Forensic Science International: Digital Investigation 40 (2022) 301341

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2022 EU - Selected Papers of the Ninth Annual DFRWS Europe Conference

A live digital forensics approach for quantum mechanical computers

Dayton Closser*, Elias Bou-Harb

The Cyber Center For Security and Analytics, University of Texas at San Antonio, San Antonio, TX, USA

ARTICLE INFO

Article history:

Keywords:
Quantum computers
Quantum forensics
Physics
Cybersecurity

ABSTRACT

In this paper, an exploration of reversing quantum computer gates is addressed as an avenue for collecting forensic evidence from a quantum computer. To date, little forensic research exists on quantum computing systems in general, and practically no experiments exist in the live recovery context. This work discusses the means for live forensics of quantum computers via both a look at current research on the matter, and through a demonstration of live data collection. The results are a combination of analysis conducted on real quantum systems to produce a quantum forensic methodology. Furthermore, this work will highlight the viability of live forensics, and largely refute Overill's assertion that it is not possible to perform live forensics on quantum systems. We believe that this work represents a very strong step towards revolutionizing the entire field of quantum forensics.

1. Introduction and foreword

Why endeavor to put forensics and quantum physics in the same context or perhaps even the same sentence, one might boldly ask? For starters, today there exists a forensic approach that works on current quantum computers and that implores such an endeavor. Moreover, since computer systems must obey the laws of physics, a bridge between forensics and quantum physics is not so far off a concept. In this exciting field, the quantum world is on the cusp of tomorrow's dawn, and with it, a radical transformation in the digital forensics discipline. To this end, we would like to thank the major contributors to this field by Richard E Overill, Sandeep Kumar Sharma, and Kamaljit I. Lakhtaria, especially for their trailblazing literature, perspectives, and frameworks on quantum forensics.

As an outline of this paper, Section 2 will be a description of a live forensic approach, discussing tools and techniques. Section 3's experimentation and validation will emphasize decoherence, entanglement, and noise concepts. As well, this section will reveal the live forensic implications on real quantum systems. Finally, Section 4 will conclude with areas for future interest, with a consideration for anti-forensics and ending with concluding remarks.

2. Primer in quantum physics

A forensic investigator might be able to define everything about a computer system with the appropriate knowledge of physics: from ohms of resistance to the voltages within the circuits, or perhaps the magnetic charge polarities within a hard disk platter. In many ways from a physics perspective, one might consider a computer system "Classical," or perhaps "Newtonian" in nature. Foundationally, many computers rely on electrical circuits, transistors, resistors, and silicon microchips to process electrical signals. At their core, these signals represent 0, and 1, binary states. From a forensic point of view, these “strong facts” are states of electrical signals–the states of the data those signals represent–is very consequential, especially for investigators, judicial courts of law, and even for victims of cybercrime and perpetrators of it. That consequentiality ultimately depends upon whether data either exists or whether it does not. The wisdom of classical physics held that everything in nature could be well-defined, and by corollary, everything within a computer system could be calculated and determined. Imagine from this classical perspective if a forensic investigator had unlimited information about a computer system. As once put by famous physicist Pierre Simon de Laplace, in his Philosophical Essay on Probabilities (1902): "Given for one instant an intelligence which could comprehend all the forces by which nature is animated...nothing would be uncertain" (Marquis de Laplace, 1902). However, unlike as Simon de Laplace speculated, the real world and universe do not always adhere to such ideal concepts; such is the case with quantum computers. Feasibly in the future, forensic investigators will enter the realm of a world where everyday perceptions of reality collapse. The hallmarks of such a strange realm as this will no longer be well-defined by position and

* Corresponding author.
E-mail address: dayton.closser@utsa.edu (D. Closser).

https://doi.org/10.1016/j.fsidi.2022.301341

momenta, but by uncertainty and perhaps even chaos.

2.1. Related work concepts

Indeed, the quantum world is a strange place that seems to transpire at incredibly small scales, with some sources suggesting actions along the 10^{-36} order of magnitude, known as the quantum of action, Planck's constant (Quantum of action (2014)), or simply put, microscopically. Presently, debate continues where this strange world ends (Ball, 2021), and the common human perception of reality begins, yet some agreement exists in common terms and concepts that define this baffling world which seems to betray reality: The Uncertainty Principle, Stationary States, Superposition, and Entanglement (Sharma and Khaliq, 2021). Other important concepts include Quantum Supremacy, and most notably, wave functions. These functions convey much of the quantum realm describing it through advanced linear algebra, expressed with wave functions and solutions to wave functions, as the 1925 Schrödinger equation, written generally as $i\hbar\Psi = H\Psi$ (Morin, 2008). The 'i' is an imaginary component, the $\hbar$ represents the Planck constant, the Ψ (read as psi) represents the wavefunction, and the capital H represents the Hamiltonian. This is the general form, however, and the Schrödinger equation has several iterations depending on use-case (time independence versus time dependence forms, for instance).

