Quantum Key Distribution is a practically implementable information-theoretic secure method for transmitting keys to remote partners performing quantum communication. After examining various protocols from the simplest such as QC and BB84 we move on to describe BBM92, DPSK, SARG04 and finally MDI from the largest possible communication distance and highest secret key bitrate. We discuss how any protocol can be optimized by reviewing the various steps and underlying assumptions proper to every protocol with the corresponding consequence in each case.

Quantum communication uses QKD for transmitting secret keys between remote partners allowing them to encrypt and decrypt their messages over unsecure transmission channels. QKD has been introduced by Bennett and Brassard in 1984 and its most attractive feature, after a number of developments, resulted in its actual deployability. It has already been commercially implemented by a number of quantum communication (QC) companies such as SeQureNet in France, ID Quantique in Switzerland, MagiQ Technologies in the USA and QuintessenceLabs in Australia. Moreover QKD straightforwardly allows detectability of online eavesdroppers. Nevertheless a difficulty arises in QKD when it is engineered with actual fiber optic commu-
ication devices. A number of weak points emerge leading to several types of security breach and consequently rendering it prone to a variety of attacks. Those are named after each weak point exploited such as detector blinding, detector dead-time, device calibration, laser damage, time-shift, phase-remapping...

Collectively some of these attacks are qualified as side-channel since they exploit discrepancies between theoretical and experimental implementation of QKD. While practical implementation challenges is reviewed by Diamanti et al. who mention a number of issues for better tackling possible drawbacks and loopholes when moving from theory to experimentation, several methods already exist and have been developed for continually improving QKD security. One efficient protection from these attacks pioneered by Braunstein et al. suggest introducing virtual channels leading to inaccessible private spaces where detectors and processing tools are placed.

The goal of this work is about optimization of several fiber optic transmission protocols such as QC, BB84, BBM92, DPSK, SARG04 and its MDI-QKD version designed to fend off photon number splitting (PNS) attacks by considering important factors such as error correction functions, detector dark counting parameter and quantum efficiency. Optimization is about increasing secret key bitrate and communication distance and involves in general the mean photon number used during transmission or some other parameters depending on the protocol employed. One such example is the entanglement parameter $\chi$ used in the BBM92 protocol.

Presently, there exists three versions of QKD: discrete variable QKD (DV-QKD), continu-
ous variable QKD (CV-QKD) and distributed-phase-reference QKD (DPR-QKD). In DV-QKD particle-like (photon) properties of light are exploited whereas in CV-QKD, wave-like properties of light are used. In both cases, a pulse or wavefunction corresponds to a communication bit or symbol whereas in DPR-QKD the latter are encoded with several (e.g. consecutive) pulses. On the reception side, DV-QKD employs photon detectors and counters whereas CV-QKD employs homodyne or heterodyne detection techniques as in traditional telecommunication demodulation. DPR-QKD uses single-photon detectors similarly to DV-QKD, as well as planar lightwave circuit technology interferometers.

It is important to point that several workers such as Zhou et al. found that when communication resources are finite, MDI-QKD secret key rates are typically lower than that of standard decoy-state QKD. Nevertheless, a number of methods exist to circumvent this problem, such as proper basis choice along with intensity selection algorithms in order to achieve longer distances.

In this work several protocols belonging to either DV-QKD or DPR-QKD are optimized and compared on the basis of five distinct sets of experiments run at different locations: BT8, BT13 (British Telecom setups at different operating wavelengths), G13 (Geneva group), KTH15 (Royal Institute of Technology, Stockholm) and Japanese Telecom NTT company (Red, Green and Blue sets). The appropriate parameters are given in Table 1 and Table 2.

1 General protocol considerations

Alice and Bob use two channels to communicate: one quantum and private to send polarized single photons and another one classical and public (telephone or Internet) to send ordinary
messages. As an illustration we consider the BB84 protocol where Alice selects two bases in 2D Hilbert space consisting each of two orthogonal states: $\oplus$ basis with $(0, \pi/2)$ linearly polarized photons, and $\otimes$ basis with $(\pi/4, -\pi/4)$ linearly polarized photons.

A message transmitted by Alice to Bob over the Quantum channel is a stream of symbols selected randomly among the four above and Alice and Bob choose randomly one of the two bases $\oplus$ or $\otimes$ to perform photon polarization measurement.

Alice and Bob announce their respective choice of bases over the public channel without revealing any measurement results.

The raw key is obtained by a process called "sifting" consisting of retaining only the results obtained when the bases used for measurement are same.

After key sifting, another process called key distillation must be performed. This process entails three steps: error correction, privacy amplification and authentication in order to counter any information leakage from photon interception, eavesdropping detection (with the no-cloning theorem) and exploitation of information announced over the public channel.

Error correction is also called Information reconciliation and can be performed with two procedures: one possibility is to correct the errors using parity coding while the other discards errors by locating error-free subsections of the sifted key. Information reconciliation can be further divided into two classes: one uses solely unidirectional information flow from Alice to Bob, while the second uses an interactive protocol with bidirectional information flow.

For instance, the error correction function given by Enzer et al. as: $f_e(x) = 1.1581 + 57.200x^3$ with $x$ the error has been determined experimentally by Brassard et al. and originates from the CASCADE error correction algorithm. CASCADE is highly efficient because it is based on an interactive bidirectional information flow between Alice and Bob. $f_e(x)$ value depends on the various error correction algorithms used, and is typically between 1 and about 1.5. When $f_e(x) = 1$, the ideal limiting case is reached where the number of error correction
bits is equal to the Shannon limit. In some cases the value of the function is fixed to some convenient value such as 1.33. Other algorithms have been developed by Lutkenhaus and Zbinden et al. as seen further below.

