1) = (g^{k1}, h^{k1} m_1)$, $E_{k2}(m_2) = (g^{k2}, h^{k2} m_2)$ thoả mãn công thức đồng cấu:

$E_{k1}(m_1) * E_{k2}(m_2) = (g^{k1} g^{k2}, h^{k1} h^{k2} m_1 m_2)$

$= (g^{k1+k2}, h^{k1+k2} m_1 m_2)$

$= (g^k, h^k m_1 m_2) = E_k(m_1 m_2)$.

b) Trường hợp chọn thông tin $m = g^v$, *trong đó* $v = 0$ *hoặc* $v = 1$*:*

Bởi vì:

* Tác giả liên hệ. ĐT: 84-4-37547064
E-mail: tientn@vnu.edu.vn

$E_{ki}(g^{vi}) = (x_i, y_i) = (g^{ki}, h^{ki}\ g^{vi})$, $i = 1, 2$.

Do đó:

$(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1y_2) =$
$(g^{k1+k2}, h^{k1+k2}\ g^{v1+v2})$. [1]

2. Ứng dụng hệ mã hóa đồng cấu Elgamal cho loại bỏ phiếu có/ không

Bài toán: Cần lấy ý kiến về một việc nào đó, cử tri phải ghi vào lá phiếu: đồng ý (**1**) hay không đồng ý (**0**).

Nội dung lá phiếu được mã hoá và gửi về Ban kiểm phiếu. Vấn đề là Ban kiểm phiếu ***tính kết quả bỏ phiếu*** như thế nào, trong khi không biết nội dung từng lá phiếu ? (Vì chúng đã được mã hoá).

Giải quyết:

Cho dễ hiểu, chúng tôi trình bày cách giải quyết thông qua một ví dụ cụ thể.

2.1. Cử tri ghi ý kiến vào lá phiếu

Giả sử có 4 cử tri tham gia bỏ phiếu là V_1, V_2, V_3, V_4.

Lá phiếu tương ứng của họ ghi: $v_1 = 0$ (không đồng ý), $v_2 = 1$ (đồng ý), $v_3 = 1$, $v_4 = 0$.

Chọn phần tử sinh **g =3**, hệ mã hoá Elgamal được sử dụng ở đây với các khoá như sau:

Khóa bí mật a = 2, khóa công khai $h = \mathbf{g}^{a} = 3^2 = 9$.

Mỗi cử tri V_i, chọn khóa ngẫu nhiên bí mật k đề mã hóa lá phiếu m của mình thành $(x, y) = (g^k, h^k m)$.

2.2. Cử tri mã hoá lá phiếu

V_1 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_1 chọn ngẫu nhiên $k_1 = 5$, mã hóa $v_1 = 0$ thành $(x_1, y_1) = (3^5, 9^5 * 3^0) = (3^5, 9^5)$.

V_2 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_2 chọn ngẫu nhiên $k_2 = 3$, mã hóa $v_2 = 1$ thành $(x_2, y_2) = (3^3, 9^3 * 3^1) = (3^3, 9^3 * 3)$.

V_3 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_3 chọn ngẫu nhiên $k_3 = 3$, mã hóa $v_3 = 1$ thành $(x_3, y_3) = (3^3, 9^3 * 3^1) = (3^3, 9^3 * 3)$.

V_4 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_4 chọn ngẫu nhiên $k_4 = 7$, mã hóa $v_4 = 0$ thành $(x_4, y_4) = (3^7, 9^7 * 3^0) = (3^7, 9^7)$.

