Journal of Physics: Conference Series

Magnon-Photon interactions for Quantum Key Distribution

To cite this article: P Kumar and A Prabhakar 2011 *J. Phys.: Conf. Ser.* **303** 012040

View the article online for updates and enhancements.

Magnon-Photon interactions for Quantum Key Distribution

P. Kumar[1] **and A. Prabhakar**[2]

[1]Department of Electrical Engineering, I.I.T. Kanpur, Kanpur-208016, India
[2]Department of Electrical Engineering, I.I.T. Madras, Chennai-600036, India

E-mail: [1]pradeepk@iitk.ac.in [2]anilpr@iitm.ac.in

Abstract. We propose an implementation of quantum key distribution (QKD) protocol using magnon-photon interactions in dielectric waveguides. Starting from the Hamiltonian of spin wave–optical interactions in a symmetric dielectric waveguide, we derive the single-photon transformations that allow us to define two non-orthogonal basis sets, which are isomorphic to polarization basis of single-photon. Implementation of the BB84 and B92 protocols is then straightforward. The principal advantage of our scheme is the higher quantum bit error rate (QBER) (37.5%) compared to polarization-coded scheme (25%) for simple intercept/resend attack. This considerably relaxes the specifications of optical components. Finally, we consider the effect of low conversion efficiency on QBER.

1. Introduction

Spin waves (SWs) are excitations in magnetic materials. SW–optical interactions in waveguides, specifically in heterostructures made of magnetic material such as YIG, is used in applications such as optical isolators, mode converters, filters, frequency shifters etc., and has been widely studied [1–6]. More recently, there has been a lot of work on spin wave propagation in metallic thin films. However, the magnon-photon interactions in metallic films are typically based on Brillouin scattering (BLS). In this paper, we describe the use of collinear propagating optical and spin waves to implement BB84 and B92 quantum key distribution (QKD) protocols. We also estimate the quantum bit error rate (QBER) of the proposed scheme, demonstrating how a similar estimate can be obtained in other magnon-photon interactions.

In the BB84 QKD protocol [7], key bits, $\{0,1\}$ are encoded as one of the four non-orthogonal states–$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, grouped into two basis sets, $\mathcal{B}_1 = \{|0\rangle, |1\rangle\}$ and $\mathcal{B}_2 = \{|+\rangle, |-\rangle\}$ such that,

$$\langle 0|1\rangle = \langle +|-\rangle = 0, \quad \text{and} \quad \langle i|j\rangle \neq 0, \; i = \{0,1\}, \; j = \{+,-\}.$$

In the B92 protocol [8], key bits are encoded using only two non-orthogonal states, say $\{|0\rangle, |+\rangle\}$. SW–optical interactions provide a convenient way to generate the non-orthogonal states by coupling the TE and TM optical modes. The TE$\rightleftharpoons$TM mode coupling has been studied both theoretically and experimentally in the classical regime [6, 9]. Recently, we extended the treatment to the interaction of SWs with quantized optical TE and TM modes [10] and described magnon-photon interactions as:

$$
\begin{aligned}
|\omega_0 - \Omega\rangle_{\mathrm{TM}} &\to \frac{1}{\sqrt{2}}\left(|\omega_0\rangle_{\mathrm{TE}} - |\omega_0 - \Omega\rangle_{\mathrm{TM}}\right) \equiv |-\rangle \\
|\omega_0\rangle_{\mathrm{TE}} &\to \frac{1}{\sqrt{2}}\left(|\omega_0\rangle_{\mathrm{TE}} + |\omega_0 - \Omega\rangle_{\mathrm{TM}}\right) \equiv |+\rangle\,,
\end{aligned}
$$

where Ω is the angular frequency of SWs (rad/m). These states are formally isomorphic to the states of polarization of a single-photon and can therefore be used to implement both BB84 and B92 QKD protocols. The principal advantages of our proposed scheme are:

- improved key rate since SW–Optical interaction occurs at over 25GHz,
- single-sideband scheme without use of optical filtering at the transmitter as opposed to the schemes that use electro-optic modulators, and
- a QBER of 37.5% for intercept/resend attack, which relaxes specifications on the optical components.