Privacy amplification is based on randomness extraction allowing to draw from an arbitrary random source consisting of a bit sequence arbitrarily distributed a sub-sequence that has an almost uniform distribution. Mathematically it is described by the notion of Smooth entropy that is a measure for the number of almost uniform random bits.

Quantum communications based on transmitting photons across fiber optics must be able to detect accurately proper signal carrying photons and not ”dark photons” originating from noise and intermediate devices during propagation. Thus detector dark counting must be substantially reduced in order to avoid false detection events whereas quantum yield must be increased in order to enhance signal detection quality...

As a consequence, a number of issues should be addressed at the different processing steps such as photon states, bases, encoding of quantum data, determination of mean photon number, transmission handling, error detection and correction algorithms...

The secret key bit rate as a function of distance $L$ accounting for privacy amplification $PA(L)$ and error correction $EC(L)$ is given asymptotically by:

$$K(L) = PA(L) + EC(L) = Q[1 - h_2(e_b)] - Q\mu f_e(E_\mu) h_2(E_\mu)$$

where $Q$ is the signal gain, $e_b$ the bit error, $Q\mu$ and $E_\mu$ total gain and quantum bit error rate for a given mean photon number $\mu$. The first term is due to privacy amplification whereas the second stems from error correction typically based on function $f_e(x)$ and $h_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ the binary Shannon entropy.

In the following protocols, we discuss how the previous issues are dealt with.
2 Simplest protocol

In the simplest protocol case, with no consideration of privacy amplification and accounting for error correction in a rudimentary way, the transmittance versus distance $L$ is given by $\eta_t = 10^{-\alpha L/10}$ where $\alpha$ is the wavelength dependent transmission loss along the optic fiber.

The probability of photon detection after traveling a distance $L$ is $p_{signal} = \mu \eta_t \eta$ where $\eta$ is the receiver or detector quantum yield.

$\mu$ is optimized versus distance in order to yield the largest secret key rate or may be considered as constant regardless of traveling distance.

The probability of dark photon detection is $p_{dark}$ and the probability of false detection of a photon is $p_{noise} = (1 - \eta_t \eta)p_{dark}$.

The Quantum Bit Error Rate (QBER) is given by $Q_B = \frac{p_{noise}}{p_{signal} + p_{noise}}$ and displayed in fig. 10. The resulting secret key rate without accounting for pulse frequency is given by: $K(L) = (p_{signal} + p_{noise})(1 - Q_B/Q_t)$ where $Q_t$ is a threshold QBER value. Using the parameters $\mu = 0.1$ and $Q_t = 0.01, 0.02, 0.04, 0.08$ the results are displayed in fig. 10. In general the QBER depends on several parameters such as channel depolarization (considered as White noise) as well as other types of noise and dark count rate as described next. Error correction algorithms employed to reduce the QBER (see Methods) should be tailored to combat specifically these effects.
3 QC protocol

This protocol is a slightly more sophisticated version of the previous protocol. Taking account of receiver loss one estimates error correction, privacy amplification effects as a function of QBER and the secret key bitrate is estimated in a simple probabilistic manner, in contrast with the ensuing protocols that we consider in this work. The transmittance versus distance \( L \) is given by:

\[
\eta_t = 10^{-(\alpha L + L_c)/10}
\]

where \( L_c \) is receiver loss. After traveling distance \( L \), the probability of photon detection is:

\[
p_{\text{signal}} = \mu \eta_t \eta
\]

with \( \eta \) the receiver quantum yield. Considering \( p_{\text{dark}}, p_{\text{noise}} \) as respectively the probabilities of dark counting, and false detection of a photon, we deduce the QBER from:

\[
Q_B = \frac{p_{\text{noise}} p_{\text{signal}} + p_{\text{dark}}}{p_{\text{signal}} + n_D p_{\text{dark}}}
\]

where \( n_D \) is the number of detectors. This is a more elaborate definition than the previous simple expression:

\[
Q_B = \frac{p_{\text{noise}} p_{\text{signal}}}{p_{\text{signal}} + p_{\text{noise}}}
\]

since it accounts for noise and dark counting processes.

In order to evaluate the secret key bitrate, two operations are performed: error correction and privacy amplification that are given approximately by:

\[
EC(L) = 7Q_B/2 - Q_B \log_2(Q_B) \quad \text{and} \quad PA(L) = 1 + \log_2[(1 + 4Q_B - 4Q_B^2)/2]
\]

respectively. Note that the resulting secret key rate given by:

\[
K(L) = Q_B \eta_t \eta (1 - EC(L))(1 - PA(L))
\]

and displayed for all experiments in fig. 10 is not of the Shannon asymptotic form (see eq. 1).

4 BB84 protocol

This protocol is based on four states originating from four photon polarizations: \(|\rightarrow\rangle, |\uparrow\rangle, |\uparrow\rangle, |\downarrow\rangle\) that are used to transmit quantum data with:

\[
|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle)
\]

\[
|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle)
\]

A message transmitted by Alice to Bob over the Quantum channel is a stream of symbols selected randomly among the four above and Alice and Bob choose randomly one of the two bases \( \oplus \) or \( \otimes \) to perform photon polarization measurement. We consider below two possi-
ble sources: the non-entangled Weak Coherent Pulse (WCP) and the entangled Spontaneous Parametric Down Conversion (SPDC) source.

