Shor's quantum algorithm using electrons in semiconductor nanostructures

Fabrizio Buscemi*

Department of Electronics Computer Science and Systems, University of Bologna, Viale Risorgimento 2, I-40136 Bologna, Italy,
ARCES, Alma Mater Studiorum, University of Bologna, Via Toffano 2/2, I-40125 Bologna, Italy, and
Center S3, CNR-Institute of Nanosciences, Via Campi 213A, I-41125 Modena, Italy

(Received 11 November 2010; published 12 January 2011)

Shor's factoring algorithm illustrates the potential power of quantum computation. Here, we present and numerically investigate a proposal for a compiled version of such an algorithm based on a quantum-wire network by exploiting the potential of fully coherent electron transport assisted by the surface acoustic waves. Specifically, a nonstandard approach is used to implement, in a simple form, the quantum circuits of the modular exponentiation execution for the simplest instance of Shor's algorithm, that is, the factorization of $N = 15$. The numerical procedure is based on a time-dependent solution of the multiparticle Schrödinger equation. The near-ideal algorithm performance and the large estimated fidelity indicate the efficiency of the protocol implemented, which also is almost insensitive to small destabilizing effects during quantum computation.

DOI: 10.1103/PhysRevA.83.012302 PACS number(s): 03.67.Ac, 73.63.Nm

I. INTRODUCTION

Quantum computers can efficiently solve some problems that are unaffordable on classical computers, and processing the information encoded in quantum systems can be extremely powerful for particular tasks. Specifically, quantum-mechanics effects such as entanglement and wave-function superposition turn out to be fundamental building blocks, and they allow for the quantum computational speedup over classical computation. Shor's algorithm [1–4] has undoubtedly been widely investigated among those illustrating the power of quantum computation. In fact, it plays a key role in cryptographic protocols, because it allows one to factorize a composite number with a computational time that is a polynomial function instead of an exponential function of the number itself.

The practical implementation of Shor's algorithm represents a challenge for quantum information science. Two possible physical architectures have been proposed: nuclear magnetic resonance (NMR) [5,6] and photonic [7–9] systems, even though some open questions exist in both cases. While in NMR it is difficult to prepare the qubits in pure states and control their coherent evolution, thus leading to a controversial quantum nature of the experiments, photonic systems cannot be scaled to a larger number of qubits due to their size and stability limitations. Nevertheless, a recent experimental demonstration of Shor's algorithm was obtained by means of optical waveguides integrated on silica-on-silicon chips. Even if the efficiency of the single-photon source and detectors still does not appear to be very good [9], the suggested architecture is promising for the implementation of large-scale quantum circuits on many qubits.

No evidence of a compiled version of a quantum factoring algorithm using electron qubits has been achieved so far. The approach of using charge carriers in solid-state systems is very appealing because it not only allows the scalability problem to be overcome, but it also provides a valid guideline for the design of devices easily integrable in the traditional electronic circuitry. Specifically, the possibility of implementing Shor's quantum factoring algorithm on an electronic chip would certainly represent an essential test to verify the potential of quantum cryptography in everyday life.

In this paper, we propose and numerically simulate a compiled version of Shor's algorithm. Electronic quantum logic gates in one-dimensional (1D) semiconductor channels are used to realize the necessary processes and to produce multiparticle entanglement and multipath interference. In particular, we have considered the fully coherent surface-acoustic-wave (SAW) assisted electron transport in couples of GaAs quantum wires [10], with the qubit defined by the localization of a single carrier in one of the coupled channels [11].

Quantum-wire systems have been shown to be suitable to produce bipartite entangled states [12] and to perform quantum teleportation [13]. Here, the numerical implementation of the quantum factoring algorithm can be much more demanding in comparison with the previous works [12,13], due to the higher number of the simulated quantum logic operations over many qubits. Specifically, we design the quantum circuits of the modular exponentiation execution for the easiest meaningful instance of Shor's algorithm, that is, the factorization of $N = 15$ for two different co-primes $C = 11$ and $C = 2$ (defined in Sec. II), corresponding to the periods $r = 2$ and $r = 4$, respectively. The circuit performing the modular exponentiation function is brought to a form different from the one given in the literature [1,4]. This procedure allows one to move on toward simpler networks of electron quantum gates, and it aims at future research leading to a scalable full realization of Shor's algorithm in quantum-wire devices. In our implementation the inverse quantum Fourier transformation (QFT) is not present since it is not necessary for any order-2^l circuit (with $l \in \mathbb{N}$), as shown in the literature [7]. For sake of completeness, a description of the circuit realizing the inverse QFT in a quantum-wire network has been given elsewhere [14].

This paper is organized as follows. In Sec. II we illustrate the theoretical features of Shor's algorithm, while the description

[*] fabrizio.buscemi@unimore.it

of the physical implementation in a quantum-wire device and the discussion of the numerical approach adopted are given in Sec. III. In Sec. IV we show the results obtained from the numerical simulations of two quantum circuits for the factorization of $N = 15$ corresponding to two different parameter choices. Comments on the results and final remarks are made in Sec. V.

II. SHOR'S ALGORITHM

The strategy to find a nontrivial prime factor of the positive integer N is described in the following. A random co-prime C is chosen, i.e., N and C have no common factors. Euler's theorem states that there exists an integer r such that $C^r = 1 \bmod N$ (that is, $C^r - 1$ is an integer number multiple of N), with $1 \leqslant r < N$. The number r is called the *order* of $C \bmod N$. Provided that the latter is even, then it follows that $C^r - 1 = (C^{r/2} - 1)(C^{r/2} + 1) = 0 \bmod N$ and this implies that N is a divisor of the product $(C^{r/2} - 1)(C^{r/2} + 1)$. By assuming that $(C^{r/2} \neq -1 \bmod N)$, it follows that N must have a common factor with both $(C^{r/2} \pm 1)$. Therefore, this implies that the factors of N are given by the greatest common divisor of N and $(C^{r/2} \pm 1)$, which can be efficiently computed by means of Euclid's classical algorithm. It is worth noting that in order to guarantee the algorithm validity the two conditions stating that r is even and $(C^{r/2} \neq -1 \bmod N)$ must be satisfied. These conditions are met with high probability for N odd, except in the case where N is a prime power ($N = p^\alpha$ with p a prime). Thus, the smallest composite integer N that can be successfully factored by Shor's method is $N = 15$. If N is an even number or a prime power, other classical methods should fruitfully be applied for the factorization instead of Shor's method.

Shor's algorithm needs quantum computation only in the evaluation of the order r. The quantum order-finding routine commonly uses two registers of qubits [1,3]: the argument register with $n = 2\log_2 N$ qubits, and the function register with $m = \log_2 N$ qubits. Its implementation can be separated into three distinct steps. The first one is the register initialization corresponding to

$$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \longmapsto \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}\,|0\rangle^{\otimes m-1}|1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle^{\otimes m-1}|1\rangle, \qquad (1)$$

where the argument register is prepared by means of the Hadamard transformations in an equal superposition of all n-qubit computational bases $|0(1)_{x_1}\rangle|0(1)_{x_2}\rangle\cdots|0(1)_{x_i}\rangle\cdots|0(1)_{x_n}\rangle$. In the second step, also known as modular exponentiation, the function $C^x \bmod N$ is implemented on the function register, while the argument register remains in x. The global state is thus given by

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|C^x \bmod N\rangle. \qquad (2)$$

The state of Eq. (2) is highly entangled and exhibits the so-called massive parallelism; i.e., the execution entangles in parallel all the 2^n input values with the corresponding values of $C^x \bmod N$, although the algorithm has run only once [3,15]. Finally, the inverse QFT is applied on the argument register yielding the state

$$\frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}e^{2\pi xz/2^n}|z\rangle|C^x \bmod N\rangle, \qquad (3)$$

where, due to the interference, only the terms $|z\rangle$ with

$$z = a2^n/r \qquad (4)$$

have a significative amplitude. Here, a is a random integer ranging from 0 to $r-1$. Thus, if one performs measurements on the outcome of the argument register, one would get $a2^n/r$ for some a, and the order r can be deduced after the classical procedure with probability greater than $1/2$ (see Ref. [3]).

