# Using fewer Qubits in Shor's Factorization Algorithm via Simultaneous Diophantine Approximation

Jean-Pierre Seifert*

Infineon Technologies
Security and ChipCard IC's
Concept Engineering
D-81609 München
Germany

**Abstract.** While quantum computers might speed up in principle certain computations dramatically, in pratice, though quantum computing technology is still in its infancy. Even we cannot clearly envison at present what the hardware of that machine will be like. Nevertheless, we can be quite confident that it will be much easier to build any practical quantum computer operating on a few number of quantum bits rather than one operating on a huge number of of quantum bits. It is therefore of big practical impact to use the resource of quantum bits very spare, i.e., to find quantum algorithms which use as few as possible quantum bits.

Here, we present a method to reduce the number of actually needed qubits in Shor's algorithm to factor a composite number $N$. Exploiting the inherent probabilism of quantum computation we are able to substitute the continued fraction algorithm to find a certain unknown fraction by a simultaneous Diophantine approximation. While the continued fraction algorithm is able to find a Diophantine approximation to a single known fraction with a denominator greater than $N^2$, our simultaneous Diophantine approximation method computes in polynomial time unusually good approximations to known fractions with a denominator of size $N^{1+\varepsilon}$, where $\varepsilon$ is allowed to be an arbitrarily small positive constant.

As these unusually good approximations are almost unique we are able to recover an unknown denominator using fewer qubits in the quantum part of our algorithm.

## 1 Introduction

The discovery of a fast quantum factorization algorithm for large composite numbers (cf. [Sho]) has boosted over the last few years quantum computing tremendeously. This earth-shaking result lead to the proposal of several experimentally realizable implementations of quantum computers. Among them, there is the Ion Trap system (cf. [CZ]), the Nuclear Magnetic Resonance scheme (cd. [CH$^+$] and even a Silicon based system (cf. [Kan]). While the noise rate in these systems can be brought to a constant in principle (cf. [ABO]), it nevertheless imposes limits to the maximal size of the quantum computer. Thus, it is of big practical impact to use the resource of quantum bits very spare, i.e., to find quantum algorithms which need as few as possible quantum bits.

Therefore, several attempts werde made (cf. [ME,PP,Z]) to come up with very clever and spare quantum implementations of Shor's quantum algorithm. However, all these attempts still used Shor's idea to use the continued fraction algorithm to find a certain

* This work was initiated while visiting and with full support by ETH - Institut für Theoretische Informatik.

unkown fraction. Unfortunately, using the continued fraction algorithm leads inevitably to a squaring of the number to be factored. This in turn doubles the length of the quantum registers. To avoid this squaring of the number to be factored is the subject of the present paper.

This paper presents a method to reduce the number of actually needed qubits in Shor's algorithm to factor a given composite number $N$, where $N$ is the product of two randomly chosen primes of equal size. Although our method easily extends to a wider class of randomly chosen modules, we will concentrate here for clarity to this special case. Moreover, from a practical point of view, this is the most interesting case.

By exploiting the inherent probabilism of quantum computation we are able to substitute the continued fraction algorithm to find a certain unknown fraction by a simultaneous Diophantine approximation. While the continued fraction algorithm is able to find a Diophantine approximation to a single known fraction with a denominator greater than $N^2$, our simultaneous Diophantine approximation method computes in polynomial time unusually good approximations to known fractions with a denominator of size $N^{1+\varepsilon}$, where $\varepsilon$ is an arbitrarily small positive constant.

The paper is organized as follows. We assume that the reader is familiar with the concept of quantum computing, and especially with Shor's algorithm [Sho] and the so called measurement concept. For a thorough introduction into quantum computing we refer to Gruska [Gru] or even Shor [Sho] itself. In section 2 we briefly review Shor's factorization algorithm up to the point what is needed for our algorithm. Section 3 provides a short introduction to simultaneous Diophantine approximations which is needed for our later purposes in subsequent sections. Next, in section 4 we will present our algorithm which reduces the quantum register size of Shor's algorithm from $\approx 2\log_2(N)$ to $(1+\varepsilon)\log_2(N)$. Finally, we will discuss in section 5 some open problems and possible further applications of our method to other quantum algorithms.

