

## Maurer 法をベースとした確定的素数判定による Safe Prime 生成法とその高速化

熊給 英洋 丹羽 朗人

東芝ソリューション株式会社 IT 技術研究所 〒183-8512 東京都府中市片町 3-22

あらまし 暗号分野においては、 $p$  を素数としたとき、 $2p+1$  という形の素数が、しばしば用いられる。この形の素数は Safe Prime と呼ばれ、Diffie-Hellman 鍵交換を始めとして、多くの暗号プロトコルで用いられている。この Safe Prime の高速生成法としては、これまで Miller-Rabin 法をベースとする方法があった。しかしながら確率的素数判定法であるため、僅かではあるが Safe Prime でないものを生成する可能性があった。本稿では確定的素数判定である Mauer 法をベースに用いた Safe Prime の効率的な生成法を複数取り上げ、それらの理論的な検討と実験による検証を行う。結論として Mauer 法を用いた最も効率の良い Safe Prime 生成法を 1 つ導き出した。また確率的素数判定法を用いた生成法に比べても同等の速度が実現できるという結果を得た。

キーワード Safe Prime, Sophie Germain Prime, Maurer 法, Euler-Lagrange の定理, Miller-Rabin 法, 素数生成法

## Fast Generation of Safe Primes using Deterministic Primality Tests based on Maurer Method

Hidehiro Kumakyu Akito Niwa

Advanced IT Laboratory, Toshiba Solutions Corporation 3-22 Katamachi, Fuchu-shi, Tokyo, 183-8512 Japan

E-mail: Kumakyu.Hidehiro@toshiba-sol.co.jp, Niwa.Akito@ toshiba-sol.co.jp

**Abstract** A prime number of the form  $2p + 1$ , where  $p$  is also a prime is often used in cryptography. The prime of this form is called "Safe Prime". Safe prime is used by a lot of cryptographic protocols including Diffie-Hellman key exchange. To generate the Safe Prime, some methods based on the Miller-Rabin method are known, however these methods can generate prime numbers probabilistically. We analyzed several determinate methods based on the MaurerMethod, and the result was verified experimentally. We deduced the most effective method, whose efficieancy was almost same as the probabilistic methods.

**Keyword** Safe Prime, Sophie Germain Prime, Maurer Method, Euler-Lagrange theorem, Miller-Rabin method, Prime Generation

### 1. はじめに

暗号分野においては、 $p$  を素数としたとき、 $2p+1$  という形の素数 Safe Prime が暗号の安全性を高めるために、しばしば用いられる。Safe Prime は Diffie-Hellman 鍵交換を始めとして、多くの暗号プロトコルで用いられている。

この Safe Prime の生成法の中で最も素朴な方法として、文献 [2] の方法が挙げられるが、その後、種々の工夫がなされており(文献 [6] [12])、現在最も効率的と思われる方法としては文献 [1] に記述された方法が挙げられる。しかしながら、この方法は確率的素数判定法である Miller-Rabin 法をベースとするものであり、僅かではあるが誤判定により Safe Prime でない数を生成す

る可能性がある。

本稿では、確定的な素数生成法である Mauer 法をベースに用いた Safe Prime の確定的な生成法を検討する。この方法は手順を変えることにより複数の生成法を考えることができるために、それらの理論的な検討と実験による検証を行う。ここで速度比較のため、従来の Safe Prime 生成法についても実装する。そして検討の結果、Mauer 法を用いた最も効率の良い Safe Prime 生成法を 1 つ導き出した。一般に確定的素数生成法は、確率的素数生成法よりも速度的に劣るとされるが本手法では文献 [1] の方法と比べて同等な速度が実現できることがわかった。

## 2. 準備

### 2.1. 定義

#### 定義 1. Safe Prime

奇数の整数  $q$  が Safe Prime であるとは、次の 2 条件が成り立つことをいう。

$$q = 2p + 1$$

とする時、

1.  $q$  は素数
2.  $p$  は素数

#### 定義 2. Sophie Germain 素数

奇数の整数  $p$  が Sophie Germain 素数であるとは、次の 2 条件が成り立つことをいう。

$$q = 2p + 1$$

とする時、

1.  $p$  は素数
2.  $q$  は素数

従って、整数  $p$  が Sophie Germain 素数であることと、 $q = 2p + 1$  が Safe Prime であることは、同値である。

### 2.2. 記号

本稿では、Safe Prime を表す文字として  $q$  を用い、その  $q$  は

$$q = 2p + 1, \quad p \text{ は奇数}$$

の関係式を満たすものとする。

また、表 1 の略号を使用する。

表 1 本稿で使用する略号

MR	Miller-Rabin テスト（底の数は各々括弧内に明示）
EEL	拡張された Euler-Lagrange の定理による素数判定
LL	Lucas-Lehmer テスト
Maurer	Maurer 法
PL	Pocklington の定理
PL_1	Pocklington の定理の Fermat テスト
PL_2	Pocklington の定理の最大公約数テスト
L+1	生成する Safe Prime のビット数
L	生成する Sophie Germain 素数のビット数

