On Zero-Knowledge Proofs over the Quantum Internet

Mark Carney[1]

[1] *Quantum Village Inc.*

February 2023

Abstract

This paper presents a new method for quantum identity authentication (QIA) protocols. The logic of classical zero-knowledge proofs (ZKPs) due to Schnorr [9] 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 is achieved by moving away from the hardness of the Discrete Logarithm Problem towards the hardness of estimating quantum states. This paper presents a method with which this can be achieved and some bounds for the security of the protocol provided. 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 [5] 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 [5].

Schnorr introduced in [9] 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 [6].

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 [11]. 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 four and three respectively.

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 circuits are formed from products and tensor products of 2×2 unitary matrices, referred to as quantum gates (analogous to binary gates), preserving the unitary property [7].

Define the R_x gate as [7]:

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

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 gates $G_p(a)$ and $H_p(a)$ shall be utilised, defined as follows:

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

$$H_p(a) = R_x\Big((a \mod 2p) \times \frac{\pi}{p}\Big) \tag{4}$$

Intuitively, we split the π 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. The important thing to note here is that $G_p(a)G_p(b) = H_p(a+b)$, which can be made $G_p(a+b)$ by applying X if $(a+b \mod 2p) > p$. This will be useful later.

Let $k_p(n)$ be defined as

$$k_p(n) = \begin{cases} 0 & \text{if } (n \mod 2p) < p \\ 1 & \text{otherwise} \end{cases} \tag{5}$$

and let $C_m = X$ gate if $m = 1$, else $C_m = I$.

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.

As before, P wishes to prove they know x to V, in this case such that they can create a state $G_p(x)|0\rangle$. Both the gate G_p and value of p are known publicly.

1. $\underline{V \text{ selects}}$ random values c and n.

2. $\underline{V \to P}$: Let V have $|x\rangle = G_p(x)|0\rangle$, but no knowledge of x. V sends to P

$$|x + (c-1)n\rangle = G_p((c-1)n)\,|x\rangle \tag{6}$$

3. $\underline{P \to V}$ P selects some random r and sends the state:

$$|A\rangle = G_p(r)\,|x + (c-1)n\rangle \tag{7}$$

4. $\underline{V \to P}$: V sends c over a classical channel and sends the state

$$|S_1\rangle = G_p(n)\,|A\rangle$$

5. $\underline{P \text{ computes}}$ $s = r + cx$. Let $b = k_p(t)$ where

$$t = \Big((x \mod p) + (r \mod p) + (x(c-1) \mod p)\Big)$$

6. $\underline{P \to V}$: P sends s and b and then sends the state:

$$|S_2\rangle = G_p(x(c-1))\,|S_1\rangle$$

7. $\underline{V \text{ constructs}}$

$$|B\rangle = G_p(-cn)\,|S_2\rangle \tag{8}$$

and calculates

$$a = k_p\Big(((c-1)n \mod p) + (n \mod p) + (-cn \mod p)\Big) \tag{9}$$

8. $\underline{V \text{ checks}}$ that

$$G_p(p-s)C_{a\oplus b}\,|B\rangle = |1\rangle$$

by seeking a 1 under the normal z axis measurement.

4.1.1 Note on Notation

It should be made clear that the various states are applied successively to received states. Whilst combining rotations from distinct states is hard, applying rotations to received states is straightforward theoretically, especially for commutative gates that are in use here. Following, for example, a quantum teleportation operation receiving state $|\Psi\rangle$, we apply gate G_1 then G_2 to obtain $G_2G_1|\Psi\rangle$.