These advantages are offset to somewhat from a low TE⇌TM mode conversion efficiency which introduces an "intrinsic" QBER.

2. SW–Optical interactions in a waveguide

The optical modes of the symmetric waveguide can be quantized starting with Maxwell equations and following a canonical procedure leading to the Hamiltonian,

$$
H_0 = \sum_m \hbar\omega_m \left(a^\dagger_{xm}a_{xm} + a^\dagger_{ym}a_{ym}\right), \tag{1}
$$

where the first and second terms represent transverse magnetic (TM) and transverse electric (TE) modes respectively [11]. In the collinear geometry, spin waves (SWs) propagating parallel to the optical modes lead to TE⇌TM mode conversion [6, 12]. When the SW has the form, $\mathbf{M}(t) = M_S\hat{\mathbf{x}} + m_y\hat{\mathbf{y}} + m_z\hat{\mathbf{z}}$, where the small signal components are time varying, and M_S is the saturation magnetization, the SW–optical interaction can be modeled by the effective permittivity tensor,

$$
\bar{\epsilon} = \epsilon_0 \begin{pmatrix} \epsilon_r & -jfm_z & jfm_y \\ jfm_z & \epsilon_r & jfM_S \\ -jfm_y & jfM_S & \epsilon_r \end{pmatrix},
$$

where we have assumed that the medium is isotropic in the absence of SW excitation and $m_y, m_z \ll M_s$. Assuming that TE ⇌TM mode conversion is due only to the SW–optical interactions, the interaction Hamiltonian is given by,

$$
H_{\mathrm{int}} = \int_V dv \frac{1}{2}\epsilon_0(-jfm_zE^*_xE_y),
$$

where $m_z(t) = m_{0z}(x)\exp(j(\mathbf{k}_{\mathrm{SW}}\cdot\mathbf{r} - \Omega t))$ is the SW and $\mathbf{k}_{\mathrm{SW}}$ and Ω are the SW vector and angular frequency respectively. Replacing the classical fields by the respective quantized mode operators and carrying out the integration, we obtain,

$$
H_{\mathrm{int}} = j\hbar\sum_{m,n}\left(\gamma_{mn}a^\dagger_{ym}a_{xn} - \gamma^*_{mn}a^\dagger_{xm}a_{yn}\right), \tag{2}
$$

where γ_{mn} is the coupling coefficient between TE$_m$ and TM$_n$ modes. In writing (2), we have assumed energy and momentum conservation relations,

$$
\omega^{(m)}_{\mathrm{TE}} - \omega^{(n)}_{\mathrm{TM}} \mp \Omega = 0, \text{ and } \left(\mathbf{k}^{(m)}_{\mathrm{TE}} - \mathbf{k}^{(n)}_{\mathrm{TM}} \mp \mathbf{k}_{\mathrm{SW}}\right)\cdot\hat{\mathbf{z}} = 0.
$$

Under the *tight-binding approximation* [12], we can write (2) as

$$H_{\text{int}} = j\hbar \left(\gamma \left|x\right\rangle \left\langle y\right| - \gamma^* \left|y\right\rangle \left\langle x\right|\right), \tag{3}$$

where $|x\rangle$ and $|y\rangle$ denote the TM and TE modes respectively and we have dropped the subscript m for notational simplicity. A general state vector,

$$|\psi(t)\rangle = A(t)\,|x\rangle + B(t)\,|y\rangle\,, \quad |A(t)|^2 + |B(t)|^2 = 1 \;\; \forall\, t,$$

evolves according to the Schrödinger's equation:

$$j\hbar \frac{\partial}{\partial t}\,|\psi(t)\rangle = H_{\text{int}}\,|\psi(t)\rangle\,. \tag{4}$$