### 2.3. 素数判定/生成法、関連する定理

本節では本稿で用いる一般的な素数判定/生成法及び関連する定理について概説する。特に Safe Prime 判定に用いられる Euler-Lagrange の定理について述べる。

#### 2.3.1. 試行割算テスト

試行割算は、対象整数の平方根以下の素数で割った余りが全て 0 ではないことを検証する確定的素数判定法である（文献[5]）。しかし対象整数が大きい場合、

処理時間が増大するという問題があり、他の判定の前処理として一定程度の大きさまで試行割算する、という使われ方がなされる。

#### 2.3.2. Miller-Rabin テスト

Miller-Rabin テストは多くの標準規格（文献[5]等）に取り入れられるなど、最も広く利用されていると考えられる素数判定法であり、実際に他の判定法に比べ短時間で効率よく素数を判定することが可能である。

この判定法は、確率的判定法であり、入力が素数の場合は必ず素数と判定されるが、入力が合成数の場合はある確率で合成数を素数と誤判定することがある。従って実際には異なる数種類の底に対して Miller-Rabin テストを行い、誤判定する確率を出来る限り低減することが行われる。例として文献[5]では、512 ビットの素数生成には、後に述べる Lucas-Lehmer 法と組み合わせた場合、8 個の底に対する Miller-Rabin テストを行うことで、誤判定率を

$$\frac{1}{2^{100}}$$

にまで低減することが出来ると記述されている。

入出力・ステップは、以下の通りである。尚、詳細は[5]を参照のこと。

##### Miller-Rabin テスト

入力：判定対象の整数  $n$ 、底  $a$

出力：probable prime/composite

ステップ：

MR-1 次の形に分解

$$n = 2^s \cdot t + 1, \quad t \text{ は奇数}$$

MR-2 次の式を計算し、 $g$  が  $n$  を法として、 $\pm 1$  と合同であれば、恐らく素数(probable prime)と判定

$$g = a^t \pmod{n}$$

MR-3 次の計算を  $s-1$  回行い、途中で  $g$  が  $n$  を法として  $-1$  と合同であれば、恐らく素数(probable prime)と判定

$$g = g^2 \pmod{n}$$

MR-4 合成数(composite) と判定

#### 2.3.3. Lucas-Lehmer テスト

Lucas-Lehmer テストは MR テストと同様な確率的判定法であり、次に述べる理由により単体としてではなく、複数回の MR テストと組み合わせて利用される事が多い。一般に MR テストを通過する整数は強擬素数と呼ばれるが、複数回の MR テストを通過した場合も、僅かな確率で合成数となることがある。LL と MR を組み合わせているのは、LL と MR の擬素数のグループ

が異なるためであり、この強擬素数を排除するため MR テストと組み合わせて用いられる。本稿では LL テストに対する効率化は行わないため、ステップについては記述しない。詳細は文献[5]を参照のこと。

### 2.3.4. Euler-Lagrange の定理

Euler-Lagrange の定理は  $p \equiv 3 \pmod{4}$  が素数であるという仮定の元で、 $q$  が素数であるための必要十分条件を与える定理である。Safe Prime の判定等に用いられる。

#### Euler-Lagrange の定理

$p \equiv 3 \pmod{4}$  が素数とする。X を

$$X = 2^p - 1 \pmod{q}$$

とすると次が成り立つ。

X が 0 である  $\Leftrightarrow q$  は素数

本定理では  $p \equiv 1 \pmod{4}$  が素数の場合に対応出来ないため、Safe Prime 生成には、それを補う任意の奇数  $p$  に適用可能な次の定理が用いられる。

