J. Math. Crypt. **3** (2009), 1–13
DOI 10.1515 / JMC.2009.xxx

The Miller-Rabin test with randomized exponents

Gebhard Böckle

Communicated by xxx

Abstract. We analyze a variant of the well-known Miller-Rabin test, that may be useful in preventing side-channel attacks to the random prime generation on smart cards: In the well-known Miller-Rabin primality test for a positive integer n, one computes repeatedly the expression $a^\omega \pmod n$ for random bases $a \in \mathbb{N}$ and exponents ω such that ω divides $n-1$ and $(n-1)/\omega$ is a power of 2. In each round one chooses, at random, a different base a, and uses binary exponentiation to compute $a^\omega \pmod n$. 'Listening' to many rounds, it seems at least plausible that an outside spy could retrieve the integer $n-1$.

In the variant we consider, one chooses in each round two positive random integers a and ρ and applies the test with base a and exponents $\omega\rho$, ω as above. This increases the safety against side-channel attacks. However at the same time, it decreases the performance of the Miller-Rabin test. In this article we use elementary means to analyze this variant. We will not be able to obtain results as strong as those by Damgård, Landrock and Pomerance on prime generation using the original Miller-Rabin test. However by imposing restrictions on the random parameter ρ, we obtain satisfactory estimates on the variant described here which justify practical implementation.

Keywords. Miller-Rabin test, secure prime generation, side channel attacks.

AMS classification. .

1 Introduction

To generate random prime numbers on smart cards, one typically uses the probabilistic primality test of Miller-Rabin. If an integer passes many rounds of this test, it is very likely that it is a prime number. If one chooses at random a k-bit integer n, and if it successfully passes t rounds, then very good estimates for the probability that n is prime, have been obtained by Damgård, Landrock and Pomerance in [3].

However if one implements the Miller-Rabin test straightforwardly on a smart card, then using side-channel attacks it seems possible that an outside spy can retrieve the integer n. The point is that in the Miller-Rabin test, one uses binary exponentiation, always with the same exponents, namely the divisors ω of $n-1$ such that $(n-1)/\omega$ is a power of 2. So if a spy can 'listen' to many rounds of the test, it seems probable that the secret n is revealed. This attack was first observed in the seminal article [5] by Kocher. To avoid this kind of attack, we analyze here a variant of the Miller-Rabin test. We also refer to [2] for general approaches on secure prime number generation.

Let us first recall the original test for an odd integer n: One writes $n-1 = 2^s w$ for an odd integer w and $s \in \mathbb{N}$. Then one chooses an integer $a \in \{1, 2, \dots, n-1\}$ at

random and tests whether one of the following conditions hold

$$\begin{aligned} a^w &\equiv 1 \pmod{n}, \text{ or} \\ a^{2^\sigma w} &\equiv -1 \pmod{n}, \text{ for some } \sigma \in \{0, 1, \ldots, s-1\}. \end{aligned}$$

Let $\alpha(n)$ denote the ratio of those integers a in $\{1, 2, \ldots, n-1\}$ for which the above test is successful, divided by the number of all integers a in this range which are prime to n. If n is a prime, then $\mathbb{Z}_n^*$ is cyclic of order $n-1$, and the test will be successful for all such a, so that $\alpha(n) = 1$. If n is composite, then it was shown by Rabin [7] and Monier [6] that $\alpha(n) \leq 1/4$. Hence for composite n, the ratio of those integers a in $\{1, 2, \ldots, n-1\}$ for which the above test is successful, divided by the number of all integers a in this range, as smaller than $1/4$. The advantage of working with $\alpha(n)$ instead of the former ratio is that it is given by an 'explicit' formula.

The above test is then repeated a certain number of times, to improve the reliability of the outcome. To improve performance one typically takes $a = 2$ in the first round, and one also verifies by elementary means that n is not divisible by small primes.

Let us now describe the variant we are interested in: Again n will be a random odd integer and one writes $n - 1 = 2^s w$ as above. We also fix a subset $R \subseteq \mathbb{N}$ of odd integers to be specified later. Then one chooses integers $a \in \{1, 2, \ldots, n-1\}$ and $\rho \in R$ at random and one computes $w\rho$. The new test verifies whether one of the following conditions holds

$$\begin{aligned} a^{w\rho} &\equiv 1 \pmod{n}, \text{ or} \\ a^{2^\sigma w\rho} &\equiv -1 \pmod{n}, \text{ for some } \sigma \in \{0, 1, \ldots, s-1\}. \end{aligned}$$

For fixed ρ, we denote the above test by MR_ρ. For a random choice $\rho \in R$, we denote it by MR_R, and call it the *Miller-Rabin test with randomized exponent (in R)*. By $\alpha_\rho(n)$ we denote the ratio of those a for which MR_ρ is successful, divided by $\#\mathbb{Z}_n^*$, and by $\alpha_R(n)$ the average over the $\alpha_\rho(n)$ for $\rho \in R$. It is obvious from these definitions that $\alpha(n) \leq \alpha_\rho(n), \alpha_R(n)$.

