Письма в ЖЭТФ, том 94, вып. 11, с. 900 – 903 © 2011 г. 10 декабря

Энтропийные соотношения неопределенностей и предельно допустимая критическая ошибка в квантовой криптографии

С. Н. Молотков

Академия криптографии РФ, 121552 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 18 октября 2011 г.

После переработки 31 октября 2011 г.

Основным параметром любого протокола квантовой криптографии является критическая ошибка Q_c, до которой гарантируется секретное распределение ключей. Критическая ошибка всех известных протоколов квантового распределения ключей не превышает 20%. Цель данной работы – предъявить протокол, в котором секретное распределение ключей возможно вплоть до $Q_c \to 50\%$, а также привести простое доказательство секретности протокола, основанное на фундаментальных энтропийных соотношениях неопределенностей. Данная величина критической ошибки является теоретическим, но достижимым пределом, который не может быть улучшен.

Введение. Предельная допустимая ошибка для классического бинарного канала связи, до которой можно безошибочно передавать информацию в асимптотическом пределе длинных последовательностей, есть $Q \to 50\%$ [1, 2]. Предельное количество информации в битах в пересчете на одну позицию, которое может быть передано через канал с шумом, ограничено пропускной способностью канала связи [1, 2]:

$$C(Q) = \max_{\{p_X(x)\}} I(X|Y) = \\ = \max_{\{p_X(x)\}} [H(X) - H(X|Y)] = 1 - h(Q), \qquad (1)$$

где $h(Q) = -Q\log Q - (1-Q)\log(1-Q)$, максимум берется по распределениям вероятности на символах входного алфавита $X = \{0,1\}$, выходной алфавит $Y = \{0,1\}$. Максимум в (1) достигается на равномерном распределении. При этом $H(X) = 1$. Условная энтропия $H(X|Y) = h(Q)$ есть минимальное количество информации в битах, необходимое для исправления ошибок. При $Q \to 50\%$ пропускная способность $C(Q) \to 0$. Это означает, что вся переданная последовательность расходуется на исправление ошибок.

В квантовой криптографии после передачи квантовых состояний и измерений на приемной стороне Алиса и Боб имеют битовые последовательности $X^n = \{0,1\}^n$ и $Y^n = \{0,1\}^n$. Последовательность Боба содержит ошибки с вероятностью Q. Для их исправления используется открытый аутентичный классический канал связи, через который для исправления ошибок требуется передать $h(Q)$ бит информации. Данная информация доступна подслушивателю (Еве). Кроме того, Ева имеет информацию о ключе, которую она получила из квантового канала связи при передаче квантовых состояний от Алисы к Бобу. Поскольку при $Q \to 50\%$ вся последовательность тратится на исправление ошибок, при этом заведомо нельзя получить секретный ключ. На первый взгляд кажется очевидным, что не может существовать протоколов квантового распределения ключей, которые гарантировали бы секретную передачу ключей при $Q \to 50\%$. Однако это не так. Ниже будет приведен такой протокол с простым доказательством его секретности на основе фундаментальных энтропийных соотношений неопределенностей, а также проведено сравнение с базовым протоколом BB84 [3] и выявлена причина достижения критической ошибки $Q_c \to 50\%$.

Энтропийные соотношения неопределенностей. Соотношения неопределенностей для канонически сопряженных x и p были введены Гейзенбергом [4], а для произвольных наблюдаемых R и L – Робертсоном [5]. Последние имеют вид

$$(\Delta R)_{|\psi\rangle}(\Delta L)_{|\psi\rangle} \geq \frac{1}{2}|\langle\psi|[RL - LR]|\psi\rangle|, \qquad (2)$$

где $|\psi\rangle$ – вектор состояния квантовой системы, $(\Delta R)^2_{|\psi\rangle} = \langle\psi|R^2|\psi\rangle - (\langle\psi|R|\psi\rangle)^2$, аналогично для $(\Delta L)^2_{|\psi\rangle}$. Эрмитовы операторы R и L имеют спектральные разложения $R = \sum_i r_i|r_i\rangle\langle r_i|$ и $L = \sum_j l_j|l_j\rangle\langle l_j|$. На пространстве исходов, нумеруемых i и j, измерение наблюдаемых порождает распределение вероятностей $p_R(i) = |\langle r_i|\psi\rangle|^2$ и $p_L(j) = |\langle l_j|\psi\rangle|^2$. Соотношения в форме (2) неоднократно под-

вергались критике, т.к. правая часть здесь зависит от состояния квантовой системы $|\psi\rangle$ и поэтому не является нижней границей. Если в качестве $|\psi\rangle$ взять один из собственных векторов R, то правая часть (2) будет равна нулю. Было показано, что более естественными являются энтропийные соотношения неопределенностей [6–9].