2.3. Ban kiểm phiếu tính kết quả

Ban KP không cần giải mã từng lá phiếu, vẫn có thể tính được kết quả bỏ phiếu bằng cách tính nhân các lá phiếu đã được mã hóa:

$$(x_1,y_1)*(x_2,y_2) = (x_1x_2, y_1y_2)$$
$$= (g^{k1+k2}h^{k1+k2}, g^{v1+v2}).$$

Theo tính chất đồng cấu thì tích của phép nhân trên chính là kết quả bỏ phiếu. Cụ thể tích của 4 giá trị lá phiếu đã được mã hóa là:

$$(X, Y) = (\prod_i x_i, \prod_i y_i)$$
$$= (g^{k1+k2+k3+k4}, h^{k1+k2+k3+k4}\ g^{v1+v2+v3+v4})$$
$$= (3^{18}, 9^{18} * 3^2).$$

Giải mã *(X, Y)* bằng cách tính:

$$\mathbf{m} = g^v = \mathbf{Y/X}^{a} = 9^{18} * 3^2 / (3^{18})^2 = \mathbf{3^2}$$

Như vậy số phiếu đồng ý (ghi 1) là **2**. [2]

3. Sơ đồ chia sẻ bí mật Shamir phối hợp với Hệ mã hoá Elgamal

Bài toán:

Ban quản lý thông tin mật (QL TTM) (Ví dụ Ban kiểm phiếu bầu cử) có t thành viên $\mathbf{A_j}$.

Một người V (Ví dụ cử tri) cần gửi Bản tin mật g^s tới Ban QL TTM.

Bài toán là hãy đề xuất giải pháp bảo đảm để tất cả **t** thành viên nhất trí, mới xem được thông tin mật. Ít hơn **t** thành viên không thể xem được thông tin này.

Giải quyết:

Chọn số nguyên tố p sao cho bài toán logarit rời rạc trong $\mathbf{Z_p}$ là khó giải, **g** là phần tử sinh của $\mathbf{Z_p^*}$.

Trong Ban QL TTM, mỗi thành viên $\mathbf{A_j}$ chọn khóa bí mật $\mathbf{z_j}$ và khóa công khai $h_j = g^{z_j}$.

Người V chia ***tin mật*** $\mathbf{g^s}$ thành **t** mảnh tin khác nhau, mã hoá chúng, sau đó chuyển cho mỗi $\mathbf{A_j}$ một mảnh mã. Khi tất cả t thành viên nhất trí cần xem ***tin mật***, họ sẽ khớp các mảnh tin đã giải mã. Cụ thể là tính ***tích*** của các mảnh tin đã giải mã. (Ta hiểu "mảnh tin" là mẩu tin, "mảnh mã" là mẩu tin đã được mã hóa).

3.1. Chia sẻ thông tin mật thành các mảnh tin

Người V chọn đa thức ngẫu nhiên bậc **t** thuộc Z_p: $P(x) = \sum_{k=0}^{t} \alpha_k x^k$

V chọn bí mật các hệ số $s = \alpha_0$ và $\alpha_1, \alpha_2, \ldots, \alpha_t \in Z_p$.

Người V tính các mảnh tin mật $\mathbf{y_j} = P(j)$, j =1, 2, .., **t**.

Các mảnh tin mật $\mathbf{y_j}$ được mã hóa thành $\mathbf{H_j} = h_j^{P(j)}$, V gửi $\mathbf{H_j}$ cho thành viên $\mathbf{A_j}$.

3.2. Khôi phục thông tin mật từ các mảnh tin

Bạn QL TTM khớp nối các mảnh tin mật $\mathbf{H_j}$ khi tất cả **t** thành viên $\mathbf{A_j}$ đều nhất trí.

Đầu tiên từng người trong Ban QL A_j giải mã $\mathbf{H_j}$ bằng cách tính $S_j = H_j^{1/z_j}$.

Theo quá trình trên, ta nhận được: $S_j = H_j^{1/z_j} = (h_j^{P(j)})^{1/zj} = (((g^{zj}))^{P(j)})^{1/zj} = g^{P(j)}$

Sau đó ***tin mật*** $\mathbf{g^s}$ được xác định nhờ ***tính chất đặc biệt*** sinh ra do sự phối hợp giữa sơ đồ Shamir và hệ mã hoá Elgamal:

$$\prod_{j\in A} S_j^{\lambda_{j,A}} = \prod_{j\in A} g^{P(j)\lambda_{j,A}} = g^{\sum_{j\in A} P(j)\lambda_{j,A}} = g^{P(0)} = g^s,$$

trong đó $\lambda_{j,A} = \prod_{l\in A-\{j\}} \frac{l}{l-j}$ là hệ số Lagrange, A = {1, 2, ... , t} [3].