Using (3), the general solution of the coefficients, $A(t)$ and $B(t)$ are

$$A(t) = C\cos(\kappa' t) + D\sin(\kappa' t), \tag{5a}$$

$$B(t) = e^{-j\phi}\left[C\sin(\kappa' t) - D\cos(\kappa' t)\right], \tag{5b}$$

where $\gamma = \kappa' e^{j\phi}$, and C and D are constants which depend on the initial conditions and we have absorbed $j\hbar$ into the definition of γ. Taking $\phi = 0$, the TE and TM mode conversions are indicated in Table. 1.

Initial state ($t = 0$)	Final state ($t = T$)
TE, $\|\omega_0\rangle$	$\cos(\kappa' T)\,\|\omega_0\rangle - \sin(\kappa' T)\,\|\omega_0 - \Omega\rangle$
TM, $\|\omega_0 - \Omega\rangle$	$\sin(\kappa' T)\,\|\omega_0\rangle + \cos(\kappa' T)\,\|\omega_0 - \Omega\rangle$

Table 1. TE and TM mode conversions.

3. Implementing BB84 and B92 protocols

Adjusting the values of coupling coefficient so that $\kappa' T = \pi/4$, we obtain the transformations:

$$|\omega_0 - \Omega\rangle_{\text{TM}} \rightarrow \frac{1}{\sqrt{2}}\left(|\omega_0\rangle_{\text{TE}} - |\omega_0 - \Omega\rangle_{\text{TM}}\right) \equiv |-\rangle \tag{6a}$$

$$|\omega_0\rangle_{\text{TE}} \rightarrow \frac{1}{\sqrt{2}}\left(|\omega_0\rangle_{\text{TE}} + |\omega_0 - \Omega\rangle_{\text{TM}}\right) \equiv |+\rangle\,, \tag{6b}$$

where we have explicitly identified the TE and TM modes. We define two non-orthogonal bases, $\mathcal{B}_1 = \{|\omega_0\rangle\,, |\omega_0 - \Omega\rangle\}$ and $\mathcal{B}_2 = \{|+\rangle\,, |-\rangle\}$ which transform a second time after interacting with the SWs to

$$|+\rangle \rightarrow |\omega_0\rangle\,, \;\text{ and }\; |-\rangle \rightarrow -\,|\omega_0 - \Omega\rangle\,. \tag{7}$$

This is equivalent to measuring the kets $|+\rangle$ and $|-\rangle$ in the "diagonal" basis $\mathcal{B}_2$. Detecting without remodulating $|\omega_0\rangle$ and $|\omega_0 - \Omega\rangle$ is equivalent to measuring them in the basis $\mathcal{B}_1$. Thus, the states in bases $\mathcal{B}_1$ and $\mathcal{B}_2$ are isomorphic to the state of polarization of a photon and are suited to implement both BB84 and B92 protocols.

Fig. 1 shows the transmitter and receiver structures to implement BB84 protocol. We first fix the encoding scheme. In basis $\mathcal{B}_1$ and $\mathcal{B}_2$, bit 0 is encoded by $|\omega_0\rangle$ and $|+\rangle$, and bit 1 is encoded by $|\omega_0 - \Omega\rangle$ and $|-\rangle$, respectively.