The modular exponentiation, that is, the evaluation of $C^x \bmod N$ for 2^n values of x in parallel, is the most demanding part of the algorithm. This can be performed by using the identity $x = x_{n-1}2^{(n-1)} + \cdots + x_1 2^1 + x_0 2^0$, where x_k are the binary digits of x. From this, it follows that

$$\begin{aligned} C^x \bmod N &= C^{2^{(n-1)}x_{n-1}}\cdots C^{2x_1}C^{x_0} \bmod N \\ &= C^{2^{(n-1)}x_{n-1}}\cdots[C^{2x_1}[C^{x_0} \bmod N] \bmod N] \\ &\quad\cdots \bmod N]. \end{aligned} \qquad (5)$$

This means that we first multiply 1 by $C \bmod N$, if and only if $x_0 = 1$; then we multiply the result by $C^2 \bmod N$ if and only if $x_1 = 1$ and so forth, until we finally multiply by $C^{2^{(n-1)}} \bmod N$ if and only if $x_{n-1} = 1$. Therefore, the modular exponentiation consists of n serial multiplications modulo N, each of them controlled by the qubit x_k. The factors $C, C^2, \ldots, C^{2^{(n-1)}} \bmod N$ can be found efficiently on a classical computer by *repeated squaring*.

As noted above, Shor's factorization algorithm fails if N is even or a prime power, and the smallest composite integer N that can be successfully factored by means of Shor's method is $N = 15$. Even if N is small, this compiled version of Shor's algorithm displays a great potential for a future realization of a large-scale quantum algorithm.

With $N = 15$, the minimum size of the function and argument registers must be $m = \log_2[15] = 4$ and $n = 2m = 8$, respectively. The algorithm would then require at least 12 qubits. However, the following comments allow us to reduce the number of qubits necessary for the purpose of a proof-of-principle demonstration. A co-prime C with 15 is one element of the set 2, 4, 7, 8, 11, 13, and 14. As shown in Table I, it comes from repeated squaring that $C^4 \bmod 15 = 1$ for all valid C. In turn, this implies that only two bits x_0 and x_1 are needed for the controlled multiplications. As a consequence, the multiplications by $C^4, C^8, \ldots$ are trivial, and all the multiplications, except the ones by C and C^2, can be left out. For $C = 4, 11, 14$, $C^2 \bmod 15 = 1$ and only the first bit x_0 is relevant. These considerations account for a reduction of the size of the argument register, which can finally be constituted by no more than two qubits ($n = 2$). By adding this latter result to the 4 qubits of the function register, only 6 qubits are needed instead of 12, as previously found.

TABLE I. The table displays C^x mod 15 for all $C < 15$ co-prime with 15 and for values of x which are powers of 2. Note that C^4 mod $15 = 1$ for all valid C.

		C						
		2	4	7	8	11	13	14
	0	1	1	1	1	1	1	1
x	1	2	4	7	8	11	13	14
	2	4	1	4	4	1	4	1
	4	1	1	1	1	1	1	1

Shor's factorization algorithm for the number 15 turns out to be particularly simple because it does not require the implementation of the inverse QFT in the quantum circuit. As shown in the literature [7], the latter is not necessary for any circuit of order 2^l and it can be replaced by a classical processing which also inverts the order of the computed quantum bits of the argument register.

In this work we implement Shor's quantum factoring algorithm and check it against two co-primes, $C = 11$ and $C = 2$, that are representative parameters for the system at hand.

A. $C = 11$

This parameter choice represent an "easy case" since the modular exponentiation can be simplified to the multiplication of the initial function register state, $|y\rangle = |0_{y_3}0_{y_2}0_{y_1}1_{y_0}\rangle = 1$, by $C = 11$ controlled only by x_0 [6].

In the left panel of Fig. 1 a compiled version of the quantum circuit for $C = 11$, using the inverse QFT, is displayed. At first, both registers are initialized: Each qubit of the argument is prepared by Hadamard gates in a superposition of 0 and 1, and the function register state is set to $|y\rangle = 1$, so that the global state $|\Phi_{C=11}\rangle$ of the system is

$$|\Phi_{C=11}\rangle = \tfrac{1}{2}\big(\big|0_{x_1}0_{x_0}\big\rangle + \big|0_{x_1}1_{x_0}\big\rangle + \big|1_{x_1}0_{x_0}\big\rangle + \big|1_{x_1}1_{x_0}\big\rangle\big)\big|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\big\rangle. \tag{6}$$

Then, the modular exponentiation is performed: The controlled multiplication of 1 by 11 is equivalent to the controlled addition of 10 to 1. The latter is implemented in the quantum circuit by two controlled-NOT (CNOT) gates: one between x_0 and y_1 and one between x_0 and y_3. It is worth noting that the qubits y_0 and y_2 evolve trivially during computation. Thus the state of the system takes the form

$$\begin{aligned}|\Phi_{C=11}\rangle &= \sum_{x=0}^{3}|x\rangle|11^x \bmod 15\rangle \\ &= \frac{1}{2}\big(\big|0_{x_1}0_{x_0}\big\rangle\big|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\big\rangle + \big|0_{x_1}1_{x_0}\big\rangle\big|1_{y_3}0_{y_2}1_{y_1}1_{y_0}\big\rangle \\ &\quad + \big|1_{x_1}0_{x_0}\big\rangle\big|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\big\rangle + \big|1_{x_1}1_{x_0}\big\rangle\big|1_{y_3}0_{y_2}1_{y_1}1_{y_0}\big\rangle\big).\end{aligned} \tag{7}$$

This means that a Greenberger-Horne-Zeilinger (GHZ) entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(\big|0_{x_0}0_{y_3}0_{y_1}\big\rangle + \big|1_{x_0}1_{y_3}1_{y_1}\big\rangle\big) \tag{8}$$

is created between qubit x_0 of the argument register and qubits y_3 and y_1 of the function registers.

The final step is represented by the inverse QFT. The right panel of Fig. 1 shows a compiled version of the quantum circuit without using the inverse QFT. Note that in this case also qubit x_1 is redundant: The corresponding Hadamard gate is unnecessary and does not need to be implemented. Here, the initial state is $\frac{1}{\sqrt{2}}(|0_{x_1}0_{x_0}\rangle + |0_{x_1}1_{x_0}\rangle)|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\rangle$ and the modular exponentiation yields $\frac{1}{\sqrt{2}}(|0_{x_1}0_{x_0}\rangle|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\rangle + |0_{x_1}1_{x_0}\rangle|1_{y_3}0_{y_2}1_{y_1}1_{y_0}\rangle)$.