Далее нам потребуются энтропийные соотношения для трехсоставных систем (*tri-partite*). Соотношения неопределенностей для таких систем были получены в [10] (см. также [11]). Пусть имеется состояние $|\psi\rangle_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ и пусть над подсистемой A проводится измерение наблюдаемой, либо R_A, либо L_A (далее для краткости измерение либо в базисе $\{|r_i\rangle_A\}$, либо в базисе $\{|l_j\rangle_A\}$). После измерения составная система переходит в одно из новых состояний:

$$\rho_{R_A BE} = \sum_i |r_i\rangle_{AA}\langle r_i| \otimes {}_A\langle r_i|\psi\rangle_{ABE}\ {}_{ABE}\langle\psi|r_i\rangle_A,$$
$$\rho_{L_A BE} = \sum_j |l_i\rangle_{AA}\langle l_j| \otimes {}_A\langle l_j|\psi\rangle_{ABE}\ {}_{ABE}\langle\psi|l_j\rangle_A. \tag{3}$$

Имеют место энтропийные соотношения неопределенностей [10, 11]:

$$H(R_A|E) + H(L_A|B) \geq 2\log\frac{1}{c}, \quad c = \max_{i,j} |{}_A\langle r_i|l_j\rangle_A|, \tag{4}$$

где $H(R_A|E) = H(R_AE) - H(E)$, $H(L_A|B) = H(L_AB) - H(B)$ – условные энтропии фон Неймана, например $H(R_AE) = -\mathrm{Tr}_{AE}\{\rho_{R_AE}\log\rho_{R_AE}\}$, $\rho_{R_AE} = \mathrm{Tr}_B\{\rho_{R_ABE}\}$ (аналогично для других частичных матриц плотности).

Далее, если над состояниями (3) над подсистемой B проводится измерение одной из наблюдаемых (L_B либо R_B), то соотношение неопределенностей принимает вид (детали см. в [12])

$$H(R_A|E) + H(L_A|L_B) \geq 2\log\frac{1}{c}, \tag{5}$$

где матрицы плотности после измерения в базисе $\{|l_k\rangle_B\}$ или в базисе $\{|r_k\rangle_B\}$

$$\rho_{L_A L_B E} = \sum_{i,k} |l_i\rangle_{AA}\langle l_i| \otimes$$
$$\otimes|l_k\rangle_{BB}\langle l_k|\otimes_A\langle l_i|\otimes_B\langle l_k|\psi\rangle_{ABE}\ {}_{ABE}\langle\psi|l_k\rangle_B\otimes|l_i\rangle_A, \tag{6}$$

$$\rho_{R_A R_B E} = \sum_{i,k} |r_i\rangle_{AA}\langle r_i| \otimes$$
$$\otimes|r_k\rangle_{BB}\langle r_k|\otimes_A\langle r_i|\otimes_B\langle r_k|\psi\rangle_{ABE}\ {}_{ABE}\langle\psi|r_k\rangle_B\otimes|r_i\rangle_A. \tag{7}$$

Основной результат. В протоколе квантового распределения ключей с фазово-временны́м кодированием биты 0 и 1 кодируются как в относительную фазу, так и во временны́е сдвиги квантовых состояний. Протокол выглядит следующим образом (детали реализации см. в [13]). Для того чтобы напрямую воспользоваться энтропийными соотношениями неопределенностей (5), при доказательстве секретности будем использовать версию протокола на запутанных состояниях (*entangled version*). Алиса готовит случайно и равновероятно одно из максимально запутанных состояний в правом (R_A) или в левом (L_A) базисах:

$$|\Phi_R\rangle_{AB} = \frac{|\overline{0}^+_R\rangle_A \otimes |\overline{0}^+_R\rangle_B + |\overline{0}^+_R\rangle_A \otimes |\overline{0}^+_R\rangle_B}{\sqrt{2}} =$$
$$= \frac{|\overline{0}^\times_R\rangle_A \otimes |\overline{0}^\times_R\rangle_B + |\overline{0}^\times_R\rangle_A \otimes |\overline{0}^\times_R\rangle_B}{\sqrt{2}}, \tag{8}$$

$$|\Phi_L\rangle_{AB} = \frac{|\overline{0}^+_L\rangle_A \otimes |\overline{0}^+_L\rangle_B + |\overline{0}^+_L\rangle_A \otimes |\overline{0}^+_L\rangle_B}{\sqrt{2}} =$$
$$= \frac{|\overline{0}^\times_L\rangle_A \otimes |\overline{0}^\times_L\rangle_B + |\overline{0}^\times_L\rangle_A \otimes |\overline{0}^\times_L\rangle_B}{\sqrt{2}}. \tag{9}$$