The reliability of t rounds of the new test MR_R is investigated in Propositions 1.2 and 1.3 and in Corollary 1.4. The improved security to side channel attacks in comparison to t rounds of the original test lies in the fact that the number ρ is changed in every round. Thus each round has its own exponent $w\rho$ for the test. While it is obvious that one has still to mask the individual rounds, the different choices of ρ make the generation more secure. Since ρ is chosen at random, partial knowledge of the $w\rho$ cannot be combined to obtain further knowledge of w and thus on n. Also note that the multiplication $w \cdot \rho$ can be regarded as secure: While binary exponentiation does reveal information on the exponent, multiplication of two random integers does not.

We introduce some more notation: By π_i we denote the i-th prime, so (π_i) is the sequence $(2, 3, 5, \ldots)$, and by P_i we denote the product of the first i primes.

In the sequel, the set R will always be an arithmetic progression of the following type: For $i \in \mathbb{N}$, $\rho_0 \in \{1, 2, \ldots, P_i - 1\}$ which is supposed to be prime to P_i, and $r \in \mathbb{N}$ we set

$$R_{i,\rho_0,r} := \{\rho_0 + \lambda P_i : \lambda = 0, 1, \ldots, r-1\}.$$

In particular any element in $R_{i,\rho_0,r}$ is prime to the first i prime numbers, and the cardinality of $R_{i,\rho_0,r}$ is r. If $i = 1$, then $R_{i,\rho_0,r}$ is simply the set of the r smallest positive odd integers.

Proposition 1.1. *If n is prime, then $\alpha_R(n) = 1$ for any set R (of odd integers).*
If n is composite, one has the following estimates:

(a) If $R = R_{1,1,r}$ where (a) $18 \leq r$, (b) $8r^2 \leq n$, and (c) r is divisible by 3, then

$$\alpha_R(n) \begin{cases} = \frac{5}{18}, & \text{if } n = p(3p-2) \text{ with } p, 3p-2 \text{ prime and } p \equiv -1 \pmod 4 \\ \leq \frac{1}{4} & \text{otherwise} \end{cases}$$

(b) If $R = R_{i,\rho_0,r}$ for some $i \geq 2$ where (a') $2\pi_{i+1}^2 \leq r$ and (b') $2r^2 P_i \leq n$, then whenever $\alpha_R(n) \neq \alpha(n)$ one has $\alpha_R(n) \leq \frac{1}{\pi_{i+1}}$.

The case (a) had been previously considered by J. Gerhardt, [4], who had essentially obtained the same result in that case, except for the precise determination of the exceptional set of composite n with $\alpha_R(n) > \frac{1}{4}$.

The integers n with $\alpha_R(n) > \frac{1}{4}$ are precisely those with $\alpha(n) = \frac{1}{6}$. The latter set had first been classified in [3, Thm. 4 (ii)]. The factorization $n = p(3p-2)$ easily implies that for such n the number $3n+1$ is a square. Hence the density of such n of bit length k is at most $2^{-k/2}$. This estimate is used in Proposition 1.2. Numerical experiments suggest that the density of such n is actually bounded by $k^{-2}2^{2-\frac{k}{2}}$. This might indicate that the density of integers p of size roughly x such that p as well as $3p-2$ is a prime is $\asymp (\log(x))^{-2}$.

We now follow the usual prime generation method described for instance in [3]: For this we fix suitable parameters i, ρ_0, r as above and set $R = R_{i,\rho_0,r}$. Then a k-bit integer n is chosen at random. If n passes the test $\mathrm{MR}_{\{1\}}$ with $a = 2$ and $t-1$ times the test MR_R, then it is declared to be prime and we stop. If not, we choose another integer n at random. If it passes the test $\mathrm{MR}_{\{1\}}$ with $a = 2$ and $t-1$ times the test MR_R, then it is declared to be prime and we stop. This process is repeated until a (probable) prime n is found. We denote the resulting algorithm, which only lets pass integers n that pass tests of the form MR_R at least t-times, by MR_R^t.

To analyze the reliability of the above algorithm, we define $q_{k,t,R}$ as the probability that a composite k-Bit integer passes the test MR_R^t. Because $\alpha(n)$ is on the average much smaller than $\frac{1}{4}$ and because of the prime number distribution, the bounds given in [3] for $q_{k,t} := q_{k,t,\{1\}}$ are much better than 4^{-t}. In Section 4 we shall prove the following bounds for the algorithm based on MR_R:

Proposition 1.2. *Suppose that $18 \leq r$, that 3 divides r and that r satisfies $8r^2 \leq 2^{k-1}$. Then*

$$q_{k,t,R_{1,1,r}} \leq \Big(\frac{1}{4}\Big)^{t-1} \frac{q_{k,1}}{1-q_{k,1}} + \Big(\frac{5}{18}\Big)^{t-1} k 2^{1-k/2}.$$

Proposition 1.3. *Suppose that $2 \leq i$, $2\pi_{i+1}^2 \leq r$ and $2r^2 P_i \leq 2^{k-1}$. Then*

$$q_{k,t,R_{i,\rho_0,r}} \leq q_{k,t} + \frac{q_{k,1}}{1-q_{k,1}} \pi_{i+1}^{1-t}.$$

By specializing Proposition 1.3 and using the known values from [3, p. 194][1] for $q_{k,1}$, it is straightforward to derive the following practical consequences.