### 2.3.5. 拡張された Euler-Lagrange の定理

#### 拡張された Euler-Lagrange の定理

X を  $p \equiv 3 \pmod{4}$  が素数の時、

$$X = 2^p - 1 \pmod{q}$$

とし、 $p \equiv 1 \pmod{4}$  が素数の時、

$$X = 2^p + 1 \pmod{q}$$

とすると次が成り立つ。

X が 0 である  $\Leftrightarrow q$  は素数

本定理を用いることで  $p$  が奇素数の場合に、誤判定することなく確実に  $q$  の素数性を判定出来る。一方  $p$  が合成数の場合、EEL を  $q$  の底 2 に対する Miller-Rabin テストと考えることができるために一定の誤判定率はあるが、 $q$  が素数の場合に通し、合成数の場合に排除する事が可能である。尚この拡張された Euler-Lagrange の定理という名称は、本稿における呼び方である点に注意する。詳細は文献[9]を参照のこと。

### 2.3.6. Pocklington の定理

Pocklington の定理は奇数が素数であるための十分条件を与える定理であり、詳細は文献[2]等に記載されている。本稿で以下に述べるのは一般的な Pocklington の定理の特別な場合であることに注意する。

#### Pocklington の定理

ある整数  $a$  が存在し、次の 2 条件 (PL\_1, PL\_2) が成り立つ時、 $p$  は素数である。

#### PL\_1

$$a^{p-1} \equiv 1 \pmod{p}$$

#### PL\_2

$$\text{g.c.d.}\left(a^{\frac{p-1}{F}} - 1, p\right) = 1$$

ここで、 $p$  は以下の条件を満たすものとする。

$$p = 2RF + 1$$

F は素数

R は  $2R < F$  を満たす整数

本稿においては、PL\_1 を Fermat テストと呼び、PL\_2 を最大公約数テストと呼ぶ。また、本稿では a を 2 として固定する。

### 2.3.7. Maurer 法

Maurer 法は文献[4], [5]に記載されている代表的な確定的素数生成法である。但し、一般的なその他の確率的素数生成法（判定法）と比べ、出力される素数の形状に制限があり、素数の一様性に関して問題があるのでとの指摘もある。しかし、僅かな誤差で合成数を誤判定する可能性のある確率的素数判定法に比べ、同程度もしくは多少劣る程度の計算量（例えば文献[1]によると、Maurer 法は底 1 つの MR テストとほぼ同等か少し悪い速度である）で、必ず素数が生成出来るという大きな利点がある。

Maurer 法では 2.3.6 節に示す Pocklington の定理を再帰的に用いて確定的に素数を生成する。具体的なステップは、以下の通りである。

#### Maurer 法

入力：生成素数のビット数 M

出力：M ビット素数

ステップ：

##### Maurer\_1

予め定められたビット数（数ビット程度）の乱数を生成し、試行割算により確定的に素数 F を生成する。

##### Maurer\_2

$2R < F$  を満たす乱数 R を用いて、 $F'$  を

$$F' = 2RF + 1$$

と置き、Pocklington の定理を用いて素数判定する。

##### Maurer\_3

Maurer\_2 において  $F'$  が素数と判定されなかった場合は Maurer\_2 へ戻り、 $F'$  が素数と判定された場合は、 $F'$  が M ビット素数となるまで  $F'$  を F に再帰的に代入し Maurer\_2 へ戻る処理を繰り返す。

### 2.4. 従来の Safe Prime 生成法

従来の Safe Prime 生成法である Test1 から Test4 について、各節に分けて説明する。

#### 2.4.1. MR&MR

実装した手法の Test1 にあたる。最も初等的な Safe Prime 生成法として文献[2]に記載されており、 $p$  及び  $q$  に複数回の Miller-Rabin テストを行う手法である。しかし本手法は処理に大変無駄が多く、以後に述べる改良法に比べ処理時間が極めて大きくなるという問題がある。この場合でも、 $p$  及び  $q$  に複数回の Miller-Rabin テストを行う前処理として、 $p$  及び  $q$  に試行割算を行うことで、大幅に処理時間を低減することが可能である。また、MR が確率的素数生成法であるため、僅かではあるが非 Safe Prime を Safe Prime と判定する可能性が残る。

##### Test1 のステップ

1.  $p$  及び  $q$  の試行割算
2.  $p$  の MR テスト（複数回）
3.  $q$  の MR テスト（複数回）

#### 2.4.2. MR&EEL

実装した手法の Test2 にあたる。上記2.4.1節の方法において、 $q$  の判定に MR テスト（複数回）を用いる代わりに EEL テストを用いる手法である。本手法では  $p$  が素数の場合に、 $q$  に対して複数回の MR テストを行うことにより発生する複数回の幂乗剰余算を回避し、幂乗剰余算 1 回の EEL テストで、確実に  $q$  を素数判定することが出来る点が改善されている。しかし、この手法では  $p$  が素数で  $q$  が合成数の場合に、 $p$  が素数であることを確定させるための処理（複数回の幂乗剰余算）が無駄になるという問題がある。また、本手法では  $p$  を MR テスト（複数回）で誤判定した場合、 $q$  の EEL テストで誤判定する可能性が残り、結果として非 Safe Prime を Safe Prime と判定する可能性が残る。

