Comment on "Scheme of the arrangement for attack on the protocol BB84"

Jonte Hance[1, *] and John Rarity[1]

[1]*Quantum Engineering Technology Laboratory, Department of Electrical and Electronic Engineering,*
University of Bristol, Woodland Road, Bristol, BS8 1UB, UK

In a recent paper (*Scheme of the arrangement for attack on the protocol BB84*, Optik 127(18):7083-7087, Sept 2016), a protocol was proposed for using weak measurement to attack BB84. This claimed the four basis states typically used could be perfectly discriminated, and so an interceptor could obtain all information carried. We show this attack fails when considered using standard quantum mechanics, as expected - such "single-shot" quantum state discrimination is impossible, even using weak measurement.

In his recent paper, Khoklhov claims to have developed a protocol that can be used to distinguish between the four basis states used in BB84 to encode information - the H-, V-, D- and A-polarised states of a single photon [1]. He claims this is through weak measurement - where weak coupling of a quantum variable to an ancilla allows data about a quantum state to be obtained without collapsing the state. However, weak measurement typically only obtains a small amount of information per measurement, so a large number of identically-prepared quantum objects are needed to obtain this fully. An alternative proposal given by Aharonov et al discusses the possibility of performing a weak measurement on a single particle [2] - however, this is still subject to Busch's limit on information gained for a given disturbance [3].

Khoklhov previously gave an interferometric device that he claims allows a weak measurement to tell the path a photon travelled via, without disturbing the state of that photon (see Fig.1a) [4]. For this, a photon of state $\alpha \left| H \right\rangle + \beta \left| V \right\rangle$ goes through a polarising beamsplitter (PBS), which transmits H- and reflects V-polarised components. The two components each travel down a respective arm, where they have a momentum-kick applied to them, such that their eventual arrival position on the second PBS isn't affected - here, the H-component gets a downwards kick, and the V-component an upwards kick. The two components meet at the second PBS, recombine, and then exit, but the difference in momentum allows, at a far distance from the second PBS, the respective components to be identified. Khoklhov claims, by using many photons, this allows the probability amplitudes of the two polarisation components to be determined, and so the preparation state (in truth, we only get the moduli-squared of those components, and so the classical balance of probabilities). Further, Khoklhov implies that the photon emitted into one of the two distinguishable far-field paths would still be in its original state, rather than collapsed to either H or V. This is also incorrect - as the polarisation becomes entangled with the momentum degree-of-freedom, the collapse to either upwards- or downwards-momentum causes the simultaneous collapse to either H- or V-polarisation.

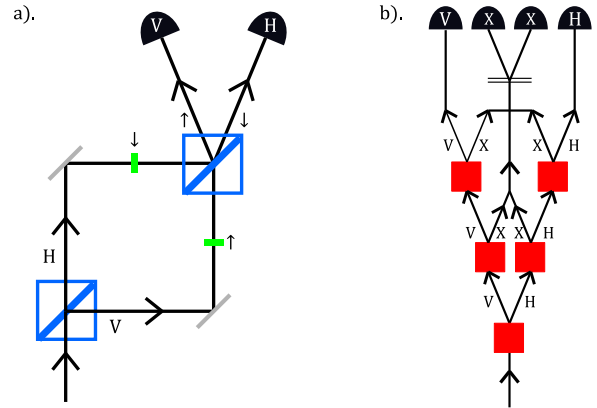In this paper, Khoklov then makes the bold claim that,

FIG. 1. Diagrams of a) the single-interferometer device, which forms the building blocks of the attack protocol, and b) the layout formed of these, where each red square is an interferometer of the sort given in a. As can be seen, once initially split by the first interferometer, the H and V components remain these separate components, and so never travel the paths marked X. Therefore, only two of the four detectors ever receive photons, making the protocol useless for determining the full initial state for a single photon.

using these single-interferometer units as building blocks, he can make a device which can perfectly distinguish between the four basis states used in BB84 - H, V, D (or $\frac{H+V}{\sqrt{2}}$) and A (or $\frac{H-V}{\sqrt{2}}$). Given the security of BB84 rests on the quantum assumption that, even with an optimal choice of measuring basis, one cannot distinguish between all four bases perfectly (thus bounding an eavesdropper's potential knowledge), this claim threatens the security of one of the most well-known QKD protocols.