The outcomes of the measurement on the inverted argument qubits x_0 and x_1 give then 00 or 10 with equal probability. Once this result is known, one can obtain the *order* r of C mod N from Eq. (4). While the output 00 corresponds to a failure, the output 10 allows one to determine the period $r = 2^2/2 = 2$ and represents a successful implementation of Shor's algorithm.

B. $C = 2$

Since the number of gates needed to perform the modular exponentiation is greater than the case of $C = 11$ [6], the choice of $C = 2$ represents a difficult case. In fact, the modular exponentiation is given by the multiplication of $|y\rangle = 1$ by 2 controlled by x_0 and by the multiplication of the obtained result by 4 controlled by x_1. The left panel of Fig. 2 shows the quantum circuit for the case at hand. The network for the modular exponentiation is composed of two CNOT followed by two controlled SWAP (CSWAP) gates; the first two correspond to the addition of 1 to $|y\rangle = 1$ controlled by x_0,

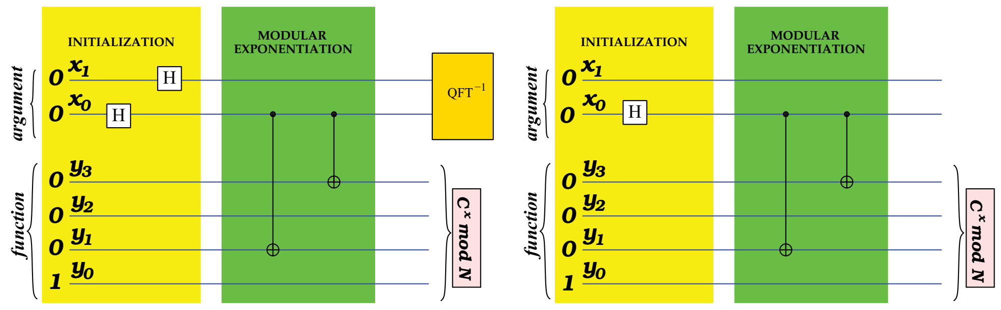

FIG. 1. (Color online) Left: Outline of the quantum circuit for quantum factorization of 15 for $C = 11$, using the inverse QFT. [8] Right: Outline of the quantum circuit for quantum factorization of 15 for $C = 11$, not using the inverse QFT.

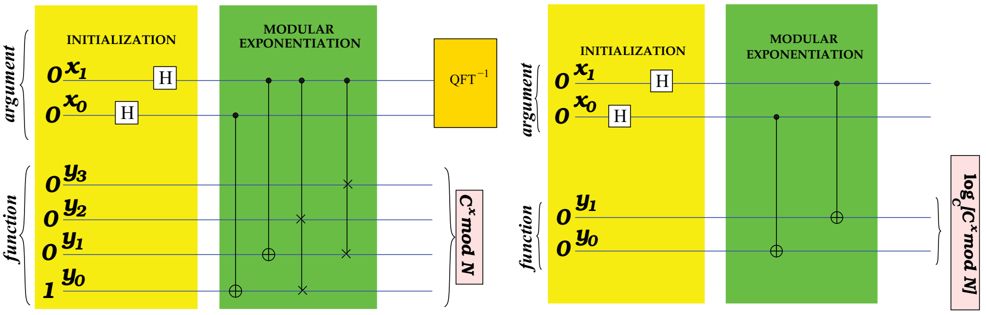

FIG. 2. (Color online) Left: Outline of the quantum circuit for quantum factorization of 15 for $C = 2$, using the inverse QFT and evaluating 2^x mod 15 in the function register. Right: Outline of the quantum circuit for quantum factorization of 15 for $C = 2$, not using the inverse QFT and evaluating $\log_2[2^x \bmod 15]$ in the function register. The two circuits correspond to the ones examined in Ref. [7].

while the CSWAP gates multiply the result by 4 controlled by x_1. The modular exponentiation leads to the state $\sum_{x=0}^{3}|x\rangle|2^x \bmod 15\rangle = \frac{1}{2}(|0_{x_1}0_{x_0}\rangle|0_{y_3}0_{y_2}0_{y_1}1_{y_0}\rangle + |0_{x_1}1_{x_0}\rangle|0_{y_3}0_{y_2}1_{y_1}0_{y_0}\rangle + |1_{x_1}0_{x_0}\rangle|0_{y_3}0_{y_2}1_{y_1}0_{y_0}\rangle + |1_{x_1}1_{x_0}\rangle|1_{y_3}0_{y_2}0_{y_1}0_{y_0}\rangle)$.

Nevertheless, a different compilation of the quantum circuit can be realized [7], and it is reported in the right panel of Fig. 2. By means of the latter, it is possible to evaluate $\log_2[2^x \bmod 15]$ in the function register in place of $2^x \bmod 15$, thus reducing the number of function qubits from $\log_2[15] = 4$ to $\log_2\{\log_2[15]\} = 2$. This compilation maintains all the features of the algorithm originally proposed [3], and it still does not make use of the inverse QFT, as in the previous case. Following this scheme, the initialization of the system leads to the state

$$|\Phi_{C=2}\rangle = \tfrac{1}{2}\big(|0_{x_1}0_{x_0}\rangle + |0_{x_1}1_{x_0}\rangle + |1_{x_1}0_{x_0}\rangle + |1_{x_1}1_{x_0}\rangle\big)|0_{y_1}0_{y_0}\rangle, \tag{9}$$

meaning that the argument register is kept in the usual equally weighted coherent superposition of all possible arguments, while the initial function register state is $|y\rangle = 0$. If we apply the procedure described in Eq. (5) to evaluate $\log_2[2^x \bmod 15]$, it can be easily shown that the modular exponentiation reduces to the sum of $\log_2[2^1 \bmod 15] = 1$ to $|y\rangle = 0$ controlled by x_0 and of $\log_2[2^2 \bmod 15] = 2$ to the obtained result controlled by x_1. These operations are implemented in the quantum circuit reported in the right panel of Fig. 2 by means of two CNOT gates: one between x_0 and y_0 and another between x_1 and y_1. It is worth noting that in this case the algorithm is very simple since it consists of only two networks of gates acting on independent qubit pairs. After modular exponentiation the state of the system takes the form

$$\begin{aligned}|\Phi_{C=2}\rangle &= \tfrac{1}{2}\big(|0_{x_1}0_{x_0}0_{y_1}0_{y_0}\rangle + |0_{x_1}1_{x_0}0_{y_1}1_{y_0}\rangle \\ &\quad + |1_{x_1}0_{x_0}1_{y_1}0_{y_0}\rangle + |1_{x_1}1_{x_0}1_{y_1}1_{y_0}\rangle\big) \\ &= \tfrac{1}{2}\big(|0_{x_1}0_{y_1}\rangle + |1_{x_1}1_{y_1}\rangle\big)\big(|0_{x_0}0_{y_0}\rangle + |1_{x_0}1_{y_0}\rangle\big),\end{aligned} \tag{10}$$

that is, the product of two entangled Bell pairs, thus confirming the manifestation of entanglement between the two registers of the algorithm. The inverse QFT is not necessary and it can be replaced by its classical counterpart, which also swaps the output quantum bit of the argument register. The two-bit outputs for the case under investigations are 00, 01,10, and 11. The second and the fourth outcomes allow the evaluation of the order $r = 4$, which efficiently yields the factors 3 and 5 via Euclid's classical algorithm; the first one corresponds to a failure mode and, lastly, the third one leads to trivial factors.