##### Test2 のステップ

1.  $p$  及び  $q$  の試行割算
2.  $p$  の MR テスト（複数回）
3.  $q$  の EEL テスト

#### 2.4.3. MR&EEL（最適化）

実装した手法の Test3 にあたる。上記2.4.2節の方法において、 $p$  が素数で  $q$  が合成数の場合に、 $p$  の素数性を判定する処理が無駄になる問題を回避するための手法である。文献[1]によると、MR と EEL を組み合わせた手法として最も利用されていると考えられる。また、MR と EEL を組み合わせた手法としては、最も高速かつ誤り率の低い方法と考えられる。このことの根拠は、文献[1]及び4章の実測結果による。本手法と上記2.4.2節の方法との違いは、 $p$  が MR テストを 1 回通過すれば素数である確率はかなり高いという経験的事実（文献[10], [11]）を仮定することで、 $p$  の MR テストを 1 回行った後、 $p$  の判定はよい精度で行えたとして、次に  $q$  の EEL テストを行い、その後  $p$  の素数性をより確

実にするために、複数回の  $p$  の MR テストに戻る点にある。本手法においても、2.4.2節と同様に、 $p$  の MR テストで失敗した場合に、非 Safe Prime を Safe Prime と判定する可能性が残る。

##### Test3 のステップ

1.  $p$  及び  $q$  の試行割算
2.  $p$  の MR テスト（底 2 に対するテスト）
3.  $q$  の EEL テスト
4.  $p$  の MR テスト（複数回）

#### 2.4.4. EEL&MR

実装した手法の Test4 にあたる。本手法は上記2.4.3における、1 回目の底 2 に関する  $p$  の MR テストと、 $q$  の EEL テストの順番を入れ替えた手法である。ここで  $q$  の EEL テストの処理時間は、

$$2^p \pmod{q}$$

を 1 回行うのに必要な処理時間程度である。一方、底 2 に関する  $p$  の MR テストの処理時間は、

$$p = 2^s \cdot t + 1, \quad t \text{ は奇数}$$

とおいた時、 $s-1$  回の幂乗剰余算を行うための処理時間程度である。従って上記2.4.3節に比べると、EEL テストを行う本テストの方がより高速に最初の判定を行うことができると言えられる。しかし、 $p$  が合成数の場合に EEL テストで誤判定する確率が明らかではないため、上記2.4.3節より高速に判定できるか否かについては不明であり、今回は実測を行って処理時間を確かめることとする。

##### Test4 のステップ

1.  $p$  及び  $q$  の試行割算
2.  $q$  の EEL テスト
3.  $p$  の MR テスト（複数回）

### 3. 提案する Safe Prime 生成法

#### 3.1. 提案法のアルゴリズム(Maurer 法をベースとする Safe Prime 生成法)

従来法では MR テスト（複数回）と EEL テストの組替え・並び替えを行うことで、無駄な計算を省き効率的に Safe Prime を生成していた。しかしこの方法では、MR テストが確率的素数判定法であるため、僅かではあるが合成数を素数と判定することにより、非 Safe Prime を Safe Prime と判定するという問題があった。また MR テストと EEL テストを用いる場合は、生成時間をこれ以上改善させるのは難しいと考えられる。

本提案では、この MR テストと EEL の並び替えのアイデアを Maurer 法と EEL を用いた場合に適用し、更に Maurer 法を用いた Safe Prime 生成法に特化した高速化を適用させた 7 つの Safe Prime 生成法について検討

する。そしてそれらを理論的に考察し、実装実験により検証することで、最も高速な確定的 Safe Prime 生成法を探る。以下 Maurer 法を用いた 7 つの実装法について説明する。

### 3.1.1. Maurer&EEL (最適化なし)

実装した手法の Test5 にあたる。Maurer 法と EEL の最も初等的な組み合わせによる Safe Prime 生成法である。次節以降の他の提案法との比較のための手法であり、ステップは、以下の通りである。