Khoklhov claims this is possible by taking the separated outputs of one of his single-interferometer devices, then putting each output through another device. Those outputs which disagree with their original polarisation-determination (due to his assumption that the photon exits in its original state) are then combined - the components which agree with their original polarisation are put through another device, and again have any further outputs which disagree combined. The combined

beam is then put through a polarising beamsplitter in the $A - D$ basis, with its two outputs sent to detectors, alongside the other two outputs (that always agreed with their initially-determined polarisation). We present this in Fig.1b. Khoklhov claims that if the input photon's initial state is D (A) it will end up in the inner left (right) detector. This claim is false.

Let us examine the path of the input photon using standard quantum mechanics (as represented by Bra-Ket notation). We can describe the action of one of Khoklhov's single-interferometer devices (pre-detection), as given in Fig.1a, on a single polarisation-encoded photon qubit by

$$\alpha \left|H\right\rangle + \beta \left|V\right\rangle \rightarrow \alpha \left|H, \downarrow\right\rangle + \beta \left|V, \uparrow\right\rangle \tag{1}$$

This effectively entangles the polarisation and path degrees of freedom. Applying this to the larger set-up (as given in Fig.1b), we then see the two components (H and V) then act as separate for the remainder of the chain, obeying

$$\alpha \left|H\right\rangle + \beta \left|V\right\rangle \rightarrow \alpha \left|H, R, R, R\right\rangle + \beta \left|V, L, L, L\right\rangle \tag{2}$$

where L and R describe the paths on the figure after each interferometer. This means the inner paths, $\left|R, L\right\rangle$, $\left|L, R\right\rangle$, $\left|L, L, R\right\rangle$ and $\left|R, R, L\right\rangle$ are never explored, so the two inner detectors never click. Given the determination of the single photon's polarisation qubit in the attack is predicated on these two detectors being able to click (being taken to represent $\frac{H+V}{\sqrt{2}}$ and $\frac{H-V}{\sqrt{2}}$), this shows the attack does not work - as expected, standard quantum mechanics preserves the security of BB84 from this attack.

We finally give a more proper account of the result of using true weak measurements to attempt Khoklhov's scheme, using the description of weak measurement from [5].

To do this, in each of Khoklhov's apparatuses, we couple our photon's polarisation

$$\left|\psi\right\rangle \in \{\left|H\right\rangle; \left|V\right\rangle; \frac{\left|H\right\rangle + \left|V\right\rangle}{\sqrt{2}}; \frac{\left|H\right\rangle - \left|V\right\rangle}{\sqrt{2}}\}$$
$$= \alpha \left|H\right\rangle + \beta \left|V\right\rangle \tag{3}$$

with the pointer (the photon's momentum)

$$\left|\phi\right\rangle = \left|\phi_d\right\rangle = \int_p \phi(p) \left|p\right\rangle dp \tag{4}$$

where p is the vertical momentum of the photon. $\hat{P}_d$ is the momentum operator such that $\hat{P}_d \left|p\right\rangle = p \left|p\right\rangle$.

We assume $\phi(p)$ has a Gaussian distribution around 0

(input vertical momentum), such that

$$\phi(p) = e^{-p^2/4\sigma^2}/\sqrt{2\pi\sigma^2} \tag{5}$$

If we define the polarisation-distinguishing operator

$$\hat{A} = \left|H\right\rangle\!\left\langle H\right| - \left|V\right\rangle\!\left\langle V\right| \tag{6}$$

we can consider an interaction Hamiltonian between the two

$$\hat{H}_{int} = g(t)\hat{A} \otimes \hat{X}_d \tag{7}$$

where $\hat{X}_d$ is the operator conjugate to $\hat{P}_d$ such that $[\hat{P}_d, \hat{X}_d] = i\hbar$, and $g(t)$ is the coupling function such that

$$\int_0^T g(t)dt = 1 \tag{8}$$

for coupling time T.