In order to evaluate the effect of the photon pulse nature on BB84 secret key bitrate we start with the WCP case. The latter are photon states with a mean photon number $\mu$ that should be low in order to approximate single photon states. The probability that one finds $n$ photons in a coherent state follows Poisson statistics (see Methods section): $P_\mu(n) = e^{-\mu} \frac{\mu^n}{n!}$ with $\mu$ the average photon number. The probability to have at least one photon is: $1 - P_\mu(0) = 1 - e^{-\mu}$.

Consequently, the probability to have at least a single count detected by Bob is: $p_{\text{single}} = 1 - e^{-\mu \eta \eta_t} \approx \mu \eta \eta_t \equiv p_{\text{signal}}$ where $\mu$ has been replaced by $\mu \eta \eta_t$, with $\eta_t$ the optical fiber transmission and $\eta$ the receiver detection efficiency. The secret key bit rate (before sifting, error correction and privacy amplification) accounting for pulse frequency $\nu$ is given by: $\nu K(L) = \nu p_{\text{signal}} \approx \nu \mu \eta \eta_t$. The results for the bitrate versus distance for the four telecom company experiments are displayed in fig. 10.

The effect of entanglement on BB84 secret key bitrate is treated by considering an SPDC source (see Methods section). Entanglement increases robustness with respect to PNS attacks. The results for the bitrate versus distance for the four telecom company experiments are displayed in fig. 10.

5 BBM92 protocol

The BBM92 protocol is a two-photon variant of BB84 drawing advantage from BB84 protocol based on a SPDC source providing entanglement as in the previous section. Thus Alice and Bob each share a photon of an entangled photon pair, for which they measure the polarization state in a randomly chosen basis out of two non-orthogonal bases. There is no analog
to a photon-number splitting attack in BBM92 and since it is an entanglement-based protocol, expectations indicate it should be more robust than BB84. Moreover it is less vulnerable to errors caused by dark counts, since one dark count alone cannot produce an error in this protocol. The expressions for the probability of a true coincidence, \( p_{\text{true}} \), and the probability of a false coincidence, \( p_{\text{false}} \), are different for an ideally-entangled photon source and a SPDC-entangled photon source. The secret key bitrate is displayed in fig. 10 for three different sources: Arbitrary, ideal and SPDC. The major parameters are \( p_{\text{dark}} \) the dark counting probability equal to \( n_Dd_B \) where \( n_D \) is the number of detectors and \( d_B \) the dark count rate and \( \chi \) controlling entanglement through SPDC. \( \chi \) and the mean photon number \( \mu \) should both be optimized in order to achieve the best secret key bitrate.

6 DPSK protocol

This is the quantum version of the classical Differential Phase Shift Keying protocol based on coding binary information with phase difference of successive symbols (fixed length bit sequences) instead of coding information with absolute phase of individual symbols (as in PSK modulation). Similarly to BB84, DPSK uses four nonorthogonal states. A photon originating from a single-photon source takes three different paths, the time delays between them being same, using beam splitters or optical switches. Alice randomly modulates by \([0, \pm \pi]\) the phase of the photon retrieved from different routes and sends it to Bob.

Bob measures the phase difference of each consecutive pulse with a 1-bit delay interferometer. Two detectors D1 and D2 are placed at the interferometer output ports. D1 clicks when the phase difference is 0 whereas D2 clicks when the phase difference is \( \pm \pi \). The average photon number per pulse being less than 1, Bob observes clicks occasionally and at random times.
Bob informs Alice of the time instances at which he observes clicks, thus no bit information is leaked to the intruder. Alice is able to identify, from her modulation data, the detector that clicked at Bob location. Transforming D1 and D2 clicks into 0 and 1, Alice and Bob are able to extract an identical bit string.

Eve cannot obtain bit information perfectly from a photon intercepted with beam splitting. In this type of attack, Eve taps one photon out of multiple photons in a coherent pulse and then obtains bit information by measuring the photon after Alice and Bob exchange supplementary information through a public channel. In conventional BB84, Eve can measure bit information perfectly from a tapped photon. Eve cannot do so in the present scheme, because she cannot measure one of the two phase differences with 100% probability.

For this protocol, we have three sets of results, two for the four European Telecom company experiments BT13, BT8, G13 and KTH15 displayed in fig. 10 and one for the Japanese Telecom company NTT (called Red, Green, Blue) set of experiments displayed in fig. 10. The experiments differ not only by the parameters as displayed in table 1 and table 2 but also from the algorithms used for evaluating the secret key rate (see Methods section). The parameters are given in table 2.

7 SARG04 protocol

SARG04 protocol has been developed to combat PNS attacks that are targeted toward intercepting photons present in weak coherent pulses (WCP) that are used for communication. This stems from the fact, it is not possible presently to commercially exploit single photons in a pulse. However, progress in developing large scale methods targeted at using single photons in a pulse is advancing steadily. PNS attacks can be strongly reduced by the decoy method
consisting of using states with slightly different intensities than the signal and will be employed in this protocol to further strengthen it. SARG04 being very similar to BB84 protocol, the simplest example of secret key sharing among sender and receiver (Alice and Bob), we review first the BB84 case below. Alice prepares many pairs of qubits and sends each one of them to Bob after performing a random rotation over different axes with $T_lR^k$ where $l \in \{0, 1, 2\}$ and $k \in \{0, 1, 2, 3\}$.