Wherein classical physics define everything about a system, quantum mechanics takes an operational approach defining systems in terms of preparation and measurement states, describing these elements in terms of probabilities and wave-function amplitudes. This operational approach to quantum mechanics is likely best exemplified in Werner Heisenberg's Uncertainty Principle. This principle describes uncertainty about the exact position and momenta of particles. In quantum mechanics, the instant a particle is measured, it is formalized as a "collapse" from coherent, uncertain quantum "eigenstates," and "de-coheres" into one basis state, a classical state. In the context of information, these basis states might be the binary values $|0\rangle$ or $|1\rangle$. The "rangles" are a way of expressing vectors or states in what is known as Dirac bra-ket notation (Morin, 2008), designed by the great British physicist Paul Dirac (important to note, this bra-ket notation for the basis states is the convention in quantum mechanics, and is written in the computer science disciplines as just 0 and 1). In short, observation mathematically shows how a quantum system breaks down from a "fog of war" into singular defined components. In short, the action of observation affects quantum systems, known perhaps aptly as the "Observer Effect".

Profoundly, particles at this scale can also exist in states of superposition (Sharma and Khaliq, 2021). Simply put, "superposition is like a special mixture of the energy levels" (Sharma and Khaliq, 2021). For instance, a bit represented in this way could assume a value of "1, 0, or 1 and 0 simultaneously, "overlapping (superposition) and intertwining (entanglement) according to the laws of physics" (Quantum computing, 2019). Think of superposition as two ripples in a pond converging so that they overlap, and entanglement as mixing the two colors blue and yellow to make green. How we might express this superposition becomes crucial as these states including the states of overlapping duplicity are foundational to how quantum computers work, and the "qubits" that are at the essence of them (Sharma and Khaliq, 2021). So, when, and why will quantum forensics matter? At present, quantum computers like IBM Q Systems "are not suitable for performing day-to-day tasks... don't have memory or a processor...but their computing power for very specific problems is much greater than a traditional computer's"(Quantum computing, 2019). These systems are not built for a single user's web browsing tasks in mind, but rather for solving tough problems, like prime number factorization, and ironically simulating quantum mechanics. Moreover, "Quantum (computing) is very effective at encoding and processing certain kinds of information, but it cannot efficiently mimic many useful aspects of its classical counterpart" (Sharma and Khaliq, 2021). Instead, specific mathematical jobs are queued to these systems (like a mainframe), and run in the order of job priority, a kind of batch methodology. At present, quantum systems require ultra-cold refrigeration of roughly "-273 °C (−459 °F)" (Quantum computing, 2019), to foster the superconductivity of the qubits (no exact value since the temperatures can vary by implementation of quantum systems). "At the same time, information cannot be stored in a quantum computer because the operational window is limited. This "computing time is finite: at some point the quantum properties of the computer are destroyed. They run for very short periods of time" (Quantum computing, 2019). Generally, we can only speculate on whether quantum systems will ever replace classical computers in entirety, or perhaps hybrid classical/quantum systems will leverage the capabilities of both implementations as is necessary and the case with today's "standalone" IBM Q Systems which interfaces with the cloud. Put another way, these modern quantum systems are dependent upon classical systems, and in a way, can be thought of as hybrid classical/quantum computers, of which is how we will refer to them in this paper. Regardless of how these systems transform taking root in the future, quantum systems will have to adhere to the limitations and principles of the universe, just as classical systems do. In other words, we should be able to forensically leverage these systems utilizing our knowledge and framework of physics.

2.2. Some current forensic literature considerations

Undesirably for the forensic investigator, some quantum principles–especially as the Observer Effect–present some immediate problems about the veracity of data collected from a quantum state, such as through "in vivo" live analysis. This challenge was identified by Richard E Overill at King's College (Overill, 2012). Overill went on so far as to assert that "it is not possible to perform live system forensics on a quantum computer, since any observation or measurement made on an evolving superposed state will cause it to collapse to a single randomly selected component" (Overill, 2012). Furthermore, due to the No-Cloning Theorem, copying of an unknown quantum state is also impossible (Overill, 2012). However, at present, current quantum systems still rely on classical hardware, such as cables, connections, and components which are susceptible to traditional analysis. Moreover, they are made possible by quantum principles and techniques which do present other avenues for live forensic collection, discussed in Section 3. Admittedly, Overill recognized the potential for postmortem artifacts; "a single classical output may remain for conventional digital forensic recovery and analysis" (Overill, 2012). Even though the architecture of quantum computers is not yet standardized, forensic tests to measure and record forensic artifacts on modern hybrid classical/quantum computers is a reality we can reveal and showcase today.

3. Description of a live forensic approach

In this paper, we will perform a proof-of-concept forensic experiment to "recover" binary values from a quantum system. At present, no experiments to our knowledge have been performed in the digital forensic investigator context on quantum systems. Therefore, our threshold of success for this proposal is to merely show a successful means for acquisition of data from such a quantum system. Furthermore, we propose to accomplish this demonstration via the IBM Quantum Composer, the Quantum

Information Software Kit (Qiskit) and Open Quantum Assembly Language (OpenQASM). This system leverages the IBM Quantum System One platform and can utilize Jupyter Notebooks as an accessible graphical interface(Qiskit Textbook - Descri).

3.1. Testbed, tools, and techniques

Qiskit's principal design allows for the creation of basic circuits, which offers a prospective of both a classical bit, and quantum bit (qubit). The circuits can be manipulated with quantum gates, which we will leverage as shown in Fig. 1.