Corollary 1.4. *Let* $k = 512$ *and* $R = R_{6,1,2^{17}}$. *Then* $q_{k,t,R} \leq 2^{-57-4(t-1)}$.
Let $k = 1024$ *and* $R = R_{11,1,2^{27}}$. *Then* $q_{k,t,R} \leq 2^{-150-2(t-1)}3^{-2(t-1)}$.

The set R in the corollary consists of 32- and 64-bit integers, respectively.

It seems likely to the present author that in fact one can prove estimates similar to those in [3] without restrictions on the set of random exponents. However a straightforward adaption of the method of [3] seems not possible. The only information used in the proof in op.cit. are a bound on the number of n such that $\alpha(n)$ is above a certain size. However the randomized $\alpha_\rho(n)$ may be much larger than $\alpha(n)$ for a positive density of ρ. To adapt [3] one would therefore also need to analyze the number and size of prime factors in the prime decomposition of $p-1$ for the prime divisors p of n.

At the same time, it seems very likely that, by analyzing a small number of exceptional cases, one can improve the base $\frac{1}{\pi_{i+1}}$ in Proposition 1.3 by $\frac{1}{2\pi_{i+1}}$, or even further. This would yield better bounds in Corollary 1.4.

Acknowledgments: I would like to express many thanks to the technical support group of cryptovision who brought the above problem to my attention, and gave me access to the unpublished work [4] of J. Gerhardt who had first analyzed the above randomization algorithm for $i = 1$ systematically. Also thanks to S. Wentzig for a very careful reading of a preliminary version and many suggestions to improve the readability of the manuscript. Finally I also want to thank the referee whose many comments further improved the readability of the present article.

2 A probabilistic lemma

Fix $r, d \in \mathbb{N}$ and $b \in \mathbb{N}$ relatively prime to d such that $1 \leq b < d$. Let $R \subseteq \mathbb{N}$ be the arithmetic progression $\{b + ds : 0 \leq s \leq r-1\}$ of r elements.

For an integer m, we define $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) := |\{\rho \in R : m \text{ divides } \rho\}|/|R|$, i.e. the probability that a random integer of R is divisible by m.

Lemma 2.1. *(a) If* $m \geq dr$, *then* $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) = 0$.
(b) If $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) > 0$, *then* $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) < \frac{1}{m} + \frac{1}{r}$.
(c) If $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) > 0$ *and if* $m | r$, *then* $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) = \frac{1}{m}$.

Proof. Since (a) is obvious, we now turn to (b) and (c). If $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) > 0$ then m is relatively prime to d, since if a prime p divides $b + ds$ and d at the same time, it will also divide b and d at the same time which is impossible since $\gcd(b, d) = 1$.

Because m is prime to d, the residue classes $ds \pmod m$, $s = 0, \ldots, m-1$, are a complete list of the elements of $\mathbb{Z}/(m)$. Since R is an arithmetic progression, with steps of length d, it follows that the progression modulo m is m-periodic, and not

[1] The values $q_{512,1} \approx 2^{-57}$ and $q_{1024,1} \approx 2^{-150}$ are obtained by extrapolation from the table in [3]

periodic for any number smaller than m. In particular if r is a multiple of m, then any residue class occurs exactly r/m many times. This shows (c).

For general r, the residue class zero modulo m occurs most often if it occurs for $s = 0, m, 2m, \ldots$ If λ denotes the number of occurrences of zero, then we must have $m(\lambda - 1) \leq r - 1$, i.e., $\lambda \leq (r-1)/m + 1$. Dividing by r, we find $\mathrm{prob}(m \text{ div. } \rho | \rho \in R) = \lambda/r < \frac{1}{m} + \frac{1}{r}$, as asserted. □

The main problem in obtaining the estimates for Proposition 1.1 will be that the set R is typically relatively small compared to n. Thus if q is a prime divisor of $n-1$ or of $p-1$ for p a prime dividing $n-1$, then $\mathrm{prob}(q \text{ div. } \rho | \rho \in R)$ may differ by up to $1/|R|$ from the expected number $\frac{1}{q}$ that is obtained for $|R| \to \infty$. The quantity $a_R(n)$ will by a weighted average over the probabilities $\mathrm{prob}(q \text{ div. } \rho | \rho \in R)$, with possibly many summands. Therefore the 'error terms' $1/|R|$ may sum up to a significant error term in the sum, if one is not careful. The following simple probabilistic lemma will be used to show that indeed the error terms do not add up.

Let us introduce some notation. Let $S := \{1, 2, \ldots, h\}$ be a subset of consecutive integers. Let μ be a probability measure on the power set $\{0,1\}^S$ of S, i.e., we regard the subsets of S as points of some space and attach to each such a point mass. Fix some function $g \colon S \to \mathbb{R}_{>0} : j \mapsto g_j$ and abbreviate $g_J := \prod_{j \in J} g_j$ for any $J \subseteq S$ (note that whenever a product is formed over the empty set as an index set, the value of the product is supposed to be one). We define the g-weighted average over μ as

$$\alpha(g, \mu) := \sum_{J \subseteq S} \mu(J) g_{S \smallsetminus J}.$$

Lemma 2.2. *With the notation as above one has*

$$\alpha(g, \mu) = \sum_{J \subseteq S} g_{S \smallsetminus J} \Big(\sum_{K \supseteq J} \mu(K) \Big) \Big(\sum_{L \subseteq J} (-1)^{|L|} g_L \Big).$$

Lemma 2.2 may be regarded as a multi-dimensional version of Abel summation, cf. (AS) on page 9.