Upon receiving the qubits, Bob first applies:

- A random reverse multi-axis rotation $R^{-k'}T^{-1}_l$,

- Afterwards, he performs a local filtering operation in order to retrieve one of the maximally entangled EPR Bell states (see Methods section).

- After, Alice and Bob compare their indices $k, l$ and $k', l'$ via public communication, and keep the qubit pairs with $k = k'$ and $l = l'$ when Bob’s filtering operation is successful.

- They choose some states randomly as test bits, measure them in the $Z$ basis, and compare their results publicly to estimate the bit error rate and the information acquired by the eavesdropper.

- Finally, they utilize the corresponding Calderbank-Shor-Steane (CSS) code to correct bit and phase errors and perform a final measurement in the $Z$ basis on their qubits to obtain the secret key.

The secure key rate with infinite decoy states using one and two photon source contributions, is given by:

$$K(L) = Q_0 + \sum_{n=1}^{n=2} Q_n [1 - H(e_{p_n}|e_{b_n})] - Q_{\mu}f_e(E_{\mu})h_2(E_{\mu})$$

(2)
where \( Q_n \) is the gain of the \( n \)-photon signal states which can be estimated from the decoy-state method; \( e_{pn}, e_{bn} \) are phase and bit error for the \( n \)-photon state; \( Q_\mu \) and \( E_\mu \) are total gain and quantum bit error rate for a given mean photon number \( \mu \). The conditional Shannon entropy \( H(e_{pn}|e_{bn}) \) depends on phase and bit errors as well as on the probability \( a \) that bit flip and phase shift occur (see Methods section). Comparison of the secret key rate versus distance for the four-state and six-state SARG04 protocol using GYS \( \eta = 0.045, e_D = 0.033, p_{dark} = 10^{-6} \) and Tang et al. \( \eta = 0.43, e_D = 0.005, p_{dark} = 10^{-7} \) parameters is displayed in fig. 10. The results show clearly that Tang et al. results are compatible with present experimental values that travel beyond 200 kms whereas the GYS results are limited to distances below 150 kms.

8 MDI version of the SARG04 protocol

Following Lo et al. and Mizutani et al. modified the original SARG04 protocol by including an intermediate experimental setup run by Charlie, at mid-distance between Alice and Bob, consisting of Bell correlation measurements. The setup contains a half beam-splitter, two polarization beam-splitters to simulate photonic Hadamard and CNOT gates in order to produce Bell states, as well as photodiode detectors. This additional step will help discard non perfectly anti-correlated photons and thus reduce transmission error rates. In addition, Alice and Bob not only choose photon polarization randomly, they also use WCP amplitude modulation to generate decoy states in order to confuse the eavesdropper.

The protocol runs as follows:

- Charlie performs Bell measurement on the incoming photon pulses and announces to Alice and Bob over the public channel whether his measurement outcome is successful
or not. When the outcome is successful, he announces the successful events as being of Type1 or Type2. Type1 is coincidence detection events of $AT$ and $BR$ or $BT$ and $AR$. Type2 is coincidence detection events of $AT$ and $AR$ or $BT$ and $BR$ where $AT$, $BT$ stand for detecting transmitted ($T$) photon events from Alice ($A$) or Bob ($B$) linearly polarized at $45^\circ$ whereas $AR$, $BR$ are for detecting reflected ($R$) photon events at $-45^\circ$.

- Alice and Bob broadcast $k$ and $k'$, over the public channel. If the measurement outcome is successful with Type1 and $k = k' = 0, \ldots, 3$, they keep their initial bit values, and Alice flips her bit. If the measurement outcome is successful with Type2 and $k = k' = 0, 2$, they keep their initial bit values. In all the other cases, they discard their bit values.

- After repeating the above operations several times, Alice and Bob perform error correction, privacy amplification and authentication as described previously.

In the ideal case (no transmission errors, no eavesdropping) Alice and Bob should discard results pertaining to measurements done in different bases (or when Bob failed to detect any photon). In QKD, Alice and Bob should be able to determine efficiently their shared secret key as a function of distance $L$ separating them. Since, the secure key is determined after sifting and distillation, secure key rate is expressed in bps (bits per signal) given that Alice sends symbols to Bob to sift and distill with the remaining bits making the secret key. For Type $i$ event, we define $e_{i,p}^{(m,n)}$ as the phase error probability that Alice and Bob emits $m$ and $n$ photons respectively, and Charlie announces a successful outcome with $Q_i^{(m,n)}$, the joint probability. Consequently the asymptotic key rate for Type $i$ is given as a sum over partial private amplification terms of the form $Q_i^{(m,n)}[1 - h_2(e_{i,p}^{(m,n)})]$ and one error correction term $Q_i^{\text{tot}} f_{\text{e}}(e_i^{\text{tot}}) h_2(e_i^{\text{tot}})$ related to total errors as \cite{33,34}:

$$K_i(L) = \sum_{m,n=1}^{2} Q_i^{(m,n)}[1 - h_2(e_{i,p}^{(m,n)})] - Q_i^{\text{tot}} f_{\text{e}}(e_i^{\text{tot}}) h_2(e_i^{\text{tot}}). \quad (3)$$
where the highest index $Q_i^{(2,2)}$ gain term is omitted. The total probabilities $Q_i^{tot} = \sum_{m,n} Q_i^{(m,n)}$ and total error rates are given by $e_i^{tot} = \sum_{m,n} Q_i^{(m,n)} e_i^{(m,n)}/Q_i^{tot}$ where $e_i^{(m,n)}$ is the “Type i” bit error probability and $h_2$ is the binary Shannon entropy. Moreover, the above asymptotic key rate is obtained in the limit of infinite number of decoy states (see Methods).