Initially, running on Linux and NetBSD systems, we have devised a Qubit circuit with Qiskit in a simulation mode. At this stage, we elected to assign the variable qc = QuantumCircuit because of convention from the Qiskit documentation, and this "qc" variable allows for easy identification alongside applied quantum logic gates (Qiskit Textbook - Descri). In the first qubit, we applied the Pauli X gate, also known as a NOT gate, represented by an X and coded as qc.x(0). This X applied to q0 is shown and drawn at the bottom of Fig. 1. The gate is restricted to only one of two states, 0 and 1 binary values, so the NOT gate merely flips the qubit to the opposite value. Important to note, “using only the Pauli-gates it is impossible to move our initialized qubit to any state other than $|0\rangle$ or $|1\rangle$” (Qiskit Textbook - Descri), so we must consider other gates outside of these deterministic gates to achieve superposition. Other important gates are the CNOT, Toffoli, and Hadamard gates, of which some have equivalents as classical logic gates listed in Table 1.

Crucially by convention, qubits always start in the state 0, as they are initialized this way on modern quantum systems (Qiskit Textbook - Descri).

Furthermore, there are “an infinite number of possible gates” since quantum gates can be used in unison to create other gates and manipulate circuits (Qiskit Textbook - Descri). Some gates as the Pauli Y and Z do not really have classical equivalents since they are designed to cause rotations in Hilbert space (space with potentially infinite dimensions), which conveniently for us can be visualized around a Bloch sphere (literally a geometric sphere that represents quantum states) (Qiskit Textbook - Descri). Intended for the purposes of this paper, we have included them to merely show how quantum gates can differ, and to keep aware of these variations from quantum implementations. For the understanding of a forensic investigator though, the power of gates is in their ability to logically manipulate the state of qubits. Important to note, some gates like the NOT gate are reversible unitary operations, while other gates as the classical AND gate are unidirectional

```
qc = QuantumCircuit(1,1)
# quantum and classical circuit
qc.x(0)
#Pauli X Gate
qc.draw()
# display function of circuit
```

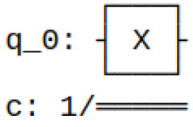

Fig. 1. An example circuit and Pauli-X gate.

Table 1
Quantum gate corollaries to Classical gates.

Quantum	Corollary to:	Classical
Pauli X	=	NOT
“controlled” not cnot	=	XOR
“Toffoli” ccnot (Deutsch)	=	AND
NAND gate	=	Two NOTs
cswap gate	≠	No equivalent
Hadamard	≠	No equivalent
Pauli- Y and Z Gate	≠	No equivalent

(Reversibility and Quantum c, 2003). Implications of the reversible nature of gates will be further discussed in Section 4.1.

Let us now devise a 2-Qubit circuit with Qiskit, applying the reversible NOT gates and the superposing Hadamard gates, this time on a real quantum computer, the "ibmq-santiago." This 5-qubit Falcon r4L quantum system displays an average frequency of 4.767 GHz, gate-time of 408.889 ns, and a C-NOT error rate of $7.413e^{-3}$ as of 26th September 2021. Specifically, this system will produce a lot of "noise" into calculations, unlike a quantum simulator, which in contrast simulates an ideal quantum computer. As Overill pointed out, observation will affect the data encoded in a state of superposition. Overill suggested "it is then necessary to extract the single required component from the output state" (Overill, 2012).

However, this is not necessarily the case. The Principle of Deferred Measurement (Nielsen and Chuang, 2018) can be used to the advantage of a forensic investigator. While it is true that data cannot exist permanently in a quantum system, the data does not have to ever be observed as an output from superposition. "In fact, though, it does not matter whether we measure the fresh qubits before or after running the quantum circuit. In fact, we can delay their measurement arbitrarily long, or just avoid it altogether...Measurement is equivalent to entanglement of the system with its environment" (Reversibility and Quantum c, 2003).

4. Experimentation and validation

4.1. Reversible gate basics

However, instead of observing the qubit following computation, a forensic investigator can apply the physics of forensics, and utilize reversible quantum gates. Think of reversal like a domino game. After the dominoes collapse into chaos, the exact alignment of them can only be restored if they are replaced by the exact displacements from their undisturbed state. Moreover, some functions can be restored in a similar fashion, bound by the fact "quantum computation is restricted to reversible functions" (Omer, 2000). In this demonstration, qubit 0 (q0) starts at a value of 0, is flipped to 1 by a Pauli-X gate and is superposed by the Hadamard. At this point, the data in q0 is in superposition and the binary output could either be "01" or perhaps "00."

Nevertheless, if we apply the Hadamard and Pauli-X gates again as in Fig. 2, something peculiar happens as shown in Fig. 3. The probability amplitude of '00' becomes 1. This is because "[t]o preserve the total probability in all cases, our operations need to be reversible. This means we can perform our quantum gates backwards to 'undo' them (remembering to reverse any rotations) and be left with the state we started with" (“Qiskit Textbook - Descri). Expressed in terms of probability (y-axis) and the qubit values (x-axis), we calculated this on ibm-santiago as shown in Fig. 3.