#### Test5 のステップ

1.  $p$  及び  $q$  の試行割算
2.  $p$  を Maurer 法で生成
3.  $q$  の EEL テスト

この単純な手法ではステップ 3 で失敗した場合、ステップ 2 で  $p$  が素数であることを確定させた処理が無駄になってしまふ。この処理の無駄を省くための工夫を行ったのが、次節に述べる手法である。

### 3.1.2. Maurer&EEL (最適化：組替え・MR 法)

実装した手法の Test6 から Test11 にあたる。本手法では、Sophie Germain 素数候補  $p$  を

$$p = 2RF + 1$$

と置く時の  $F$  を Maurer 法で生成し、以後はこの  $F$  を固定させたまま、 $R$  を変化させて  $p$  を生成する。 $p$  の生成後、本手法では

- (A)  $p$  を PL\_1 で素数判定
- (B)  $p$  を PL\_2 で素数判定
- (C)  $q$  を EEL で素数判定

という 3 つのステップを行う必要がある。今回は (A)・(B)・(C) の順番を並び替えた 6 つの手法を実装する。

ここで、(A) の処理を

#### (A)'…底 2 に対する MR テスト

に置き換える。この置き換えを行っても本アルゴリズムにより確定的に Safe Prime を生成することが出来る。何故なら (A)' を通過する  $p$  は (A) を通過するので、(B) と合わせて Pocklington の定理が成り立つ十分条件が成り立つためである。この変更によるメリットは、

- Fermat テストより高速
  - Fermat テストより効率よく合成数を排除可能
- の 2 つが考えられる（文献[4]）。以後 (A)' を (A) とする。このとき、(A) 及び (C) を  $p$  及び  $q$  の MR テストと考えることが出来る。すると 2.4.3 の時と同様に考え、1 度の MR テストにより、 $p$  および  $q$  の素数性をほぼ確定することが出来ると仮定すると、(A) 及び (C) を (B) より先に行う手法が効率的と考えられる。すなわち (B) を最後に行う、Test7 と Test10 が 6 つの手法の中で最速な手法の候補と考えられる。また、

一般にあるビット数の整数が

- 1 つの底に対する MR テストを通過する確率
- EEL テストを通過する確率

を比べると、EEL テストを通過する確率の方が低いという事実により、(C) を先に行う Test10 が最速であると考えられる。

#### Test6 から Test11 のステップ

1.  $p=2RF+1$  の  $F$  を Maurer 法で生成
  2.  $p$  及び  $q$  の候補を生成
  3.  $p$  及び  $q$  の試行割算
  4. (A)から(C)のテストを行い  $p$  および  $q$  を素数判定
- Test5～Test11 の各判定法の詳細をまとめると表 2 のようになる。

表 2 Safe Prime 生成法(Test5～Test11)

名称	判定法の詳細		
Test5 (※ 1)	①	A	
	②	B	
	③	C	
Test6 (※ 1)	①	A	
	②	B	
	③	C	
Test7	①	A	
	②	C	
	③	B	
Test8	①	B	
	②	A	
	③	C	
Test9	①	B	
	②	C	
	③	A	
Test10	①	C	
	②	A	
	③	B	
Test11	①	C	
	②	B	
	③	A	

(※ 1) Test5 と Test6 の違い… Test5 では Maurer 法を用いて毎回素数  $F$  を生成するが、Test6 では一度生成した  $F$  を再利用し、 $p$  に対して Pocklington の定理による素数判定を行う。また Test7 から Test11 についても、Test6 と同様に一度生成した  $F$  を元に  $p$  を生成する。

### 3.2. 通過確率見積もり

本節では、

- 単純に Maurer 法と EEL の組み合わせた Test6
- 高速と考えられる Test10

について、通過確率を理論的に比較する。

表 3 Test6 と Test10 のステップ

	①	②	③
Test6	$P$ の MR(底 2)	$p$ の PL_2	$q$ の EEL

Test10	q の EEL	p の MR (底 2)	p の PL_2
--------	---------	--------------	----------

※①から③は処理の順番を示す。

まず Test10 が Test6 より演算負荷が少ないと思われる直感的な理由を示す。

Test6 では p が①を通過した（すなわち、強擬素数である）場合、経験上、2 が p を法とする原始根である可能性が高いため、ほぼすべての p は②も通過すると考えられ、結果として③までたどり着く Safe Prime 候補は多くなると考えられる。