We should stress that this method differs from Ma et al. who used a special sifting technique to handle single-photon detector dead-time constraints without considering Type 1 and 2 bit error probabilities depending on photon emission.

Since Charlie is in the middle between Alice and Bob, the channel transmittance to Charlie from Alice is the same as that from Bob. Considering that $L$ is the distance between Alice and Bob, the channel transmittance $\eta_T$ is obtained by replacing $L$ by $L/2$ resulting in: $\eta_T = 10^{-\alpha L/20}$. For the standard Telecom wavelength $\lambda = 1.55\mu m$, the loss coefficient with distance is $\alpha=0.21$ dB/km. The quantum efficiency and the DCR of the detectors are taken as $\eta = 0.045$ and $d = 8.5 \times 10^{-7}$, respectively as in the GYS case. In Fig 10 secret key rates for Type 1 and Type 2 events are displayed versus distance for two classes of parameters: GYS and Tang et al. parameters with freely varying error correction function $f_e$, $\alpha = 0.12$ and mean number of photons $\mu$ optimized versus distance.

9 Discussion

Communication distances and secret key bitrates obtained in this work can be improved when we vary the error correction function, DCR and quantum efficiency of the detectors. Our results show that the most sensitive way to increase communication distance substantially is to decrease the DCR. The least sensitive parameter is the error correction function choice and in spite of exaggerating the values of the quantum efficiency in order to probe the largest possible range...
of communication distances, the DCR parameter is the most promising, consequently future research efforts ought to be directed towards reducing it considerably. This improvement relies on developing special algorithms that will allow to discriminate between different events occurring around the photodetectors, developing materials with selective specially tailored higher thresholds preventing false "clicks" triggered by "irrelevant" events or using ultralow loss optical fibers that will preserve the signal over longer distances as has been used recently by Yin et al. who managed to attain 404 kms with MDI-QKD.

10 Methods

**Weak Coherent pulse source** Coding a sequence of $n$ symbols $s_1, ..., s_n$ entails taking the tensor product resulting in the total wavefunction $|\Psi\rangle = |\psi(s_1)\rangle \otimes ... \otimes |\psi(s_n)\rangle$ where each individual wavefunction $|\psi(s_i)\rangle$ corresponds to a symbol $s_i$.

The quantum state $|\psi\rangle$ emitted by a laser is a coherent state depending on a complex value $\alpha = \sqrt{\mu} e^{i\theta}$ with $\sqrt{\mu}$ the intensity corresponding to an average number of photons $\mu$ per pulse and $\theta$ the phase. In photon number $n$ space (also called Fock space), the symbol wavefunction is given by:

$$|\psi\rangle = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle.$$  \hspace{1cm} (4)

The probability that $n$ photons are in the coherent state is given by:

$$p(n) = |\langle n|\psi\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!},$$  \hspace{1cm} (5)

recovering the above cited Poissonian result $p(n) \equiv P_\mu(n) = e^{-\mu} \frac{\mu^n}{n!}$ with average photon number $\langle n \rangle = \mu = |\alpha|^2$. Poisson distribution indicates that photons are statistically independent. A single-photon source is aproximated by taking a weak intensity $\mu$ such that the probability of
emitting a two-photon state is small.

**Distributed-Phase-Reference source** Alice produces a sequence of coherent states of same intensity resulting in $|\Psi\rangle = \ldots |e^{i\theta_{k-1}} \sqrt{\mu}\rangle |e^{i\theta_k} \sqrt{\mu}\rangle |e^{i\theta_{k+1}} \sqrt{\mu}\rangle \ldots$ where each phase $\theta$ can be 0 or $\pi$. Bits are coded in the difference between two successive phases with value 0 if $e^{i\theta_k} = e^{i\theta_{k+1}}$ and 1 otherwise. This contrasts with the WCP case where a bit or a symbol is related to a single coherent state.

**Spontaneous Parametric Down Conversion (SPDC) source** Entanglement of photon pairs is produced by conversion of some photons from a pump laser beam after interacting with a non-linear crystal like KNbO$_3$, LiNbO$_3$...

In the approximation of two output modes, the state can be written as [13]

$$|\Psi\rangle = \frac{1}{\cosh \chi} \sum_{n=0}^{\infty} (\tanh \chi)^n |n_A, n_B\rangle,$$

where $\chi$ is proportional to the second-order dielectric susceptibility $\chi^{(2)}$, pump amplitude and interaction time. $|n_A, n_B\rangle$ denotes the state with $n_A$ photons in the mode pertaining to Alice and $n_B$ photons in the mode proper to Bob.

**Optimization** Several protocols require optimization techniques in order to extract the secret key bitrate. Optimization entails varying the mean photon number $\mu$ or the entanglement parameter $\chi$ until we obtain the largest key bitrate for the longest communication distance. We have used several minimization techniques based on Linear Optimization methods such as the Simplex method in the linear case, whereas a combination of Golden section, Brent or Broyden techniques were used in the non-linear cases.[17]

**Rotation operations** In the basic four-state SARG04 protocol which is similar to BB84 a num-
ber of steps are added to improve it and protect it against PNS attacks. The steps entail introducing random rotation and filtering of the quantum states. Rotation operators use Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$: $R = \cos(\frac{\pi}{4})I - i \sin(\frac{\pi}{4})\sigma_Y$ is a $\pi/2$ rotation operator about $Y$ axis, $T_0 = I$ is the $(2\times2)$ identity operator, $T_1 = \cos(\frac{\pi}{4})I - i \sin(\frac{\pi}{4})\sigma_Y\sigma_X/\sqrt{2}$ is a $\pi/2$ rotation operator around the $(Z+X)$ axis, $T_2 = \cos(\frac{\pi}{4})I - i \sin(\frac{\pi}{4})\sigma_Z\sigma_X/\sqrt{2}$ is a $\pi/2$ rotation operator around the $(Z-X)$ axis.