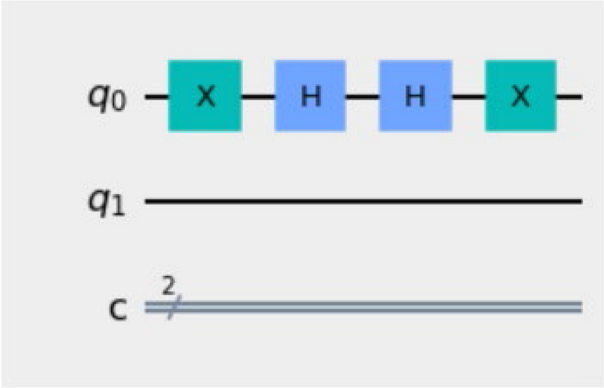

Fig. 2. Pauli-X and Hadamard gates applied to q0.

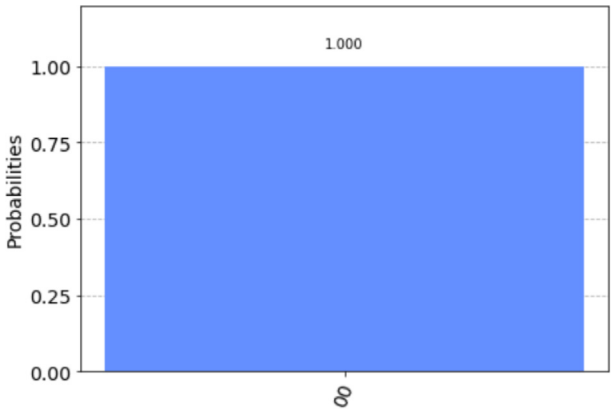

Fig. 3. Probability of 1.0 after two Hadamard quantum gates are applied to q0 (00).

4.2. Decoherence

Moving away from deterministic gates to gates that leverage the exotic nature of qubits, there are a few considerations for the forensic investigator to keep in mind. For instance, "if you leave [a] Qubit...over time, the quantum information stored in them will decay away. This process is known as de-coherence" (Sharma and Khaliq, 2021). If the information is not measured or reversed in this period, it will be lost. Furthermore, "modern quantum computers do not perform exactly as we specify in the circuit model" (Sharma and Khaliq, 2021), so we should expect errors, discussed in Section 4.4. To tackle decoherence, there exists a Quantum Error Correction (QEC) solution, which effectively is "a procedure for turning a bunch of noisy Qubits into a fewer number of much less noisy Qubits" (Sharma and Khaliq, 2021). Some suggest that a major division between today's "Noisy Intermediate Scale Quantum" or NISQ computers, and future error correcting systems, remains in how these systems handle these errors (Sharma and Khaliq, 2021). Presently, the NISQ systems are predominant, and the IBM quantum systems we employ are NISQ.

4.3. Entanglement

Another avenue with gates has to do with the concept of quantum entanglement. Perhaps rather obviously, un-entangled particles are separable, whereas entangled particles are a case where they cannot be described independently of one another (Quantum computing, 2019). Metaphorically speaking in more associable terms, think of this such as sugar and cake, a horse and carriage, highways, and traffic. Entanglement is a state where it makes little sense to describe one without the other.

Such cases also present some unique scenarios forensically. Especially when we consider a quantum Bell State, which is merely the simplest case of quantum entanglement between two qubits. In this situation, note the application of a Hadamard and a controlled C-NOT gate, as shown in Fig. 4. First in our 2-qubit example, the C-NOT gate applied to q1, controlled by q0 will only flip the qubit value if q0, the control qubit, is in a state of 1. This is represented by the following state vectors of $(1/\sqrt{2})$, 0, 0, $(1/\sqrt{2})$. Important to note, we did not have to measure the data, we only do so now to show the probabilities of the states and state vectors for purposes of explaining the states of entanglement further. Intrinsically, the two qubits are entangled by the Hadamard, and until observation or rather measurement, remain in states of superposition or entanglement, not any defined values.

4.4. Noise and errors

Additionally, a forensic investigator must consider noise introduced into a quantum system and recognize that while the Hadamard gates are designed to enlist equal probability in circuits, errors can and do occur in probability computations. For instance, we selected another IBM quantum computer, the ibmq_lima, and it reported the following probabilities for our devised Bell state, as outlined in Fig. 5. Immediately, the error induced by current quantum hardware becomes clear and obvious, as the Bell state produces uneven results, only accounted for as noise introduced into the probabilities. To help reduce the errors caused by these calculations, we ran them with varying numbers of "shots" to garner larger populations and generally see how the error might fluctuate with the counts. Following this first run on ibmq_lima, it produced the following results, read left-to-right as binary state, and counts, respectively: {'00': 56, '11': 44}. A second run resulted at five-hundred shots yielded perfect 50-50 odds with the following counts as shown the second graph: {'00': 250, '11': 250}. A third run at one thousand shots yielded almost perfect odds and equal counts: {'00': 502, '11': 498}.

While the idea of whether quantum systems and circuits are ever perfected to be error-free is speculative, these examples demonstrate the characteristic of Bell states in a present-day setting. We reveal these probabilities to show several features and limitations of quantum implementations.

Firstly, because we can, and that we consider that in and of itself very impressive since such quantum systems are no longer textbook theories but real systems. Secondly, to show that real-world quantum circuits are noisy, and this noise contributes to error.