III. THE PHYSICAL IMPLEMENTATION AND THE NUMERICAL APPROACH

Here, we describe the implementation of Shor's algorithm in a specific semiconductor nanostructure. It consists of a number of couples of GaAs quantum wires where surface acoustic waves (i.e., sinusoidal piezoelectric potential) propagate and trap charged carriers into their moving minima, letting one particle fill in each minimum [16]. The so-called flying qubits are realized by means of the states $|0\rangle$ and $|1\rangle$, encoded through the localization of a single electron in one of the two 1D channels [11]. Here, the SAWs are used to inject and drive the electron thanks to their efficiency in preventing the natural spatial spread of the wave function [17] and in making the carriers more immune to the decohering effects [18]. Moreover, in this investigation the carrier transport is assumed to be fully coherent.

As shown in the literature [19,20], such a system is able to provide the universal set of gates useful for realizing any quantum computational network. Specifically, the basic building blocks are $R_x(\theta)$, $R_{0(1)}(\phi)$, and $T(\gamma)$ [21]. The former two gates implement one-qubit logical operations, whereas the latter is a two-qubit gate.

$R_x(\theta)$ acts as an electronic beam splitter and can be materialized through a coupling window between the two wires of the qubit [22]. Its matrix representation on the basis $\{|0\rangle,|1\rangle\}$ is given by

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}. \tag{11}$$

$R_{0(1)}(\phi)$ is an electronic phase shifter obtained by inserting a potential barrier in the wire 0(1), thus inducing a delay phase ϕ in the propagation of wave function. Its action is described in the one-qubit basis by

$$R_0(\phi) = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1\end{pmatrix} \quad \text{and} \quad R_1(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi}\end{pmatrix}. \tag{12}$$

$T(\gamma)$ is a conditional phase gate exploiting the Coulomb interaction between two electrons. It consists of a region in which the carriers propagate along two different wires close enough to give rise to an effective interaction able to delay both particles. The matrix representation of $T(\gamma)$ in the two-qubit basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ is

$$T(\gamma)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&e^{i\gamma}&0\\0&0&0&1\end{pmatrix}. \tag{13}$$

The phases θ, ϕ, and γ of these quantum gates depend upon the physical and geometrical parameters of the systems such as velocity, amplitude and wavelength of the SAW potential, strength of the electron-electron interaction, coupling window length, and shape of the potential barrier. In order to perform any transformation of the many-qubit state, an appropriate tuning of these parameters in a given network of $R_x(\theta)$, $R_{0(1)}(\phi)$, and $T(\gamma)$ gates is required.

In the compiled versions of Shor's algorithm illustrated in the right panels of Figs. 1 and 2, corresponding to $C=11$ and $C=2$, respectively, the two logical operations involved are only the Hadarmad H and CNOT gates. In terms of $R_x(\theta)$, $R_{0(1)}(\phi)$, and $T(\gamma)$, these operations can be reworked as [14]

$$H=R_0\left(\frac{3\pi}{2}\right)R_x\left(\frac{\pi}{2}\right)R_0\left(\frac{\pi}{2}\right)R_1(\pi)=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \tag{14}$$

and

$$\text{CNOT}=R_0^{(2)}\left(\frac{3\pi}{2}\right)R_x^{(2)}\left(\frac{3\pi}{2}\right)T^{(1,2)}(\pi)R_x^{(2)}\left(\frac{\pi}{2}\right)R_0^{(2)}\left(\frac{\pi}{2}\right)\times R_1^{(1)}(\pi)=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}. \tag{15}$$

The numerical implementation of the quantum circuits described in the previous section is extremely challenging due to the large number of basic building blocks needed to realize the H and CNOT gates. Furthermore, the experimental realization of such devices would also certainly meet serious obstacles stemming from the difficulty of preserving the coherent evolution of the qubits during a number of logical operations, from decoherence effects due to interactions with the environment, as well as from possible structural defects induced by the processes of fabrication and tuning of each quantum gate. The theoretical and experimental implementation of two-qubit quantum circuits by means of a minimum amount of operations has been widely discussed in the literature [23,24]. Different protocols have been proposed, ranging from the special perfect entanglers [23] to the use of a given tunable entangling interaction [24]. Here, we propose in the followings a scheme suitable to perform the quantum factoring algorithm in devices formed by semiconductor quantum wires with a minimal number of the fundamental gates $R_x(\theta)$, $R_{0(1)}(\phi)$, and $T(\gamma)$. The proposed implementation satisfies the main requirements of Shor's algorithm as originally formulated [1,3]. In fact, "massive parallelism" is maintained, since entanglement is created between argument and function registers, and the binary output of the argument qubits are unchanged, as will be shown in the following. In the left and right panels of Fig. 3 we report the quantum-wire networks implementing the circuits displayed in the right panels of Figs. 1 and 2, respectively.

In the first case, corresponding to $C=11$, the network implemented reads

$$R_x^{(x_0)}\left(\frac{\pi}{2}\right)R_x^{(y_1)}\left(\frac{\pi}{2}\right)T^{(x_0,y_1)}(\pi)R_x^{(y_1)}\left(\frac{\pi}{2}\right)R_x^{(y_3)}\left(\frac{\pi}{2}\right)\times R_0^{(y_3)}(\pi)T^{(y_3,x_0)}(\pi)R_1^{(x_0)}(\pi)R_x^{(y_3)}\left(\frac{\pi}{2}\right), \tag{16}$$

where the superscripts of the quantum gates indicate which qubit they act on. The three-qubit output state is

$$\frac{1}{\sqrt{2}}\big(-\left|0_{x_0}0_{y_3}0_{y_1}\right\rangle+i\left|1_{x_0}1_{y_3}1_{y_1}\right\rangle\big). \tag{17}$$