4.2 Correctness and Completeness

Lemma 4.1.

$$R_x(b)R_x(a)|0\rangle = R_x(a+b)|0\rangle \tag{10}$$

Proof.

$$\begin{aligned} R_x(a)|0\rangle &= \begin{pmatrix} cos(\frac{a}{2}) \\ -isin(\frac{a}{2}) \end{pmatrix} = |a\rangle \\ R_x(b)|a\rangle &= \begin{pmatrix} cos(\frac{a}{2})cos(\frac{b}{2}) - sin(\frac{a}{2})sin(\frac{b}{2}) \\ -i(cos(\frac{a}{2})sin(\frac{b}{2}) + sin(\frac{a}{2})cos(\frac{b}{2})) \end{pmatrix} \\ &= \begin{pmatrix} cos(\frac{a+b}{2}) \\ -isin(\frac{a+b}{2}) \end{pmatrix} \\ &= R_x(a+b) \end{aligned}$$

□

From this follows also the commutativity of single axis rotations

$$R_x(a)R_x(b) = R_x(b)R_x(a) \tag{11}$$

It then further follows that in equation (8)

$$G_p(x(c-1))|A\rangle = G_p(r)H_p(xc)|0\rangle \tag{12}$$

Next we need to take $H_p(r+xc)$ which is formed from full rotations about the x axis, and restrict it down to half-axis rotations. This is where C_b 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

$$XH_p(xc)G_p(r) = G_p(xc)G_p(r) \tag{13}$$

This gives us, given a correct choice of C_b

$$BC_b = G_p(xc+r) = G_p(s) \tag{14}$$

We use this for the *cn* construction also, noting that if both overflow then we need do nothing, and so use the XOR of our two evaluations as two overflows do not need correcting.

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

Theorem 4.2. *Let $C_{a\oplus b}$ be chosen appropriately as above. When V implements the protocol as outlined above the output will always be a $|1\rangle$ 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

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

By Lemma 4.1 and equation (13),

$$C_aG_p(-cn)G_p(n)G_p((c-1)n) = G_p(0)$$

It then follows that, equations (7) and (14):

$$\begin{aligned} &G_p(p-s)C_bG_p(x(c-1))G_p(x+r)|0\rangle \\ &\quad = G_p(p-(r+xc))G_p(r+xc)|0\rangle \\ &\quad = G_p(p) = R_x(\pi)|0\rangle = |1\rangle \end{aligned} \tag{15}$$

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 $|1\rangle$.

Therefore have a 1 measurement, modulo some error ϵ.

($\rightarrow$) If the measurement output is (almost) always 1 modulo some noise, then the states received from P by V matches the $|1\rangle$ state expected by V.

By equation (15) a $|1\rangle$ state, and subsequent 1 measurement means that everything required to line up in this scheme has done so, and P's proof is correct. □

4.3 Security

If we paraphrase Shannon [10], a perfectly secure zero-knowledge proof is one in which the information disclosed about x in a proof P is null, essentially

$$I(x;P) = 0$$

Whilst it may be correct for V to arrive at a $|1\rangle$ state, there are several considerations that make sure that only a party P who can generate a valid state $|x\rangle = G_p(x)|0\rangle$ can successfully complete a proof and satisfy verifier V, and that some attacker/eavesdropper cannot either discern the value

of x nor impersonate P maliciously by inserting themselves midway through a ZKP sequence.

With the advent of Shor's algorithm (see [7, Appendix 4]) it is clear that for the classical scheme due to Schnorr, 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, which this protocol attempts to provide.

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.

There are two sides to this proof scheme's security; a classical side and a quantum one. Let E denote some attacker/eavesdropper.

4.3.1 Classical Security

The classical security concerns the classical channels, and we assume some eavesdropper on these. The variables c and s can be publicly disclosed, as knowing c does not help you in discerning the secret x given the additive r that is used.

Theorem 4.3. *The classical security of the variables x, r, and n is that an attacker E has at most a $1/p$ chance to provide a malicious proof.*

Proof. There are three options classically for an attacker to try and pursue when attacking this protocol:

1. **Guess** x - this would be the most direct method, and would correctly compromise any proof from P. Given p is prime, there are p many options for both values but they can be checked against s given c is public. Therefore the probability of this occurring would be $1/p$.