**State encoding** In the four-state SARG04 QKD protocol, there are four linearly polarized states to encode quantum data: $|\rightarrow\rangle, |\uparrow\rangle, |\swarrow\rangle, |\nearrow\rangle$ with: $|\swarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle)$ and $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle)$.

In the six-state SARG04 QKD protocol, there are six polarization states to transmit quantum data, four linearly polarized $|\rightarrow\rangle, |\uparrow\rangle, |\swarrow\rangle, |\nearrow\rangle$, and two circularly polarized $|\circ\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + i|\uparrow\rangle)$, and $|\bullet\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - i|\uparrow\rangle)$.

The states are arranged into twelve sets with each set member corresponding respectively to either 0 or 1 binary $\{|\rightarrow\rangle, |\nearrow\rangle\}, \{|\swarrow\rangle, |\uparrow\rangle\}, \{|\bullet\rangle, |\rightarrow\rangle\}, \{|\circ\rangle, |\bullet\rangle\}, \{|\bullet\rangle, |\uparrow\rangle\}, \{|\circ\rangle, |\bullet\rangle\}, \{|\circ\rangle, |\nearrow\rangle\}, \{|\swarrow\rangle, |\circ\rangle\}, \{|\swarrow\rangle, |\nearrow\rangle\}, \{|\bullet\rangle, |\circ\rangle\}, \{|\bullet\rangle, |\nearrow\rangle\}, \{|\circ\rangle, |\bullet\rangle\}.$

**Decoy states** are described by yields $Y_n$ and gains $Q_n$ of $n$-photon states such that:

$$Q_n = e^{-\mu} \frac{\mu^n_n}{n!} Y_n, \quad Q_\mu = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n_n}{n!} Y_n, \quad E_\mu = \frac{1}{Q_\mu} e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n_n}{n!} Y_n e_{ba}$$

where total gain $Q_\mu$ and total quantum error $E_\mu$ are given by the weighted average of their corresponding $n$-photon state contributions. For the four-state SARG04 protocol, the $Y_n$ and $e_{ba}$ is given by\(^{39}\)

$$Y_n = \frac{1}{2}[\eta_n(e_d + \frac{1}{2}) + (1 - \eta_n)p_{dark}], \quad e_{ba} = \frac{\eta_n e_d + \frac{1}{2}(1 - \eta_n)p_{dark}}{2Y_n}.$$  

whereas in the six-state SARG04 protocol, the $Y_n$ and $e_{ba}$ is given by\(^{39}\)

$$Y_n = \frac{1}{3}[\eta_n(e_d + \frac{1}{2}) + (1 - \eta_n)p_{dark}], \quad e_{ba} = \frac{\eta_n e_d + \frac{1}{2}(1 - \eta_n)p_{dark}}{3Y_n}.$$
with \( \eta_n = 1 - (1 - \eta)^n \) where \( \eta = \eta_d 10^{-\alpha L/10} \) and \( L \) is the transmission length.

**Multiphoton states** Working with \( \nu \)-photon states amounts to prepare pairs of qubits are in the state:

\[
|\psi^{(\nu)}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |\phi_0\rangle_B \mp |1\rangle_A |\phi_1\rangle_B \),
\]

where \( A, B \) denote Alice and Bob and \( |\phi_0\rangle = \cos(\frac{\pi}{8}) |0_x\rangle + \sin(\frac{\pi}{8}) |1_x\rangle, |\phi_1\rangle = \cos(\frac{\pi}{8}) |0_x\rangle - \sin(\frac{\pi}{8}) |1_x\rangle \).

**Depolarizing quantum channel** The QBER or ratio of the number of wrong bits to the total number of bits in the sifted key, is strongly affected by channel depolarization characterized by a single parameter \( D \) called “disturbance”. \( D \) is the probability of receiving a wrong bit after transmission through channel. In the BB84 protocol, a sifted key bit is generated when Alice and Bob choose the same basis and consequently the wrong bit in the sifted key depends on \( D \). The probabilities of obtaining the wrong and right bit in the BB84 protocol are given by \( p_w = D \) and \( p_r = 1 - D \), respectively and the QBER = \( \frac{p_w}{p_w + p_r} = D \). In the SARG04 protocol, the probability of receiving the wrong bit is \( p_w = D \) whereas for the right bit, it is \( p_r = \frac{1}{2} \). Thus the QBER = \( \frac{D}{1 + D} \).

