Using Evolutionary Techniques to Analyze the Security of Quantum Key Distribution Protocols

Walter O. Krawec
Stevens Institute of Technology
Hoboken NJ, 07030
walter.krawec@gmail.com

ABSTRACT

In this paper, we describe a new real coded GA which may be used to analyze the security of quantum key distribution (QKD) protocols by estimating the maximally tolerated error rate - an important statistic and, for many newer more complicated protocols, still unknown. Our algorithm takes advantage of several nice features of QKD protocols to simplify the search process and was evaluated on several protocols and can even detect security flaws in a protocol thus showing our algorithm's usefulness in protocol design.

Categories and Subject Descriptors

I.2.8 [**Artificial Intelligence**]: Problem Solving, Control Methods, and Search

Keywords

Quantum Computing; Quantum Key Distribution

1. THE ALGORITHM

A Quantum Key Distribution (QKD) protocol [6] allows two users, referred to as Alice (A) and Bob (B), to agree on a secret key (a string of random classical bits) which is secure against even an all-powerful adversary (referred to as Eve, E). QKD protocols have the nice property that one may estimate the amount of information E holds on the secret key by measuring the "noise" or error rate in the quantum channel. In this paper we describe a new real-coded GA which can estimate an upper-bound on the maximally tolerated quantum bit error rate (QBER) of a QKD protocol - any noise level higher than this and E may hold too much information to distill a secure secret key. While this value is known for many protocols, some newer ones (especially two-round protocols) do not yet have this value computed. Since QKD protocols are implementable (and in use) with today's hardware, this is an important question.

These protocols typically work by first performing a quantum communication stage where the two parties communicate by sending qubits over several independent iterations (see [4] for information on quantum computation), each iteration divided into $K \geq 1$ rounds. After this stage, A and B each have a "raw key" - a string of classical bits from which they perform an error correction (EC) and privacy amplification (PA) protocol to distill a (shorter) secure secret key. For more detailed information on this process, the reader is referred to [6].

Our algorithm considers *collective attacks* in the *asymptotic scenario* [6] (where E uses the same strategy each iteration - security in this setting usually implies security against arbitrary attacks [3]) thus we need only consider a single iteration of a QKD protocol. Eve's attack consists of K unitary operators $\{U_i\}_{i=1}^K$ with U_r being used on round r. These operators act on the qubit sent and Eve's private ancilla.

In this scenario, to compute a bound on the maximally tolerated QBER τ_Q, we will consider the key-rate of a QKD protocol defined as: $r := \lim_{n\to\infty} \frac{l(n)}{n}$, where $l(n)$ is the number of secure key bits generated by PA and n is the number of iterations used by A and B (the number of qubits sent). Clearly it is desired that $r > 0$. If $r = 0$, no secret key may be generated. Since we are not considering post processing, we may simplify the equation of [5] which, assuming collective attacks, upper bounds $r \leq \max(0, R)$ where: $R = \min(S(A|E) - H(A|B)))$. Here, given ρ_{ABE}, a density matrix describing a single iteration of the QKD protocol, $S(A|E) = S(\rho_{AE}) - S(\rho_E)$ is the conditional von Neumann Entropy (see [4]); $H(\cdot|\cdot)$ is the (classical) conditional entropy; and the minimum is over all attack operators $\{U_i\}_{i=1}^K$ inducing a certain QBER τ_Q such that, for any observed QBER larger than τ_Q, both parties abort.

We wrote a quantum simulator specific to this problem which allows the user to describe, easily, a QKD protocol (i.e., construct density matrix ρ_{ABE}). The simulator also allows us to easily "swap" in new attack operators to recompute R. Our system stores this density matrix description as a linked list, which we call a `DensityList`, of `KetBra` structures. Each `KetBra` represents a value of the form: $p\,|i_1, i_2, \cdots, i_n\rangle\langle j_1, j_2, \cdots, j_n|$, where $p \in \mathbb{C}$ (represented as two double precision floating point values) and each i_k are integers between 0 and one less than the dimension of the k'th subspace. These i's and j's represent either orthonormal basis states or they may index arbitrary states which we may define at a later time. For clarity in this paper, if an index represents a basis state we will either write it as an integer or denote with a non-e prefix (e.g., i_k or a_j); otherwise, if it represents an arbitrary state, we will denote this using an e prefix (e.g., $e^r_{i_k}$).

GECCO'14, July 12–16, 2014, Vancouver, BC, Canada.
ACM 978-1-4503-2881-4/14/07.
http://dx.doi.org/10.1145/2598394.2598410.