Proof. The proof is given by rewriting and simplifying the right hand side:

$$\begin{aligned}
&\sum_{J \subseteq S} \sum_{K \supseteq J} \sum_{L \subseteq J} g_{S \smallsetminus J}\, \mu(K)\, (-1)^{|L|} g_L \\
&\quad = \quad \sum_{K \subseteq S} \mu(K) \sum_{L \subseteq J \subseteq K} g_{S \smallsetminus J}\, (-1)^{|L|} g_L \\
&\quad = \quad \sum_{K \subseteq S} \mu(K) g_{S \smallsetminus K} \sum_{L \subseteq J \subseteq K} (-1)^{|L|} g_{(K \smallsetminus J) \cup L} \\
&\quad \overset{M = (K \smallsetminus J) \cup L}{=} \quad \sum_{K \subseteq S} \mu(K) g_{S \smallsetminus K} \sum_{M \subseteq K} g_M \sum_{L \subseteq M} (-1)^{|L|} \\
&\quad = \quad \sum_{K \subseteq S} \mu(K) g_{S \smallsetminus K} \sum_{M = \varnothing} g_M \sum_{L \subseteq M} (-1)^{|L|} = \sum_{K \subseteq S} \mu(K) g_{S \smallsetminus K},
\end{aligned}$$

where in the last line we use $\sum_{L\subseteq M}(-1)^{|L|}=0$ for $M\neq\varnothing$. □

The above lemma will be applied in the following situation:
We will consider h distinct prime numbers $q_1,\dots,q_h$. For each there is an exponent $f_j\in\mathbb{N}$, and we will set $g_j:=q_j^{-f_j}$. Moreover we will consider the following three probability measures:

$$\mu_0(J):=\text{prob}\Big(\Big(\prod_{j\in J}q_j \text{ div. } \rho\Big) \text{ and } \Big(\prod_{j\notin J}q_j \text{ is prime to } \rho\Big)\ \Big|\ \rho\in R\Big). \tag{2.1}$$

$$\mu_1(J):=\prod_{j\in J}q_j^{-1}\prod_{j\notin J}(1-q_j^{-1}). \tag{2.2}$$

$$\mu_2(J):=\begin{cases}0, & \text{if } J\neq S\\ 1, & \text{if } J=S.\end{cases} \tag{2.3}$$

The measure μ_1 is so to speak the limit of μ_0 as $r\to\infty$ (for a random set R). Note that for fixed $J\subseteq S$ we have the following expressions for $\sum_{K\supseteq J}\mu_i(K)$:

$$\sum_{K\supseteq J}\mu_i(K)=\begin{cases}\text{prob}(\prod_{j\in J}q_j \text{ div. } \rho\mid\rho\in R)\overset{2.1(b)}{\leq}\prod_{j\in J}q_j^{-1}+\frac{1}{r} & \text{for } i=0;\\ \prod_{j\in J}q_j^{-1} & \text{for } i=1;\\ 1 & \text{for } i=2.\end{cases} \tag{2.4}$$

3 A single round of the Miller-Rabin variant

This section is mainly concerned with the proof of Proposition 1.1. Throughout this section we fix an odd integer $n\geq 3$ and write $n=p_1^{e_1}\cdots p_\ell^{e_\ell}$ for its factorization into distinct prime powers. We define odd integers w and w_i and integers s and s_i such that $2^sw=n-1$ and $2^{s_i}w_i=p_i-1$. For $x\in\mathbb{N}$ we set

$$\gamma(x):=\prod_{i=1}^{\ell}\frac{\gcd(w_ip_i^{e_i-1},x)}{w_ip_i^{e_i-1}}. \tag{3.1}$$

We also set $\underline{s}:=\min\{s_i:i=1,\dots,\ell\}$, and define

$$\beta(n):=2^{-\sum_i s_i}\Big(1+\frac{2^{l\underline{s}}-1}{2^\ell-1}\Big).$$

Recall that by $\alpha_\rho(n)$ we denote the ratio of the number of those $a\in\{1,\dots,n\}$ for which the variant MR_ρ of the Miller-Rabin test is successful, divided by $\#\mathbb{Z}_n^*$.

Lemma 3.1. *One has* $\alpha_\rho(n)=\beta(n)\gamma(\rho(n-1))$ *and* $\beta(n)\leq 2^{1-\ell}$.

Proof. We consider the sets $G_0 := \{a \in \mathbb{Z}_n^* : a^{w\rho} = 1\}$, and

$$G_j := \{a \in \mathbb{Z}_n^* : a^{2^{j-1}w\rho} = -1\}$$

for $j = 1, \ldots, s$. By the Chinese remainder we have

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_\ell^{e_\ell}}^*.$$

Since the p_i are all odd, the factors on the right are all cyclic. The elements ± 1 in $\mathbb{Z}_n$ have component ± 1 in each of the rings $\mathbb{Z}_{p_i^{e_i}}$, and the sets G_j are products of corresponding sets for each $i = 1, \ldots, \ell$.

