Factorization of large tetra and penta prime numbers on IBM quantum processor

Preprint · April 2023

CITATIONS
0

READS
88

3 authors, including:

Ritu Dhaulakhandi
Indian Institute of Science Education and Research, Pune
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Bikash K. Behera
Bikash's Quantum (OPC) Pvt. Ltd.
213 PUBLICATIONS **1,705** CITATIONS
SEE PROFILE

Factorization of large tetra and penta prime numbers on IBM quantum processor

Ritu Dhaulakhandi,[1,*] Bikash K. Behera,[2,†] and Felix J. Seo[3,‡]

[1] *Department of Physics, Indian Institute of Science Education and Research, Pune, 411008, Maharastra, India*

[2] *Bikash's Quantum (OPC) Private Limited, Balindi, Mohanpur 741246, Nadia, West Bengal, India*

[3] *Department of Physics, Hampton University, Hampton, Virginia, 23668, USA*

The factorization of a large digit integer in polynomial time is a challenging computational task to decipher. The exponential growth of computation can be alleviated if the factorization problem is changed to an optimization problem with the quantum computation process with the generalized Grover's algorithm and a suitable analytic algebra. In this article, the generalized Grover's protocol is used to amplify the amplitude of the required states and, in turn, help in the execution of the quantum factorization of tetra and penta primes as a proof of concept for distinct integers, including 875, 1269636549803, and 4375 using 3 and 4 qubits of IBMQ Perth (7-qubit processor). The fidelity of quantum factorization with the IBMQ Perth qubits was near unity.

I. INTRODUCTION

Computation problems are often classified by the difficulty of getting their solutions. The concept of difficulty is explained by the theory of computational complexity [1], which specifies the time required to perform a problem using a specific approach. It is well known that cryptography technology utilizes the difficulty of factorizing large numbers to secure data storage and information transmission [2]. If the factorization is a polynomial-time problem, the security system is not secure. In order to factorize an n-bit integer on a quantum computer, Shor presented a polynomial-time approach in 1994 [3]. Later, the procedure is put into practice by factorizing the numbers $N = 15$ and $N = 21$ [4] and $N = 15$ [5]. The only shortcoming of implementing Shor's algorithm is the need for robust error correction schemes and noise-free qubits [4–6]. More specifically, a high number of qubits are needed to factorize an integer without knowing the solution beforehand. For instance, using Shor's algorithm without knowing the solution, factorizing the number 15 would require at least 8 qubits (and more for error correction) [7].

Many alternative methods [8] have been developed to overcome the disadvantage of implementing Shor's algorithm. The adiabatic quantum computation [9] method, which transforms the factorization problem into an optimization problem [10], is one of these techniques. The factorization target number's binary system multiplication table is expressed in variable form. Using the reduction technique, the problem is reduced to a list of equations [7]. A complex Hamiltonian is expressed using those equations. The ground states of the Hamiltonian carry the solutions (zero eigenvalue states). The use of quantum annealing methods and computational algebraic geometry to factorize the bi-primes was also suggested by Dridi and Alghassi in their 2017 paper [12]. The theoretical and experimental quantum factorization have been reported utilizing Shor's algorithm [4, 5, 13], adiabatic quantum computation [7, 9, 11, 14–16], and quantum annealing principles [12]. The final number of variables in the equation, calculated using the minimization strategy for a certain integer, determines the total amount of qubits required for the experimental quantum factorization. The largest integers factorized using different algorithms are listed in Table I.

TABLE I: *Quantum Factorization Methods*

Largest number	Protocol used	No. of qubits
21 [5]	Shor's algorithm	10
21 [9]	Quantum adiabatic algorithm	3
1829 [17]	Quantum variational imaginary time evolution	9
1005973 [18]	Quantum Annealing	89
4088459 [19]	Minimization	2

This article utilizes the minimization method [14, 19] for pre-processing, like the adiabatic approach [11]. After applying the minimization method, the Hamiltonian is written down using the final equations. A unitary operator is then defined as the exponential function of the said Hamiltonian. The unitary operator marks the Hamiltonian's ground states (states with zero eigenvalues). The states obtained after the application of the Hamiltonian unitary operator will be referred to as marked states in this article. To distinguish the marked states from the unmarked states, the generalized Grover's method [20, 21] was used to amplify the marked states. The initial state (uniform superposition of qubit system) progresses to the target state (marked states) by repeated application of the oracle and diffuser operator. The multiple target states' amplitudes are increased by the generalized Grover's technique. The quantum factoriza-

* ritudhaulakhandi3626@gmail.com
† bikas.riki@gmail.com
‡ jaetae.seo@hamptonu.edu

tion protocol was utilized for the quantum computation experiment to factorize the integers, including 875 and 1269636549803 using 3-qubit systems and 4375 using 4-qubit system on IBM's quantum processor ibmq_perth (7-qubit) for the proof-of-concept. The following sections describe the quantum factorization protocol and the properties of the factors of integers used in detail.

II. BACKGROUND

A. RSA and Quantum factorization

When factoring an integer, the needed time order is $O(bk)$ with the k-th order of b-bit number, indicating that the factorization takes a polynomial amount of time. Equally challenging as the factorization problem is figuring out how many prime factors there are in an integer. There are no effective number-theoretic functions to determine the number of prime factors of an integer in number theory [22]. The sieve theory, for instance, calculates the approximate number of prime factors in an integer. The inability of sieve theory to distinguish between numbers having an odd or even number of prime elements is known as the parity problem. A lot of cryptographic protocols benefit from the factorization problem's complexity. Often employed in cryptography, the RSA [23] relies on the challenge of factoring a big bi-prime integer in polynomial time to secure data transmission. With the RSA protocol, a public key is made available based on a massive bi-prime number. The decryption key, or private key, is different from the public key [24]. The two prime elements of the employed bi-prime number are kept a secret. Huge bi-prime numbers are used to make the RSA encryption unbreakable. The steps involved in RSA encryption and decryption [25, 26] are listed below.

- Choose two unique prime numbers. Calculate their product (n).
- Carmichael's totient function ($\lambda(n)$) is evaluated using the least common multiple to fix the range of e between 1 and $\lambda(n)$.
- Using e and modular multiplicative inverse, the encryption and decryption functions are defined for the public and private keys, respectively.

Shor's approach, which is implemented on a quantum computer, can be used to find an integer's prime factors [3]. Shor demonstrates how RSA encryption may be broken using a quantum computer approach to factor huge integers in polynomial time. Based on the complexity of the factorization issue, it enables a quantum computer to decrypt the public key. This demands new cryptographies that provide security against the capability of quantum algorithms [27]. Therefore, the quantum cryptography field has been intensively studied for secure data transmission [28, 29].

B. Existing Methods

Burges introduced the quantum adiabatic theorem in 2001 [10]. In the quantum adiabatic method, a Hamiltonian is constructed from the multiplication table of the integer to be factorized. By reducing the number of variables in the problem, this strategy is effective for integers with unique features [7, 14]. Because the minimizing method makes the factorization model more complex, it cannot be used in all cases. This prompted a search for a more inclusive prime factorization procedure. On the basis of the quantum annealing principle, certain generalized models have been put out; however, they are still constrained by the hardware capabilities of quantum machines [12, 30]. A new prime factorization model that uses less quantum annealing and fewer qubits was proposed by Wang, B. *et al.* in 2020.