## 2 Preliminaries

Following Shor's algorithm to factor a given $N$, one computes for a random $x \bmod N$ its order in the multiplicative group $\mathbb{Z}_N^*$, i.e., the least positive integer $r < N$ such that $x^r \equiv 1 \bmod N$. Essentially, this algorithm terminates in the classical computational problem to find for a known fraction $\alpha/A$ an unknown fraction $m/r$ for which it is known that

$$\Pr_{\text{measure } \alpha}\left[\exists m : \left|\frac{\alpha}{A} - \frac{m}{r}\right| \leq \frac{1}{2A}\right] \approx \frac{4}{\pi^2}$$

and $\Pr[\gcd(m,r) = 1] \geq \Omega(1/\log\log r)$. Now, choosing $A > N^2$ enables unique recovery of the fraction $m/r$ via the continued fraction algorithm in polynomial time, since $m/r$ is with reasonable probability in lowest terms. This unique recovery of an unknown fraction is due to Legendre [Leg] and is described in detail in Schrijver [Sch]. For how to factor $N$ with large probability given the order $r$ of a randomly chosen $x \in \mathbb{Z}_N^*$, we refer to Shor [Sho].

However, our goal is to avoid the choice of $A > N^2$ as this doubles the bitlength of the numbers involved in the quantum algorithm. Instead, we will present a method which for every constant $\varepsilon > 0$ only needs a choice of $A \geq N^{1+\varepsilon}$. As our new method to find the order of a random $x \in \mathbb{Z}_N^*$ is mainly based on the theory of so called simultaneous Diophantine approximations, we will first give a short introduction into this subject and hereafter state some important results for later use. We also note that simultaneous Diophantine approximations are the natural extensions of continued fractions to higher dimensions. However, in higher dimensions things become very subtle as there is in general no higher dimensional analogue of Legendre's unique recovery method.

For a thorough discussion of simultaneous Diophantine approximations and especially its interrelations to continued fractions we refer to Cassels [Cas], Lagarias [Lag1,Lag2], Lovasz [Lov] and Schrijver [Sch].

## 3 Simultaneous Diophantine Approximation

Simultaneous Diophantine approximation is the study of the approximation properties of real vectors $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ by rational vectors $\boldsymbol{\xi} = (\frac{p_1}{Q}, \ldots, \frac{p_n}{Q})$. As measure for the *quality* of an approximation to a vector $\boldsymbol{\alpha}$ with denominator $Q$ we use the function

$$\|Q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty,$$

which is given by

$$\|\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty := \max_{1\leq i\leq n} \min_{p_i \in \mathbb{Z}} |\alpha_i - p_i|.$$

The following classical result of Dirichlet (see e.g. Cassels [Cas]) describes us how well vectors $\boldsymbol{\alpha} \in \mathbb{R}^n$ can be simultaneously approximated.

**Proposition 1.** *For every $\boldsymbol{\alpha} \in \mathbb{R}^n$ there are infinitely many positive integer solutions to $\|Q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq Q^{-1/n}$.*

However, the diophantine approximations that we will consider do no involve approximations to real vectors $\boldsymbol{\alpha}$, but instead involve approximations to rational vectors $\boldsymbol{\alpha} \in \mathbb{Q}^n$. And in general, such approximations to rational vectors behave completely different than those from Dirichlet's result, cf. Lagarias [Lag2,Lag3].

We therefore use a slightly different measure of quality of approximation. Namely, we will call a vector $\boldsymbol{\xi} = (\frac{x_1}{X}, \ldots, \frac{x_n}{X})$ with $1 \leq X < A$ a *$\Delta$-good approximation* to a vector $\boldsymbol{\alpha} = (\frac{\alpha_1}{A}, \ldots, \frac{\alpha_n}{A})$ satisfying $\gcd(\alpha_1, \ldots, \alpha_n, A) = 1$ if

$$\left|\frac{\alpha_i}{A} - \frac{x_i}{X}\right| \leq \frac{\Delta}{XA} \quad \text{for} \quad 1 \leq i \leq n.$$

For abbreviation we define the set $S_n(A)$ of all primitive rational vectors $\boldsymbol{\alpha}$ with denominator $A$, i.e.,

$$S_n(A) := \left\{ \boldsymbol{\alpha} = \left(\frac{\alpha_1}{A}, \ldots, \frac{\alpha_n}{A}\right) \,\middle|\, 0 \leq \alpha_i < A \text{ and } \gcd(\alpha_1, \ldots, \alpha_n, A) = 1 \right\}.$$

Moreover, we define for a vector $\boldsymbol{\alpha} \in \mathbb{Q}^n$ satisfying $\gcd(\alpha_1, \ldots, \alpha_n, A) = 1$ $N(\boldsymbol{\alpha}, \Delta)$ as the number of its $\Delta$-good approximations. As we are interested in the average number $N(\boldsymbol{\alpha}, \Delta)$ for those $\boldsymbol{\alpha}$ with $N(\boldsymbol{\alpha}, \Delta) \geq 1$ we define the conditional probabilities

$$p_k(A, \Delta, n) := \Pr_{\boldsymbol{\alpha} \in S_n(A)}[N(\boldsymbol{\alpha}, \Delta) \geq k \mid N(\boldsymbol{\alpha}, \Delta) \geq 1].$$

For the former conditional probabilities, Lagarias and Håstad [LH] proved the following Theorem. It confirms the intuition that "most" rational vectors do not have very many simultaneous Diophantine approximations of the Dirichlet quality, i.e., their approximations satisfying the Dirichlet bound are "almost" unique approximations.