一方 Test10 では q が①を通過した場合、②で p が MR テストを通過する確率は高くはなく、従って③までたどり着く Safe Prime 候補は少なくなり、トータルとして p の PL\_2 テストを行う回数を減らすことが出来ると考えられる。

次に Test10 が Test6 より演算負荷が少ない理由を理論的に調べる。最初に、Test10 を最後まで通過する確率と、Test6 を最後まで通過する確率は、同内容のテストを順番を変えて行っているため、等しくなる事に注意する。すなわち Test10 と Test6 は①から③まで通りテストを通過する確率が等しいため、Test10 及び Test6 がそれぞれ①と②を連続して突破する確率を比較することで、どちらがより効率よく合成数を排除出来るのか判定することが出来る。

以下、事象 X が起こる確率を

$$\Pr(X)$$

と表す。また以下の記号を用いることとする。

A1 … Test6 の①を通過する事象

A2 … Test6 の②を通過する事象

A3 … Test6 の③を通過する事象

B1 … Test10 の①を通過する事象

B2 … Test10 の②を通過する事象

B3 … Test10 の③を通過する事象

まず始めに Test6 の場合を考える。A1 を通過して A2 を通過する確率  $\Pr(A2 | A1)$  を求めると、

$$\Pr(A2 | A1) = \Pr(A2 \cap A1) / \Pr(A1)$$

である。一方 K を “p が素数である” 事象とすると、

$$\Pr(A2 \cap A1) = \Pr(A2 \cap A1 \cap K)$$

より、

$$\begin{aligned} & \Pr(A2 \cap A1) / \Pr(K) \\ &= \Pr(A2 \cap A1 \cap K) / \Pr(K) \\ &= \Pr(A2 \cap K) / \Pr(K) \\ &= \Pr(A2 | K) \end{aligned}$$

すなわち、

$$\begin{aligned} & \Pr(A2 \cap A1) / \Pr(K) \\ &= \Pr(A2 | K) \end{aligned}$$

となる。ここで  $\Pr(A2 | K)$  は、“2 が p を法とする原始根である” 確率よりも高い。これは Pocklington の定理で底を 2 としていることによる。そして、“一般 Riemann 予想”を仮定すると、それは、0.37395 以上である(文献[8])。また、

$$\begin{aligned} & \Pr(K) / \Pr(A1) \\ &= \Pr(K \cap A1) / \Pr(A1) \\ &= \Pr(K | A1) \end{aligned}$$

となるが、これは強擬素数が素数である確率である。L ビット整数に対して k 個の底に関する MR テストを行った時に誤判定する確率の上界を  $p(L, k)$  とおくと、

$$\Pr(K) / \Pr(A1) \geq 1 - p(L, 1)$$

となるため、以上をまとめて、

$$\begin{aligned} & \Pr(A2 | A1) \\ &= \Pr(A2 \cap A1) / \Pr(A1) \\ &= \Pr(A2 \cap A1) / \Pr(K) \times \Pr(K) / \Pr(A1) \\ &\geq 0.37 \times (1 - p(L, 1)) \end{aligned}$$

となる。次に Test10 の場合を考え、B1 を通過して B2 を通過する確率  $\Pr(B2 | B1)$  を求める。

まず始めに、EEL で行われるテストは 2 を底とする MR テストとほぼ同一なので、両者を同一視することで、

$$\Pr(B1) = \frac{\Pr(K)}{1 - p(L+1, 1)}$$

となる。

次に C を “p が Sophie Germain 素数である” 事象とすると、

$$\begin{aligned} & \Pr(B1 \cap B2) \\ &= \Pr(B1 \cap B2 \cap K) + \Pr(B1 \cap B2 \cap \bar{K}) \\ &= \Pr(C) + \Pr(B1 \cap B2 \cap \bar{K}) \end{aligned}$$

である。ここで B1 と  $B2 \cap \bar{K}$  が独立であることを仮定すると、

$$\Pr(B1 \cap B2 \cap \bar{K}) = \Pr(B1) * \Pr(B2 \cap \bar{K})$$

となる。また、

$$\Pr(B2 \cap \bar{K}) = \frac{p(L, 1)}{1 - p(L, 1)} * \Pr(K)$$

であるから、

$$\frac{\Pr(B_1 \cap B_2 \cap \bar{K})}{\Pr(B_1)} = \frac{p(L, 1)}{1 - p(L, 1)} * \Pr(K)$$