Because $w\rho$ is odd and $\mathbb{Z}_{p_i^{e_i}}^*$ is cyclic of order $2^{s_i} w_i p_i^{e_i - 1}$, it is easy to see that for each i, j

$$\left|\left\{a \in \mathbb{Z}_{p_i^{e_i}}^* : a^{2^{j-1}w\rho} = -1\right\}\right| = \begin{cases} 2^{j-1} \gcd(w\rho, w_i p_i^{e_i - 1}) & \text{for } j \le s_i \\ 0 & \text{otherwise,} \end{cases}$$

and moreover $\left|\left\{a \in \mathbb{Z}_{p_i^{e_i}}^* : a^{w\rho} = 1\right\}\right| = \gcd(w\rho, w_i p_i^{e_i - 1})$. Combining these results for fixed j and all the i, we find

$$|G_j| = \begin{cases} 2^{\ell \max\{0, j-1\}} \prod_{i=1}^{\ell} \gcd(w\rho, w_i p_i^{e_i - 1}) & \text{for } j \le \underline{s} \\ 0 & \text{otherwise.} \end{cases}$$

Thus, summing over all j we have

$$\sum_{j=0}^{s} |G_j| = \left(1 + \sum_{j=0}^{\underline{s}-1} 2^{\ell j}\right) \prod_{i=1}^{\ell} \gcd(w\rho, w_i p_i^{e_i - 1}).$$

Dividing by the order of $\mathbb{Z}_n^*$, i.e., by $\prod_{i=1}^{\ell} 2^{s_i} w_i p_i^{e_i - 1}$ yields the desired result.

Finally, by looking at the 2-adic expansion of $1 + \sum_{j=0}^{\underline{s}-1} 2^{\ell j}$ one finds that this sum is at most $2^{\ell(\underline{s}-1)+1}$. Because $\underline{s} \le s_i$ for all i, the asserted bound on $\beta(n)$ follows. □

We fix a set R which as usual is an arithmetic progression. From its definition, it is clear that $\gamma(n-1)^{-1}$ is an odd integer. Therefore we can write

$$\gamma(n-1)^{-1} = q_0 \prod_{j=1,\ldots,h} q_j^{f_j} \tag{3.2}$$

such that q_0 is an odd integer relatively prime to $\prod_{\rho \in R} \rho$, such that $q_1, \ldots, q_h$ are those (distinct) prime divisors of $\gamma(n-1)^{-1}$ which divide $\prod_{\rho \in R} \rho$, and where $f_j \in \mathbb{N}$ is the order of q_j as a divisor of $\gamma(n-1)^{-1}$. Define $S := \{1, 2, \ldots, h\}$. To apply the lemma of the previous section in the proof of Proposition 1.1, we first rewrite $\alpha_R(n)$ in terms of the measure μ_0 from defining equation (2.1):

Lemma 3.2.

$$\alpha_R(n) \le \beta(n)\frac{1}{q_0}\cdot\sum_{J\subseteq S}\mu_0(J)\prod_{j\notin J} q_j^{-f_j}.$$

Proof. For $J\subseteq S$, we define $R_J := \{\rho\in R : q_j|\rho \Leftrightarrow j\in J\}$. Then

$$\frac{\alpha_R(n)}{\beta(n)} \overset{\text{by def.}}{=} \frac{1}{|R|}\sum_{\rho\in R}\frac{\alpha_\rho(n)}{\beta(n)} \overset{\text{Lem. 3.1}}{=} \frac{1}{|R|}\sum_{\rho\in R}\gamma(\rho(n-1)) = \sum_{J\subseteq S}\frac{1}{|R|}\sum_{\rho\in R_J}\gamma(\rho(n-1)).$$

From the defining equation (3.1) for $\gamma(x)$ and the above product representing $\gamma(n-1)^{-1}$, we have for any $\rho\in R_J$ the inequality

$$\gamma(\rho(n-1)) \le q_0^{-1}\prod_{j\notin J} q_j^{-f_j}. \tag{3.3}$$

Substituting this and $\mu_0(J) = |R_J|/|R|$ in the above expression for $\alpha_R(n)$, we find

$$\frac{\alpha_R(n)}{\beta(n)} \le \sum_{J\subseteq S}\mu_0(J)\, q_0^{-1}\prod_{j\notin J} q_j^{-f_j}. \qquad \square$$

Remark 3.3. (a) If S is empty, then $\gamma(n-1) = q_0^{-1} = \gamma(\rho(n-1))$ for all $\rho\in R$, and so $\alpha_R(n) = \alpha(n)$.

(b) If for a given R the product $\prod_{\rho\in R}\rho$ is prime to $\gamma(n-1)^{-1}$, then S is empty.

(c) If $S = \{q_1\}$ consists of a single element, $f_1 = 1$ and $q_1|r$, then, arguing as in the previous proof, one obtains $\alpha_R(n) = \beta(n)\frac{1}{q_0 q_1}\big(1-\frac{1}{q_1}\big)$.