**Theorem 1.** *There are positive constants $c_n$ such that for $n \geq 5$ and all $A \geq 2$ and all $\Delta$ with $c_n d(A) \leq \Delta \leq A^{1-1/n}$, we have*

$$p_k(A, \Delta, n) \leq \frac{c_n}{k^2},$$

*where $d(A)$ denotes the number of divisors of $A$.*

Although in general it is difficult to compute for a given rational vector "good" simultaneous Diophantine approximations (cf. Lagarias [Lag4]), it will suffice for our purposes to find "good" approximations in polynomial-time only for fixed dimension $n$. Luckily, to compute approximations in fixed dimensions of given quality with a prescribed size for the denominators we can use the following Theorem due to Lagarias [Lag4].

**Theorem 2.** *For any fixed $n$ there exists a polynomial-time (polynomial in the length of the input) algorithm to solve the following problem: Given a vector $\boldsymbol{\alpha} \in \mathbb{Q}^n$ und positive integers $N$, $s_1$ und $s_2$, find a denominator $Q$ with $1 \leq Q \leq N$ such that $\|Q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \frac{s_1}{s_2}$, provided that at least one exists.*

# 4 Finding an unknown denominator with fewer qubits

We will now describe our new algorithm to compute for a random $x \bmod N$ its order in the multiplicative group $\mathbb{Z}_N^*$, where $N$ is the product of two randomly chosen primes of equal size.

Although our factorization algorithm also computes for a random $x \bmod N$ its order in the multiplicative group $\mathbb{Z}_N^*$, i.e., the least positive integer $r < N$ such that $x^r \equiv 1 \bmod N$, we must now ensure that the order $r$ of the random $x \bmod N$ is *large*. The following proposition from [HSS] examines the simplest and most interesting circumstances for which it can be proved that the order of a random $x \in \mathbb{Z}_N^*$ is large.

**Proposition 2.** *Let $p$ and $q$ be randomly chosen primes of equal size, $N = p \cdot q$ with binary length $\ell$ and $x$ randomly chosen from $\mathbb{Z}_N^*$, then for all $k \geq 6$,*

$$\Pr\left[\mathrm{ord}_N(x) \geq \frac{(p-1)(q-1)}{\ell^k}\right] \geq 1 - O\left(\frac{1}{\ell^{(k-5)/5}}\right).$$

In fact, a more general statement can be shown to hold for a wider class of randomly generated modules (see Ritter [Rit]). However, for simplicity and practical purposes we will always assume in the following that we want to factor a typical RSA modulus $N = p \cdot q$ for some randomly chosen primes $p$ and $q$ of equal size.

The building block in the quantum part of our algorithm is essentially Shor's quantum part which computes for a random $x \bmod N$ its order in the multiplicative group $\mathbb{Z}_N^*$. Through several unitary transformations Shor's algorithm works towards the state

$$\frac{1}{A}\sum_{c=0}^{A-1}\sum_{a=0}^{A-1} e^{\frac{2\pi i a c}{A}} |c\rangle |x^a \bmod N\rangle.$$

Finally, one measures the first register and following Shor's analysis [Sho] one finds that for the final measurement $\alpha$ there exists a fraction $m/r$ with $r = \mathrm{ord}_N(x)$ and $\Pr[\gcd(m,r) = 1] \geq \Omega(1/\log\log r)$ such that

$$\Pr_{\text{measure } \alpha}\left[\exists m : \left|\frac{\alpha}{A} - \frac{m}{r}\right| \leq \frac{1}{2A}\right] \approx \frac{4}{\pi^2}.$$

More precisely, our new algorithm performs for the same randomly chosen $x \in \mathbb{Z}_N^*$ $n$ independent repetions of Shor's above quantum part to get $n$ independent measurements $\alpha_1, \ldots, \alpha_n$ where

$$\left|\frac{\alpha_i}{A} - \frac{m_i}{r}\right| \leq \frac{1}{2A}$$

and $\gcd(m_i, r) = 1$ holds with the appropriate probabilities. Note that (see Knuth [Knu]) with overwhelming probability (over the measurements of the $\alpha_1, \ldots, \alpha_n$) we will have

$$\gcd(\alpha_1, \ldots, \alpha_n, A) = 1.$$

Thus, the $n$ independent measurements $\alpha_1, \ldots, \alpha_n$ with $\gcd(\alpha_1, \ldots, \alpha_n, A) = 1$ and $0 \leq \alpha_i < A$ form a uniform chosen element $\boldsymbol{\alpha} := (\frac{\alpha_1}{A}, \ldots, \frac{\alpha_n}{A})$ from the set $S_n(A)$.