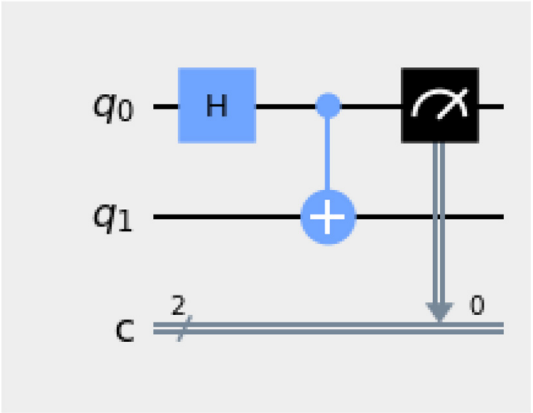

Fig. 4. Hadamard and CNOT gate applied and measured in quantum "Bell State".

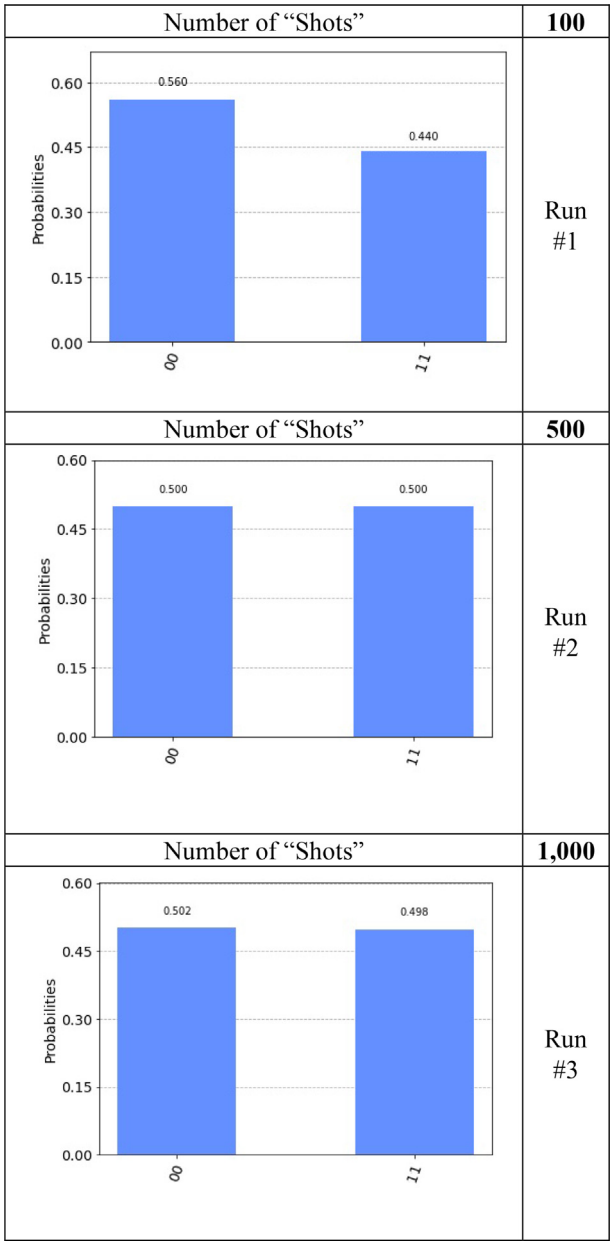

Fig. 5. Probabilities 00 and 11 after varying numbers of shots.

Thirdly, to show on current hardware, these probabilities do not always correspond to the theoretical probabilities of the gates.

These concepts we have discussed about quantum behavior are also evident in the demonstration we provide. Note that with the operational approach of quantum mechanics, the measurement of the system can possibly produce two states of the qubits, which until measured exist in both states. Confounding in theory, but, for future forensic investigators, also fascinating.

4.5. Entanglement and transmission

For our purposes, we have employed and reversed basic deterministic gates as the Pauli-X alongside the Hadamard, to prove that what was started with can be restored. With entanglement, other points become extremely interesting, such as a third party, termed "Telamon" ("Qiskit Textbook - Descri). The qubits may be initialized, and entangled by said party, which prepares them for the peers that require them, such as two recipients in a context of exchanging qubit states. This quantum behavior diverges somewhat from a classical two-party relationship, whereby only sources and destinations are necessary to exchange data, for example, a phone conversation requiring a caller and receiver. To this end, we can leverage superposition and entanglement's exotic behavior in a way that is perfectly baffling. For instance, if the q0 is entangled, it could be transmitted to a second party, before it is encoded. In other words, the proverbial message sent before it is written, and then written later or perhaps never at all. While this exotic transfer of qubits between parties cannot be performed on present-day IBM quantum hardware, the implications of this bizarre entanglement phenomena can be partially demonstrated, as shown in Fig. 6.

Once an entangled pair of qubits has been provided to both sender and recipient (shown in the first barrier), the data can be encoded by the sender (second barrier) and following this, the sender needs only to send the qubits to the recipient who then would decode the quantum data with the correct gate, as outlined in Table 2 ("Qiskit Textbook - Descri).