This article implements the quantum factorization protocol for factorizing tetra and penta prime numbers. The protocol includes a pre-processing part and a quantum computation part and overcomes the shortcoming of Shor's algorithm. The pre-processing part changes the factorization problem into an optimization problem. The prime factors of the integer are expressed in binary form. Then the binary product of the prime factors is evaluated. A set of equations are obtained from the binary product. The number of variables present in these equations is reduced using binary arithmetic rules. This simplification is called minimization [11, 14, 19]. After obtaining the final set of equations, the bit variables are mapped with the quantum operators. This mapping of variables to operators is defined so that the Hamiltonian encodes the solutions (required bit values) as its ground states (states with eigenvalue as zero). The zero eigenvalue states of the Hamiltonian are then marked by a conditional phase shift carried out by the unitary operator defined using the Hamiltonian. The marked states become more pronounced using the generalized Grover's algorithm. The factorization problem is shown schematically in Fig. 1. A few integers are factorized as a confirmation for the quantum computation experiment. The tetra prime integers 875 and 1269636549803 consist of four prime factors. The penta prime integer 4375 consists of five prime factors. The experimental results' fidelity [32] was examined with the help of quantum state tomography [34]. The following sections include the quantum computation experiment of prime factorization based on the protocol.

III. METHODOLOGY

The following general procedure is applied for the factorization problem. Let N denote an odd composite integer with α number of prime factors. Each prime factor of N is represented as n_i, where i=1, 2, . . ., α ($\alpha \in \mathbb{N}$). The prime factors are written in binary form, and the binary product is evaluated in the form of vari-

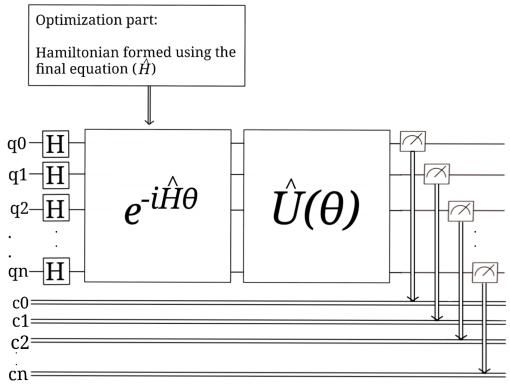

FIG. 1: **Schematic diagram of Factorization Protocol** The protocol begins with the optimization part. The integer's prime factors are expressed in binary form, and their product is evaluated to form equations. Using the minimization strategy, the equations' variable count is decreased. The final set of equations obtained is used to write down the Hamiltonian ($\hat{H}$). The operator is defined by this Hamiltonian. The superposition state is initially produced on the qubits using the Hadamard gate. Then, the operator described using the Hamiltonian marks the Hamiltonian's ground states (states with eigenvalue zero) by applying a phase shift to the states. To boost the amplitude of the marked states, the operator $\hat{U}(\theta)$ is defined using the generalized Grover's search technique. Finally, the measurements are recorded for the different computational basis to obtain the experimental density matrix.

ables. Then the set of equations are given by the binary product $(n_1)_{bin} \times (n_2)_{bin} \ldots . (n_\alpha)_{bin} = N_{bin}$ where $(n_i)_{bin}$ indicates integer n_i in binary system (or representation as a binary number) [7, 10, 11, 14, 15]. The equations are optimized by reducing the number of variables with the arithmetic of binary numbers, called the minimization method. The prime factors n_α of the N satisfy the property that all the prime factors have an equal number of digits in their binary form (number of digits in $(n_\alpha)_{bin}$ is same for all α). And

$$(n_1)_{bin} = (n_2)_{bin} = ... = (n_{\alpha-1})_{bin} \neq (n_\alpha)_{bin} \tag{1}$$

The case for $\alpha = 2$ is worked out to understand the optimization part more clearly. Let N=35 and n_1 and n_2 be the prime factors of N. The number of digits in $(n_1)_{bin}$=$(n_2)_{bin}$=3, and $(n_1)_{bin} \equiv (1b_1 1)$, $(n_2)_{bin} \equiv (1c_1 1)$.

From Fig. 2, the equations obtained after adding each column are as follows:

	2^5	2^4	2^3	2^2	2^1	2^0
$(n_1)_{bin}$				1	b_1	1
$(n_2)_{bin}$				1	c_1	1
				1	b_1	1
			c_1	b_1c_1	c_1	
		1	b_1	1		
carries	z_{14}	z_{13}	z_{12}	z_{11}		
	z_{22}	z_{21}				
$(n_1 \times n_2)_{bin}$=$(35)_{bin}$	1	0	0	0	1	1

FIG. 2: *Multiplication table for* α=2 *case,* N=35.

$$\begin{aligned} b_1 + c_1 &= 1 + 2z_{11} \\ 2 + b_1c_1 + z_{11} &= 0 + 2z_{12} + 4z_{21} \\ b_1 + c_1 + z_{12} &= 0 + 2z_{13} + 4z_{22} \\ 1 + z_{13} + z_{21} &= 0 + 2z_{14} \\ z_{14} + z_{22} &= 1 \end{aligned} \tag{2}$$

These equations are further simplified with binary number arithmetic to obtain:

$$\begin{aligned} z_{11} &= 0 \\ z_{12} &= 1 \\ z_{21} &= 0 \\ z_{13} &= 1 \\ z_{22} &= 0 \\ z_{14} &= 1 \end{aligned} \tag{3}$$

Therefore, the equation used to formalize the Hamiltonian for N=35 is an equation in one variable, q_1. The minimization method reduced the N=35 factorization problem to a single variable problem.

$$\begin{aligned} b_1 + c_1 &= 1 \\ b_1c_1 &= 0 \\ \implies c_1 - c_1^2 &= 0 \end{aligned} \tag{4}$$

The set of equations obtained after evaluating the binary product $((n_1)_{bin} \times (n_2)_{bin})$ in Eq. 2 have 8 variables. The minimization method reduces the number of variables, as seen in Eq. 4. The minimization method uses arithmetic of binary numbers (Eq. 3) where each binary digit takes the value of either 0 or 1. The final equation is used to write down the Hamiltonian. In this article, the quantum factorization procedure is carried out for the odd composite number with $\alpha = 4$, and 5 that satisfies the mentioned property (Eq. 1 and the number of digits in binary form are the same for all prime factors). The details for the quantum computation part and the results of tetra and penta prime quantum factorization are explained.

IV. RESULTS

A. Quantum factorization of tetra prime number

The binary representations of the prime factors p, q, r, and s of N=875 are $(1p_11)$, $(1q_11)$, $(1r_11)$, and $(1s_11)$, respectively.

