# ĐỀ XUẤT DẠNG THAM SỐ CHO CÁC HỆ MẬT CÓ ĐỘ AN TOÀN DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC TRÊN TRƯỜNG GF(P)

Hoàng Văn Việt[1*], Vũ Bá Nhã[2]

***Tóm tắt:*** *Khi sử dụng các hệ mật khóa công khai như RSA, Elgamal, Diffie-Helman, ... ngoài việc quan tâm hàng đầu là tính an toàn thì một quan tâm nữa của người ứng dụng là tính hiệu quả của chúng. Bài báo đề xuất một dạng tham số nguyên tố p với mục tiêu hỗ trợ việc tính toán nhanh trên GF(p) mà không ảnh hưởng đến độ an toàn của các hệ mật có độ an toàn dựa trên bài toán logarit rời rạc trên trường này.*

**Từ khóa**: Mật mã khóa công khai, Logarith rời rạc, Giao thức trao đổi khóa.

## 1. ĐẶT VẤN ĐỀ

Trong thực tế, sử dụng các hệ mật khóa công khai như RSA, Elgamal, Diffie-Helman, ... ngoài việc quan tâm hàng đầu là tính an toàn thì một quan tâm nữa của người ứng dụng là tính hiệu quả của chúng. Nhiều nghiên cứu có tính hệ thống tập trung vào vấn đề tìm ra các thuật toán nhanh cho phép tính modulo trên vành $\mathbb{Z}_n$ được phát triển nhiều nhất trong đó kết quả tốt nhất là thuật toán của Barrett [1], trong đó, có thể kể đến việc tìm ra các loại modulo đặc biệt hỗ trợ cho việc tính toán nhanh điển hình là các số nguyên tố NIST (National Institute of Standards and Technology) được đưa vào chuẩn FIPS 186-2 [2] để dùng cho các ứng dụng hệ mật trên các đường cong elliptic. Đối với những ứng dụng của các hệ mật có độ an toàn dựa trên bài toán logarit rời rạc trên trường GF(p) thì ngoài như một điều kiện bắt buộc trong việc sử dụng phần mềm LINUX (freesoftware) là các số nguyên tố p phải có 64 bít cao nhất bằng 1 thì chưa có một công bố nào liên quan đến tham số p nhằm hỗ trợ tính toán nhanh phép rút gọn trên GF(p). Trong bài này, chúng tôi tập trung tìm ra một dạng tham số nguyên tố p với mục tiêu hỗ trợ việc tính toán nhanh trên GF(p) mà không ảnh hưởng đến độ an toàn của các hệ mật có độ an toàn dựa trên bài toán logarit rời rạc trên trường này với mục đích khuyến cáo người dùng sử dụng chúng và có thể cao hơn là đưa chúng vào các chuẩn để sử dụng.

Phần còn lại của bài báo được cấu trúc như sau: Mục 2 trình bày về phép rút gọn trên GF(p); Mục 3 và 4 trình bày về việc tồn tại và cách sinh các tham số p an toàn có dạng đặc biệt; Cuối cùng là phần kết luận.

## 2. PHÉP RÚT GỌN TRÊN GF(p)

Trong các ứng dụng mật mã chúng ta thường xuyên phải thực hiện phép toán rút gọn các số nguyên $x$ nào đó theo modulo $p$, thực chất là tính $x \bmod p$. Hiển nhiên phép rút gọn có thể thực hiện thông qua một phép chia $x$ cho $p$, tuy nhiên việc làm này sẽ phải trả một chi phí cao cho việc tính toán. Bằng cách "*tránh*" việc chia Barrett đã đưa ra một thuật toán chi phí thấp hơn.

### 2.1. Chi phí tính toán cho một số phép toán số học

Theo như Donald E. Knuth [4] thì số phép toán cơ bản (còn gọi là chi phí) cho một số phép toán số học theo thuật toán của Karatsuba và Ofman [5] trên các số nguyên k-bít như sau:

Phép nhân: $O(k^{1.5})$; Phép chia là: $O(k^2)$.

Thuật toán của Karatsuba và Ofman dựa trên kết quả sau:

**Định lý Karatsuba-Ofman** "Để nhân hai số nguyên k-bits chỉ cần tiến hành nhân 3 cặp số nguyên $\lceil k/2 \rceil$-bít".

**Rút gọn theo thuật toán Barrett [4]**

*Thuật toán Barrett.*

Input: p, b ≥ 3, k = $\lfloor \log_b p \rfloor + 1$, 0 ≤ z < $b^{2k}$, m = $\lfloor b^{2k}/p \rfloor$.