Note it is imperative for the forensic investigator to make his or her analysis before the actual qubits are measured in later phases. While they are entangled, the qubits can be fully reversed with the same reversible gates applied, in the same order they were applied. If the qubits are also encoded before entanglement, they can be decoded as follows. Suppose for instance we have a Bell State after a NOT gate on q0, and it becomes entangled by that Bell State, as drawn in Fig. 7. Suppose now we want to disentangle that Bell State to recover the NOT encoded data on q0. Firstly, how this is performed is by reversing both the CNOT gate and the Hadamard, by applying in the exact reverse order. Important to note, we should not apply the control on q0, but rather on q1, and the Hadamard on q1 instead of q0 to complete the reversal and disentangle. And to demonstrate this reversible Bell state is correct, we should get a binary of 01.

Now, we only measure to highlight these results (as well as introduce a barrier line to divide and isolate the gates of the experiment into a left and right section), but the technique of evaluating applied gates will derive the same values. Q0 undergoes from initialization 0 → 1 → superposed 0 and 1 → entangled with q1 → disentangled with q1 → de-superposed → 1. This of course is exactly what we expected, and the measurements confirm this, which again are only measured for illustration of this point. To understand how this might look in terms of probabilities, we calculated this reversed Bell State with 1000 shots on ibmq_lima as shown in Fig. 8. And then again for validation, the test was performed at 2000 shots in a second run.

Results as this will give the forensic investigator an understanding of how the system, and ultimately the qubits have been

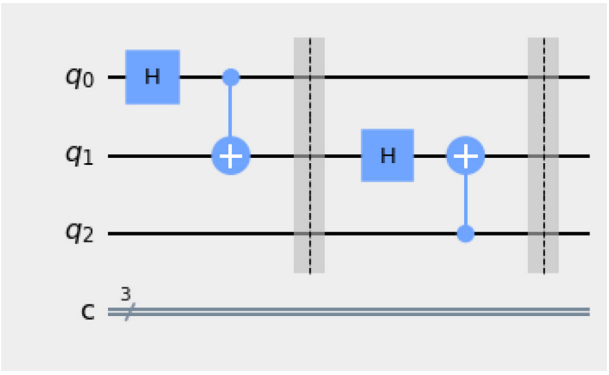

Fig. 6. Entangled qubits ready for transmission.

Table 2
Application of quantum gate to decode entangled state.

Binary value	Action:	Gate to Apply
00	→	Do nothing
01	→	X gate
10	→	Z gate
11	→	ZX gate

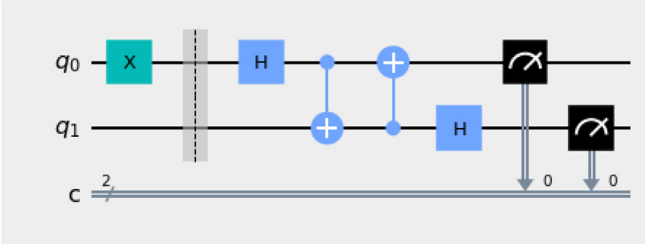

Fig. 7. Encoded Quantum Bell State reversed.

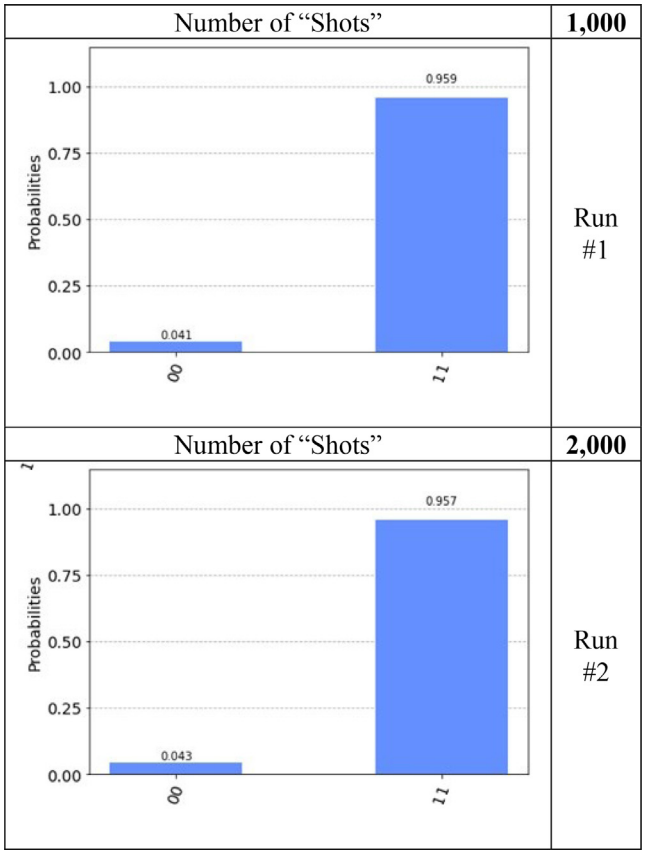

Fig. 8. Probabilities 00 and 11 after 1000 and 2000 "shots" following a Bell State reversal.