が成り立つ。一方、Sophie Germain 素数の分布予想（文献[13]）より、

$$\Pr(C) = \frac{1.32}{(\log 2)^2} * \frac{L^2 - 4L + 2}{L^2(L-1)^2}$$

であるから、

$$\frac{\Pr(C)}{\Pr(B_1)} = \frac{1.32}{(\log 2)^2} * \frac{L^2 - 4L + 2}{L^2(L-1)^2} * \frac{1 - p(L+1, 1)}{\Pr(K)}$$

となるので、まとめて、

$$\begin{aligned} & \Pr(B_2 | B_1) \\ &= \frac{\Pr(B_1 \cap B_2)}{\Pr(B_1)} \\ &= \frac{\Pr(C)}{\Pr(B_1)} + \frac{\Pr(B_1 \cap B_2 \cap \bar{K})}{\Pr(B_1)} \end{aligned}$$

となり、従って

$$\begin{aligned} & \Pr(B_2 | B_1) \\ &= \frac{1.32}{(\log 2)^2} * \frac{L^2 - 4L + 2}{L^2(L-1)^2} * \frac{1 - p(L+1, 1)}{\Pr(K)} \\ &+ \frac{p(L, 1)}{1 - p(L, 1)} * \Pr(K) \end{aligned}$$

を得る。ここで素数定理と MR テストの誤判定率（いずれも文献[2]記載）について、

$$\Pr(K) = \frac{2}{\log 2} * \frac{L-2}{L(L-1)}$$

$$p(L, k) \leq \left(\frac{1}{4}\right)^k$$

であるから、例えば L=512 の時、

$$\Pr(A_2 | A_1) \geq 0.2775$$

$$\Pr(B_2 | B_1) \leq 0.004453$$

となる。従って Test10 は Test6 に比べ②を通過する Safe Prime 候補の数が約 1/62 倍になる。

また L=1024 の時、

$$\Pr(A_2 | A_1) \geq 0.2775$$

$$\Pr(B_2 | B_1) \leq 0.001868$$

となり、Test10 は Test6 に比べ②を通過する Safe Prime

候補の数が約 1/148 倍になる。

すなわちいずれの場合も Test10 の手法は、Test6 の手法より計算量を少なく出来ると考えられる。

ここで  $\Pr(B_2 | B_1)$  の上界を見積もる際に、第一項の  $1 - p(L+1, 1)$  を 1 としている点に注意する。

## 4. 実装結果と考察

### 4.1. 実装する Safe Prime 生成法一覧

今回実装する、既知の Safe Prime 生成法と、提案する Safe Prime 生成法をまとめると表 4 の通りである。

表 4 Safe Prime 生成法一覧（全判定法）

名称	試行割算	p の判定法	q の判定法	判定順	節
Test1	無	MR	MR	$p \rightarrow q$	2.4.1
Test2	有	MR	EEL	$p \rightarrow q$	2.4.2
Test3	有	MR	EEL	$p \rightarrow q \rightarrow p$	2.4.3
Test4	有	MR	EEL	$q \rightarrow p$	2.4.4
Test5	有	Maurer	EEL	$p \rightarrow p \rightarrow q$	3.1.1
Test6	有	Maurer	EEL	$p \rightarrow p \rightarrow q$	3.1.2
Test7	有	Maurer	EEL	$p \rightarrow q \rightarrow p$	3.1.2
Test8	有	Maurer	EEL	$p \rightarrow p \rightarrow q$	3.1.2
Test9	有	Maurer	EEL	$p \rightarrow q \rightarrow p$	3.1.2
Test10	有	Maurer	EEL	$q \rightarrow p \rightarrow p$	3.1.2
Test11	有	Maurer	EEL	$q \rightarrow p \rightarrow p$	3.1.2

Test1 から Test4 は MR と他の手法を組み合わせる既存の手法であり MR テスト（複数回）を用いる際に LL テストを合わせて行う。Test5 から Test11 は提案法の実装であり p を Maurer 法で生成し q を EEL で判定する。

### 4.2. 実装結果

従来法と提案法の実装結果を表 5 に示す。

表 5 平均速度測定結果

	Test名	Safe Prime 1 個あたりの平均生成時間（※注）	p の判定法	q の判定法
従来法	Test1	5.950	MR 法 (底 6 個)	MR 法 (底 6 個)
	Test2	4.989		
	Test3	4.745		
	Test4	4.633		
提案法	Test5	12.077	Maurer 法	EEL
	Test6	6.580		
	Test7	4.762		
	Test8	6.298		
	Test9	4.696		
	Test10	4.066		
	Test11	6.051		