The set of equations found from the binary product (Fig. 3) followed by minimization are:

$$\begin{aligned} &p_1+q_1+r_1+s_1=1\\ &p_1q_1+q_1r_1+p_1r_1+s_1p_1+s_1q_1+s_1r_1=0\\ &p_1q_1r_1+p_1r_1s_1+p_1q_1s_1+q_1r_1s_1=0 \end{aligned} \tag{5}$$

which are reduced to a single equation with three variables:

$$\begin{aligned} &-p_1-q_1-r_1+2p_1^2+2q_1^2+2r_1^2-p_1^3-q_1^3-r_1^3\\ &+4p_1r_1+4p_1q_1+4q_1r_1-3p_1^2q_1-3p_1^2r_1-3q_1^2p_1\\ &-3q_1^2r_1-3r_1^2p_1-3r_1^2q_1-5p_1q_1r_1=0 \end{aligned} \tag{6}$$

After multiplying Eq. 6 with -1 on both sides, the variables (p_1, q_1, r_1) are mapped with the operators $(\hat{a_1}, \hat{a_2}, \hat{a_3})$ where $\hat{a_i}=\frac{I-\sigma_z^i}{2}$, I is the 1-qubit identity operator, and the σ_z^i operator in the quantum circuit acting on the ith qubit is the Pauli Z operator. This mapping transforms the Hamiltonian from a variable equation to a diagonal matrix form with non-negative number entries. The ground states of Hamiltonian encode the solutions. For example, if $H\left|qu_1\right\rangle\left|qu_2\right\rangle\left|qu_3\right\rangle=0\left|qu_1\right\rangle\left|qu_2\right\rangle\left|qu_3\right\rangle$ then b_1=p_1, b_2=q_1, and b_3=r_1 are the required bit values. For example, from Eq. 9 it is observed that the Hamiltonian for N=875 has ground states (states with zero eigenvalue) $|000\rangle$, $|001\rangle$, $|010\rangle$, and $|100\rangle$. Operator $\hat{a_i}$ also satisfies the property $\hat{a_i}^2$=$\hat{a_i}$. As a result, the following is the Hamiltonian for the factorization problem:

$$\hat{H}=5\hat{a_1}\hat{a_2}\hat{a_3}+2\hat{a_1}\hat{a_2}+2\hat{a_1}\hat{a_3}+2\hat{a_2}\hat{a_3} \tag{7}$$

The $\hat{a_i}$ operators are substituted in the above Hamiltonian to obtain:

$$\begin{aligned} \hat{H}=&\frac{17}{8}(I_3)-\frac{13}{8}(\sigma_z^1\otimes I\otimes I+I\otimes\sigma_z^2\otimes I+I\otimes I\otimes\sigma_z^3)\\ &+\frac{9}{8}(\sigma_z^1\otimes\sigma_z^2\otimes I+\sigma_z^1\otimes I\otimes\sigma_z^3+I\otimes\sigma_z^2\otimes\sigma_z^3)\\ &-\frac{5}{8}(\sigma_z^1\otimes\sigma_z^2\otimes\sigma_z^3) \end{aligned} \tag{8}$$

TABLE II: *For N=875. The phase shift relative to the state $|000\rangle$ when the operator $e^{-i\hat{H}\theta}$ is applied to the z-basis states.*

Quantum State	Relative Phase shift	Quantum State	Relative Phase shift
$\|000\rangle$	0	$\|100\rangle$	0
$\|001\rangle$	0	$\|101\rangle$	-2θ
$\|010\rangle$	0	$\|110\rangle$	-2θ
$\|011\rangle$	-2θ	$\|111\rangle$	-11θ

$$\hat{H}=\begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&2&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&2&0&0\\ 0&0&0&0&0&0&2&0\\ 0&0&0&0&0&0&0&11 \end{bmatrix} \tag{9}$$

where I_3 is the 3-qubit identity operator. The Hamiltonian's ground state ($|qu_1qu_2qu_3\rangle$) are the solutions for the binary digits (p_1=qu_1, q_1=qu_2, and r_1=qu_3). Since $\hat{H}$ is a diagonal matrix, the operator $e^{-i\hat{H}\theta}$ can be expressed as a diagonal matrix too. The $e^{-i\hat{H}\theta}$ operator applies a conditional phase shift (relative to $|000\rangle$ state) to the initial superposition state as shown in Table II. The initial uniform superposition state $|\psi_0\rangle$=$\frac{1}{2\sqrt{2}}\Sigma_{i=0}^{i=7}|i\rangle$ is obtained by applying Hadamard gate $H^{\otimes 3}$ to the $|000\rangle$ state. The ground states of Hamiltonian are called marked states after applying the $e^{-i\hat{H}\theta}$ operator. For the purpose of differentiating the marked states from the unmarked ones, the amplitudes of the marked states are enhanced. The amplification procedure is carried out by an exact search method. This is accomplished by using an oracle $\hat{U}(\theta)$ that was obtained using the generalized Grover's search technique [20]. The way the search algorithm operates is similar to how resonance works. By re-expressing the state $|\psi_0\rangle$, one may determine the phase shift angle (θ). $|\psi_0\rangle$ can be written in terms of the normalized sum of marked states $|x_0\rangle$ ($|x_0\rangle$=$\frac{1}{\sqrt{M}}\sum_{t=0}^{M-1}|MS_t\rangle$, where $|MS_t\rangle$ are the marked states) and the normalized sum of remaining states $|x_0^\perp\rangle$ ($|x_0^\perp\rangle$=$\frac{1}{\sqrt{N-M}}\sum_{f=0}^{N-M-1}|S_f\rangle$, where $|S_f\rangle$ are the remaining states). The expression of $|\psi_0\rangle$ in terms of $|x_0\rangle$ and $|x_0^\perp\rangle$ is:

$$|\psi_0\rangle=\sin\phi\,|x_0\rangle+\cos\phi\,|x_0^\perp\rangle \tag{10}$$

where the angle ϕ is the reflection angle of the uniform superposition state w.r.t. the unmarked states. The phase shift angle θ and ϕ are related by the following equation: θ=$2\sin^{-1}(\frac{\sin\frac{\pi}{4j+2}}{\sin\phi})$, where j is the smallest number of iterations of Grover's protocol necessary to

	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
$(p)_{bin}$										1	p_1	1
$(q)_{bin}$										1	q_1	1
										1	p_1	1
									q_1	p_1q_1	q_1	
								1	p_1	1		
carries							z_{14}	z_{13}	z_{12}	z_{11}		
							z_{22}	z_{21}				
							$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1
$(r)_{bin}$										1	r_1	1
							$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1
						$r_1(z_{14}+z_{22})$	$r_1(1+z_{13}+z_{21})$	$r_1(p_1+q_1+z_{12})$	$r_1(2+p_1q_1+z_{11})$	$r_1(p_1+q_1)$	r_1	
					$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1		
carries				z'_{15}	z'_{14}	z'_{13}	z'_{12}	z'_{11}	z'_{10}	z''_{00}		
				z'_{25}	z'_{24}	z'_{23}	z'_{22}	z'_{21}				
				T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1
$(s)_{bin}$										1	s_1	1
				T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1
			s_1T_1	s_1T_2	s_1T_3	s_1T_4	s_1T_5	s_1T_6	s_1T_7	s_1T_8	s_1	
		T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1		
carries	z''_{18}	z''_{17}	z''_{16}	z''_{15}	z''_{14}	z''_{13}	z''_{12}	z''_{11}	z''_{10}	z''_{00}		
	z''_{28}	z''_{27}	z''_{26}	z''_{25}	z''_{24}	z''_{23}	z''_{22}	z''_{21}				
N_{bin}=$(875)_{bin}$	0	0	1	1	0	1	1	0	1	0	1	1