encoded, allowing them to reconstruct and trace the inputs of the quantum system. In a nutshell, performing live forensics on this entangled set-up requires not only knowledge of the gates applied, but an understanding of whether observation has occurred or not. If observation has occurred, then the forensic analysis of the entangled qubits can no longer be reversed, since measurement effectively destroys these delicate quantum states. In contrast to the suggestion by Overill, superposition and entanglement themselves are not the main culprits preventing live analysis, but rather factors as the potential observation by another party, and likely in the real world, time to decoherence, are. Moreover, if a third party observes the qubit before the system has been analyzed, data will collapse from the entangled state. For our purposes, a forensic investigator will likely have a short window of time (which will vary in length depending upon the decoherence conditions of the qubits) to perform his or her analysis, for in entangled cases, the data will decohere if left unattended in a quantum state. This is in part because the state must be reversed from its state of superposition before decoherence since it cannot be copied or "refreshed" from a state of superposition due to the No-Cloning Theorem. In other words, waiting too long will lead to a loss of data. If none of these impediments have occurred, the forensic investigator will be able to backtrack as normal.

4.6. Live forensic implications

Crucially, Overill's assertion that it is not possible to perform live forensics on quantum systems is misleading and incorrect because, measurement of a quantum superposed, and entangled state is not entirely necessary to determine data input into a quantum system, gates are. The key here then to live forensics on quantum systems is determining which reversible gates become applied to the quantum system, and merely reversing the gate logic from there, and of course, not to measure the system. In other words, gathering essential information from the preparation stage of a quantum system. Keep in mind that quantum systems are defined in terms of preparation and measurement states, it no longer becomes necessary to observe anything–the very fact we know what these gates do, (in their prepared state) and the fact that gates in question are reversible allows us to determine what value the qubit must be, even if the current running state of it is obscured by quantum behavior. Supposing if a cybercriminal applies a superposing Hadamard gate giving two possible amplitudes of $\sqrt{1/2}$ ("Qiskit Textbook - Descri), we can simply backtrack by applying the reverse Hadamard and NOT gates and the qubit is back in the state it was before. This approach itself is reversible and no data is lost, allowing us to recover data simply and efficiently. This is analogous to connecting a USB drive to a computer of forensic interest and copying the content without tarnishing the authenticity or forensic chain of custody's fidelity. This was originally demonstrated in Fig. 3, which gave a probability amplitude of 1, since we should get back what was started with in the system, or in other words, a qubit state of zero. And since we can backtrack, we need only deduce what state the qubit must be in via gates.

4.7. Some additional considerations with quantum gates

Admittedly, there are some other considerations with the gate reversal approach. As the intricacy of gates expands outside the realm of simple deterministic gates, this methodology could become extremely cumbersome. Consider complex systems with more qubits than simply two qubits, such as IBM's new 1000 qubit system (Gambetta, 2020). To this point, perhaps automated gate screening tools will have to be created to address this complexity when performing analysis on future quantum systems. Furthermore, it is important to note that not all gates are reversible (consider classical computer gates). As well, future hybrid classical-quantum systems may also hide their gates from being determined by investigators. Forensic investigators will then have to devise means to defeat these measures. Additionally, while the architecture right now to quantum gates is open source, and accessible, this may not be the case in the future, further confounding an investigation.

Also, of significance, investigators will have to consider the gates to apply in the exact reverse order for "whenever we use a logically irreversible gate, we dissipate energy into the environment" (Kerntopf). This would be equivalent to destruction of data and must be avoided at all costs. As an analogy, think of this as accidently taking an image of a classical computer's hard drive and erasing the original copy. This accidental destruction is not a desired outcome of an investigation with classical computers and must be avoided as well on quantum computers. Furthermore, the gate reversal approach does not capture computations beyond the initial input of quantum gates. Data passed from a state of superposition and measured may be inaccessible and not captured in the reversal. For instance, the result of some prime number calculation following quantum computation would be unknown from an analysis of a quantum preparation state. Similarly, if the original state of a qubit is obscured (say for instance it starts at 1 instead of 0), it becomes nearly impossible to "back-trace" the gates without measurement at some point along the circuit. However, if an investigator knows the initial value, the analysis can be performed just as we have demonstrated. In other words, this approach is confined largely to input collection from a well-defined initial state of a quantum system, not the output and corresponding computations of that output.

However, it is conceivable that gates following the output and thus at a state requiring more input from the user, could be captured in the same fashion. As an analogy, think of a computer program prompting a user for more information (such as Form B) after they have already entered input (say for instance Form A). Between these prompts, this gate approach might be applied, though among the individual user inputs will have no bearing on one another. In other words, Form A will tell nothing to a forensic investigator about Form B. Moreover, it is likely that data not in a quantum system will have to be saved, and for the time being, that relies upon classical computers, and thus, such systems would still be susceptible to current forensic techniques. Put another way, data not in a quantum state, but in a preparation state, will be exploitable per the gate reversal approach.

5. Conclusion

5.1. Areas for future research — anti-forensics with Deferred Measurement

Conceivably in the same way investigators will be challenged by the limitations of controlled "decoherence," cybercriminals will "convert" classical data into a quantum system to mask it from analysis. For instance, classical probability distributions of data might be converted into quantum states, so analysis of the data will be impossible without observation. To that end, cybercriminals might allow the data to perish without ever being observed, using the Principle of Deferred Measurement against investigators so their crimes would be cleanly destroyed. This approach may not be any cleaner or any more effective than conventional data destruction and could prove more complicated. However, it is yet another possible technique that has not seen any research consideration in the quantum anti-forensics field.

