On Zero-Knowledge Proofs over the Quantum Internet

Mark Carney[1] [1]Quantum Village, mark@quantumvillage.org

Abstract

This paper presents a new method for quantum identity authentication (QIA) protocols. The logic of classical zero-knowledge proofs (ZKPs) due to Schnorr [3] 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.

Background

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.

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 [2].

ZKPs have been used to create quantum proof systems that have also been shown to be possible in a quantum setting [4]. 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.

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 in [3]:

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

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

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

Preliminaries

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

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

$$H_p(a) = R_x\Big((a \mod 2p) \times \frac{\pi}{p}\Big) \tag{3}$$

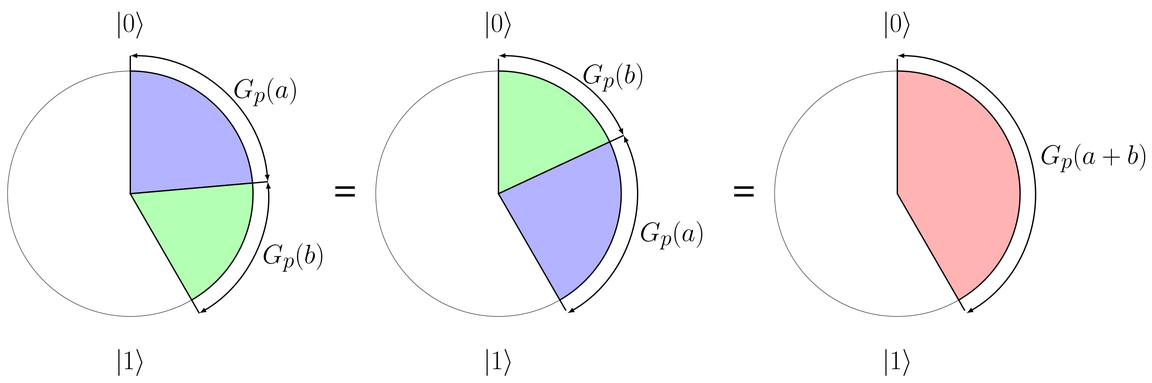
Let $k_p(n)$ be defined as

$$k_p(n) = \begin{cases} 0 & \text{if } (n \mod 2p) < p \\ 1 & \text{otherwise} \end{cases} \tag{4}$$

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

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 $(a+b \mod 2p) > p$.

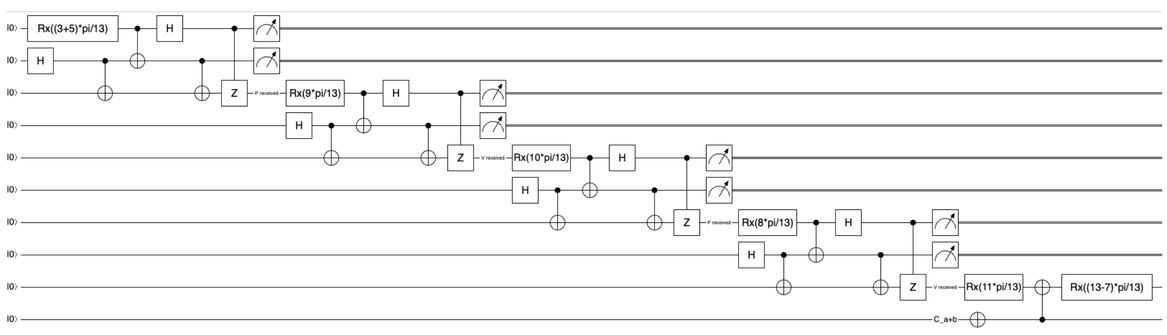
This picture illustrates this equivalence:



Protocol

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.

This protocol can be viewed as the following circuit (using quantum teleportation between Alice and Bob), and is given in full in table 1:



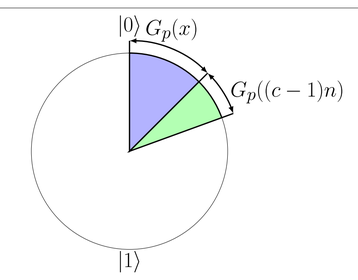
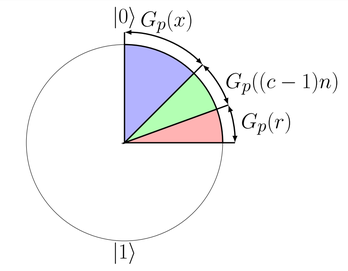
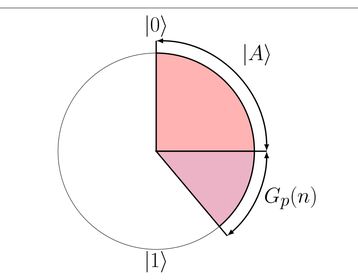
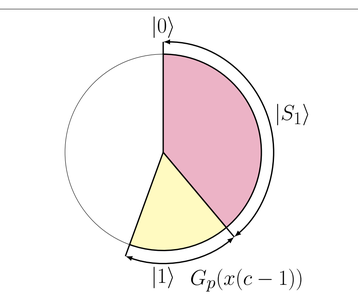
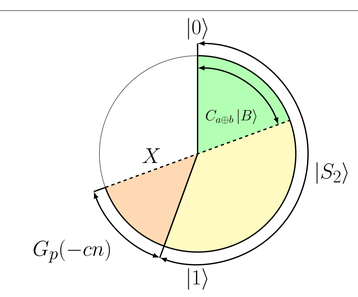
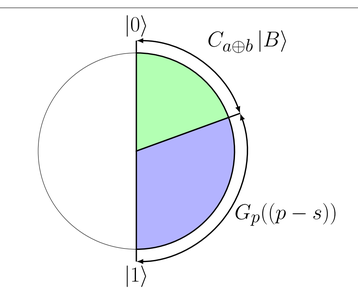
Step	Action	Qubit
1	$\underline{V \text{ selects}}$ random values c and n.	
2	$\underline{V \to P}$: Let V have $\|x\rangle = G_p(x)\,\|0\rangle$, but no knowledge of x. V sends to P: $\|x + (c-1)n\rangle = G_p((c-1)n)$	
3	$\underline{P \to V}$ P selects some random r and sends the state: $\|A\rangle = G_p(r)\,\|x + (c-1)n\rangle$	
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	$\underline{V \text{ constructs}}$ $\|B\rangle = G_p(-cn)\,\|S_2\rangle$ and calculates $a = k_p\Big(((c-1)n \mod p) + (n \mod p) + (-cn \mod p)\Big)$	
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.	

Table 1: Table showing the QZKP protocol.

Security and Correctness Proofs

Our work prepares several steps to prove the correctness, completeness, zero knowledge, and security of the protocol, captured by the following theorems:

Theorem 0.1. *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.*

Theorem 0.2. *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.*

Theorem 0.3. *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.*

Considerations

Of course, modern hardware for Quantum Networking is not yet sufficient for this protocol to take place. There are 3 quantum and 3 classical exchanges, which adds significant error without sufficient error correction, for example in [1].

References

[1] A. R. Calderbank and P. W. Shor. "Good quantum error-correcting codes exist". In: *Physical Review A* 54.2 (Aug. 1996), pp. 1098–1105.

[2] A. Dutta and A. Pathak. *A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice?* 2021.

[3] C. P. Schnorr. "Efficient Identification and Signatures for Smart Cards". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Springer New York, 1989, pp. 239–252.

[4] J. Watrous. *Zero-knowledge against quantum attacks*. 2005.