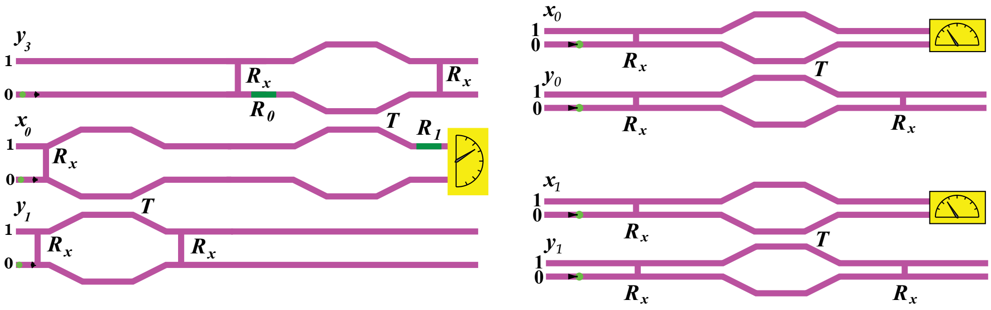

FIG. 3. (Color online) Left: Sketch of the physical system used to factorize $N=15$ with $C=11$, corresponding to the quantum circuit displayed in the right panel of Fig. 1. The beam splitter R_x of the qubit x_0 mimics the initialization procedure, that is, the equal splitting of electron wave function of the qubit x_0 in the two wires. The next two sets of gates, first R_xTR_x acting on $\{x_0,y_1\}$ and then $R_xR_0TR_1R_x$ on $\{x_0,y_3\}$, play the role of two CNOT gates creating the maximum entanglement of the qubits $\{x_0,y_1,y_3\}$ in the modular exponentiation step. For sake of clarity the qubits y_0 and y_2 evolving trivially during the computation have not been reported. Right: Sketch of the physical system used to factorize $N=15$ with $C=2$, corresponding to the quantum circuit displayed in the right panel of Fig. 2. In the initialization procedure two gates R_x act on the couple of the argument register qubits $\{x_0,x_1\}$ and split each of them in an equal superposition of the $|0\rangle$ and $|1\rangle$ states. The modular exponentiation consists of two networks R_xTR_x, each operating onto $\{x_0,y_0\}$ and $\{x_1,y_1\}$ mimicking the action of two CNOT gates. Note that here, for brevity, the phases of the quantum gates involved in the networks and explicitly indicated in Eqs. (16) and (18), are omitted.

For $C = 2$ the global logical transformation can be written as

$$R_x^{(x_0)}\left(\frac{\pi}{2}\right)R_x^{(y_0)}\left(\frac{\pi}{2}\right)R_x^{(x_1)}\left(\frac{\pi}{2}\right)R_x^{(y_1)}\left(\frac{\pi}{2}\right)T^{(x_0,y_0)}(\pi)T^{(x_1,y_1)} \times(\pi)R_x^{(y_0)}\left(\frac{\pi}{2}\right)R_x^{(y_1)}\left(\frac{\pi}{2}\right) \tag{18}$$

and, after being applied to the input state $|0_{x_1}0_{x_0}0_{y_1}0_{y_0}\rangle$, it yields

$$\tfrac{1}{2}\left(|0_{x_1}0_{y_1}\rangle - |1_{x_1}1_{y_1}\rangle\right)\left(|0_{x_0}0_{y_0}\rangle - |1_{x_0}1_{y_0}\rangle\right). \tag{19}$$

In both cases, the degree of the entanglement created between the qubits of the argument and the function register is equal to the one of the standard formulation of Shor's quantum factoring algorithm [1,3]. While for $C = 11$ the output state is GHZ-like (i.e. the maximum amount of quantum correlations is built up among three qubits), when $C = 2$ the four-qubit state is the product of two entangled Bell pairs. Furthermore, the reduced density matrices of the argument qubits correspond to the ones calculated from the quantum states of Eqs. (8) and (10). In turn, this implies that the binary output of the algorithm, i.e., the outcome measurements on the argument register, be identical.

The networks of the gates described in Eqs. (16) and (18) have been simulated by solving numerically the time-dependent Schrödinger equations for three and four electrons injected in the GaAs quantum-wire devices of Fig. 3. While for $C = 2$ the four-particle dynamics reduces to the time evolution of a pair of separable two-particle systems, when $C = 11$, a solution of the Schrödinger equation for the whole three-carrier wave function is required [25]. To minimize the computational burden of the two reported cases, a semi-1D approach has been used to investigate the time evolution of the system in place of a two-dimensional (2D) computational scheme. This approach was already introduced to simulate a teleportation protocol in a quantum-wire device [13]. According to this simplified scheme, the direction $\mathbf{y}$ of the particles along the wires is fully included in the simulation ($\mathbf{y}$ being discretized with a point-grid resolution of $\Delta\mathbf{y} = 1$ nm), while the two variables describing the longitudinal direction $\mathbf{x}$ and identifying the wire where the carriers are localized can only assume one of the two values, 0 or 1.

Though the numerical procedure adopted here does not allow simulation of the gate $R_x(\theta)$, which would require a full 2D analysis, it does make it possible to move from a time-dependent Schrödinger equation for a multivariable wave function $\Phi(\mathbf{X},\mathbf{Y},t)$ (seven unknowns for the device with $C = 11$ and nine when $C = 2$) to many coupled Schrödinger equations of the following kind:

$$i\hbar\frac{\partial}{\partial t}\Phi_{\mathbf{X}}(\mathbf{Y},t) = \left(-\frac{\hbar^2}{2m}\nabla^2_{\mathbf{Y}} + V_{\mathbf{X}}(\mathbf{Y},t)\right)\Phi_{\mathbf{X}}(\mathbf{Y},t), \tag{20}$$

where $\mathbf{X} \equiv (\mathbf{x}_{x_0},\mathbf{x}_{y_0},\mathbf{x}_{x_1},\mathbf{x}_{y_1},\ldots)$ and $\mathbf{Y} \equiv (\mathbf{y}_{x_0},\mathbf{y}_{y_0},\mathbf{y}_{x_1},\mathbf{y}_{y_1},\ldots)$. Specifically, when $C = 11$ a system of eight coupled equations is obtained, while for $C = 2$ two independent systems of four equations are found since the qubit pairs $\{x_0,y_0\}$ and $\{x_1,y_1\}$ are independent. In both cases a Crank-Nicholson finite difference scheme [26] has been applied to get a numerical solution. The potential term $V_{\mathbf{X}}(\mathbf{Y},t)$ appearing in Eq. (20) sums up the SAW time-dependent potential, the Coulomb interaction between electrons, and the static potential profile. The simulations presented here make use of a sinusoidal potential mimicking a SAW of amplitude and wavelength equal to 20 meV and 200 nm, respectively, and propagating with a sound velocity $v_s = 3.3 \times 10^3$ m s^{-1}. Screening effects have been included in the Coulomb potential between the carriers by inserting an exponential damping term [27] with a Debye wave vector of 0.2 nm^{-1}.

In order to numerically implement the networks described in Eqs. (16) and (18), one must first find the suitable geometrical parameters of the device for the gates $R_{0(1)}(\phi)$ and $T(\gamma)$ giving the required value π of the phases ϕ and γ. To this aim, we have performed a number of simulations, testing different geometries for the phase shift and the conditional phase gate. The phase ϕ is found to depend on the height and the length of the potential barrier. The values of these parameters obtained from the optimization procedure are 2.82 meV and 8 nm, respectively, corresponding to a delay phase ϕ of 0.92π, which is good enough for our purposes, as will be shown in the next section. It is worth noting that the barrier height is significantly smaller than the amplitude of the SAW potential, this making the spatial spreading of the electron wave packet negligible and letting it be entirely transmitted through the barrier. The main geometrical parameters affecting the phase γ of the conditional phase gate are the length of the coupling region and the distance between the coupled wires. Their optimal values used in the numerical implementation of the algorithm are 150 and 5 nm, respectively. They lead to a γ value of about 0.88π, which allows us to simulate satisfactorily the two-qubit logical operation of a CNOT-like gate. By applying the described geometry for $T(\gamma)$, both the tunneling effects between the two wires and the reflection phenomena in the coupling region are negligible.

From a computational point of view, the numerical simulation of the $T(\gamma)$ gate is more challenging than that of the phase shift $R_{0(1)}(\phi)$. While the latter involves a one-particle potential, the former exploits a two-particle interaction that builds up an amount of quantum correlations between the wire degrees of freedom of the particles, as expected. However, it also creates an undesired entanglement between the variables defining the position of the carriers along the wires. As a consequence, the evaluation of the effects of the controlled phase gate on the multiparticle wave function is a demanding task because it implies that a number of two-particle simulations must be combined together to obtain the time-evolved state of the overall system.