5.2. Areas for future research — anti-forensics with hardware approaches

Feasibly, investigators will be challenged as well by hardware extraction of data from qubits, even utilizing microwave capture or tapping of the classical framework of quantum systems. Moreover, quantum supremacy suggests that quantum computers will replace classical computers, and perhaps undergo a similar miniaturization into desktops and servers, perhaps even microcomputers in terms of hardware. Or, this transformation may never happen as witnessed by classical computers, but if it does, it holds that the reliance on classical hardware will leave open the same anti-forensic tricks available to forensic investigators today. Even in the event of quantum keyboards, mice, and other such classical equivalents becoming a reality, we are curious how much reliance will still rest in classical hardware. For, if quantum systems rely on any old-fashion real-world hardware, so too will they be vulnerable as their classical computer counterparts. In short, hardware forensics of quantum systems will prove yet another exciting field that presently remains lacking in research.

5.3. Areas for future research — anti-forensics with people

Perhaps in the future, quantum computers will coincide with people with a similar status as present-day classical computers. Imagine offices, universities, hospitals, residences, and perhaps even spacecraft filled with these systems, performing operations specifically suited to their strengths as computers. Perhaps these computers will be of vital consequence to future infrastructure and national security. Speculation perhaps, but these systems may prove to be essential towards future technologies. Perhaps the way in which these systems are breached, targeted, and how the relationships with quantum computers and people coincide will be of interest to the forensic investigator.

5.4. Concluding remarks

While the potential for live forensics is in some ways a topic for a problem that does not quite exist yet, it one day may have significant relevance. We demonstrated that live forensics and recovery through quantum gates on current quantum computers is viable, that these quantum computer systems open incredibly new and exciting avenues forensically, and with it, opportunity for the whole digital forensics field and community. To that end, it is important for forensic investigators to remain prepared, and ready not just for the challenges of the 21st century, but for perhaps the challenges of the 22nd century that remain lingering ahead. Perhaps most crucially, forensic investigators must retain the upper hand in both technique and knowledge of computer systems, furthering their expertise proactively ahead of cybercriminals and their unscrupulous wit. At the same time, with collaboration, with the research communities, it may prove possible to engineer solutions to problems pre-emptively, keeping an aspirational approach to forensics and quantum computers.

Acknowledgements

We thank the reviewers and our Shepherd for their constructive feedback that greatly enhanced this work. This work was partially supported by a grant from the U.S. National Science Foundation (NSF), Office of Advanced Cyberinfrastructure (OAC), #2104273.

We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors, and do not reflect the official policy or position of IBM or the IBM Quantum team. Special thanks to the NetBSD foundation, the Qiskit Community, and all other open-source projects for their efforts in providing quality software for research. Special thanks to Qiskit for their excellent documentation.

Lastly, special thanks to UTSA quantum mechanics professor Dr. Tyler Sutherland for his advice and counsel regarding technical concepts, and support in making this paper possible.

References

Ball, P., 2021. Where does quantum weirdness end? New Sci. 251 (3349), 38–39. https://doi.org/10.1016/S0262-4079(21)01518-9 bll.

Gambetta, J., 2020. IBM's Roadmap for Scaling Quantum Technology. IBM Research Blog. Available at: https://research.ibm.com/blog/ibm-quantum-roadmap.

Kerntopf, P. (no date) "REVERSIBLE LOGIC CIRCUITS". Warsaw University of Technology Warsaw, Poland.

Marquis de Laplace, P.S., 1902. A Philosophical Essay on Probabilities. Wiley.

Morin, D., 2008. Introduction to Quantum Mechanics. Cambridge University Press, uk.

Nielsen, M.A., Chuang, I.L., 2018. Quantum Computation and Quantum Information: 10th ANNIVERSARY. Cambridge University Press.

Omer, B., 2000. Quantum Programming in QCL. Master's thesis. Institute of Information Systems Technical University of Vienn na.

Overill, R.E., 2012. Digital quantum forensics: future challenges and prospects. Communications and Convergence 5. Inderscience Publishers Ltd Int. J. Inf. Technol. 2 (3), 205–211. bll.

Sharma, S.K., Khaliq, M., 2021. The role of quantum computing in software forensics and digital evidence: issues and challenges. Limit. Future Appl. Quant. Cryptogr. IGI Global 21–46, 169–185 bll.

"Qiskit Textbook - Describing quantum computers" (no date) Qiskit Textbook. IBM Research / Qiskit community. Available at: https://learn.qiskit.org/course/introduction/describing-quantum-computers.

Quantum Computing: How it Differs from CLASSICAL COMPUTING?, 2019. NEWS BBVA. BBVA. Available at: https://www.bbva.com/en/quantum-computing-how-it-differs-from-classical-computing/.

Quantum of action Dictionary Geotechnical Engineering/Wörterbuch GeoTechnik: English-German/Englisch-Deutsch, 2014. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1063–1064. https://doi.org/10.1007/978-3-642-41714-6_170042 bll.

Reversibility, Quantum circuits.", first ed., 2003. UC Berkeley, Berkeley [ebook].