2. **Guess** n - Focusing again on a PitM attack taking place after the initial state $|A\rangle$ was sent from P; E does not know n as it is multplied by c, and so cannot simply subtract the value. E could guess the value for n, then apply the following attack to defeat the proof:

   (a) The attacker knows c and correctly guesses n, chooses some t and then sends to V:

   $$|S_2\rangle = G_p(t)G_p(cn)\,|0\rangle$$

   (b) Set $s = t$ and $b = 0$, which completes a valid proof.

   There is a $1/p$ chance that this works.

3. **Guess** r - An unlikely attack, this would compromise the proof but only for one instance, and is only effective if the attacker graduates from eavesdropper to an active person-in-the-middle attack (PitM). As above, the likelihood this works is $1/p$.

By this argument, E has at best a $1/p$ chance to guess a value that could allow them to provide a valid malicious proof. □

4.3.2 Quantum Security

Next follows the analysis of the security of this system over noisy quantum channels - both error corrected and not.

I. Error Corrected Case

If we first assume an error corrected channel (*e.g.* using a scheme found in Calderbank and Shor [3]) then the security relies upon the fact that states are only transmitted once. As such, an attacker having to measure say $|A\rangle$ multiple times in order to produce any kind of valid amplitude estimation, *e.g.* in [1], becomes a very difficult attack vector. Given each value is only transmitted at most once in its original state such an attack is not viable, and so E would likely not attempt to carry it out.

Therefore the security in this case falls back to the classical case above.

II. The Noisy Case

For a given quantum channel that has noise, the probability that a qubit is successfully transmitted is $1 - \epsilon$, for some (hopefully) small error term ϵ. Whilst an attacker E listening in on the channel will raise the noise by means of incorrect guesses and interference, these may be detected by comparing the number of 0 measurements with an accepted bound given by the error. If we let P_{valid} represent a valid proof from the protocol in section 4, the fidelity of the protocol with noise can be characterised as the expectation

$$E\,\langle 1|\,P_{valid}\,|0\rangle = 1 - \epsilon$$

Note that the usual convention of talking about bit errors in our rotations does not apply necessarily to our axis rotation inputs x, r, n, or s. This is because an error of $G_p(a \pm 2^{w+1})$ would be considerably more noticeable from $G_p(a \pm 2^w)$ for most choices of w. Therefore we can assume that any channel noise will largely only affect the least significant bits of our single qubit rotation parameters.

Theorem 4.4. *Let p be given, and let the quantum channel error term $\epsilon = 1/e$, then there is at best a*

$$\frac{1}{p} + \frac{2p}{e^2}$$

chance that an attacker E can successfully pass an incorrect proof as a valid one to V in the scheme above.

Proof. To begin with let

$$\frac{1}{e} \geq \frac{1}{p}$$

Taking the most likely attack scenario in theorem 4.3, we may reason as follows; Suppose an attacker makes a close guess $cn_{guess} = cn \pm 1$, the resulting error in the final sum in equation 15 with noise ϵ will give measurement expectations of

$$\begin{aligned} E\langle 1|\, G_p(p)\, |0\rangle &= 1 - \epsilon \\ &\equiv E\langle 1|\, R_x((p \pm 1)\pi/p)\, |0\rangle \end{aligned} \tag{16}$$

With the error in the channel as above then this would not be distinguishable from the value of cn transmitted with noise.

Therefore the likelihood that the attacker chooses n_{guess} that is close enough to n to be masked by noise and thereby have a successful attack to give a malicious valid proof P_{valid} is the same as choosing n with no error $(1/p)$ or making one of two valid choices from $\{cn-1, cn+1\}$ with noise masking it:

$$Pr(P_{valid}|cn_{guess}) = \frac{1}{p} + \frac{2}{e} = \frac{2p+e}{pe}$$

For e close to p, this would be around $3/p$, which is what should be expected.

However, in general we may find that $e > p$. Thereby this $2/e$ term decomposes as two instances of the proportion of p to e over e, or $\frac{p}{e^2}$; one for the likelihood of E guessing $n+1$ and one for guessing $n-1$. This gives a combined upper bound of

$$Pr(P_{valid}|n_{guess}) = \left(\frac{1}{p} + \frac{2p}{e^2}\right) \tag{17}$$

□

Note that because the 'guess n' attack only affects one quantum transmission, we only need to consider the error once.