We now describe the technique we use to compute $U_i \rho U_i^*$ where ρ is a `DensityList`. Let $\mathcal{H}_T$ be the two-dimensional "transit" space (modeling the sent qubit) and $\mathcal{H}_{E,r}$ is Eve's private ancilla for round r. We assume, without loss of generality, that on round i, U_i acts only on $\mathcal{H}_T \otimes \mathcal{H}_{E,1} \otimes \cdots \otimes \mathcal{H}_{E,i}$ and given ρ, the state of the $\mathcal{H}_{E,i}$ subspace is "cleared" to the basis state $|0\rangle_{E,i}$. Let $d_0 = \dim \mathcal{H}_T = 2$ and $d_j := \dim \mathcal{H}_{E,i}$ for $j = 1, 2, \cdots, K$ (these are, without loss of generality, finite). Also, define $D_0 = 1$ and $D_{i \geq 1} = \prod_{j=0}^{i-1} d_j$.

If $K = 1$, U_1 acts as: $U_1 |0\rangle = |0, e_0^1\rangle + |1, e_1^1\rangle$ and $U_1 |1\rangle = |0, e_2^1\rangle + |1, e_3^1\rangle$ (these e states are not necessarily normalized or orthogonal). For $K > 1$, we proceed inductively. At the start of round r, before E applies U_r, assume that we have a `DensityList` ρ_{r-1} where each `KetBra` is of the form:

$$p \, |i_0, \cdots, i_{r-2}, e_l^{r-1}, 0\rangle \langle j_0, \cdots, j_{r-2}, e_m^{r-1}, 0| \, .$$

Note that all indices in this structure are orthonormal basis states except for $\mathcal{H}_{E,r-1}$ which are non-basis states $|e_{l/m}^{r-1}\rangle$. E now applies U_r which acts on basis states as follows: $U_r |a_0, \cdots, a_{r-1}, 0\rangle = \sum_{\vec{k}} |\vec{k}\rangle \otimes f_r(\vec{a}, \vec{k})$, where the sum is over all vectors $\vec{k} = (k_0, k_1, \cdots, k_{r-1})$ with $k_i \in \{0, \cdots, d_i - 1\}$, $\vec{a} = (a_0, \cdots, a_{r-1})$, and $f_r(\vec{a}, \vec{k})$ is a function mapping the value $(\vec{a}, \vec{k})$ to a vector in $\mathcal{H}_{E,r}$. That is to say, $f_r(\vec{a}, \vec{k})$ represents a state vector (not necessarily normalized) in the r'th subspace of E's system (we will convert this to an "e^r" state shortly). Unitarity of U_r requires:

$$\begin{array}{l} \sum_{\vec{k}} f_r(\vec{a}, \vec{k})^* \cdot f_r(\vec{a}, \vec{k}) = 1, \ \forall \ \vec{a} \\ \sum_{\vec{k}} f_r(\vec{a}, \vec{k})^* \cdot f_r(\vec{b}, \vec{k}) = 0, \ \forall \ \vec{a} \neq \vec{b}. \end{array} \quad (1)$$

Of course ρ_{r-1} contains non-basis states $|e_j^{r-1}\rangle$. Choosing a basis for $\mathcal{H}_{E,r-1}$ (the choice is irrelevant to entropy computations), we may write each $|e_j^{r-1}\rangle$ as a vector: $(\alpha_{j,1}^{r-1}, \alpha_{j,2}^{r-1}, \cdots, \alpha_{j,d_{r-1}}^{r-1})^T$. Thus:

$$\begin{array}{l} U_r \, |a_0, \cdots, a_{r-2}, e_j^{r-1}, 0\rangle \\ = U_r (\sum_{l=1}^{d_{r-1}} \alpha_{j,l}^{r-1} \, |a_0, \cdots, a_{r-2}, l-1, 0\rangle \\ = \sum_{l=1}^{d_{r-1}} \alpha_{j,l}^{r-1} \sum_{\vec{k}} |\vec{k}\rangle \otimes f_r(\vec{a}||l, \vec{k}) \\ = \sum_{\vec{k}} |k\rangle \otimes \sum_{l=1}^{d_{r-1}} \alpha_{j,l}^{r-1} f(\vec{a}||l, \vec{k}), \end{array}$$

