# On Zero-Knowledge Proofs over the Quantum Internet

Mark Carney[1]

[1] *Quantum Village Inc.*

December 2022

## Abstract

This paper presents a new method for quantum identity authentication (QIA) protocols. The logic of classical zero-knowledge proofs (ZKPs) due to Schnorr [8] is applied in quantum circuits and algorithms. This novel approach gives an exact way with which a prover $P$ can prove they know some secret by encapsulating it in a quantum state before sending to a verifier $V$ by means of a quantum channel - allowing for a ZKP wherein an eavesdropper or manipulation can be detected with a fail-safe design. This paper presents a method with which this can be achieved. With the anticipated advent of a 'quantum internet', such protocols and ideas may soon have utility and execution in the real world.

## 1 Introduction

With the advent of Quantum Computing comes with it the idea of the Quantum Internet - the ability to transfer a quantum state $|\Psi\rangle$ from one quantum computer/device to another. There are many challenges with this kind of networking [2], as well as many benefits. As Cacciapuoti [2] points out, with a quantum internet we get Quantum Key Distribution 'for free', a major benefit to quantum communications infrastructure. There are many existing Quantum Identity Authentication (QIA) protocols [4] and this paper adds a new approach to the collection.

Existing approaches make use of various features of QKD, quantum teleportation techniques, Physically Unclonable Functions (PUFs), distributed Bell states, quantum private queries, quantum secure direct communications, etc. Many of these details may be found in [4].

Schnorr introduced in [8] the idea of efficient identification signatures, initially designed for use with smart cards. This method of 'proving' your identity without disclosing a secret became known as 'zero-knowledge proofs' and have recently found much use in many cryptographic protocols [5].

The benefits of ZKPs over other past approaches are that there needs be no prior exchange or other pre-sharing, nor any explicit statement of what the hidden information is. The proof system itself carries the correctness and soundness that guarantees the validity of a proof presented by the prover to the verifier, and that the claim by the prover to know such a secret is 'true'.

ZKPs have been used to create quantum proof systems that have also been shown to be possible in a quantum setting [9]. These make use of graph isomorphism problems, which this approach does not. The method herein takes advantage of a quantum communications network to reduce the number of quantum and classical transmissions down to 3 each.

The work presented here aims to demonstrate how a quantum ZKP protocol might look by coding Schnorr's original method into quantum states. Some benefits and restrictions of this approach are included.

## 2 Schnorr ZKP Protocol

In its simplest form, a zero-knowledge proof is a method for a prover $P$ to provide a way of showing that they know some secret $x$ to a verifier $V$, but without exposing the secret at any point, hence 'zero-knowledge'.

The following algorithm is the usual presentation of Schnorr's work. $P$ wants to prove that they know $x$ such that $Y = g^x \mod p$, for prime $p$ and generator $g$, with $g$, $p$, and $Y$ public. The following method is presented:

1. $\underline{P \to V}$: $P$ chooses some $r$ and sends $t = g^r \mod p$ to $V$.

2. $\underline{V \to P}$: $V$ sends a random $c$ to $P$.

3. $\underline{P \to V}$: $P$ sends $s = r + cx$ to $V$

4. $\underline{V \text{ checks}}$ that $g^s \equiv t \times Y^c \mod p$.

This works as

$$\begin{aligned} t \times Y^c &\equiv g^r \times (g^x)^c && \mod p \\ &\equiv g^{r+cx} && \mod p \\ &\equiv g^s && \mod p \end{aligned} \tag{1}$$

This very neat scheme was a very important development in authentication schemes, and will form the basis for the quantum protocol presented next.

# 3 Quantum Preliminaries

This protocol utilises a single qubit, and only two quantum gates. Qubits are assumed to be initialised in $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ with our target state $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. With $\alpha, \beta \in \mathbb{C}$, $|\psi\rangle = \left(\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right)$, such that $|\alpha|^2 + |\beta|^2 = 1$. Quantum gates are formed from collections and tensor products of $2 \times 2$ unitary matrices, relying on the fact that composing unitary matrices with each other preserves this property [6].

Define the $R_x$ gate as [6]:

$$\begin{aligned} R_x(\theta) &= e^{i\theta X/2} \\ &= \cos(\theta/2) I + i \sin(\theta/2) X \\ &= \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \end{aligned} \tag{2}$$

where $I = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and $X = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. With the representation of the Bloch sphere, this gate is usually interpreted as a rotation along the $x$ axis.

The following gate $G_p(a)$ shall be utilised, defined as follows:

$$G_p(a) = R_x\Big((a \mod p) \times \frac{\pi}{p}\Big) \tag{3}$$

Intuitively, we split the $\pi$ rotation about the $x$ axis on the Bloch sphere into $p$ many steps, and then apply a rotation on our qubit, moving that number of steps around.