※注・・・平均生成時間は、通常の素数を MR 法と LL 法の組み合わせによって生成するための時間を 1 として、それに対する比率で表している

表 6 平均速度結果（従来法）

	Test 名	Safe Prime 1 個あ たりの平均生成 時間 (10 回平均)	p の 判定法	q の 判定法
従 来 法	Test1'	385.715	MR 法 (底 6 個)	MR 法 (底 6 個)

Test1 と Test1' の違い・・・Test1 では p 及び q の MR テスト（複数回）を行う前に、p 及び q の試行割算を行なう。一方 Test1' では p 及び q の試行割算を行わない。ここでも、試行割算の効果は非常に高いことが分かる。また、速度実測環境は下記の通りとする。

表 7 速度実測環境

生成 Safe Prime の ビット長	512 ビット
CPU	Pentium4 2.40GHz
メモリ	760MB
コンパイラ	VC++7.0
OS	Windows XP Pro
開発言語	C 言語
Safe Prime の生成回数	100 回

#### 4.3. 考察

表 5 からは、以下の結果を読み取ることができる。すなわち、

- ・ 今回の Safe Prime 生成手法の実測では予測通り Test10 が最速であった
- ・ 従来法で最も高速な Test3 は、本実験でも既存の手法中で最速であり、今回提案した Maurer 法をベースとする手法の大部より高速であった
- ・ 今回行った 100 回の平均では処理速度が一様とならなく、実際には多少のばらつきが出る結果となった。これは、試行割算の占める時間の割合が大きいためであると考えられる。しかし概ね従来法と提案法との間に大きな差ではなく、十分実用に耐える時間で確定的に Safe Prime を生成できることが分かった

#### 5.まとめ

本稿では、従来確率的素数判定による生成法しか知られていなかった、Safe Prime の確定的素数判定による生成法を検討した。そのために、Maurer 法をベースに用いた Safe Prime の効率的な生成法を複数取り上げ、それらの理論的な検討と実験による検証を行い、最も効率的な手法を導き出した。また確率的素数判定法を用いた生成法に比べても同等の速度が実現できるという結果を得た。

但し理論的な検討には、

- ・ Sophie Germain 素数の分布予想
- ・ q が EEL を通過することと、p が合成数の時に PL\_2 を通過することは独立であるという仮定

といった、ヒューリスティックな部分も残されているため、これらの十分な検討とそれに基づく計算量の導出が今後の課題として挙げられる。

#### 文 献

- [1] R.Cramer, V.Shoup, "Signature Schemes Based on the Strong RSA Assumption", Feb. 2000.
- [2] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, FL, 1997.
- [3] I.Damgård, P.Landrock, and C.Pomerance, Average case error estimates for the strong probable prime test, Math. Comp. 61, pp.177-194, 1993.
- [4] 情報処理振興事業協会セキュリティセンター, "素数生成アルゴリズムの調査・開発 調査報告書", Feb. 2003.
- [5] ANSI X 9.80, "American National Standard for Financial Services - Prime Number Generation, Primality Testing and Primality Certificates", American National Standard Institute, 2001.
- [6] M.J.Wiener, "Safe Prime Generation with a Combined Sieve", Sep. 2003.
- [7] 中島俊哉, "Sophie Germain 素数に対する Euler の判定方法の披張について", 日本応用数理学会 "数論アルゴリズムとその応用" 研究部会 (JANT) 第 14 回研究集会プログラム, Jun. 2005
- [8] P.MOREE, "ARTIN'S PRIMITIVE ROOT CONJECTURE. - a survey -", Mathematics, abstract math.NT/0412262, Dec. 2004.
- [9] Henri Lifchitz, "Generalization of Euler-Lagrange theorem and new primality tests" available at "<http://ourworld.compuserve.com/homepages/hlifchitz/Henri/us/NouvThlus.htm>", Nov. 1998.  
(Last visited June 26, 2006)
- [10] J. Brandt, I. Damgård and P. Landrock, "Speeding up prime number generation", ASIACRYPT 91, LNCS 739, pp.440-449, 1991
- [11] 村上恭道、森井昌克、笠原正雄、"素数生成法の効率化に関する二、三の考察", Technical Report of IEICE, IT89-15, pp.19-22, 1989.
- [12] D.Naccache, "Double-Speed Safe Prime Generation", Cryptology ePrint Archive, Report 2003/175 available at "<http://eprint.iacr.org/>", 2003.  
(Last visited June 26, 2006)
- [13] P.Bateman and R.Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers" Math. Comp., 1962.