FIG. 3: *Multiplication table for* α=4 *case,* N=875.
T_1=$z'_{15}+z'_{25}$, T_2=$z_{14}+z_{22}+z'_{14}+z'_{24}$, T_3=$r_1(z_{14}+z_{22})+1+z_{13}+z_{21}+z'_{13}+z'_{23}$,
T_4=$z_{14}+z_{22}+r_1(1+z_{13}+z_{21})+p_1+q_1+z_{12}+z'_{12}+z'_{22}$, T_5=$1+z_{13}+z_{21}+r_1(p_1+q_1+z_{12})+2+p_1q_1+z_{11}$,
T_6=$p_1+q_1+z_{12}+r_1(2+p_1q_1+z_{11})+p_1+q_1$, T_7=$3+p_1q_1+z_{11}+r_1(p_1+q_1)$, T_8=$p_1+q_1+r_1$

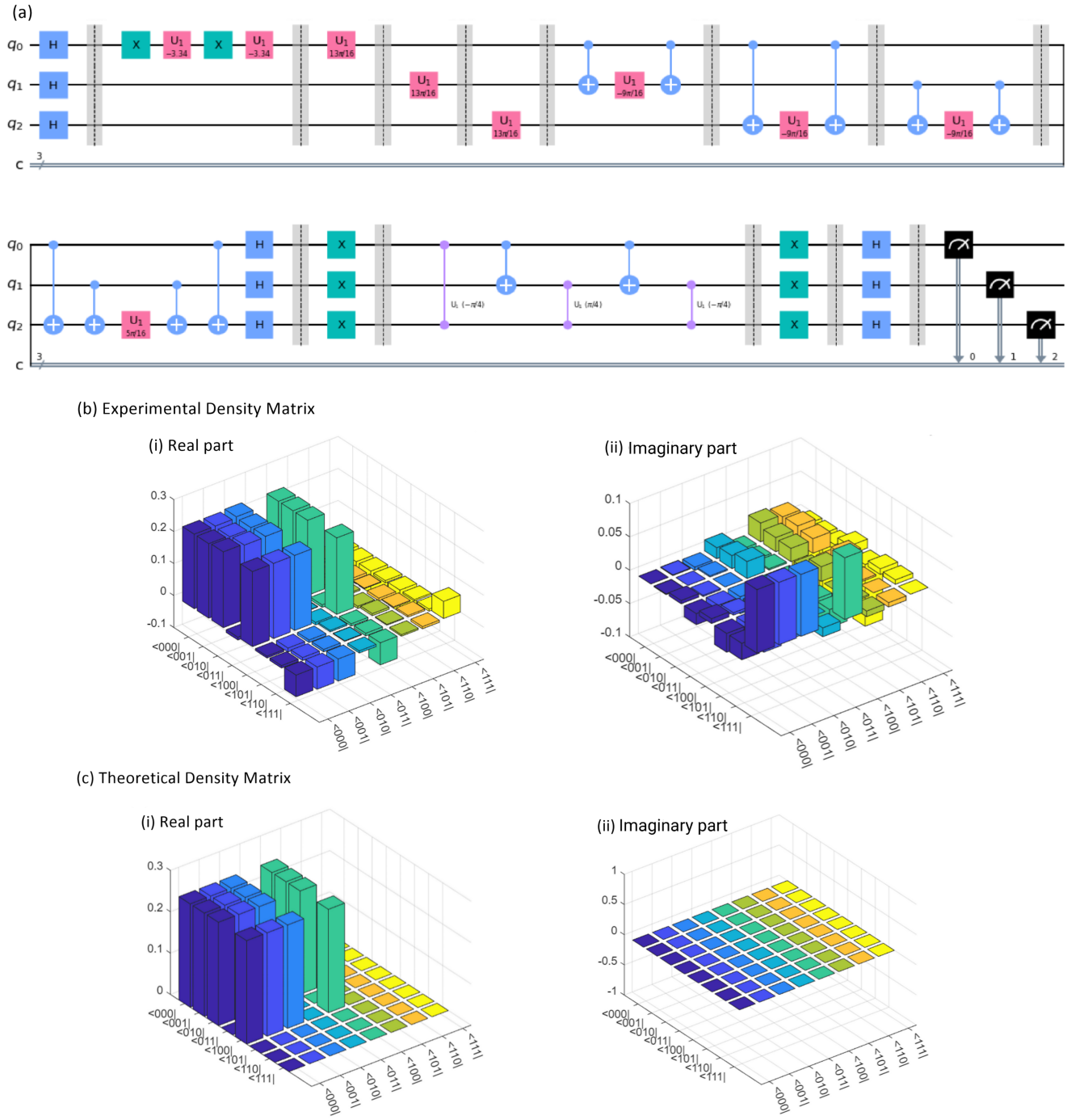

FIG. 4: **(a)Quantum factorization circuit, (b) Experimental density matrix (EDM), and (c) Theoretical density matrix (TDM)** The circuit, which uses 3 qubits to factorize N=875, is implemented on IBM's quantum processor. The experiment and simulation are performed on the ibmq_perth system, a 7-qubit processor. The final measurements are obtained in the Z-basis, forming the EDM. The EDM has a non-zero complex part, as shown in (b)(ii). As indicated in (b) and (c), the numerical values of the real component and imaginary component of the density matrix elements are shown separately. The fidelity of the result was found to be 0.9683 (The EDM and fidelity calculation are provided in the link [33]). The U_1 gate is a 2×2 diagonal matrix with diagonal entries $\left(1, e^{i\phi}\right)$ which is equivalent to the operation of $e^{\frac{i\phi}{2}} R_z(\phi)$ where R_z performs a rotation around z-axis by an amount ϕ.

maximize the amplitude of the solution states while minimizing the amplitude of the remaining states [20, 21]. Quantum tomography is used to examine the accuracy of the experimental result after the quantum circuit results have been obtained. Quantum tomography uses a sequence of measurements on several bases to capture the complete quantum state. It provides fidelity between the density matrices of experimental data and theoretical values for the factorization problem. The TDM is given as ρ^T=$|\Psi\rangle\langle\Psi|$, where $|\Psi\rangle$=$\hat{U}(\theta)e^{-i\hat{H}\theta}|\psi_0\rangle$ is the final state obtained after implementing the quantum circuit for a given factorization problem. The EDM is given by the Stokes parameters S_a [34, 35] and Pauli matrices σ_a. The EDM is given as ρ_3^E=$\frac{1}{N}\Sigma_{i,j,k}(S_i\otimes S_j\otimes S_k)(\sigma_i\otimes\sigma_j\otimes\sigma_k)$ for the 3 qubit system, and ρ_4^E=$\frac{1}{N}\Sigma_{i,j,k,l}(S_i\otimes S_j\otimes S_k\otimes S_l)(\sigma_i\otimes\sigma_j\otimes\sigma_k\otimes\sigma_l)$ for the 4 qubit system, where i, j, k, l go from zero to three, and σ_a belongs to the set of $\{I,\sigma_X,\sigma_Y,\sigma_Z\}$. The following are the Stokes parameters:

$$\begin{aligned} S_3 &= P_{|0_z\rangle} - P_{|1_z\rangle} \\ S_2 &= P_{|0_y\rangle} - P_{|1_y\rangle} \\ S_1 &= P_{|0_x\rangle} - P_{|1_x\rangle} \\ S_0 &= 1 \end{aligned} \tag{11}$$

where the probability of discovering state $|i\rangle$ in basis j is $P_{|i_j\rangle}$. For Pauli-Z matrix (σ_z), the eigenvectors are $|0\rangle$ and $|1\rangle$. In the Bloch sphere, Z basis measurement gives the probability of states $|0\rangle$ and $|1\rangle$, X basis measurement gives the probability of finding states $|+\rangle$=$H|0\rangle$ and $|-\rangle$=$H|1\rangle$, where H is the Hadamard matrix, and Y basis measurement gives the probability of finding states $|+i\rangle$=$SH|0\rangle$ and $|-i\rangle$=$SH|1\rangle$, where $SS^\dagger$=$\mathbb{I}$ [36].