Next, we want to establish the choice of $A = N^\delta$ for which the vector $(\frac{m_1}{r}, \ldots, \frac{m_n}{r})$ is a $\Delta$-good approximation to our randomly chosen $\boldsymbol{\alpha} \in S_n(A)$ where $\Delta = A^{1-1/n}$. Setting

$$\frac{1}{2A} \;\leq\; \frac{\Delta}{r\,A} \;=\; \frac{1}{r\,A^{1/n}}$$

and using Proposition 2, i.e., $r \geq \frac{(p-1)(q-1)}{\ell^k}$ with large probability, we find

$$\frac{N}{\ell^k}\,A^{1/n} \;\leq\; 2A,$$

and finally that we need for some constant $k$

$$\delta \geq \frac{1}{1-1/n}\left(1 - \log_N(2) - k\log_N(\lceil \log_2 N \rceil)\right)$$

in order to state that $(\frac{m_1}{r}, \dots, \frac{m_n}{r})$ is a $\Delta$-good approximation to $\boldsymbol{\alpha}$. In terms of a choice of $A = N^{1+\varepsilon}$ and ignoring lower oder terms for $\delta$, this means that we need for our simultaneous Diophantine approximation a dimension of at least

$$n \geq \left\lceil \frac{1}{1 - 1/(1+\varepsilon)} \right\rceil .$$

Now we will show how to compute in polynomial-time the above unknown $A^{1-1/n}$-good approximation $(\frac{m_1}{r}, \dots, \frac{m_n}{r})$ to $\boldsymbol{\alpha}$. Here we will take advantage of the fact that $\boldsymbol{\alpha}$ is chosen uniform from the set $S_n(A)$ and that $(\frac{m_1}{r}, \dots, \frac{m_n}{r})$ is a $A^{1-1/n}$-good approximation to $\boldsymbol{\alpha}$. Namely, these facts enable the application of Theorem 1 to the vector $\boldsymbol{\alpha}$ and we get that for some constants $c_n$

$$\Pr_{\boldsymbol{\alpha} \in S_n(A)} [N(\boldsymbol{\alpha}, \Delta) \leq k \mid N(\boldsymbol{\alpha}, \Delta) \geq 1] \geq 1 - \frac{c_n}{k^2}.$$

Thus, for constant $n$ there exist with extremely large probability at most a polynomially number of $A^{1-1/n}$-good approximations to $\boldsymbol{\alpha}$. Therefore we are able to compute with Theorem 2 and a bisection strategy all denominators $Q$ with $1 \leq Q < A$ such that

$$\| Q\boldsymbol{\alpha} \bmod \mathbb{Z} \|_\infty \leq \frac{\Delta}{A}.$$

After having found these polynomially number of candidate denominators, we simply check every denominator whether it is indeed the order $r := \mathrm{ord}_N(x)$ of the random $x \in \mathbb{Z}_N^*$, and with reasonable probabilty one of these denominators happens to be the order $r$. We stress that this reasonable success probability strongly depends on the fact that we only work with a constant $n$ to be able to apply Theorem 2. Indeed, our polynomially success probability depends on a lot of different probabilities, which however, can easily seen to be polynomially bounded as long as the dimension $n$ of our diophantine approximations problems is fixed.

Thus, we have proved the following Theorem, which can clearly extended to a wider class of composite numbers.

**Theorem 3.** *Let $N$ be the product of two randomly chosen primes of equal size. There exists a randomized polynomial-time quantum-algorithm that factors $N$ and uses quantum registers of binary length $\lceil (1+\varepsilon) \log_2(N) \rceil$, where $\varepsilon$ is an abitrarily small positive constant.*

## 5 Discussion

Exploiting the inherent probabilism of quantum computing we were able to substitute the continued fraction algorithm by its higher dimensional extension — the simultaneous Diophantine approximation. This resulted in around half of the length of the quantum registers compared to Shor's algorithm. This smaller bit-length of the first register might also be useful when performing the quantum Fourier transform over the first register. Also note that we have not added any new computation steps to Shor's order finding algorithm. Instead we shifted more computation from the quantum compuation part to the classical computation part which might be of importance conc. practical realizations of a quantum computer.