Output: z mod p.

1. q ← $\left\lfloor \lfloor z/b^{k-1} \rfloor . m/b^{k+1} \right\rfloor$.
2. r ← $(z \bmod b^{k+1}) - (q.p \bmod b^{k+1})$.
3. if r < 0 then $r \leftarrow r + b^{k+1}$.
4. while r ≥ p do: $r \leftarrow r - p$.
5. return (r).

Chi phí tính toán cho một phép rút gọn của thuật toán Barrett được đánh giá trong kết quả dưới đây.

**Kết quả 1.** Chi phí tính toán cho thuật toán rút gọn Barrett theo modulo $p$ gồm k ký tự bằng chi phí của hai phép nhân hai số nguyên k ký tự.

*Chứng minh*

Để thực hiện thuật toán trên chúng ta cần đến hai phép nhân số lớn, một là $\lfloor z/b^{k-1} \rfloor . m$ ở bước 1 và một là q.p trong bước 2. Rõ ràng cả 4 giá trị $\lfloor z/b^{k-1} \rfloor$, m, q và p đều là các số k ký tự nên kết quả 1 đã được chứng minh.

### 2.2. Rút gọn với giá trị p đặc biệt

**Định nghĩa 1.** Cho b là một số tự nhiên lớn hơn 1 bất kỳ, số nguyên tố p = $b^k - a$ (1) được gọi là có dạng đặc biệt nếu a < $b^{\lfloor k/2 \rfloor}$ (2).

**Thuật toán đề xuất.** (rút gọn theo modulo p dạng đặc biệt)

Input: p = $b^k - a$, b ≥ 3, a < $b^{\lfloor k/2 \rfloor}$, 0 ≤ z < $b^{2k}$.

Output: z mod p.

1. r ← z mod $b^k$; q ← z div $b^k$.
2. u ← q.a.
3. $r \leftarrow r + u \bmod b^k$; v ← u div $b^k$.
4. r ← r + v.a.
5. while r ≥ p do: r ← r − p.
6. return (r).

Kết quả sau đây cho ta chi phí tính toán cho một phép rút gọn của thuật toán 1.

**Kết quả 2.** Chi phí tính toán cho thuật toán rút gọn theo modulo p đặc biệt gồm k ký tự bằng chi phí cho ba phép nhân hai số nguyên $\lfloor k/2 \rfloor$ ký tự.

*Chứng minh*

Để thực hiện thuật toán trên chúng ta cần đến hai phép nhân số lớn, một là q.a ở bước 2 và một là v.a trong bước 4.

Từ điều kiện z < $b^{2k}$ nên q là số k ký tự và từ a < $b^{\lfloor k/2 \rfloor}$ nên q.a là tích của một số k ký tự với một số $\lfloor k/2 \rfloor$ ký tự. Đương nhiên tích trên là một số trong phạm vi $k + \lfloor k/2 \rfloor$ ký tự nên giá trị v trong bước 3 là số $\lfloor k/2 \rfloor$ ký tự dẫn đến v.a là tích của hai số $\lfloor k/2 \rfloor$ ký tự và giá trị của tích này là số k ký tự. Biết rằng phép nhân một số k ký tự với một số $\lfloor k/2 \rfloor$ ký tự bằng hai phép nhân hai số $\lfloor k/2 \rfloor$ ký tự cho nên thuật toán 2 cần tính 3 phép nhân hai số $\lfloor k/2 \rfloor$ bít và theo định lý Karatsuba - Ofman kết quả đã được chứng minh.

Từ hai kết quả 1 và 2, cùng với việc dùng thuật toán nhân hai số nguyên của A. Karatsuba và Y.Ofman (chi phí cho phép nhân hai số nguyên k ký tự bằng chi phí cho 3 phép nhân hai số $\lfloor k/2 \rfloor$ ký tự) ta có thể đưa ra kết luận sau.

**Kết luận 3.** Việc dùng modulo p đặc biệt sẽ giúp cho phép rút gọn theo modulo này nhanh gấp hai lần so với thuật toán Barrett.