# 4 Quantum Internet ZKPs

This section brings these two domains together to propose an authentication scheme that makes use of a quantum internet with additional classical channel.

## 4.1 Q-ZKP Protocol

The Quantum Internet, loosely defined, is a quantum communications protocol that permits the transfer of some quantum state $|\Psi\rangle$ from one quantum computer/device to another. Utilising this property, the following zero-knowledge proof can be constructed.

With the advent of Shor's algorithm (see [6, Appendix 4]) it is clear that if $Y = g^x \mod p$ is public alongside $g$ and $p$, then $x$ may be recovered by means of this algorithm. As such, a way of sharing quantum states that encode $x$ and the subsequent proof is needed.

To do this, we substitute exponents over some $g$ for rotations about the $x$ axis on a qubit, relying on the hardness of decoding quantum states rather than the discrete logarithm problem.

As before, $P$ wishes to prove they know $x$ to $V$, only this time they have a quantum internet. Both the rotation $G_p$ and value of $p$ are known publicly.

1. <u>$P \to V$:</u> $P$ sends a commitment state $|G_p(x)\rangle$ to $V$.

2. <u>$P \to V$:</u> $P$ chooses some $r$ and sends $|G_p(r)\rangle$ to $V$.

3. <u>$V$ constructs</u> the state

   $$|A\rangle = |G_p(x)\rangle\,|G_p(r)\rangle \tag{4}$$

   and chooses a random $c$ and $n$.

4. <u>$V \to P$:</u> $V$ sends $c$ and $|G_p(n)\rangle$ to $P$.

5. <u>$P$ computes</u> $s = r + cx$ and

   $$b = \begin{cases} 0 & \text{if } (r + xc \mod 2p) \le p \\ 1 & \text{if } (r + xc \mod 2p) > p \end{cases} \tag{5}$$

6. <u>$P \to V$:</u> $P$ sends $s$ and $b$ and then sends

   $$|S\rangle = |G_p(x(c-1))\rangle\,|G_p(n)\rangle$$

   to $P$.

7. <u>$V$ constructs</u>

   $$\begin{aligned} |B\rangle &= |A\rangle\,|S\rangle\,|G_p(-n)\rangle && (6) \\ &= |A\rangle\,|G_p(x(c-1))\rangle && (7) \end{aligned}$$

8. <u>$V$ sets</u> $|C\rangle = X$ gate if $b$ is 1, else $|C\rangle = I$.

9. <u>$V$ checks</u> that

   $$|B\rangle\,|C\rangle\,|G_p(p-s)\rangle = 1$$

   under the normal $z$ axis measurement.

## 4.2 Correctness

We first note that due to the commutativity of single axis rotations

$$|G_p(a)\rangle\,|G_p(b)\rangle = |G_p(b)\rangle\,|G_p(a)\rangle \tag{8}$$

From this it follows that

$$|A\rangle\,|G_p(x(c-1))\rangle = |G_p(r)\rangle\,|G_{2p}(xc)\rangle \tag{9}$$

Next we need to take $|G_{2p}(r+xc)\rangle$ which is formed from full rotations about the $x$ axis, and restrict it down to half-axis rotations. This is where $|C\rangle$ comes in to play.

Note that if some $(a \mod 2p) > p$ then $(a+p \mod 2p) < p$. Given our $X$ gate effectively fulfils this function, it is conditional on $P$'s assessment in witness $b$ whether it is applied or not. As such if $(r+xc \mod 2p) > p$ then

$$|G_p(r)\rangle\,|G_{2p}(xc)\rangle\,X = |G_p(r)\rangle\,|G_p(xc)\rangle \tag{10}$$

This gives us, given a correct choice of $|C\rangle$

$$|B\rangle\,|C\rangle = |G_p(r)\rangle\,|G_p(xc)\rangle \tag{11}$$

We then need the following theorem to complete our proof's validity:

**Theorem 4.1.** *Let $|C\rangle$ be chosen appropriately as above. When $V$ checks*

$$|G_p(r)\rangle\,|G_p(xc)\rangle\,|C\rangle\,|G_p(p-s)\rangle$$

*the output will always be a* 1 *if and only if $V$ agrees that $P$ has a valid proof that they know $x$.*

*Proof.* ($\leftarrow$) Start by re-asserting the interpretation of equation (1) in this scheme, namely that for a valid proof it follows that

$$s \equiv r + xc \mod p$$

With this, it then follows that $|G_p(r)\rangle\,|G_p(xc)\rangle\,|C\rangle$ should be the same $R_x$ rotation as $|G_p(s)\rangle$.