Lemma 3.4. *One has*

$$\frac{\alpha_R(n)q_0}{\beta(n)} \le \frac{1}{r} + \prod_{j\in S} q_j^{-1}\sum_{J\subseteq S}\prod_{j\notin J}(q_j^{1-f_j} - q_j^{-f_j}) \le \frac{1}{r} + \prod_{j\in S}\frac{2}{q_j}.$$

Proof. The inequality on the right follows readily from the first, since all the expressions $q_j^{1-f_j} - q_j^{-f_j}$ are smaller than 1, and since $\sum_{J\subseteq S} 1 = 2^{|S|}$. We prove the inequality on the left:

$$\begin{aligned}\frac{\alpha_R(n)q_0}{\beta(n)} &\overset{\text{Lem. 3.2}}{\le} \sum_{J\subseteq S}\mu_0(J)\prod_{j\notin J} q_j^{-f_j}\\ &\overset{\text{Lem. 2.2}}{=} \sum_{J\subseteq S}\Big(\prod_{j\notin J} q_j^{-f_j}\Big)\sum_{K\supseteq J}\mu_0(K)\Big(\sum_{L\subseteq J}(-1)^{|L|}\prod_{j\in L} q_j^{f_j}\Big).\end{aligned}$$

Applying all three parts of formula (2.4) we find

$$\sum_{K\supseteq J}\mu_0(K) \le \frac{1}{r} + \prod_{j\in J} q_j^{-1} = \frac{1}{r}\Big(\sum_{K\supseteq J}\mu_2(K)\Big) + \sum_{K\supseteq J}\mu_1(K).$$

Thus

$$\begin{aligned}\frac{\alpha_R(n)q_0}{\beta(n)} &\leq \frac{1}{r}\sum_{J\subseteq S}\Big(\prod_{j\notin J} q_j^{-f_j}\Big)\sum_{K\supseteq J}\mu_2(K)\Big(\sum_{L\subseteq J}(-1)^{|L|}\prod_{j\in L} q_j^{f_j}\Big) + \\ &\quad \sum_{J\subseteq S}\Big(\prod_{j\notin J} q_j^{-f_j}\Big)\sum_{K\supseteq J}\mu_1(K)\Big(\sum_{L\subseteq J}(-1)^{|L|}\prod_{j\in L} q_j^{f_j}\Big) \\ &\overset{\text{Lem. 2.2}}{=} \frac{1}{r}\sum_{J\subseteq S}\mu_2(J)\prod_{j\notin J} q_j^{-f_j} + \sum_{J\subseteq S}\mu_1(J)\prod_{j\notin J} q_j^{-f_j}.\end{aligned}$$

Since $\mu_2(J) = 0$ for $J \neq S$, the first sum adds up to one. In the second sum, we substitute the definition of $\mu_1(J)$, and obtain:

$$\frac{\alpha_R(n)q_0}{\beta(n)} \leq \frac{1}{r} + \sum_{J\subseteq S}\prod_{j\in J} q_j^{-1}\prod_{j\notin J}(1-q_j^{-1})\prod_{j\notin J} q_j^{-f_j}.$$

Pulling out the factor $\prod_{j\in S} q_j^{-1}$ from the sum, yields the desired estimate. □

For arbitrary n (and $S \neq \varnothing$), the estimates in inequality (3.3) and in Lemma 3.4 can not be improved. However, if $e_i \geq 2$ for some factor $p_i^{e_i}$ of n, then better bounds can be obtained. The proof of Proposition 1.1 will need such an improved estimate in one particular case, which we now derive:

Lemma 3.5. *As before, let d be the width of the arithmetic progression R of length r. Suppose that $n = p^e$ is a prime power and that $n > dr$. If $p \geq dr$, then $\alpha_R(n) = \alpha(n)$, else*

$$\alpha_R(n) \leq \frac{1 + (e-1)(1-p^{-1})}{p^{e-1}} + \frac{1-p^{1-e}}{r}. \tag{3.4}$$

Proof. In the situation at hand we have $\beta(n) = 1$ and $\gamma(n-1) = p^{1-e}$, and therefore $\alpha(n) = p^{1-e}$ as well. Note that for $n = p$ one has $\alpha(n) = \alpha_R(n) = 1$ and the right hand side of equation (3.4) is 1 as well. Thus from now on, we assume $e \geq 2$.

We first consider the case where p is not a divisor of $\prod_{\rho\in R}\rho$. Then $\gamma(n-1)^{-1}$ is prime to $\prod_{\rho\in R}\rho$, and so $\alpha_R(n) = \alpha(n) = p^{1-e}$ by Remark 3.3. If $p \geq dr$, i.e., if p is larger than the largest element of the arithmetic expression R, then $\alpha_R(n) = \alpha(n)$, as asserted. If $p < dr$ (and still p does not divide any of the $\rho \in R$), then equation (3.4) holds because the right hand side of equation (3.4) is larger than p^{1-e}, as $e \geq 2$.

From now on, we assume that p divides one of the $\rho \in R$. In formula (3.2) we have $q_0 = 1$, $h = 1$, $q_1 = p$ and $f_1 = e - 1$. Clearly now $p < dr$, and so we need to prove equation (3.4).