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\ X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{12}$$

The fidelity value is calculated using the ρ^T and ρ^E matrices which tells the extent of overlap between EDM and TDM, $F(\rho^T,\rho^E)$=$Tr(\sqrt{\sqrt{\rho^T}\rho^E\sqrt{\rho^T}})$.

For N=875, the four solutions obtained ($|p_1q_1r_1\rangle$) are as expected. Four marked states are obtained from the Hamiltonian's ground states by applying $e^{-i\hat{H}\theta}$. The exact search algorithm searches for the four marked solution states and amplifies their amplitude. The phase shift angle to achieve maximum amplification is given as $\theta = 2sin^{-1}\left(\frac{\sin\frac{\pi}{4j+2}}{\sin\phi}\right)$ where ϕ=$\frac{\pi}{4}$ and j=1 iteration [20, 21]. The EDM is given in Fig. 4 (b). The TDM for N=875 is given as ρ^T=$|\Psi\rangle\langle\Psi|$ where $|\Psi\rangle = \frac{1}{2}[|000\rangle+|001\rangle+|010\rangle+|100\rangle]$.

$$\rho^T = \frac{1}{4}\begin{bmatrix} 1&1&1&0&1&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix} \tag{13}$$

The aforementioned conclusion is further generalized for tetra prime numbers of the type $N = p^3q$, where the other prime numbers p and q differ by one binary digit. The simplification for N=1269636549803 is provided. For N=1269636549803, there are four prime factors are denoted as $\{1p_9p_8...p_11\}_{bin}$, $\{1q_9q_8...q_11\}_{bin}$, $\{1r_9r_8...r_11\}_{bin}$, and $\{1s_9s_8...s_11\}_{bin}$ in binary system. From minimization, it is obtained that p_i=q_i=r_i=s_i=0 for $i = 3,4,6,7,8,9$, and $p_i = q_i = r_i = s_i = 1$ for $i = 2,5$. The final set of equation for N=1269636549803 is same as Eq. (5) for p_1, q_1, r_1, and s_1. Further implementation is the same as the tetra prime quantum factorization protocol. The solutions obtained from the ground states of the Hamiltonian result in the values of prime numbers to be p=1061, q=1061, r=1061, and s=1063, which are the required prime factors.

B. Quantum factorization of penta prime number

Applying the quantum factorization protocol to a number with five prime factors, N=4375. The binary form of the prime factors are expressed as $\{1p_11\}_{bin}$, $\{1q_11\}_{bin}$, $\{1r_11\}_{bin}$, $\{1s_11\}_{bin}$, and $\{1t_11\}_{bin}$ respectively. The binary multiplication table for N=4375 is provided in Fig. 5. The value of T_i (i goes from 1 to 8) variables are the same as the ones given in Fig. 3. The remaining expressions are given as:

$$\begin{aligned} T_1' &= z_{18}'' + z_{28}'' \\ T_2' &= T_1 + z_{17}'' + z_{27}'' \\ T_3' &= s_1T_1 + T_2 + z_{16}'' + z_{26}'' \\ T_4' &= T_1 + s_1T_2 + Tr_3 + z_{15}'' + z_{25}'' \\ T_5' &= T_2 + s_1T_3 + Tr_4 + z_{14}'' + z_{24}'' \\ T_6' &= T_3 + s_1T_4 + Tr_5 + z_{13}'' + z_{23}'' \\ T_7' &= T_4 + s_1T_5 + Tr_6 + z_{12}'' + z_{22}'' \\ T_8' &= T_5 + sr_1T_6 + T_7 + z_{11}'' + z_{21}'' \\ T_9' &= T_6 + s_1Tr_7 + T_8 + z_{10}'' \\ T_{10}' &= T_7 + s_1T_8 + 1 + z_{00}'' \\ T_{11}' &= T_8 + s_1 \end{aligned} \tag{14}$$

The set of equations found after applying the minimization procedure to the equations obtained from binary multiplication is given by:

	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
$(p)_{bin}$													1	p_1	1
$(q)_{bin}$													1	q_1	1
													1	p_1	1
												q_1	p_1q_1	q_1	
											1	p_1	1		
carries										z_{14}	z_{13}	z_{12}	z_{11}		
										z_{22}	z_{21}				
										$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1
$(r)_{bin}$													1	r_1	1
										$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1
									$r_1(z_{14}+z_{22})$	$r_1(1+z_{13}+z_{21})$	$r_1(p_1+q_1+z_{12})$	$r_1(2+p_1q_1+z_{11})$	$r_1(p_1+q_1)$	r_1	
								$z_{14}+z_{22}$	$1+z_{13}+z_{21}$	$p_1+q_1+z_{12}$	$2+p_1q_1+z_{11}$	p_1+q_1	1		
carries							z'_{15}	z'_{14}	z'_{13}	z'_{12}	z'_{11}	z'_{10}	z'_{00}		
							z'_{25}	z'_{24}	z'_{23}	z'_{22}	z'_{21}				
							T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1
$(s)_{bin}$													1	s_1	1
							T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1
						s_1T_1	s_1T_2	s_1T_3	s_1T_4	s_1T_5	s_1T_6	s_1T_7	s_1T_8	s_1	
					T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	1		
carries				z''_{18}	z''_{17}	z''_{16}	z''_{15}	z''_{14}	z''_{13}	z''_{12}	z''_{11}	z''_{10}	z''_{00}		
				z''_{28}	z''_{27}	z''_{26}	z''_{25}	z''_{24}	z''_{23}	z''_{22}	z''_{21}				
				T'_1	T'_2	T'_3	T'_4	T'_5	T'_6	T'_7	T'_8	T'_9	T'_{10}	T'_{11}	1
$(t)_{bin}$													1	t_1	1
				T'_1	T'_2	T'_3	T'_4	T'_5	T'_6	T'_7	T'_8	T'_9	T'_{10}	T'_{11}	1
			$t_1T'_1$	$t_1T'_2$	$t_1T'_3$	$t_1T'_4$	$t_1T'_5$	$t_1T'_6$	$t_1T'_7$	$t_1T'_8$	$t_1T'_9$	$t_1T'_{10}$	$t_1T'_{11}$	t_1	
		T'_1	T'_2	T'_3	T'_4	T'_5	T'_6	T'_7	T'_8	T'_9	T'_{10}	T'_{11}	1		
carries	z'''_{111}	z'''_{110}	z'''_{19}	z'''_{18}	z'''_{17}	z'''_{16}	z'''_{15}	z'''_{14}	z'''_{13}	z'''_{12}	z'''_{11}	z'''_{10}	z'''_{00}		
	z'''_{31}	z'''_{30}	z'''_{29}	z'''_{28}	z'''_{27}	z'''_{26}	z'''_{25}	z'''_{24}	z'''_{23}	z'''_{22}	z'''_{21}				
$(4375)_{bin}$	0	0	1	0	0	0	1	0	0	0	1	0	1	1	1