The $R_x(\theta)$ gate has not directly been simulated; nevertheless, its action has been taken into account by means of the transformation matrix of Eq. (11), validated by the results of appropriate 2D simulations [20].

IV. RESULTS

We first present the results obtained for $C = 11$ and then those for $C = 2$.

A. $C = 11$

Figure 4 shows the density matrix describing the qubits of the argument and function register, $\{x_0,y_1,y_3\}$, at three

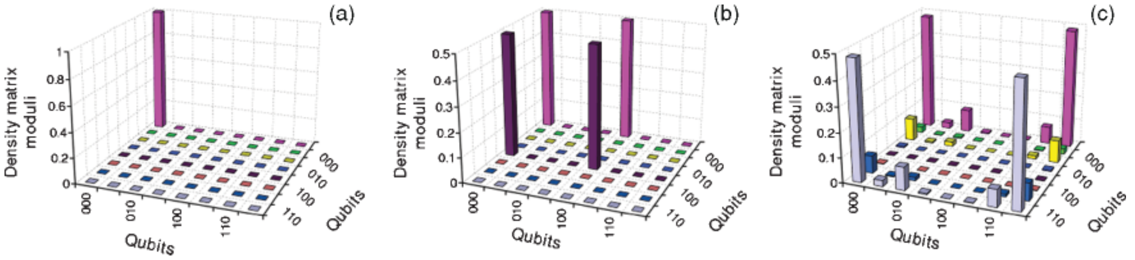

FIG. 4. (Color online) The density matrix of the qubits $\{x_0,y_1,y_3\}$ evaluated at three different time steps: (a) input, (b) initialization procedure, and (c) after the modular exponentiation. Note that these matrices have been obtained from the full density matrices of the electrons of the qubits $\{x_0,y_1,y_3\}$ by integrating over the variables defining the position of three carriers along the channels. Here the moduli of the density matrix elements are plotted.

different stages: input, initialization procedure, and modular exponentiation. For sake of simplicity, we do not consider the x_1, y_0, and y_2 qubits that evolve trivially during the computation. Knowledge of the joint state of both registers after modular exponentiation is essential for the estimation of the device performance. In particular, we find that the output quantum state corresponds to the GHZ-like entangled state $|\Psi\rangle$ of Eq. (17) with a good approximation. For a more quantitative evaluation of the reliability of the algorithm, we have also calculated the fidelity $F=\langle\Psi|\rho_{\rm out}|\Psi\rangle$, where $\rho_{\rm out}$ is the output density matrix of the full system. The high value found, $F=0.97$, evidences the very good efficiency of the implementation. Such a result is certainly related to the fact that our numerical simulations have been performed by setting the device temperature at 0 K, that is, by neglecting any effect of decoherence induced by the environment on the carrier transport properties. In particular, this means that the electron-phonon interaction has not been included in the simulations. These assumptions are physically sound when we take into account that the experimental investigations of the low-dimensional structures used as the basic blocks for our device are usually performed at very low temperatures [10,22]. Moreover, one of the pros of our results certainly relies on the high fidelity value, which has not been obtained under ideal geometries for the $R_0(1)(\phi)$ and $T(\gamma)$ gates. Once more, this off-ideality situation is close to the experimental conditions.

The density matrix of the argument register after modular exponentiation is displayed in Fig. 5. Specifically, we show the reduced density matrix $\rho_{\{x_0,x_0'\}}(\mathbf{y},\mathbf{y})$ of the electron of qubit x_0, without the redundant qubit x_1. The output of the quantum circuit is the logical state probability, that is, the probability of finding the electron of the qubit x_0 in the wire 0 or 1. This is described by the integral over $\mathbf{y}$ of the diagonal elements of $\rho_{x_0,x_0'}(\mathbf{y},\mathbf{y})$. The off-diagonal terms are very small, thus proving that the argument register becomes a full quantum statistical mixture because of its entanglement with the function register. To better quantify the amount of the quantum correlations created between x_0 and $\{y_1,y_3\}$, we evaluate the linear entropy ε_L of the qubit x_0 as [28] $\varepsilon_L=2(1-{\rm Tr}\rho_r^2)$, where the factor 2 stems out from the normalization condition and ρ_r^2 is the square of the reduced density matrix $\rho_{\{x_0,x_0'\}}(\mathbf{y},\mathbf{y})$ of the electron of the qubit x_0 integrated over $\mathbf{y}$. We find that $\varepsilon_L=0.999$ and therefore a maximal correlation between the two registers of the quantum circuit is built up, which unambiguously proves the quantum nature of the simulated circuit, as required by Shor's algorithm. Once the logical state probabilities of the qubit x_0 are known, the latter are combined with the qubit x_1 in the zero state and then, as required, the order of the argument bits is inverted. This procedure allows one to obtain the binary output of the circuit already discussed in Sec. II A, namely 00 and 10. The first is found with a probability of 50,1% and represents the expected failure of Shor's algorithm, whereas the second is obtained with a 49,9% probability and leads to a successful determination of the order r. As theoretically expected [1,3], failure and success have equal probabilities. These outputs indicate an almost ideal performance of the quantum algorithm.

B. $C = 2$

The numerical investigation of the compiled version of Shor's algorithm with $C=2$ and the evaluation of the function $\log_2[2^x \bmod 15]$ in the function register required the evaluation of the time evolution of all of the qubits of the registers: x_0, x_1, y_0, and y_1. The density matrix describing the global system is displayed in Fig. 6 at three different time steps. The output quantum state describes, with a fidelity of 0.89, the

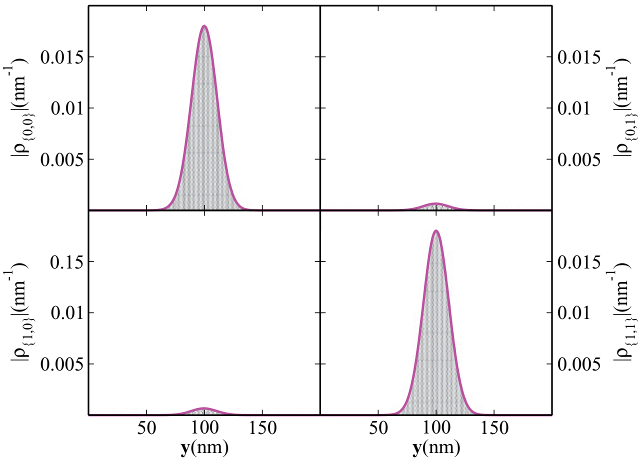

FIG. 5. (Color online) Density matrix $\rho_{\{x_0,x_0'\}}(\mathbf{y},\mathbf{y})$ of the electron of qubit x_0 after the modular exponentiation. The diagonal elements describe the density probability of finding the electron at the point $\mathbf{y}$ along wire 0 or 1. Here the moduli of $\rho_{\{x_0,x_0'\}}(\mathbf{y},\mathbf{y})$ are plotted. Note that the curves reported in the left panels refer to the left ordinate axes, while the ones reported in the right panels refer to the right ordinate axes.