Under multiplication the rotation is completed by $G_p(p-s)$, as

$$s + (p-s) \equiv p \equiv 0 \mod p \tag{12}$$

Given the protocol only divides a half, not a full, qubit rotation by $p$ this completion should always send the qubit to be in state $|1\rangle$, and therefore have a 1 measurement.

($\rightarrow$) If the measurement output is always 1 then the $|G_p(r)\rangle$ state received from $P$ by $V$ matches the $|G_p(s)\rangle$ state that $V$ can construct, when composed with the $|G_p(xc)\rangle$ states that $V$ wants to verify, sent piece-wise from $P$.

By equation (12) a $|1\rangle$ state, and subsequent 1 measurement means that everything required to line up has done so, and $P$'s proof is correct. □

Note that the proof of soundness is given by the original protocol from [8].

## 4.3 Remarks

### 4.3.1 Repetitions

Of course, just one exchange between $P$ and $V$ will likely not be convincing enough. Numerous exchanges and measurements will build the statistical significance that $P$ is indeed correct according to $V$. This significance will additionally grow as $p$ and the resolution of the qubit increase.

As the protocol is quite efficient compared to others (there are only three quantum and three classical transmissions), the overhead for multiple transmissions should be linear. The values for $r$, $n$, and $c$ may also change each time without affecting the overall validity of the proofs.

Future developments may involve multi-party distributed entangled states (such as GHZ states) where multiple verifiers can receive the same $|G_p(r)\rangle$, issue different challenges, and all verify proofs from $P$.

### 4.3.2 Error Rate

It should be noted that the error rate introduced by someone listening in on the quantum channel will also be evident very quickly, as the error rate will rise significantly when an eavesdropper tries to guess the random $r$ chosen by $P$. This is congruous with how QKD protocols add security using quantum states. The quantum channel, as with other quantum communications protocols [2], offers some significant added protection there.

It should also be noted that, because the security relies on the statistical likelihood of zero measurements, the protocol effectively fails safe for sufficiently high introductions of error.

### 4.3.3 Hardware

There are several constraints on current hardware that would preclude this from being immediately practical. Namely, the need for a very high precision on the qubit in use, and a likewise minimal amount of noise required to not skew the results.

Error corrected qubits and quantum communication channels are required to deal with the second part of these issues [7]. The resolution of the qubits and their longevity is taken into account by some benchmarks, such as 'Quantum Volume' [3]. Therefore, as quantum computers grow in reliability and complexity, and quantum networks begin to be tested and deployed and improve, we might consider such high enough resolutions, error correction, and reliability to one day be attainable.

#### 4.3.4 Security of Secret Values

The variable $n$ is included to ensure the integrity of $P$'s response in step 6, whilst $r$ assumes the same function as per the original Schnorr ZKP method. The fact that secrets are encapsulated in quantum states is the manner in which this protocol maintains its security.

Much as Schnorr's original ZKP relies on the security of the discrete logarithm problem to maintain security of that system, this system relies on the security of quantum states to preserve the encapsulated secrets $x$, $r$, and $n$. Were an eavesdropper or attacker attempt to read these states, they would not be able to easily discern accurate values for these secrets. Likewise, such an attack would also raise the noise floor above what is acceptable, and would be detected, as discussed in section 4.3.2.

As such, an attacker would have to measure $|G_p(x)\rangle$ and $|G_p(r)\rangle$ continually in order to produce any kind of valid amplitude estimation, *e.g.* in [1]. Given each value is only transmitted at most once in its original state such an attack is not viable.

# 5 Conclusion

This paper hopes to have shown that there is another possibility for performing zero-knowledge proofs using quantum algorithms over quantum communications networks. This system has been shown to have some additional benefits over purely classical approaches, despite its classical basis.

This work thereby adds to the collection of proposals for QIA and quantum zero-knowledge proofs that might help shape future quantum communications.

# 6 Acknowledgements

The author is thankful to the indulgence of discussion, expertise, and time from Dr. Joseph Wilson and Prof. Ben Varcoe, and to Christoph Graebnitz for identifying a major issue that lead to a redesign of the method in section 4.

# References

[1] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. *pre-print*, 2000.

[2] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi. Quantum internet: Networking challenges in distributed quantum computing. *IEEE Network*, 34(1):137–143, Jan. 2020.

[3] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta. Validating quantum computers using randomized model circuits. *Physical Review A*, 100(3), Sept. 2019.

[4] A. Dutta and A. Pathak. A short review on quantum identity authentication protocols: How would bob know that he is talking with alice?, 2021.

[5] E. Morais, T. Koens, C. van Wijk, and A. Koren. A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, 1(8), July 2019.

[6] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, England, Dec. 2010.

[7] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9(10):641–652, Sept. 2015.

[8] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 239–252. Springer New York, 1989.

[9] J. Watrous. Zero-knowledge against quantum attacks, 2005.