- Alice picks a basis $\mathcal{B}_1$ or $\mathcal{B}_2$ at random with equal probability. She does so by choosing between the two lasers emitting photons at frequencies ω_0 and $\omega_0 - \Omega$, polarized TE and TM respectively as shown in Fig. 1.
- Alice transmits the key bit 0 or 1 in the chosen basis. She does so by choosing to modulate or not the photons. Modulating the photons generates the states in basis $\mathcal{B}_2$ as given in Table. 1. This is shown in Fig. 1 where a RNG drives the VCO of frequency Ω rad/s. The setup is similar to the classical TM$\rightleftharpoons$TE conversion as described in the literature [6, 12].
- Alice transmits the state generated in the above step over an optical fiber.
- Bob uses a filter, say Fabry-Perot fibre grating, to separate the photons into two channels ω_0 and $\omega_0 - \Omega$.
- Bob corrects for polarization fluctuations in each channel using a polarization compensation unit (PCU), re-combines them and recovers the state transmitted by Alice.
- Bob modulates the state only half the time, but at random. He is thus choosing between basis $\mathcal{B}_1$ and $\mathcal{B}_2$ at random.
- Bob separates the photons, again using a filter, and feeds it to two detectors D_0 and D_1.
- Bob communicates to Alice whether he modulated the photons, or not, as bits 1 and 0. However, he does not communicate the results of his detection.
- Alice and Bob retain the time slots in which the basis match to form the sifted bits.
- Alice and Bob perform privacy amplification and error correction on the sifted bits to arrive at the final key.

Alice and Bob retain only 4 out of the 8 possible cases, i.e., the link has a 50% efficiency. These four cases are summarized in Table. 2. Note however that the QBER is estimated not on the full system, but after sifting, i.e., on these 4 cases. To implement B92 protocol, Alice and Bob encode the bits as two non-orthogonal states, say $|\omega_0\rangle$ and $|+\rangle$.

Table 2. Possible cases in the SW–optical interaction based BB84 protocol.

Alice's basis	$\mathcal{B}_2$	$\mathcal{B}_2$	$\mathcal{B}_1$	$\mathcal{B}_1$
Alice's bit	0	1	0	1
Txd state	$\|+\rangle$	$\|-\rangle$	$\|\omega_0\rangle$	$\|\omega_0 - \Omega\rangle$
Bob modulation?	Y	Y	N	N
Bob's state	$\|\omega_0\rangle$	$-\|\omega_0 - \Omega\rangle$	$\|\omega_0\rangle$	$\|\omega_0 - \Omega\rangle$
$\langle\omega_0\rangle$	1	0	1	0
$\langle\omega_0 - \Omega\rangle$	0	1	0	1
Sifted bits	0	1	0	1

4. QBER for intercept/resend attack

In a conventional intercept/resend attack, Eve intercepts a subset of the quantum bits transmitted by Alice, measures them in her chosen basis, and transmits to Bob a fabricated pulse in the same state as her result. In doing so, she introduces errors in the sifted bits, characterized by quantum bit error rate (QBER). It can be shown that Eve introduces a QBER of 25% in polarization coded scheme, if her basis is the same as Alice. Assuming that Eve uses the same basis as Alice and Bob, we can determine the QBER of our scheme subject to intercept/resend attack. We note the following:

- Alice is transmitting in basis $\mathcal{B}_1$. If Eve does not modulate the incoming photon, she does not change the state. However, she must still subject the intercepted photons to detectors