4.3.3 Considerations Within the Protocol

There are a number of security considerations within the protocol that we will state here.

With the communications being hybrid classical and quantum, so is our 'challenge'. Thereby we have to values, c and n that are both used in tandem to provide the challenge to P that can only be resolved if P knows x. To prevent P disregarding the $|x\rangle$ that V has, this challenge is commited to at the start of the protocol, and unwound fully at the end.

The choice of r is never transmitted classically, and so is totally unknown to V. Likewise, n is totally unknown to P, and even if P is malicious they cannot unwind $G_p(cn)$ as P is unaware how many times to apply $G_p(-c)$ as they do not know n.

Therefore by delivering $G_p((c-1)n)$ at first, P cannot simply prove they know *any* x, just specifically the one that V has in $|x\rangle$ at the start. Thereby, whilst r creates a lock on this particular proof for P, c and n create a hybrid quantum-classical zero-knowledge challenge for P to provide a resolution to.

It should be noted that if V has some gate U_x such that, without knowing x, V may obtain

$$U_x\, |0\rangle = G_p(x)\, |0\rangle$$

then some steps in the protocol become unnecessary, as V can just construct $G_p(xc)$ themselves - they only need to receive state $|A\rangle$ and s. The author is, however, unaware of how this could be achieved without falling afoul to a protracted quantum amplitude estimation attack, for example.

4.3.4 Overall Security

The attack likelihood given in theorem (4.4) is the combined 'worst-case' scenario for the protocol presented in this paper.

By theorem (4.4) as p increases and/or ϵ decreases then the number of repetitions required to validate a proof decreases according to the required confidence level.

For a 5σ confidence, with an additive noise error of ϵ as defined in theorem 4.4 we would need N-many iterations such that

$$\left(\frac{1}{p} + \frac{2p}{e^2}\right)^N < 5.733 \times 10^{-7}$$

This would give us the highest confidence that P was both honest and knew a value for x.

By analysing the effects of noise and how an attacker may leverage these, we can see the extent to which an attacker can 'hide' in noise. Any other interference in the quantum transmissions will raise the noise floor sufficiently that it goes above some calibrated value for ϵ, which would invalidate the proof for V.

The argument presented here 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 along with the classical security.

Note, because the security relies on the statistical likelihood of zero measurements, the protocol is fail safe for sufficiently high values of ϵ above a predetermined noise value from the communication channel.

4.4 Soundness and ZK

There are two conditions that ZKPs must aspire to:

- soundness - that P can only convince V if they really do know a given x and behave honestly, except for some small probability.
- zero-knowledge - that an neither V nor an eavesdropper E can learn anything about the secret x.

Both of these follow naturally from the details in section 4.3.

Soundness follows directly from the limits given in theorems 4.3 and 4.4, specifically that the only reliable way to attain the correct measurements within error tolerances is for P to provide an honest proof.

Similarly, owing to the structure of s in relation to p and the minimal number of quantum communications from which any value of x could be estimated, the zero-knowledge condition is satisfied.

4.5 Remarks

4.5.1 Mutual ZKP

Future developments may involve developing the protocol and extending it slightly such that both parties can verify each other - take the challenge committed to in n by V. With the addition of another c_2 term from P, P could also validate V concurrently for the potential of mutual authentication.

4.5.2 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 [8]. The resolution of the qubits and their longevity is taken into account by some benchmarks, such as 'Quantum Volume' [4]. 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.

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. The protocol in this paper has shown a method to swap out the use of a generator g in Schnorr's scheme for a qubit rotation, and the extra steps required to make a zero-knowledge proof work with currently available algorithms. This system has been shown to have some additional benefits over purely classical approaches, despite its classical origins.

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. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, Aug. 1996.

[4] 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.

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

[6] 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.

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

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

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

[10] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, Oct. 1949.

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