This means, applying this Hamiltonian

$$e^{i\hat{H}t/\hbar} \left|\psi\right\rangle \otimes \left|\phi\right\rangle \tag{9}$$

we see for each of $\left|H\right\rangle \otimes \left|\phi(p)\right\rangle$, $\left|V\right\rangle \otimes \left|\phi(p)\right\rangle$, the Hamiltonian takes $\hat{P}_d$ to $\hat{P}_d + 1$, $\hat{P}_d - 1$ respectively, as

$$\hat{P}_d(T) - \hat{P}_d(0) = \int_0^T \frac{i}{\hbar}[\hat{H}, \hat{P}_d]dt \in \{+1, -1\} \tag{10}$$

Therefore, the corresponding transformation is

$$e^{i\hat{H}t/\hbar} \left|\psi\right\rangle \otimes \left|\phi(p)\right\rangle$$
$$= \alpha \left|H\right\rangle \otimes \left|\phi(p-1)\right\rangle + \beta \left|V\right\rangle \otimes \left|\phi(p+1)\right\rangle$$
$$= \int_p \left(\alpha \left|H\right\rangle \otimes \phi(p-1) + \beta \left|V\right\rangle \otimes \phi(p+1)\right) \left|p\right\rangle dp \tag{11}$$

The above wavefunctions $\phi(p-1)$ and $\phi(p+1)$ need to overlap each other for the measurement to be weak - and so need to have high variance, σ. The higher the variance, the weaker the measurement - if these Gaussian wavefunctions don't overlap, them the measurement is strong. Given σ is initially defined from the vertical momentum of the photon, this means the photon input into the system must also have high σ.

The effect of the strength of the measurement can be most readily seen when observe and collapse the pointer to a specific momentum-value, p_0, to read out our weak measurement, which gives

$$\left(e^{-\frac{(p_0-1)^2}{4\sigma^2}} \alpha \left|H\right\rangle + e^{-\frac{(p_0+1)^2}{4\sigma^2}} \beta \left|V\right\rangle\right) \otimes \left|p_0\right\rangle \tag{12}$$

where both the coefficients on $\left|H\right\rangle$ and $\left|V\right\rangle$ are biased slightly depending on where they are in relation to p_0. This makes sense, analogous to how measuring an eigenvalue for an observable collapses the measured state to the relevant eigenstate - the only difference here is the

variance σ providing some uncertainty in that measurement.

The far-field vertical position of the photon will depend on the vertical momentum of the photon, as Khoklhov rightly says. However, the variance in this momentum (which must be large enough to allow overlap between the momenta for up and for down in order for the measurement to be weak, and the final polarisation state to not have changed too far) means that these positions must overlap heavily too. While, in the limit of many identically-prepared photons, we could obtain information about whether the polarisation-state was $|H\rangle$, $|V\rangle$, or a superposition of the two, we cannot gain this for a single run without inducing collapse. Therefore, a protocol built up of several of these devices, as Khoklhov's attack protocol is, either doesn't work due to collapse (as we show with the standard quantum-mechanical approach above), or gains effectively no information about the polarisation state of the photon, making it useless as an attack.

---

* jonte.hance@bristol.ac.uk

[1] Dmitri L Khokhlov. Scheme of the arrangement for attack on the protocol bb84. *Optik*, 127(18):7083 – 7087, 2016.

[2] Yakir Aharonov, Eliahu Cohen, and Avshalom C Elitzur. Foundations and applications of weak quantum measurements. *Physical Review A*, 89(5):052105, 2014.

[3] Paul Busch. "no information without disturbance": Quantum limitations of measurement. In *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle*, pages 229–256. Springer, 2009.

[4] DL Khokhlov. Scheme of the weak measurement of the polarization state of the photon. *Optik*, 127(8):4089–4091, 2016.

[5] Boaz Tamir and Eliahu Cohen. Introduction to weak measurements and weak values. *Quanta*, 2(1):7–17, 2013.