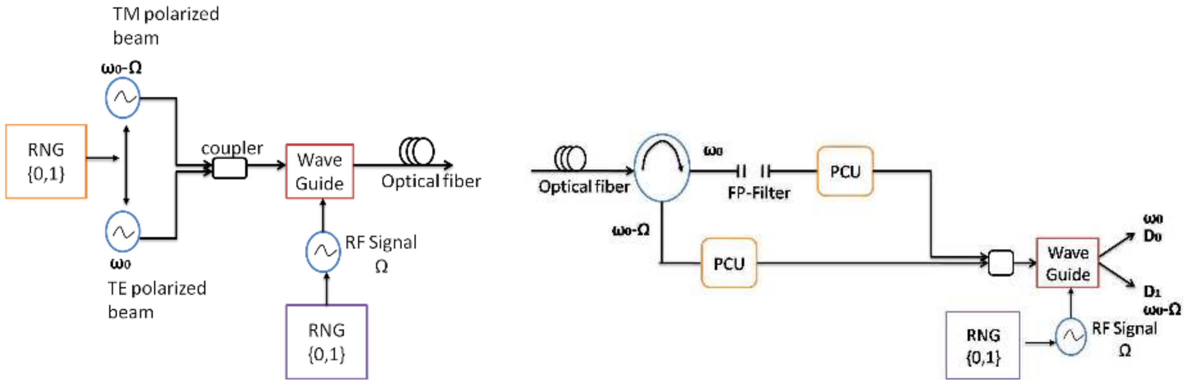

Figure 1. Transmitter and receiver to implement BB84 protocol. RNG=random number generator, FP=Fabry-Perot, D_0 and D_1 are single-photon detectors [10]. (©IEEE.)

D_0 and D_1 in order to distinguish between $|\omega_0\rangle$ and $|\omega_0 - \Omega\rangle$. For the intercepted pulse, Eve transmits a photon in the same state that she detects.

- Alice is transmitting in basis $\mathcal{B}_2$. If Eve does not modulate the incoming photon, she collapses the state into one of the sidebands–ω_0 and $\omega_0 - \Omega$. She then transmits in the same state that she detects. On the other hand, if she modulates the incoming photon, she again collapses the state into one of the sidebands, depending on the state Alice has transmitted.
- Thus, in both cases, Eve effectively transmits in basis $\mathcal{B}_1$. This is completely different from the polarization-coded setup in which Eve sends fabricated pulse in both the bases.

In Fig. 2, we show the results of Eve's intercept/resend attack. We have not indicated the outputs when Alice and Bob's bases differ, since they do not contribute to the sifted key. Similar results are obtained if Alice transmits the remaining kets: $|\omega_0\rangle$ and $|+\rangle$. We see that Eve's intercept/resend attack introduces a QBER of $\simeq 37.5\%$ in the sifted bit string. This is different from the QBER of polarization coded scheme with intercept/resend attack. The difference is due to the fact that Eve introduces errors even if she chooses the same basis as Alice(See Fig. 2). Further, we can show that any other strategy for Eve will result in higher error probability than 37.5%. For example, if Eve sends Bob a modulated photon whenever she modulates the photon from Alice, she introduces error of at least 50%. Thus, the intercept/resend strategy described in Fig. 2 represents the minimum error probability introduced by Eve as long as she uses the same basis as Alice and Bob.

It is instructive to consider the effect of low conversion efficiency on the BEP of the scheme. Due to low conversion efficiency, Alice will not be able to prepare states in $\mathcal{B}_2$ by modulating the states in $\mathcal{B}_1$. We take the worst case scenario in which Alice cannot transform the states $|\omega_0 - \Omega\rangle$ and $|\omega_0\rangle$ into the states $|+\rangle$ and $|-\rangle$ respectively. The "intrinsic" QBER, when Alice sends $|\omega_0 - \Omega\rangle$ instead of the ideal state $|+\rangle$ can be seen to be $\simeq 33.33\%$ from Table. 3. We note that ideally, Bob would transform the states $|\omega_0 - \Omega\rangle$ and $|\omega_0\rangle$ into $|+\rangle$ and $|-\rangle$. However, due to low conversion efficiency the state remains unchanged.

Summary

Spin wave excitations in magnetic thin films are a well documented phenomena. While optical modulation using spin waves was also researched, devices that leveraged the phenomena could not compete with electro-optic modulators. The unique feature of magnon-photon interaction is its single-sideband nature at GHz frequencies. This is the primary requirement in FC-QKD systems and we have quantified the secure nature of the protocol, against an Intercept-Resend