## 3. SỰ TỒN TẠI CÁC THAM SỐ p AN TOÀN CÓ DẠNG ĐẶC BIỆT

### 3.1. Điều kiện an toàn đối với tham số p

Theo FIPS 186-3 (xem [FIPS 186-3]) thì các tham số p cần thỏa mãn điều kiện sau: $p$ có độ dài bít là L và cấp của cơ số g bằng q là ước của p-1 có độ dài là N. Cặp (L,N) được gọi là cặp kích thước an toàn cho cặp tham số (p,q) và cho trong bảng sau:

***Bảng 1.*** *Bảng tiêu chuẩn kích thước an toàn cho cặp tham số nguyên tố (p,q) theo FIPS 186-3.*

| L | 1024 | 2048 | 2048 | 3072 |
|---|---|---|---|---|
| N | 160 | 224 | 256 | 256 |

### 3.2. Sự tồn tại và số lượng các tham số p an toàn có dạng đặc biệt

Biết rằng các số p thỏa mãn q|(p-1) là các số có dạng p = x.q+1, còn theo định nghĩa về các số đặc biệt thì p = $b^k - a$ với a < $b^{\lfloor k/2 \rfloor}$. Lấy b = 2 thì với ký hiệu như đã đưa ra trong bảng 2 ta có đẳng thức sau:

$$2^L - a = x.q + 1 \quad (3)$$

Và từ điều kiện đối với a < $2^{\lfloor L/2 \rfloor}$ ta có các giá trị x trong đẳng thức trên thỏa mãn bất đẳng thức sau:

$$(2^L - 2^{\lfloor L/2 \rfloor} - 1)/q \leq x \leq (2^L - 1)/q \quad (4)$$

Như vậy, ứng với mỗi q thì số các số nguyên x, ký hiệu là X(q), trong khoảng trên có thể coi là xấp xỉ

$$X(q) \approx (2^L - 2^{\lfloor L/2 \rfloor} - 1) - (2^L - 1)/q = 2^{\lfloor L/2 \rfloor}/q \approx 2^{\lfloor L/2 \rfloor}/2^N = 2^{\lfloor L/2 \rfloor - N} \quad (5)$$

Theo định lý Gauss về số các số nguyên tố không vượt quá giá trị B nguyên dương cho trước là một vô cùng lớn tương đương với B/ln(b) nên áp dụng cho B=$2^L$ và với số lượng các số nguyên dạng $x.q + 1$ được xét (là X(q)) chúng ta có thể ước lượng được số các số nguyên tố an toàn theo FIPS 186-3 có dạng đặc biệt ứng với mỗi q cụ thể, ký hiệu là P(q,L), được cho bởi xấp xỉ sau:

$$P(q,L) \approx (2^{\lfloor L/2 \rfloor - N})/L.\ln 2. \quad (6)$$

Cũng theo lập luận trên thì số các số nguyên tố M bít q, ký hiệu là Q(M), được xấp xỉ

$$Q(M) \approx 2^N/N.\ln 2 \quad (7)$$

Tóm lại, số các cặp số nguyên tố (p,q), ký hiệu là PQ(L,M), an toàn theo chuẩn kích thước (L,M) của FIPS186-3 có dạng đặc biệt được đánh giá theo xấp xỉ sau:

$$PQ(L,M) = P(q,L).Q(M) \approx 2^{\lfloor \frac{L}{2} \rfloor}/(L.M.\ln^2 2). \quad (8)$$

## 4. SINH CÁC CÁC THAM SỐ p AN TOÀN CÓ DẠNG ĐẶC BIỆT

### 4.1. Thuật toán sinh các tham số p an toàn dạng đặc biệt

Input: L, N là hai số nguyên dương (theo một cột nào đó của bảng 1).

Output: (p, q) là cặp số nguyên tố an toàn theo độ dài tương ứng theo FIPS 186-3.

1 q ← random$(2^{N-1}, 2^N)$.

2 if (q is not prime) theo goto 1.

3 A ← $\lceil (2^L - 2^{\lfloor L/2 \rfloor} - 1)/q \rceil$; B ← $\lfloor 2^L - 1)/q \rfloor$.

4 x ← random[A,B].

5 p ← x.q+1.

6 if (p is not prime) theo goto 4.

7 return (p,q).

### 4.2. Một số nguyên tố an toàn có dạng đặc biệt

Chúng tôi đã tiến hành lập trình việc tìm các số nguyên tố an toàn theo bảng 1 và có dạng đặc biệt với hai cặp kích thước an toàn (2048, 256).

*4.2.1. Năm số nguyên tố 256 bít nhỏ nhất*

q1=57896044618658097711785492504343953926634992332820282019728792003956564820063 (77 chữ số thập phân);

q2=57896044618658097711785492504343953926634992332820282019728792003956564820109 (77 chữ số thập phân);

q3=57896044618658097711785492504343953926634992332820282019728792003956564820243 (77 chữ số thập phân);

q4=57896044618658097711785492504343953926634992332820282019728792003956564820301 (chữ số thập phân);

q5=57896044618658097711785492504343953926634992332820282019728792003956564820411 (77 chữ số thập phân).