The key point in the following chain of inequalities is Abel summation

$$(AS): \quad \sum_{i=0}^{g}(a_i - a_{i+1})b_i = a_0b_0 + \sum_{i=1}^{g} a_i(b_i - b_{i-1}) - a_{g+1}b_g :$$

and the observation that in the case at hand the defining formula (3.1) simplifies to $\gamma(\rho(n-1)) = \frac{\gcd(p^{e-1},\rho)}{p^{e-1}}$:

$$\begin{aligned}\alpha_R(n) = \ & \frac{1}{r}\sum_{\rho\in R}\alpha_\rho(n) \overset{\text{Lem. 3.1}}{=} \frac{1}{r}\sum_{\rho\in R}\gamma(\rho(n-1)) \\ & \overset{(3.1)}{=} \sum_{t=0}^{e-1}(\text{prob}(p^t \text{ div. } \rho|\rho\in R) - \text{prob}(p^{t+1} \text{ div. } \rho|\rho\in R))p^{1-e+t} \\ & \overset{(AS)}{=} p^{1-e} + \sum_{t=1}^{e-1}\text{prob}(p^t \text{ div. } \rho|\rho\in R)(p^{1-e+t}-p^{-e+t}) - \text{prob}(p^e \text{ div. } \rho|\rho\in R)\end{aligned}$$

To obtain an upper bound we may drop the last term and estimate the remaining summands using Lemma 2.1. This implies

$$\alpha_R(n) \quad \leq \quad p^{1-e} + \sum_{t=1}^{e-1}\Big(p^{-t}+\frac{1}{r}\Big)(p^{1-e+t}-p^{-e+t}).$$

The terms involving $\frac{1}{r}$ form a telescoping sum, the other ones a sum over constants. Evaluation of the expressions now yields the estimate (3.4). □

Proof of Proposition 1.1. From now on, we take $R := R_{i,\rho_0,r}$, so that R is an arithmetic progression of length r and width P_i. We first consider the case where n is a power p^e of some prime p but not a prime number. In this case $\alpha(n)$ and $\alpha_R(n)$ are typically very small, provided in case (b) that the elements in R are small compared to n: Note first that by Remark 3.3 for $p \geq P_i r$ we have $\alpha(n) = \alpha_R(n)$, so that we may assume $p < P_i r$. Since $P_i \geq 2$, we have $\ln(P_i r) \geq \ln(2r)$, and hence also $2\ln(P_i r) \geq \ln(2P_i r^2)$. Because $n \geq 2P_i r^2$ and $x \mapsto \frac{x}{\ln(x)}$ is strictly increasing for $x > \exp(1)$, this shows

$$\frac{n}{\ln(n)} \geq \frac{2P_i r^2}{\ln(2P_i r^2)} \geq \frac{P_i r}{\ln(P_i r)} r.$$

Since $P_i r > p \geq 3$, the previous inequality yields

$$n \geq \frac{\ln(n)}{\ln(p)} pr,$$

which is equivalent to $n \geq epr$, or to $\frac{p^{e-1}}{e} \geq r$. Hence our hypotheses yield

$$\alpha_R(n) \overset{\text{Lem. 3.5}}{\leq} \frac{1+(e-1)(1-p^{-1})}{p^{e-1}} + \frac{1-p^{-e}}{r} \leq \frac{e}{p^{e-1}} + \frac{1}{r} \leq \frac{2}{r} \leq \frac{1}{2\pi_{i+1}},$$

where for the last inequality we use $r \geq 2\pi_{i+1}^2$.

Next we consider the case where n has at least three prime factors, or where n has two prime factors and $s_1 \neq s_2$. In either case $\beta(n) \leq \frac{1}{4}$. If $S = \varnothing$, then $\alpha_R(n) = \alpha(n)$ and there is nothing to prove. If $|S| = 2$, then Lemma 3.4 yields

$$\alpha_R(n) \leq \frac{1}{4}\Big(\frac{1}{r} + \frac{4}{\pi_{i+1}\pi_{i+2}}\Big) \leq \frac{1}{2\pi_{i+1}},$$

because ρ has no prime divisor smaller than π_{i+1} and $r \geq 2\pi_{i+1}^2$. If $|S| = 1$, then again from Lemma 3.4 we obtain

$$\alpha_R(n) \leq \frac{1}{4}\Big(\frac{1}{r} + \frac{1}{\pi_{i+1}}(2 - \frac{1}{\pi_{i+1}})\Big) \leq \frac{1}{2\pi_{i+1}},$$

using the same hypothesis $r \geq 2\pi_{i+1}^2$.

Finally, we assume that $n = p_1^{e_1}p_2^{e_2}$ has exactly two prime factors and that $s_1 = s_2$. Then for $s_1 = 1$ one has $\beta(n) = \frac{1}{2}$ and for $s_1 \geq 2$ one has $\beta(n) \leq \frac{3}{8}$. As in the previous paragraph $S = \varnothing$ leads to $\alpha(n) = \alpha_R(n)$ and $|S| \geq 2$ leads to

$$\alpha_R(n) \leq \frac{1}{2}\Big(\frac{1}{r} + \frac{4}{\pi_{i+1}\pi_{i+2}}\Big).$$

In the case (a) of Proposition 1.1 one finds the estimate $\alpha_R(n) \leq \frac{29}{180} < \frac{1}{4}$, in case (b) the estimate $\alpha_R(n) \leq \frac{1}{2\pi_{i+1}}$, and in either case the proposition is proved.

It remains to consider the case $|S| = 1$. In case (b) the estimate

$$\alpha_R(n) \leq \frac{1}{2}\Big(\frac{1}{r} + \frac{1}{\pi_{i+1}}(2 - \frac{1}{\pi_{i+1}})\Big)$$

yields, by the same arguments as above, that $\alpha_R(n) \leq \frac{1}{\pi_{i+1}}$.