4. Ứng dụng Sơ đồ chia sẻ bí mật Shamir và Hệ mã hoá Elgamal cho loại bỏ phiếu chọn L trong K.

Bài toán:

Giả sử có 3 ứng cử viên: 0: Lý Văn Nghêu. 1: Trần Văn Sò. 2: Lê Thị Ốc.

Có 3 người kiểm phiếu là A_1, A_2, A_3.

Đây là cuộc bỏ phiếu chọn 2 trong 3 người (Ví dụ vào chức vụ Giám đốc và phó Giám đốc). Cử tri không tin vào một số thành viên trong Ban kiểm phiếu (Ban KP), nên họ dùng sơ đồ chia sẻ bí mật Shamir để chia lá phiếu của mình thành các mảnh tin và gửi cho mỗi người kiểm phiếu một mảnh.

Vấn đề là Ban KP phải khớp nối các mảnh tin để biết nội dung từng lá phiếu? (Vì nội dung mỗi lá phiếu được chia thành nhiều mảnh tin, từng mảnh lại được mã hoá trước khi gửi về Ban KP).

Giải quyết:

Chọn số nguyên tố p sao cho bài toán logarit rời rạc trong $\mathbf{Z_p}$ là khó giải, **g** là phần tử sinh của $\mathbf{Z_p^*}$.

Sử dụng Sơ đồ chia sẻ bí mật Shamir và Hệ mã hoá Elgamal.

4.1. Biểu diễn sự lựa chọn ứng cử viên (Nội dung phiếu bầu cử)

Cử tri V bầu cử cho ông Nghêu và bà Ốc tương ứng với lựa chọn 0 và 2.

Để diễn đạt sự lựa chọn của mình, cử tri dùng hệ số cơ số **3**.

Nội dung lá phiếu của V được biểu diễn là $\mathbf{s} = 0*3^0 + 2*3^1 = 6$.

4.2. Ban kiểm phiếu chuẩn bị

Trong Ban KP, phần tử sinh của $\mathbf{Z_p^*}$ là **g=3**, mỗi thành viên $\mathbf{A_j}$ chọn khóa bí mật $\mathbf{z_j}$ và khóa công khai $h_j = g^{z_j}$. Cụ thể là:

A_1 chọn khóa bí mật $z_1=2$, khóa công khai là $h_1=3^2$

A_2 chọn khóa bí mật $z_2=3$, khóa công khai là $h_2=3^3$

A_3 chọn khóa bí mật $z_3=5$, khóa công khai là $h_3=3^5$.

4.3. Cử tri V chia sẻ nội dung lá phiếu (tin mật) thành các mảnh tin

Với nội dung lá phiếu là s = **6**, cử tri V chọn đa thức ngẫu nhiên bí mật:

$$P(x) = 6 + 2x + 5x^2$$

Ở đây $\alpha_0 = \mathbf{s} = 6$, $\alpha_1 = 2$, $\alpha_2 = 5$.

V tính các mảnh tin mật: $y_j = P(j)$, theo đa thức trên, P(1) =13, P(2) =30, P(3) =57.

V mã hoá các mảnh tin mật trên thành $\mathbf{H_j}= h_j^{P(j)}$, cụ thể là:

$H_1 = h_1^{P(1)} = (3^2)^{13}$,

$H_2 = h_2^{P(2)} = (3^3)^{30}$,

$H_3 = h_3^{P(3)} = (3^5)^{57}$

Cử tri V chuyển H_1, H_2, H_3 tương ứng cho các thành viên Ban KP: A_1, A_2, A_3.