FIG. 5: *Multiplication table for α=5 case, N=4375. The expressions for the variables are given in Eq. 14.*

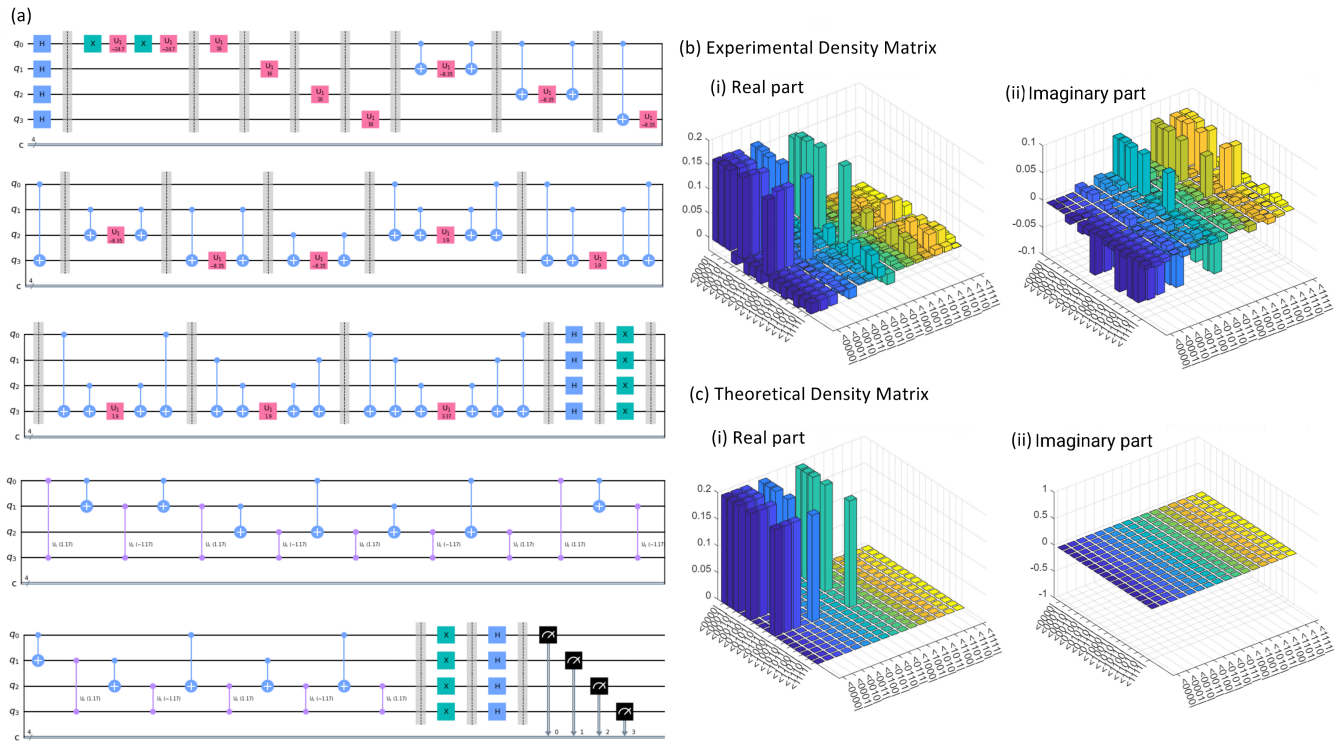

FIG. 6: **(a)Quantum factorization circuit, (b) Experimental density matrix (EDM), and (c) Theoretical density matrix (TDM)** The circuit, which uses 4 qubits to factorize N=4375, is implemented on IBM's quantum processor. The experiment and simulation are performed on the ibmq_perth system, a 7-qubit processor. The final measurements are obtained in the Z-basis, which gives the EDM. The EDM has a non-zero complex part, as shown in (b)(ii). As indicated in (b) and (c), the numerical values of the real component and imaginary component of the density matrix elements are shown separately. The fidelity of the result was found to be 0.9081. The expansion of $\hat{H}$ in Pauli basis only involves I and Z Pauli matrices. They all commute with one another since they are diagonal matrices. Therefore, the product of particular unitary gates can be used to express the exponential Hamiltonian function [37]. In order to get an equal superposition of states, $H^{\otimes n}$ is applied at the beginning. The first part of the circuit between U=$H^{\otimes n}$ applies the exponential operator $e^{-i\hat{H}\theta}$. The remaining portion of the circuit offers the $|0^{\otimes n}\rangle$ state an $e^{-i\theta}$ phase shift before delivering the final solution state.

$$
\begin{aligned}
&p_1+q_1+r_1+s_1+t_1=1\\
&p_1q_1+q_1r_1+p_1r_1+s_1p_1+s_1q_1+s_1r_1+p_1t_1+q_1t_1\\
&+s_1t_1+r_1t_1=0\\
&p_1q_1r_1+p_1r_1s_1+p_1q_1s_1+q_1r_1s_1+p_1q_1t_1+p_1r_1t_1\\
&+q_1r_1t_1+p_1s_1t_1+q_1s_1t_1+r_1s_1t_1=0\\
&p_1q_1r_1s_1+q_1r_1s_1t_1+p_1r_1s_1t_1+p_1q_1s_1t_1+p_1q_1r_1t_1=0
\end{aligned}
\tag{15}
$$

The set of equations is further simplified to a single equation in four variables:

$$
\begin{aligned}
&p_1+q_1+r_1+s_1-3p_1^2-3q_1^2-3r_1^2-3s_1^2+3p_1^3+3q_1^3\\
&+3r_1^3+3s_1^3-p_1^4-q_1^4-r_1^4-s_1^4-6p_1q_1-6r_1s_1-6p_1r_1\\
&-6p_1s_1-6q_1r_1-6q_1s_1+9p_1^2q_1+9p_1^2r_1+9p_1^2s_1+9q_1^2p_1\\
&+9q_1^2r_1+9q_1^2s_1+9r_1^2p_1+9r_1^2q_1+9r_1^2s_1+9s_1^2p_1+9s_1^2q_1\\
&+9s_1^2r_1+18p_1q_1r_1+18p_1r_1s_1+18p_1q_1s_1+18q_1r_1s_1\\
&-4p_1^3q_1-4p_1^3r_1-4p_1^3s_1-4q_1^3p_1-4q_1^3r_1-4q_1^3s_1\\
&-4r_1^3p_1-4r_1^3q_1-4r_1^3s_1-4s_1^3p_1-4s_1^3q_1-4s_1^3r_1\\
&-6p_1^2q_1^2-6p_1^2r_1^2-6p_1^2s_1^2-6q_1^2r_1^2-6q_1^2s_1^2\\
&-6r_1^2s_1^2-12p_1q_1^2r_1-12p_1q_1^2s_1-12p_1r_1^2q_1-12p_1r_1^2s_1\\
&-12p_1s_1^2q_1-12p_1s_1^2r_1-12q_1p_1^2r_1-12s_1p_1^2r_1\\
&-12q_1p_1^2s_1-12q_1r_1^2s_1-12q_1s_1^2r_1-12s_1q_1^2r_1\\
&-23p_1q_1r_1s_1=0
\end{aligned}
\tag{16}
$$