where $\vec{a}||l = (a_0, \cdots, a_{r-2}, l)$. If we define $|e^r(j, \vec{a}, \vec{k})\rangle = \sum_l \alpha_{j,l}^{r-1} f(\vec{a}||l, \vec{k})$, then U_r sends state $|a_0, \cdots, a_{r-2}, e_j^{r-1}\rangle$ to $\sum_{\vec{k}} |k, e^r(j, \vec{a}, \vec{k})\rangle$. This process may be repeated for the `bra` portion $\langle \cdot |$ of each `KetBra` (bras are the conjugate transpose of kets). Thus, after choosing a suitable ordering $i \leftrightarrow (j, \vec{a}, \vec{k})$, which is straight-forward to do, we may equate the state $|e_i^r\rangle$ to the state $|e^r(j, \vec{a}, \vec{k})\rangle$ and we have a `DensityList` ρ_r which contains only basis states except for $\mathcal{H}_{E,r}$ and may therefore apply this process for round $r + 1$.

A candidate solution, which is a description of these K unitary attack operators $\{U_i\}$, will consist of vectors of the form: $\mathcal{G}_r(\vec{a}) = (g_r(\vec{a}, 1), g_r(\vec{a}, 2), \cdots, g_r(\vec{a}, D_r))$, for all possible $\vec{a}$ as defined before, where each $g_r(\vec{a}, k)$ is a vector of size d_r for $r = 1, 2, \cdots, K$. Each element in these vectors is a complex number represented by two double precision floating point values. The total number of variables is $2 \sum_{r=1}^{K} \cdot D_r \cdot D_{r+1}$.

We then, individually for each r, orthogonalize these $\mathcal{G}_r(\vec{a})$ vectors using the Gram Schmidt process resulting in orthonormal vectors $\mathcal{F}_r(\vec{a}) = (f_r(\vec{a}, 1), \cdots, f_r(\vec{a}, D_r))$. It is clear that, if we write each $f_r(\vec{a}, k)$ as a column vector (thus corresponding to kets), they satisfy Equation 1. From this we iteratively construct each $|e_i^r\rangle$ (starting with $r = 1$).

To create an initial population of such operators, we use, for $X, Y \in [0, 1]$, the following distribution:

$$\begin{array}{lll} g_r(\vec{a}, \vec{k})[j] = 1 - U(0, X) & \vec{k} = \vec{a}, & j = 0 \\ g_r(\vec{a}, \vec{k})[j] = U(0, X) & \vec{k} = \vec{a}, & j > 0 \\ g_r(\vec{a}, \vec{k})[j] = U(0, Y) & \vec{k} \neq \vec{a}, & j \geq 0 \end{array} \quad (2)$$

where the function $U(0, X)$ chooses a complex number whose real and imaginary components are drawn independently, and uniformly from the interval $[0, X]$. Note if $X = Y = 0$, all operators are the identity operator. We found choosing $X = Y = .25$ produced good results in our evaluations.

Crossover is done using simple one-point crossover. Mutation will alter 25% of the elements in $\mathcal{G}_r(\vec{a})$ adding to the real and imaginary components by a random $x \in [-1/10, 1/10]$ (choosing different random amounts for each component). The fitness of a candidate solution is: $\text{fit}(\mathcal{G}) = \frac{1}{2}(Q - \tilde{\tau}_Q)^2 + \frac{1}{2}(R + .01)^2$ (we wish to minimize this function), where Q is the induced QBER of the solution, R is the key rate (mentioned above - to compute this, we construct a density matrix from the `DensityList`, and find its eigenvalues to compute $S(A|E)$; computing $H(A|B)$ and Q from this matrix is also straightforward), and $\tilde{\tau}_Q$ is the target QBER. If we find a solution $\{U_i\}$ that induces a QBER of Q with a key rate $R < 0$, we can upper-bound the maximal tolerated QBER by this Q. Thus we want to find the smallest such Q.

We evaluated our algorithm on BB84 [1] where it found a maximal QBER of .11118 (the theoretical maximum is .11 [3]). We also tested it on a "flawed" version of BB84 - this insecurity was detected by finding a solution with Q close to zero and $R < 0$. Finally, we tested it on a two-round QDK protocol of [2]. Here it found a maximal QBER of .84. This is a new result in QKD research. It was also able to determine a modified version of this protocol was insecure.

2. REFERENCES

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. New York, 1984.

[2] Michel Boyer, D. Kenigsberg, and T. Mor. Quantum key distribution with classical bob. In *Quantum, Nano, and Micro Technologies, 2007. ICQNM '07. First International Conference on*, pages 10–10, 2007.

[3] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, Aug 2005.

[4] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, MA, 2000.

[5] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.

[6] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.