In case (a) a direct application of Lemma 3.2 provides the estimate

$$\alpha_R(n) \leq \frac{\beta(n)}{q_0}\Big(q_1^{-f_1} + \text{prob}(q_1 \text{ div. } \rho \mid \rho \in R)(1 - q_1^{-f_1})\Big).$$

Using the bound on $\beta(n)$, the fact that q_0 is an odd natural number and that q_1 is an odd prime, and that $\text{prob}(q_1 \text{ div. } \rho \mid \rho \in R) \leq \frac{1}{r} + \frac{1}{q_1}$, a short calculation proves the following: Unless $q_1 = 3$, $q_0 = 1$ and $\beta(n) = \frac{1}{2}$, the quantity $\alpha_R(n)$ is bounded above by $\frac{1}{4}$. In the remaining case, one computes $\alpha_R(n) = \frac{5}{18}$ using Remark 3.3(c) which applies due to our hypothesis that 3 divides r.

To complete the proof, we need to characterize those n for which $\alpha_R(n) = \frac{5}{18}$ can occur: We must have $s_1 = s_2 = 1$ and $\gamma(n-1)^{-1} = 3$. The case $e_1 \cdot e_2 > 1$ is easily refuted, since here $\gamma(n-1) = \frac{1}{3}$ only leaves $n = 45$ as a possibility contradicting the hypothesis $n \geq 8 \cdot 18^2$. It follows that $n = pq$ for primes $p \neq q$ such that $p - 1$ divides $n - 1$ and $(q-1)/3$ divides $n - 1$. From $n - 1 = (p-1)(q-1) + (p-1) + (q-1)$ one deduces $q - 1 = 3(p-1)$, and hence $n = (3p-2)p$ for some prime p. Moreover $s_1 = s_2 = 1$ implies that $p \equiv -1 \pmod 4$. This completes the proof of the proposition. □

4 Prime generation using the Miller-Rabin variant

We now prove Proposition 1.3. The method is taken from [1], and is also present in [4]; but might go back at least to [3].

Proof of Proposition 1.3. Let $\sum'$ denote the sum over all composite integers in a given range and let M_k denote the set of all k-bit integers. Then

$$\begin{aligned}
q_{k,t,R} &= \frac{\text{the probability that a composite } k\text{-Bit integer passes MR}_R^t}{\text{the probability that a } k\text{-Bit integer passes MR}_R^t} \\
&= \frac{\sum'_{n\in M_k}\alpha(n)\alpha_R(n)^{t-1}}{\sum_{n\in M_k}\alpha(n)\alpha_R(n)^{t-1}} \\
&\overset{\alpha_R(n)\le\alpha(n)}{\le} \frac{\sum'_{n\in M_k,\alpha(n)=\alpha_R(n)}\alpha(n)^t+\sum'_{n\in M_k,\alpha(n)\neq\alpha_R(n)}\alpha(n)\alpha_R(n)^{t-1}}{\sum_{n\in M_k}\alpha(n)^t} \\
&\overset{\text{Prop. 1.1}(b)}{\le} q_{k,t}+\pi_{i+1}^{1-t}\frac{\sum'_{n\in M_k,\alpha(n)\neq\alpha_R(n)}\alpha(n)}{\sum_{n\in M_k,n\text{ prime}}1} \\
&\le q_{k,t}+\pi_{i+1}^{1-t}\frac{\sum'_{n\in M_k}\alpha(n)}{\sum_{n\in M_k}\alpha(n)-\sum'_{n\in M_k}\alpha(n)} \\
&= q_{k,t}+\pi_{i+1}^{1-t}\frac{q_{k,1}}{1-q_{k,1}}.
\end{aligned}$$

□

In a similar way, however using directly the density of squares and of primes of bit length k, one may derive Proposition 1.2. We omit the details.

Acknowledgments. I would like to express many thanks to the technical support group of cryptovision who brought the above problem to my attention, and gave me access to the unpublished work [4] of J. Gerhardt who had first analyzed the above randomization algorithm for $i = 1$ systematically. Also thanks to S. Wentzig for a very careful reading of a preliminary version and many suggestions to improve the readability of the manuscript. Finally I also want to thank the referee whose many comments further improved the readability of the present article.

References

[1] R. J. Burthe, Further Investigations with the Strong Probable Prime Test, *Math. Comp.* **65** (1996), 373–381.

[2] H. Chabanne, E. Dotton, L. Ramsamy, Masked Prime Number Generation, *First Benelux Workshop on Information and System Security* (2006).

[3] I. Damgård, P. Landrock, C. Pomerance, Average Case Error Estimates for the Strong Probable Prime Test, *Math. Comp.* **61** (1993), 177–194.

[4] J. Gerhard, Randomizing the Exponent in the Miller-Rabin Test, *preprint*, Dec. 10, 2002.

[5] P. C. Kocher, Attacks on Implementations of Diffie-Hellmann, RSA, DSS and Other Systems, *LNCS* **1109** (1996), 104–113.

[6] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms, *Theoret. Comp. Sci.* **12** (1980), 97–108.

[7] M. O. Rabin, Probabilistic Algorithms for Testing Primality, *J. Number Theory* **12** (1980), 128–138.

Received xxx; revised xxx

Author information

Gebhard Böckle, Fakultät für Mathematik, Universität Duisburg-Essen, Campus Essen, 45117 Essen, Germany.
Email: gebhard.boeckle@uni-due.de