**Filtering** A local filtering operation is defined by \( F = \sin(\frac{\pi}{8}) |0_x\rangle \langle 0_x| + \cos(\frac{\pi}{8}) |1_x\rangle \langle 1_x| \) where \( \{|0_x\rangle, |1_x\rangle\} \) are \( X \)-eigenstate qubits; they are also eigenvectors of \( \sigma_X \) with eigenvalues \(+1\), and \(-1\) respectively. \( |0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \). \(|0\rangle, |1\rangle \) are \( \sigma_Z \) eigenvectors \( \begin{pmatrix} 1 \\ 0 \end{pmatrix} \) and \( \begin{pmatrix} 0 \\ 1 \end{pmatrix} \) expressed in the \( Z \) basis with eigenvalues \(+1\), and \(-1\) respectively. Local filtering enhances entanglement degree and the \( \frac{\pi}{8} \) angle helps retrieve one of the maximally entangled EPR Bell states i.e. polarization entangled photon pair states given by:

\[
|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\uparrow\rangle \pm |\uparrow\rightarrow\rangle), |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rightarrow\rangle \pm |\downarrow\downarrow\rangle).
\]

They form a complete orthonormal basis in 4D Hilbert space for all polarization states of a two-photon system and the advantage of local filtering is to make Alice and Bob share pairs of a Bell state making the shared bits unconditionally secure.

**Asymptotic Entropy** In the presence of bit and phase errors, the asymptotic conditional entropy
is given by [39]:

\[
H(e_p|e_b) = -(1 + a - e_b - e_p) \log_2 \left( \frac{1 + a - e_b - e_p}{1 - e_b} \right) - (e_p - a) \log_2 \left( \frac{e_p - a}{1 - e_b} \right) \\
- (e_b - a) \log_2 \left( \frac{e_b - a}{e_b} \right) - a \log_2 \left( \frac{e_b}{e_b} \right)
\] (10)

Acknowledgments

This work has been supported by UBO and Laboratoire des Sciences et Techniques de l’Information, de la Communication et de la Connaissance, UMR-6285 CNRS.

Author Contributions

C.T. and J. L. both felt the need to write a report about optimizing QKD. All results acquired in the report have been thoroughly discussed by both authors. Both authors contributed to writing and reviewing the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

1. C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175, IEEE, New York (1984).

2. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon. 4, 686 (2010).

3. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar and C. Kurtsiefer, Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Commun. 2, 349
4. H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New J. Phys. 13, 073024 (2011).

5. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution. Phys. Rev. Lett. 107, 110501 (2011).

6. A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography Phys. Rev. Lett. 112, 070503 (2014).

7. B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, Quantum Inf. Comput. 7, 73 (2007).

8. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K Lo, Phys. Rev. A 78, 042333 (2008).

9. F. Xu, B. Qi and H.-K. Lo, Experimental demonstration of phase remapping attack in a practical quantum key distribution system. New J. of Phys. 12, 113026 (2010).

10. E. Diamanti, H-K Lo, B. Qi and Z. Yuan, "Practical challenges in quantum key distribution”, npj Quantum Information-Nature 2, 16025 (2016).

11. S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).

12. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Rev. Mod. Phys. ”The security of practical quantum key distribution” 81, 1304 (2009); see also V. Scarani, A. Acín, G. Ribordy and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004);

13. E Waks A. Zeevi and Y. Yamamoto, Phys. Rev. A 65, 052310 (2002).
14. E. Diamanti, H Takesue, T Honjo, K Inoue and Y Yamamoto, Phys. Rev. A 72, 052311 (2005).

15. C. Zhou, W-S Bao, H-L Zhang, H-W Li, Y Wang, Y. Li and X. Wang, Phys. Rev. A 91, 022313 (2015).

16. N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000).

17. C Tannous and J Langlois, Eur. J. Phys. 37 013001 (2016).

18. C-H F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A 81, 012318 (2010).

19. D. G Enzer, P. G Hadley, R. J Hughes, C. G Peterson and P. G Kwiat, New Journal of Physics 4, 45 (2002).

20. G. Brassard and L. Salvail, Advances in Cryptology-Eurocrypt 1993, edited by T. Helleseth, Lecture Notes in Computer Science Vol. 765 Springer, Berlin, p. 410 (1994).

21. N. Lütkenhaus, Phys. Rev. A 59, 3031 (1999).

22. H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin and G. Ribordy, Appl. Phys. B 67, 743 (1998).

23. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992).

24. A. B. Carlson and P. B. Crilly Communication systems: An Introduction to Signals and Noise in Electrical Communication, 5th Edition, McGraw-Hill, New York (2010).

25. K. Inoue, E Waks and Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002).

26. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).

27. P. G. Kwiat, K. Mattle, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. 75, 4337 (1995).
28. A. R. Calderbank and P. W. Shor, Phys. Rev. A 54, 1098 (1996).

29. H-K Lo, X. Ma and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).

30. C. Gobby, Z. L. Yuan and A. J. Shields, App. Phys. Lett. 84, 3762 (2004).

31. Y-L Tang, H-L Yin, S-J Chen, Y. Liu, W-J Zhang, X. Jiang, L. Zhang, J. Wang, L-X You, J-Y Guan, D-X Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T-Y Chen, Q. Zhang, and J-W Pan, Phys. Rev. Lett. 113, 190501 (2014).

32. H-K Lo, M Curty and B Qi, Phys. Rev. Lett. 108, 130503 (2012).

33. A Mizutani, K Tamaki, R Ikuta, T Yamamoto and N Imoto, Sci. Rep. 4, 5236, doi: 10.1038/srep05236 (2014).

34. H-K Lo, X. Ma and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).

35. X. Ma and M. Razavi, Phys. Rev. A 86, 062319 (2012).

36. H-L Yin, T-Y Chen, Z-W Yu, H. Liu, L-X You, Y-H Zhou, S-J Chen, Y Mao, M-Q Huang, W-J Zhang, H Chen, M-J Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X-B Wang and J-W Pan, Phys. Rev. Lett. 117, 190501 (2016).