To form the Hamiltonian, $46p_1q_1r_1s_1$ is added to the left side of Eq. 16 and then the equation expression

TABLE III: *For N=4375. The phase shift relative to the state $|0000\rangle$ when the operator $e^{-i\hat{H}\theta}$ is applied to the z-basis states.*

Quantum State	Relative Phase shift	Quantum State	Relative Phase shift
$\|0000\rangle$	0	$\|1000\rangle$	0
$\|0001\rangle$	0	$\|1001\rangle$	-2θ
$\|0010\rangle$	0	$\|1010\rangle$	-2θ
$\|0011\rangle$	-2θ	$\|1011\rangle$	-24θ
$\|0100\rangle$	0	$\|1100\rangle$	-2θ
$\|0101\rangle$	-2θ	$\|1101\rangle$	-24θ
$\|0110\rangle$	-2θ	$\|1110\rangle$	-24θ
$\|0111\rangle$	-24θ	$\|1111\rangle$	-61θ

TABLE IV: *The equations' values for the two scenarios are given. In instances 1 and 2, n_1=1, n_2=n_3=...=n_α=0 and n_1=0, n_2=n_3=...=n_α=1 respectively.*

Equations	Case 1	Case 2
$n_1+n_2+...+n_\alpha$	1	$\alpha-1$
$\Sigma_{i_1<i_2} n_{i_1} n_{i_2}$	0	$\binom{\alpha}{2}-\binom{\alpha-1}{1}$
$\Sigma_{i_1<i_2<i_3} n_{i_1} n_{i_2} n_{i_3}$	0	$\binom{\alpha}{3}-\binom{\alpha-1}{2}$
.	.	.
.	.	.
.	.	.
$\Sigma_{i_1<i_2<...<i_{\alpha-1}} n_{i_1} n_{i_2} .... n_{i_{\alpha-1}}$	0	$\binom{\alpha}{\alpha-1}-\binom{\alpha-1}{\alpha-2}$

is multiplied by -1. The variables (p_1, q_1, r_1, s_1) are mapped with the operators $(\hat{a_1}, \hat{a_2}, \hat{a_3}, \hat{a_4})$ to encode the required states in the Hamiltonian:

$$\begin{aligned}\hat{H} =& -23(\hat{a_1}\hat{a_2}\hat{a_3}\hat{a_4}) + 18(\hat{a_1}\hat{a_2}\hat{a_3} + \hat{a_1}\hat{a_2}\hat{a_4} \\ &+\hat{a_2}\hat{a_3}\hat{a_4} + \hat{a_1}\hat{a_3}\hat{a_4}) + 2(\hat{a_1}\hat{a_2} + \hat{a_1}\hat{a_3} + \hat{a_2}\hat{a_3} \\ &+\hat{a_3}\hat{a_4} + \hat{a_1}\hat{a_4} + \hat{a_2}\hat{a_4}) \end{aligned} \tag{17}$$

The mapping encodes the solution in the ground states (states with zero eigenvalues) of the Hamiltonian of the factorization problem. Applying the definition of $\hat{a_i}$ operators, the Hamiltonian in Eq. 17 is given by:

$$\begin{aligned}\hat{H} =& \frac{169}{16}(I_4) - \frac{109}{16}(\sigma_z^1 \otimes I \otimes I \otimes I + I \otimes \sigma_z^2 \otimes I \otimes I \\ &+I \otimes I \otimes \sigma_z^3 \otimes I + I \otimes I \otimes I \otimes \sigma_z^4) \\ &+\frac{57}{16}(\sigma_z^1 \otimes \sigma_z^2 \otimes I \otimes I + \sigma_z^1 \otimes I \otimes \sigma_z^3 \otimes I \\ &+I \otimes \sigma_z^2 \otimes \sigma_z^3 \otimes I + \sigma_z^1 \otimes I \otimes I \otimes \sigma_z^4 \\ &+I \otimes \sigma_z^2 \otimes I \otimes \sigma_z^4 + I \otimes I \otimes \sigma_z^3 \otimes \sigma_z^4) \\ &-\frac{13}{16}(\sigma_z^1 \otimes \sigma_z^2 \otimes \sigma_z^3 \otimes I + \sigma_z^1 \otimes \sigma_z^2 \otimes I \otimes \sigma_z^4 \\ &+\sigma_z^1 \otimes I \otimes \sigma_z^3 \otimes \sigma_z^4 + I \otimes \sigma_z^2 \otimes \sigma_z^3 \otimes \sigma_z^4) \\ &-\frac{23}{16}(\sigma_z^1 \otimes \sigma_z^2 \otimes \sigma_z^3 \otimes \sigma_z^4) \end{aligned} \tag{18}$$

where I_4 is the 4-qubit identity operator.

$$\hat{H} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&24&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&24&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&24&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&24&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&61
\end{bmatrix} \tag{19}$$

The ground states of the above Hamiltonian (Eq. 19) give the required bit solutions. The ground states ($|p_1q_1r_1s_1\rangle$) are $|0000\rangle$, $|0001\rangle$, $|0010\rangle$, $|0100\rangle$, and $|1000\rangle$, which gives factors 5, 5, 5, 5, and 7 after inputting the values of p_1, q_1, r_1, and s_1 in Eq. 15. The phase shift angle is specified as $\theta = 2\sin^{-1}\left(\frac{\sin\frac{\pi}{4j+2}}{\sin\phi}\right)$ where ϕ=$\sin^{-1}\left(\frac{\sqrt{5}}{4}\right)$ and j=2 iterations for the search algorithm to function and amplify the desired results [20, 21]. The EDM is given in Fig. 6 (b). The TDM is given by ρ^T=$|\Psi\rangle\langle\Psi|$, where $|\Psi\rangle$=$\frac{1}{\sqrt{5}}[|0000\rangle + |0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle]$.

$$\rho^T = \frac{1}{5}\begin{bmatrix}
1&1&1&0&1&0&0&0&1&0&.&.&0\\
1&1&1&0&1&0&0&0&1&0&.&.&0\\
1&1&1&0&1&0&0&0&1&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
1&1&1&0&1&0&0&0&1&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
1&1&1&0&1&0&0&0&1&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0\\
0&0&0&0&0&0&0&0&0&0&.&.&0
\end{bmatrix} \tag{20}$$

The quantum factorization of tetra and penta prime numbers provides results with high fidelity and can therefore be extended to larger integers. A general set of equations for the minimization part is provided for larger numbers that share similar properties in their prime factors. For N=$(n_1)_{bin} \times (n_2)_{bin} \ldots (n_\alpha)_{bin}$. Let $(n_j)_1$, where j going from 1 to α, and 1 denote the binary digit position. The binary position subscript (1) is dropped to avoid confusion. The form of the set of equations is shown in Table IV using the property mentioned regarding the number of digits in the binary number and Eq. 1. The final expression obtained for each case might need some modification to achieve the proper expression for the Hamiltonian of the factorization problem.