4.4. Ban KP khôi phục nội dung lá phiếu (tin mật) từ các mảnh tin

Ban KP khớp nối các mảnh tin $\mathbf{H_j}$ khi tất cả t thành viên $\mathbf{A_j}$ đều nhất trí.

Đầu tiên từng người kiểm phiếu A_j giải mã H_j bằng cách tính $S_j = H_j^{1/Z_j}$.

Theo các quá trình trên ta nhận được:

$$S_j = H_j^{1/Z_j} = (h_j^{P(j)})^{1/zj}$$

$$= (((g^{zj}))^{P(j)})^{1/zj} = g^{P(j)}$$

Cụ thể là:

A_1 giải mã H_1 thành $S_1 = ((3^2)^{13})^{1/2} = 3^{13}$

A_2 giải mã H_2 thành $S_2 = ((3^3)^{30})^{1/3} = 3^{30}$

A_3 giải mã H_3 thành $S_3 = ((3^5)^{57})^{1/5} = 3^{57}$

Bí mật $\mathbf{g^s = 3^6}$ được xác định nhờ tính chất đặc biệt sinh ra do sự phối hợp giữa sơ đồ chia sẻ bí mật Shamir và hệ mã hoá Elgamal:

$$\prod_{j\in A} S_j^{\lambda_{j,A}} = \prod_{j\in A} g^{P(j)\lambda_{j,A}} = g^{\sum_{j\in A} P(j)\lambda_{j,A}} = g^{P(0)} = g^{s}$$

trong đó $\lambda_{j,A} = \prod_{l\in A-\{j\}} \frac{l}{l-j}$ là hệ số Lagrange, A={1, 2, 3}.

Trong ví dụ trên, hệ số Lagrange được tính như sau:

$\lambda_1=2/(2-1)*3/(3-1) = 3$,

$\lambda_2=1/(1-2)*3/(3-2) = -3$,

$\lambda_3=1/(1-3)*2/(2-3) = 1$.

$\mathbf{g^s} = S_1^{\lambda 1} * S_2^{\lambda 2} * S_3^{\lambda 3}$

$= (3^{13})^3 * (3^{30})^{-3} * (3^{57})^1 = \mathbf{3^6}$.

Đây là nội dung lá phiếu đã được khôi phục sau khi "khớp nối các mảnh tin".

5. Kết luận

Bài báo đã trình bày tính chất đặc biệt của sơ đồ chia sẻ bí mật Shamir và hệ mã hoá Elgamal, đặc biệt là tính chất sinh ra khi phối hợp hai hệ mật mã trên. Sau đó chỉ ra được ứng dụng của các tính chất trên trong bỏ phiếu hay thăm dò từ xa trên mạng công khai (bỏ phiếu điện tử).

Lời cảm ơn

Cảm ơn Trung tâm hỗ trợ nghiên cứu châu Á (ĐHQGHN) đã tài trợ cho nghiên cứu của chúng tôi.

Tài liệu tham khảo

[1] Josh Cohen Benaloh, *Secret Sharing Homomorphisms:* Keeping Shares of a Secret Secret (Extended Abstract).

[2] Zuzana Rjaskova, *Electronic Voting Schemes,* 2002.

[3] Cyber Vote, *Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting,* 2002.

Homomorphisms Encryption and Applications

Trinh Nhat Tien, Dang Thu Hien, Truong Thi Thu Hien, Luong Viet Nguyen

Faculty of Information Technology, College of Technology, VNU, 144 Xuan Thuy, Hanoi, Vietnam

Elgamal encryption has homomorphisms property, determining result of electronic voting "Select one in two", without decoding all ballots. Shamir secret sharing scheme and Elgamal encryption have more special property. Voter can divide a ballot into some small pieces, after that sending one piece to one ballot checker. Checking committee combines these pieces to get the original ballot.

The article presents this property and shows its application in electronic voting.