Здесь

$$|\overline{0},\overline{1}^+_R\rangle_{A,B} = \frac{|1\rangle_{A,B} \pm |2\rangle_{A,B}}{\sqrt{2}},$$
$$|\overline{0},\overline{1}^\times_R\rangle_{A,B} = \frac{|1\rangle_{A,B} \pm i|2\rangle_{A,B}}{\sqrt{2}}, \tag{10}$$

$$|\overline{0},\overline{1}^+_L\rangle_{A,B} = \frac{|2\rangle_{A,B} \pm |3\rangle_{A,B}}{\sqrt{2}},$$
$$|\overline{0},\overline{1}^\times_L\rangle_{A,B} = \frac{|2\rangle_{A,B} \pm i|3\rangle_{A,B}}{\sqrt{2}}, \tag{11}$$

где $|1\rangle_{A,B}, |2\rangle_{A,B}, |3\rangle_{A,B}$ – однофотонные состояния (пакеты), локализованные во временны́х окнах $1, 2, 3$ соответственно. После вторжения Евы состояния (8), (9) переходят в некоторые новые состояния $|\psi\rangle_{ABE}$, которые зависят от исходных. Поскольку соотношения неопределенностей (5) справедливы для любого состояния, индексы R, L у состояния $|\psi\rangle_{ABE}$ мы опускаем.

Для получения бита ключа 0 или 1 Алиса случайно и равновероятно производит измерения над своей подсистемой в базисе собственных векторов оператора $R^+_A : \{|\overline{0}^+_R\rangle_A, |\overline{1}^+_R\rangle_A\}$ или $R^\times_A : \{|\overline{0}^\times_R\rangle_A, |\overline{1}^\times_R\rangle_A\}$, если было приготовлено состояние (8). Если же было приготовлено состояние (9) в базисе L_B, то Алиса производит измерения над своей подсистемой в базисе собственных векторов оператора $L^+_A : \{|\overline{0}^+_L\rangle_A, |\overline{1}^+_L\rangle_A\}$ или $L^\times_A : \{|\overline{0}^\times_L\rangle_A, |\overline{1}^\times_L\rangle_A\}$. Через открытый аутентичный канал связи Алиса сообщает Бобу выбор своего базиса. Боб производит измерения в том же базисе, что и Алиса: для R_B это $R^+_B : \{|\overline{0}^+_R\rangle_B, |\overline{1}^+_R\rangle_B, |3\rangle_B\}$

или $R_B^{\times}$: $\{|\overline{0}_R^{\times}\rangle_B, |\overline{1}_R^{\times}\rangle_B, |3\rangle_B\}$, а для L_B – L_B^{+} : $\{|1\rangle_B, |\overline{0}_L^{+}\rangle_B, |\overline{1}_L^{+}\rangle_B\}$ или $L_B^{\times}$: $\{|1\rangle_B, |\overline{0}_L^{\times}\rangle_B, |\overline{1}_L^{\times}\rangle_B\}$. В отсутствие Евы имеет место полная корреляция исходов измерений у Алисы и Боба. Поскольку Ева не может достоверно различать состояния из базисов L_B и R_B из-за перекрытия во временно́м окне 2, неизбежно возникнут ошибочные отсчеты в контрольных временны́х окнах 1 или 3. При наличии Евы пространство исходов измерений у Боба должно быть дополнено событиями во временны́х окнах 1 и 3, соответственно, для базисов $L_{A,B}$ и $R_{A,B}$ у Алисы и Боба.

Длина секретного ключа в асимптотическом пределе длинных последовательностей составляет (см. детали в [12])

$$l_{\rm secr} \le H(R_A|E) - H(R_A|R_B) \qquad (12)$$

(индексы "+", "×" мы опускаем). Формула (12) учитывает как коррекцию ошибок, так и сжатие ключа универсальными хэш-функциями второго порядка [12, 14].

Поскольку измерения проводятся в ортогональном базисе, с учетом симметрии по отношению к базисам R и L имеем $H(R_A^{+\times}|E) = H(L_A^{+\times}|E) = H(X_A|E)$, где $X_A = \{0,1\}$ и $H(R_A^{+\times}|R_B^{+\times}) = H(L_A^{+\times}|L_B^{+\times}) = H(X_A|Y_B)$, где $Y_B = \{0,1,?\}$. Исход "?" соответствует отсчетам в контрольных временны́х окнах 1 и 3.