*4.2.2. Năm số nguyên tố 256 bít lớn nhất*

q6=1157920892373161954235709850086879078532699846656405640394575840079131296393 19 (78 chữ số thập phân);

q7=1157920892373161954235709850086879078532699846656405640394575840079131296393 49 (78 chữ số thập phân);

q8=1157920892373161954235709850086879078532699846656405640394575840079131296395 01 (78 chữ số thập phân);

q9=11579208923731619542357098500868790785326998466564056403945758400791312963957 9 (78 chữ số thập phân);

q10=11579208923731619542357098500868790785326998466564056403945758400791312963974 7 (78 chữ số thập phân);

*4.2.3. Năm số nguyên tố dạng* $p_i = x.q_i + 1 = 2^{2048} - a$ *với a bé nhất*

p1 = x.q1+1 = 2^2048 - 1384412242564634744947518065014002407931385200982458653640883634250230765977 5 (77 chữ số thập phân);

p2 = x.q2+1 = 2^2048 - 6864059495656446178650736281709008519708177846013286003174444754242587754495 9 (77 chữ số thập phân);

p3 = x.q3+1 = 2^2048 - 2618875719086104141821463328702523553909562323294351015500749214051900762882047 (79 chữ số thập phân);

p4 = x.q4+1 = 2^2048 - 5801484143237310283387883360314272759604293399663310996762907260249941995028 47 (78 chữ số thập phân);

p5 = x.q5+1 = 2^2048 - 1526175346348151568497590469081363452440272692781144725179763817801947650850815 (79 chữ số thập phân).

## 5. KẾT LUẬN

Dựa trên thuật toán tính toán giá trị modulo của Barrett và định lý Karatsuba và Ofman, nhóm tác giả đã đề xuất thuật toán modulo dựa trên số nguyên tố p "đặc biệt" đảm bảo độ an toàn theo chuẩn FIPS 168-3 và có thời gian tính toán nhỏ hơn so với thuật toán của Barrett. Bài báo chứng minh được sự tồn tại của các số nguyên tố p dạng đặc biệt (lập trình tính toán một số cặp giá trị ví dụ trong mục 4.2). Thuật toán khi được ứng dụng vào các giao thức thiết lập khóa sẽ làm giảm thời gian tính toán để hình thành khóa bí mật chung chia sẻ, do vậy, bài báo có ý nghĩa thực tế cao, đặc biệt là đối với các hệ thống đòi hỏi thời gian thực.

## TÀI LIỆU THAM KHẢO

[1]. Darrel Hankerson, Alfred Menezes and Scott Vanstone. "*Guide to Elliptic Curve Cryptography"*. 2004 Springer-Verlag New York, Inc.

[2]. Digital Signature Standard (DSS). "*Federal Information Processing Standards Publication 186-2"*. National Institute of Standards and Technology, June 2000.

[3]. Digital Signature Standard (DSS). "*Federal Information Processing Standards Publication 186-3"*. National Institute of Standards and Technology, June 2009.

[4]. Donald E. Knuth. "*The Art of Computer Progamming (second edition)"*. Addison-Weslay Publishing Company 1978.

[5]. A. Karatsuba and Y.Ofman. "*Multiplication of multidigit numbers on automata"*. Soviet Physics-Doclady. 7: pp. 595-596. 1963.

## ABSTRACT

### A SPECIAL FORM OF PRIME PARAMETER P BASED ON THE DISCRETE LOGARITHM PROBLEM OF GF (P) FILED

*When using public key cryptosystems such as RSA, Elgamal, Diffie-Helman, etc., we are not concern only about the safety but also on their effectiveness. The paper proposes a special form of prime parameter p with the aim of supporting fast computation on GF (p) filed, without compromising the safety of the public key cryptosystems based on discrete logarithm problem of GF (p) filed.*

**Keywords:** Public key cryptosystems, Discrete logarithm problem, Key Exchange protocols.

*Nhận bài ngày 08 tháng 3 năm 2017*
*Hoàn thiện ngày 06 tháng 4 năm 2017*
*Chấp nhận đăng ngày 01 tháng 5 năm 2017*

*Địa chỉ:* [1] Binh chủng Thông tin liên lạc;
[2] Cục Cơ yếu / Bộ Công an;
[*] Email: viethv76@gmail.com.