37. T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd edition, Wiley, New-York (2006).

38. W. H. Press, W. T. Vetterling, S. A. Teukolsky and B. P. Flannery, Numerical Recipes in C: The Art of Scientific Computing Third Edition, Cambridge University Press, New-York (2007).

39. H-L Yin, Y Fu, Y-Q Mao and Z-B Chen, Sci. Rep. 6, 29482; doi: 10.1038/srep29482 (2016).
40. E. Desurvire, *Classical and Quantum Information Theory*, Cambridge University Press, New-York (2009).

41. C. Branciard, N. Gisin, B. Kraus and V. Scarani, Phys. Rev. A 72, 032301 (2005).

42. K. Tamaki and N. Lutkenhaus, Phys. Rev. A 68, 032316 (2004).

43. H Takesue, E Diamanti, T Honjo, C Langrock, M M Fejer, K Inoue and Y Yamamoto, New Journal of Physics 7, 232 (2005).
| Experiment | $\lambda$ (nm) | $\alpha$ (dB/km) | $L_c$ (dB) | $e_0$ | $d_B$ | $\eta$ |
|------------|----------------|------------------|------------|-------|-------|--------|
| BT8        | 830            | 2.5              | 8          | 0.01  | $5 \times 10^{-8}$ | 0.5    |
| BT13       | 1300           | 0.38             | 5          | $8 \times 10^{-3}$ | $1 \times 10^{-6}$ | 0.11  |
| G13        | 1300           | 0.32             | 3.2        | $1.4 \times 10^{-6}$ | $8.2 \times 10^{-5}$ | 0.17  |
| KTH15      | 1550           | 0.2              | 1          | 0.01  | $2 \times 10^{-4}$ | 0.18  |

Table 1: Fiber attenuation $\alpha$ in dB/km, receiver loss $L_c$ in dB, $e_0$ innocent bitrate, dark count parameter $d_B$ and quantum yield $\eta$ in the British Telecom experiments BT8 and BT13, Geneva G13 and Sweden KTH15.

| Experiment  | $\alpha$ (dB/km) | $L_c$ (dB) | $d_B$            | $e_0$ | $\eta$ |
|-------------|------------------|------------|------------------|-------|--------|
| NTT-Red     | 0.2              | 2          | $1.95 \times 10^{-5}$ | 0.088 | 0.03   |
| NTT-Green   | 0.2              | 1          | $1 \times 10^{-6}$ | 0.02  | 0.03   |
| NTT-Blue    | 0.2              | 1          | $1 \times 10^{-6}$ | 0.07  | 0.03   |

Table 2: Fiber attenuation $\alpha$ in dB/km, receiver loss $L_c$ in dB, dark count parameter $d_B$, detector quantum efficiency $\eta$ and $e_0$ innocent bitrate, for the Japanese NTT Telecom company Red, Green and Blue sets.
**Figure 1** (Color on-line) QBER versus distance for the simplest protocol. The parameters are: $\alpha = 0.2$, $\eta = 0.25$, $p_{dark} = 10^{-4}$ and $\mu = 0.1$.

**Figure 2** (Color on-line) Rates versus distance for the simplest protocol with different threshold QBER values $Q_t$. The parameters are: $\alpha = 0.2$, $\eta = 0.25$, $p_{dark} = 10^{-4}$ and $\mu = 0.1$.

**Figure 3** (Color on-line) QC protocol comparison in the four Telecom company experiments: BT13, BT8, G13 and KTH15. $\mu$ is optimized with distance. The number of detectors is assumed to be $n_D = 2$.

**Figure 4** (Color on-line) WCP source use for the BB84 protocol in the four Telecom company experiments: BT13, BT8, G13 and KTH15. The algorithm used is by Lütkenhaus in ref. [16]. $\mu$ is optimized with distance.

**Figure 5** (Color on-line) SPDC source use for the BB84 protocol in the four Telecom company experiments: BT13, BT8, G13 and KTH15. The algorithm used is by Lütkenhaus in ref. [16]. $\mu$ is optimized with distance.

**Figure 6** (Color on-line) BBM92 protocol in the arbitrary, ideal and SPDC entangled source case. The algorithm used is by Waks *et al.* in ref. [13][14]. In the arbitrary case, $\mu = 0.3 \times 10^{(-0.7\alpha L/10.)}$ and the dark counting parameter $d_B = 5 \times 10^{-5}$, whereas in the ideal case $\mu = 1$. The SPDC entanglement parameter $\chi = 0.1$. 
Figure 7  (Color on-line) DPSK results for the BT13, BT8, G13 and KTH15 Telecom company experiments. The algorithm employed is by Takesue et al. \cite{43}. $\mu$ is optimized with distance.

Figure 8  (Color on-line) DPSK results for the Japanese NTT Telecom company sets of experiments. $\mu$ is optimized with distance.

Figure 9  (Color on-line) Comparison of secret key rates for the 4-state and 6-state SARG04 protocol using GYS \cite{30} and Tang et al. \cite{31} parameters. For all curves $\alpha = 0.21$ and $\mu = 0.1$. Note an improvement from GYS to Tang et al. experiments by roughly a factor 10 in $\eta, e_D, P_{dark}$ parameters resulted in a gain of 100 kms.

Figure 10  (Color on-line) MDI-QKD SARG04 key rate $K(L)$ for Type 1 and Type 2 events, in bps versus distance $L$ using GYS \cite{30} and Tang et al. \cite{31} parameters. $\alpha = 0.21$, variable error correction function is used and $\mu$ is optimized with distance. Note again the 100 kms gain in moving from GYS to Tang et al. parameters.