V. DISCUSSION AND CONCLUSION

Many factorization problems were solved using different methods, including quantum annealing properties and the adiabatic principles [7, 11, 12, 14, 15, 19]. The exponential function of the Hamiltonian operator was used in this article to mark the Hamiltonian's ground states as opposed to the quantum annealing technique for the factorization problem. Following minimization, the final equation is used to create the Hamiltonian operator. To amplify the marked states, the generalized Grover's algorithm was implemented [20]. For the proof-of-concept, these numbers 875, 1269636549803, and 4375 were factorized where the first two numbers have four prime numbers, and the last number has five prime numbers that were factorized using the 7-qubit IBM quantum processor (Perth). The processor type of Perth is Falcon r5.11H. The Falcon family of devices is proven to be advantageous for medium-scale circuits. H represents the segment consisting of the chip-sub sections and is defined differently for each processor family. The r5.11 is the most updated version of the processor in the Falcon family. For N=875, the ground states of the Hamiltonian were found to be $|000\rangle$, $|001\rangle$, $|010\rangle$, and $|100\rangle$ that corresponded to the prime numbers 5, 5, 5, and 7. The fidelity of the quantum circuit for N=875 was estimated to be 0.9683. For N=1269636549803, the set of equations from the binary product has more variables, but the final equation obtained after minimization is the same. Hence, the quantum circuit for N=1269636549803 is the same as that used for N=875. For N=4375, the ground states of the Hamiltonian were found to be $|0000\rangle$, $|0001\rangle$, $|0010\rangle$, $|0100\rangle$, and $|1000\rangle$ that corresponded to the prime numbers 5, 5, 5, 5, and 7. The fidelity of the quantum circuit for N=4375 was calculated to be 0.9081. The two quantum circuits' high fidelity assures the factorization protocol's feasibility with large prime factors and more prime factors. These findings are particularly significant because the online security system is predicated on the hypothesis that factoring big numbers is an NP-hard task. Adding further to the interest in studying and implementing quantum computation techniques to build more secure systems. The optimized set of equations for larger numbers is provided at the end, bearing the same property of prime factors as the number factorized in this article. The number of qubits to solve a factorization problem depends on the simplification. The preprocessing part of the factorization problem (performing the binary product of binary numbers) is done with the help of a computer program. The other quantum factorization methods require either a large number of qubits or many iterations for evolution for implementation, but that isn't the case for the protocol used in this article. This is the first experimental realization of quantum algorithms to factor a number with four and five prime factors.

[1] Ding-Zhu Du & Ker-I Ko Theory of Computational Complexity. *John Wiley & Sons* (2011).

[2] Traversa, F. L. & Ventra, M. D. Polynomial-time solution of prime factorization and NP-complete problems with digital memcomputing machines. *Chaos* **27**, 023107 (2017).

[3] Shor, Peter W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).

[4] Vandersypen, L. M. K. *et al.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–887 (2001).

[5] Martín-López, E. *et al.* Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photon.* **6**, 773–776 (2012).

[6] Smolin, J. A., Smith, G. & Vargo, A. Oversimplifying quantum factoring. *Nature* **499**, 163–165 (2013).

[7] Dattani, Nikesh S., & Bryans, Nathaniel. Quantum factorization of 56153 with only 4 qubits. *arXiv preprint arXiv:1411.6758v3* (2014).

[8] Yan, S. Y. Quantum Algorithms for Integer Factorization. In: Quantum Computational Number Theory. *Springer, Cham* 59–119 (2015).

[9] Peng, X. *et al.* Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation. *Phys. Rev. Lett.* **101**, 220405 (2008).

[10] Burges, C. J. C. Factoring as Optimization. *Microsoft Research* **MSR-TR-200** (2002).

[11] Wang, B., Yang, X. & Zhang, D. Research on Quantum Annealing Integer Factorization Based on Different Columns. *Front. Phys.* **10:914578** (2022).

[12] Dridi, R. & Alghassi, H. Prime Factorization using Quantum Annealing and Computational Algebraic Geometry. *Sci. Rep.* **7**, 43048 (2017).

[13] Bocharov, A., Roetteler, M., & Svore, K. M. Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. *Phys. Rev. A* **96**, 012306 (2017).

[14] Xu, N. *et al.* Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System. *Phys. Rev. Lett.* **108**, 130501 (2012).

[15] Li, Zhaokai *et al.* High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311. *arXiv preprint arXiv:1706.08061* (2017).

[16] Xu, K. *et al.* Experimental Adiabatic Quantum Factorization under Ambient Conditions Based on a Solid-State Single Spin System. *Phys. Rev. Lett.* **118**, 130504 (2017).

[17] Selvarajan, R., Dixit, V., Cui, X., *et al.* Prime Factorization Using Quantum Variational Imaginary Time Evolution. *Sci. Rep.* **11**, 20835 (2021).

[18] Peng, W., Wang, B., Hu, F., *et al.* Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. *Sci. China Phys. Mech. Astron.* **62**, 60311 (2019).

[19] Dash, A., Sarmah, D., Behera, B. K. & Panigrahi, P. K. Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. *arXiv preprint arXiv:1805.10478* (2018).

[20] Liu, Y. An exact quantum search algorithm with arbitrary database. *Int. J. Theor. Phys.* **53**, 2571–2578 (2014).

[21] Li, P., & Li, S. Phase matching in grover's algorithm. *Phys. Lett. A* **366**, 42-46 (2007).

[22] Shoup, V. A Computational Introduction to Number Theory and Algebra. *Cambridge University Press* (2008).

[23] Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Comm. of the ACM* **21**, 120-126 (1978).

[24] Diffie, W. & Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory* **22**, 644-654 (1976).

[25] Sihotang, H. T.& et al Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security. *J. Phys.: Conf. Ser.* **1641**, 012042 (2020).

[26] Anada, H., Yasuda, T., Weng, J.& Sakurai, K. RSA public keys with inside structure: Proofs of key generation and identities for web-of-trust. *J. Inf. Secur. Appl.* **45**, 10-19 (2019).

[27] Lüy, E., Karatas, Z. Y. & Ergin, H. Comment on 'An Enhanced and Secured RSA Key Generation Scheme (ES-RKGS)'. *J. Inf. Secur. Appl.* **30**, 1-2 (2016).

[28] Gisin, N., Ribordy, G., Tittel, W.& Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

[29] Bhatt, A. P. & Sharma, A. Quantum Cryptography for Internet of Things Security a. *J. Electron. Sci. Technol.* **17**, 213-220 (2019).

[30] Jiang, S. *et al.* Quantum Annealing for Prime Factorization. *Sci. Rep.* **8**, 17667 (2018).

[31] Wang, B. *et al.* Prime Factorization Algorithm based on Parameter Optimization of Ising Model. *Sci. Rep.* **10**, 7106 (2020).

[32] Ansari, K., Behera, B. K. & Panigrahi, P. k. Data collection supporting the efficient working of a 12-qubit quantum repeater based communication. (2020).

[33] Github link to supplementary materials https://github.com/RituDhaulakhandi/Quantum-Factorization

[34] Altepeter, J. B., James, D. F. V. & Kwiat, P. G. Quantum State Tomography. 1-33 (2004).

[35] James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).

[36] Multiple qubit measurements https://docs.microsoft.com/en-us/azure/quantum/concepts-pauli-measurements#multiple-qubit-measurements

[37] Whitfield, James D., Biamonte, Jacob & Aspuru-Guzik, Alan. Simulation of Electronic Structure Hamiltonian Using Quantum Computers. *arXiv preprint arXiv:1001.3855v3* (2010).