Moreover, it would be interesting to see whether our simultaneous Diophantine approximation approach could be used in other quantum algorithms where currently the continued fraction algorithm is used. Namely, in the algorithms of Kitaev [K], Mosca [M] and Mosca and Ekert [ME]. This question naturally arises as these algorithms currently use the so called eigenvalue estimation method and afterwards they also use the continued fraction algorithm to find the denominator of an unknown fraction.

We also would like to note that a pretty similiar use of simultaneous diophantine approximations was used by Shamir [Sha] to break the Merkle-Hellman in polynomial-time.

## 6 Acknowledgements

I would like to thank Johannes Blömer and Jochen Giesen for lots of valuable discussions about quantum computing.

## References


[ABO] D. Aharonov, M. Ben-Or, "Fault-tolerant quantum computing with constant error", *Proc. of the 29th Ann. ACM Symp. on Theory of Comp.*, pp. 176-188, 1997.

[Cas] J. W. S. Cassels, *An Introduction to Diophantine Approximations*, Cambridge University Press, Cambridge, 1957.

[CZ] I. J. Cirac, P. Zoller, "Quantum computations with cold trapped ions", *Phys. Rev. Let.* **74**:4091-4094, 1995.

[CH$^+$] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, S. Lloyd, "Experimental realization of a quantum algorithm", *Nature* **393**:143-146, 1998.

[Gru] J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.

[HSS] J. Håstad, A. W. Schrift, A. Shamir, "The discrete logarithm modulo a composite hides $O(n)$ bits", *J. Comp. Sys. Sci.* **47**:376-404, 1993.

[K] A. Y. Kitaev, "Quantum measurements and the Abelian stabilizer problem", Technical report, quant-ph/9511026, 1995.

[Lag1] J. C. Lagarias, "Some new results in simultaneous diophantine approximation", *Queen's Pap. Pure Appl. Math.* **54**:453-474, 1980.

[Lag2] J. C. Lagarias, "Best simultaneous Diophantine approximations. I: Growth rates of best approximation denominators", *Trans. Am. Math. Soc.* **272**:545-554, 1982.

[Lag3] J. C. Lagarias, "Best simultaneous Diophantine approximations. II: Behaviour of consecutive best approximations", *Pacific J. Math.* **102**:61-88, 1982.

[Lag4] J. C. Lagarias, "The computational complexity of simultaneous Diophantine approximation problems", *SIAM J. Computing* **14**:196-209, 1985.

[LH] J. Lagarias, J. Håstad, "Simultaneous diophantine approximation of rationals by rationals", *J. Number Theory* **24**:200-228, 1986.

[Leg] A. M. Legendre, *Essai sur la théorie des nombres*, J. B. M. Duprat, Paris, 1798.

[Lov] L. Lovasz, *An Algorithmic Theory of Graphs, Numbers and Convexity*, SIAM Publications, Philadelphia, 1986.

[M] M. Mosca, "Quantum searching, counting and amplititude modification by eigenvector analysis", *Proc. of the MFCS'98 Workshop on Randomized Algorithms*, pp. 90-100, 1998.

[ME] M. Mosca, A. Ekert, "The hidden subgroup problem and eigenvalue estimation on a quantum computer", *Proc. of the 1st NASA International Conference on Quantum Computing and Quantum Communication*, 1998.

[PP] S. Parker, M. B. Plenio, "Efficient factorization with a single pure qubit", Technical report, quant-ph/0001066, 2000.

[Rit] H. Ritter, *Zufallsbits basierend auf dem diskreten Logarithmus*, Master Thesis, University of Frankfurt, Dept. of Math., 1992.

[Sch] A. Schrijver, *An Introduction to Linear and Integer Programming*, John Wiley & Sons, New York, 1986.

[Kan] B. E. Kane, "Silicon based quantum computation", Technical report, quant-ph/0003031, 2000.

[Knu] D. E. Knuth, *The Art of Computer Programming, Vol.2: Seminumerical Algorithms*, 3rd ed., Addison-Wesley, Reading MA, 1999.

[Sha] A. Shamir, "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem", *IEEE Trans. Inf. Theory* **IT-30**:699-704, 1984.

[Sho] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Computing* **26**:1484-1509, 1997.

[Z] C. Zalka, "Fast version of Shor's quantum factoring algorithm", Technical report, quant-ph/9806084, 1998.