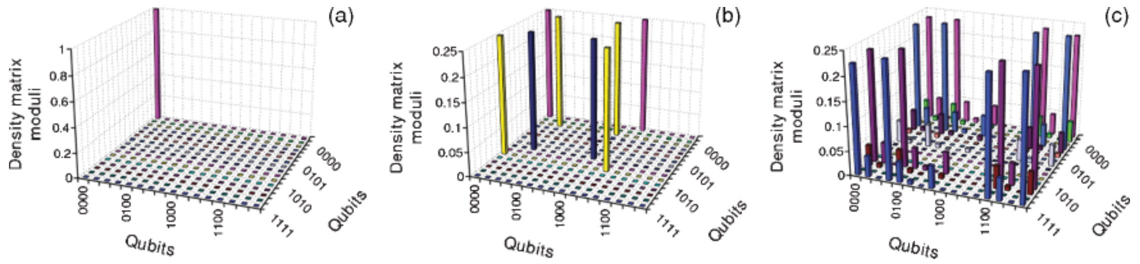

FIG. 6. (Color online) The density matrix of the qubits $\{x_0,x_1,y_0,y_1\}$ evaluated at three different time steps: (a) input, (b) initialization procedure, and (c) after the modular exponentiation. Note that these matrices have been obtained from the full density matrices of the electrons of the qubits $\{x_0,x_1,y_0,y_1\}$ by integrating over the variables defining the position of three carriers along the channels. Here the moduli of the density matrix elements are plotted.

product of two maximally entangled Bell pairs, as theoretically expected. The argument register outputs are reported in Fig. 7, where the reduced density matrix $\rho_{\{x_0,x_0',x_1,x_1'\}}(\mathbf{y},\mathbf{y},\mathbf{y}',\mathbf{y}')$ of the couple of the electrons of qubits $\{x_0,x_1\}$ is displayed. The argument register is almost maximally mixed as a consequence of the entanglement with the qubits $\{y_0,y_1\}$, as the large value of the linear entropy $\varepsilon_L = 0.976$ confirms. The binary output of the algorithm, namely one among the possible two-bit responses 00, 01, 10, and 11, is obtained by considering the probabilities of the logical state of the qubits $\{x_0,x_1\}$ and then inverting their order. The second and the fourth terms yield $r = 4$, which gives correctly the factors 3 and 5 once processed

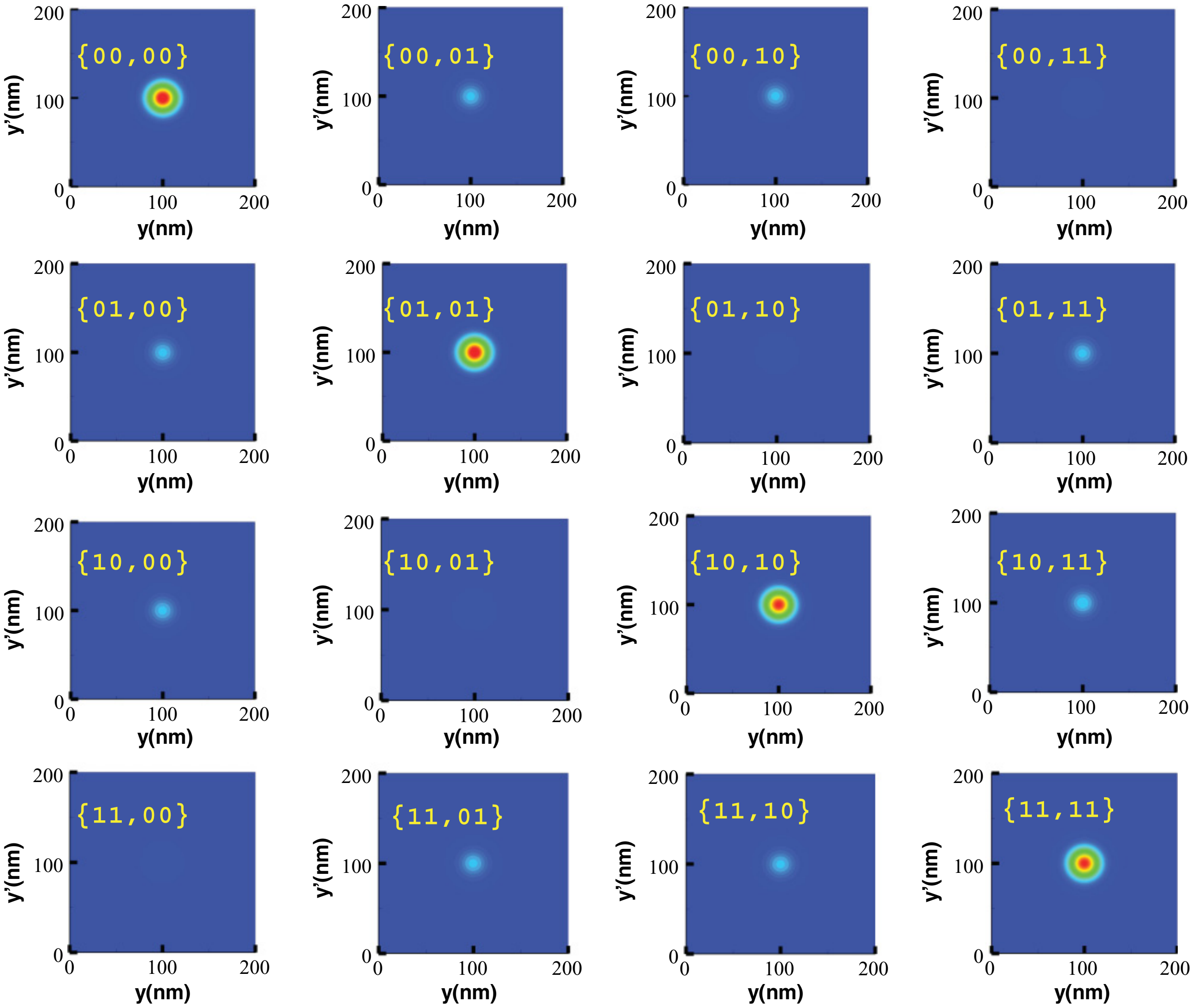

FIG. 7. (Color online) Density matrix $\rho_{\{x_0,x_0',x_1,x_1'\}}(\mathbf{y},\mathbf{y},\mathbf{y}',\mathbf{y}')$ of the couple of electrons of qubit $\{x_0,x_1\}$ after the modular exponentiation. The diagonal elements describe the density probability of finding the two electrons at the points $\mathbf{y}$ and $\mathbf{y}'$ along wire 0 or 1. Here the moduli of $\rho_{\{x_0,x_0',x_1,x_1'\}}(\mathbf{y},\mathbf{y},\mathbf{y}',\mathbf{y}')$ are plotted.

in the classical Euclid's algorithm; in contrast, the first value corresponds to a failure mode whereas the third leads to trivial factors. All of the outcomes have exactly the same probability of happening, which consequently means that the routine has a success rate of 50% like the previously discussed case of $C = 11$.

Although the binary outputs of the argument registers clearly indicate that the algorithm performance is nearly ideal both for $C = 11$ and $C = 2$, the efficiency of the quantum networks is slightly different in the two implementations investigated, as evidenced by the estimated fidelity and degree of entanglement between the registers. More specifically, the quantum circuit performance gets worse moving from $C = 11$ to $C = 2$. Such a behavior, at first sight, appears to be surprising, due to the larger number of one- and two-qubit quantum gates numerically simulated in the former implementation. A possible explanation could amazingly bring up the small errors inherent in the tuning of the quantum gates. In fact, the flaws of the one- and two-qubit logical operations could counterbalance each other, with a net effect of a higher efficiency of quantum circuits.