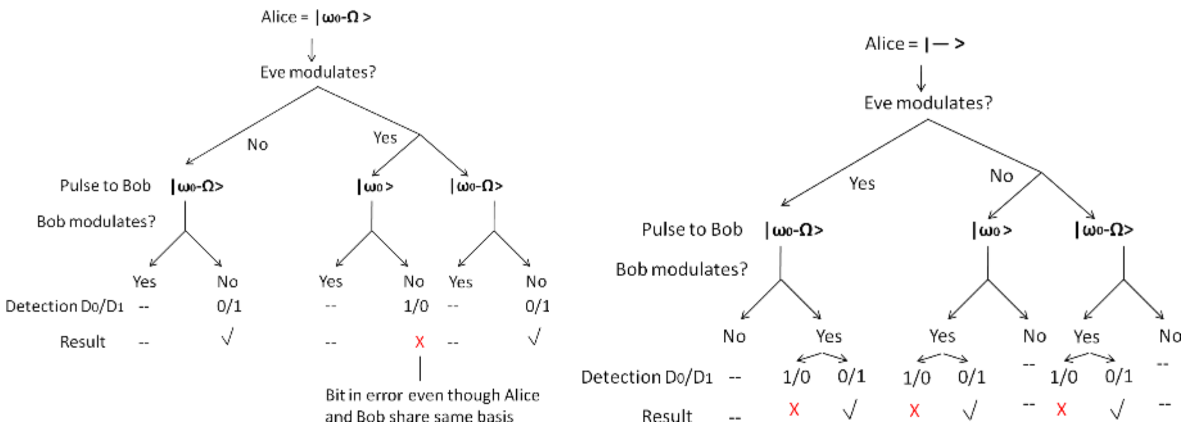

Figure 2. Intercept/Resend attack by Eve.

Table 3. Intrinsic error in sifted key due to low conversion efficiency. Alice and Bob retain slots only when Bob modulates the photon.

Alice $= \|\omega_0 - \Omega\rangle$						
Eve modulates?	N		Y			
Pulse to Bob	$\|\omega_0 - \Omega\rangle$		$\|\omega_0 - \Omega\rangle$		$\|\omega_0\rangle$	
Bob modulates?	N	Y	Y	N	Y	N
Detection $\omega_0/\omega_0 - \Omega$	−	0/1	0/1	−	1/0	−
Result	−	×	×	−	√	−

attack. We hope this encourages further development of magnon-photon interaction systems in transverse and suface spin wave geometries, in both insulating and metallic thin films.

Acknowledgments

The authors acknowledge financial support from the Department of Science and Technology, Govt. of India under the India-EU collaborative project "DYNAMAG" (grant number INT/EC/CMS(24/233552))

References

[1] Fisher A D Lee J N Gaynor E S and Tveten A B 1982 *Appl. Phys Lett.* **41** 779
[2] Tsai C S Young D Chen W Adkins L Lee C C and Glass H 1985 *Appl. Phys. Lett.* **47** 651
[3] Tamada H Kaneko M and Okamoto T 1988 *J. Appl. Phys.* **64** 554
[4] Bilaniuk N Stancil D D Talisa S H 1990 *J. of Applied Phys.* **67** 1 508-10
[5] Stancil D D 1991 *IEEE J. of Quant. Electron.* **27** 1 61-70
[6] Prabhakar A and Stancil D D 1996 *IEEE Trans., on Magnetics* **32** 3 191823
[7] Bennett C H and Brassard G 1984 *Proc., of IEEE Int., Conf., on Computers Systems and Signal Processing* Bangalore 175-9
[8] Bennett C H 1992 *PRL.* **68** 3121-24
[9] Butler J C 2007 *Optical Engineering* **46** 127-203
[10] Kumar P and Prabhakar A 2010 *IEEE J. of Quant. Electron.* **46** 11 1542-48
[11] Żakowicz, Władysław and Janowicz, Maciej 1995 *Phys. Rev. A* **52** 2 1640-50
[12] Stancil D D and Prabhakar A 2009 *Spin Waves: Theory and Applications* (Springer) chapter 8