V. CONCLUSIONS

Shor's algorithm highlights the potential power of quantum computation and nowadays its realization in scalable structures represents one of the main challenges of quantum information science. Only in recent years have experimental demonstrations of this algorithm been given in some physical scenarios ranging from NMR to photon qubits. Nevertheless, the quantum nature of the processes and/or the scalability of the investigated systems in these approaches are questionable.

In this paper we have introduced and numerically simulated an implementation of the easiest meaningful example of Shor's algorithm, that is, the factorization of $N = 15$, through co-primes $C = 11$ and $C = 2$. The idea we have proposed exploits the coherent SAW-assisted transport of electrons in networks of coupled quantum wires and has great potential in view of its integrability with conventional microelectronics and of its scalability to more complex systems containing many qubits. Quantum information is processed by means of a sequence of one- and two-qubit gates, materialized by means of an electronic beam splitter and phase shifter and a Coulomb coupler, respectively. Their experimental realization in semiconductor quantum wires is very challenging since it requires the use of frontier semiconductor technology. Only in the past few years have prototype blocks mimicking single-qubit rotations in a couple of 1D channels been experimentally demonstrated [22,29,30]. In particular, the switching of coupled quantum-wire qubit characteristics has been explored [22]. Furthermore, Fischer *et al.* controlled the coupling between two modes of a couple of 1D channels, obtained by exploiting the two minima of the conduction-band edge in the growth direction of a GaAs 2D electron gas [30] or two vertically coupled 2D electron gases [29]. No experimental evidence of two-qubit operation in quantum-wire networks has been achieved so far. On the other hand, the coherent manipulation of charge states in two spatially separated double quantum dots integrated in a GaAs-AlGaAs heterostructure has been realized [31,32]. Specifically, two-qubit operations (swap and controlled rotation) have been successfully implemented.

We stress that the protocol here proposed for the order-finding routine at the heart of Shor's algorithm represents a "nonstandard" implementation of the quantum circuits as commonly used in the literature for quantum factorization [1,4]. Such an implementation keeps the basic features of the original algorithm (i.e., "massive parallelism" given by the entanglement between the quantum registers and binary output) and also allows for a simple network with a lower number of fundamental gates. This makes the numerical simulation of the presented protocol less demanding and could also have interesting perspectives on the full-scale realization of Shor's algorithm.

The high efficiency of the quantum processes simulated is shown by the large values obtained for fidelities. Furthermore, the success rate of the algorithm is close to its ideal value, in agreement with recent experimental investigations [7]. The algorithm performance is even more noteworthy if we consider the good but not ideal geometry of the logic gates and compare our data with those of the near-ideal case. This behavior is a clear signature of the robustness of the algorithm, which is also able to accommodate small, but nonnegligible errors coming from the fabrication and tuning of the quantum gates. The capability of taking into account small deviations from ideality is certainly a plus, which makes the algorithm compare favorably to any of its experimental implementations. In fact, it offers the opportunity to let the device work correctly even in the presence of unavoidable environmental decoherence effects, which are always present even at low temperatures.

Since the recent developments in nanostructure fabrication opened new scenarios in scalable electronic quantum computation [10,29,33], the promising results presented here indicate a fruitful guideline for research in quantum information science. Specifically, this work highlights a peculiar physical architecture which could become, in the near future, a powerful means to implement a broader variety of quantum algorithms and therefore to fully exploit the whole potential of quantum computation.

ACKNOWLEDGMENTS

The author would like to thank E. Piccinini, P. Bordone, A. Bertoni, and C. Jacoboni for stimulating discussions and valuable help.

[1] P. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Golwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.

[2] P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[3] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).

[4] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).

[5] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, Phys. Rev. Lett. **85**, 5452 (2000).

[6] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 883 (2001).

[7] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Phys. Rev. Lett. **99**, 250505 (2007).

[8] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **99**, 250504 (2007).

[9] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).

[10] M. Kataoka *et al.*, Phys. Rev. Lett. **102**, 156801 (2009).

[11] R. Rodriquez, D. K. L. Oi, M. Kataoka, C. H. W. Barnes, T. Ohshima, and A. K. Ekert, Phys. Rev. B **72**, 085329 (2005).

[12] A. Bertoni, P. Bordone, R. Brunetti, C. Jacoboni, and S. Reggiani, J. Mod. Opt. **49**, 1219 (2002).

[13] F. Buscemi, P. Bordone, and A. Bertoni, Phys. Rev. B **81**, 045312 (2010).

[14] S. Reggiani, A. Bertoni, and M. Rudan, Physica B **314**, 136 (2002).

[15] D. Deutsch, Proc. R. Soc. London Ser. A **400**, 97 (1985).

[16] J. M. Shilton, V. I. Talyanskii, M. Pepper, D. A. Ritchie, J. E. F. Frost, C. J. B. Ford, C. G. Smith, and G. A. C. Jones, J. Phys. Condens. Matter **8**, L531 (1996).

[17] C. H. W. Barnes, J. M. Shilton, and A. M. Robinson, Phys. Rev. B **62**, 8410 (2000).

[18] F. Buscemi, P. Bordone, and A. Bertoni, J. Phys. Condens. Matter **21**, 305303 (2009).

[19] R. Ionicioiu, G. Amaratunga, and F. Udrea, Int. J. Mod. Phys. B **15**, 125 (2001).

[20] A. Bertoni, P. Bordone, R. Brunetti, C. Jacoboni, and S. Reggiani, Phys. Rev. Lett. **84**, 5912 (2000).

[21] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[22] A. Ramamoorthy, J. P. Bird, and J. L. Reno, Appl. Phys. Lett. **89**, 013118 (2006).

[23] A. T. Rezakhani, Phys. Rev. A **70**, 052313 (2004).

[24] M. Blaauboer and R. L. de Visser, J. Phys. A **41**, 395307 (2008).

[25] In order to make less challenging the computational procedure, in our analysis we have not taken into account the qubits y_0 and y_2 evolving trivially.

[26] W. G. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in FORTRAN* (Cambridge University Press, Cambridge, UK, 1992).

[27] D. K. Ferry, *Semiconductors* (Macmillan, New York, 1991).

[28] F. Buscemi, P. Bordone, and A. Bertoni, Phys. Rev. A **75**, 032301 (2007).

[29] S. F. Fischer, G. Apetrii, U. Kunze, D. Schuh, and G. Abstreiter, Nature Phys. **2**, 91 (2006).

[30] S. F. Fischer, G. Apetrii, U. Kunze, D. Schuh, and G. Abstreiter, Phys. Rev. B **71**, 195330 (2005).

[31] T. Hayashi, T. Fujisawa, H. D. Cheong, Y. H. Jeong, and Y. Hirayama, Phys. Rev. Lett. **91**, 226804 (2003).

[32] G. Shinkai, T. Hayashi, T. Ota, and T. Fujisawa, Phys. Rev. Lett. **103**, 056802 (2009).

[33] C. Renner and O. Fischer, Phys. Rev. B **51**, 9208 (1995).