Для вычисления условной энтропии необходимо вычислить условные вероятности $p_{X|Y}(x|y)$. Например, для базиса R имеем

$$p_{X|Y}(x|y) = \\ = {\rm Tr}_E\{{}_A\langle x| \otimes {}_B\langle y|\psi_R\rangle_{ABE}\ {}_{ABE}\langle\psi_R|y\rangle_B \otimes |x\rangle_A\}, \qquad (13)$$

где $|x\rangle_A = \{|\overline{0}_R^{+\times}\rangle_A, |\overline{1}_R^{+\times}\rangle_A\} \to \{0,1\}$ и $|y\rangle_B = \{|\overline{0}_R^{+\times}\rangle_B, |\overline{1}_R^{+\times}\rangle_B, |3\rangle_B\} \to \{0,1,?\}$.

С учетом симметрии между 0 и 1, а также симметрии между базисами после измерений можно опустить индексы "×", "+". Используя энтропийные соотношения неопределенностей (8), для длины секретного ключа находим

$$H(X_A|E) \ge 2\log\frac{1}{c} - H(X_A|Y_B), \\ l_{\rm secr} \approx 2\log\frac{1}{c} - 2H(X_A|Y_B). \qquad (14)$$

Ситуация между Алисой и Бобом теперь описывается симметричным классическим каналом связи с двумя состояниями на входе и тремя на выходе (рис. 1). С учетом симметрии и условий нормировки условных

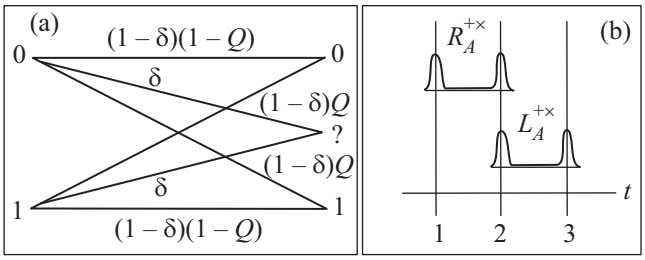

Рис. 1. (a) – Схематическое изображение классического канала связи Алиса–Боб. (b) – Информационные состояния в базисах R и L

вероятностей параметризация осуществляется однозначно. Ее удобно выбрать в следующем виде:

$$p_{X|Y}(0|0) = p_{X|Y}(1|1) = (1-\delta)(1-Q), \\ p_{X|Y}(0|1) = p_{X|Y}(1|0) = (1-\delta)Q, \qquad (15) \\ p_{X|Y}(0|?) = p_{X|Y}(1|?) = \delta.$$

Осталось вычислить константу c в (4): $c = |{}_A\langle\overline{0}_L^{+\times}|\overline{0}_R^{+\times}\rangle_A| = |{}_A\langle\overline{0}_L^{+\times}|\overline{1}_R^{+\times}\rangle_A| = |{}_A\langle\overline{1}_L^{+\times}|\overline{1}_R^{+\times}\rangle_A| = 1/2$. Окончательно для длины секретного ключа имеем[1)]

$$l_{\rm secr} \approx 2\left[1 - H(X_A|Y_B)\right] = 2\left[1 - (1-\delta)h(Q) - h(\delta)\right]. \qquad (16)$$

В протоколе квантового распределения ключей с фазово-временны́м кодированием критическая ошибка, до которой гарантируется секретное распределение ключей, зависит от двух параметров, δ и Q. Смысл этих параметров физически прозрачен. Величина $1-\delta$ равна доле отсчетов в информационных временны́х окнах (напомним, что информационные состояния являются суперпозицией состояний во временны́х окнах 1 и 2 в базисе R и 2 и 3 в базисе L). Соответственно, δ – доля отсчетов в контрольных временны́х окнах 3 в базисе R и 1 в базисе L (рис. 1). В информационных окнах доля отсчетов $1-Q$ является правильной, а Q – ошибочной.

Оба параметра находятся в руках подслушивателя. Однако Алиса и Боб перед передачей ключей могут декларировать, что протокол будет прерван, если величина δ превысит критическое значение, $\delta > \delta_c \approx \approx 0$. В результате у Евы не остается других возмож-

[1)] Отметим, что в [13] для длины ключа было получено выражение $l_{\rm secr} \approx 1 - h(Q) - h(\eta)$, $\eta = \delta/(1-\delta)$, т.к. использовалась постселекция отсчетов в контрольных временны́х окнах и величина ошибки пересчитывалась на информационные временны́е окна. Предельная величина ошибки при $\delta \to 0$ также равна $Q_c \to 50\%$, а критическое значение составляет $\delta_c = 1/3$ (вместо $\delta_c = 1/2$ в данном протоколе). Здесь же ограничение на величину $\delta \le 1/2$ возникает из условия унитарной реализуемости атаки Евы, $(I_A \otimes U_{BE})|\Phi_{R,L}\rangle_{AB} \to |\Psi_{R,L}\rangle_{ABE}$.

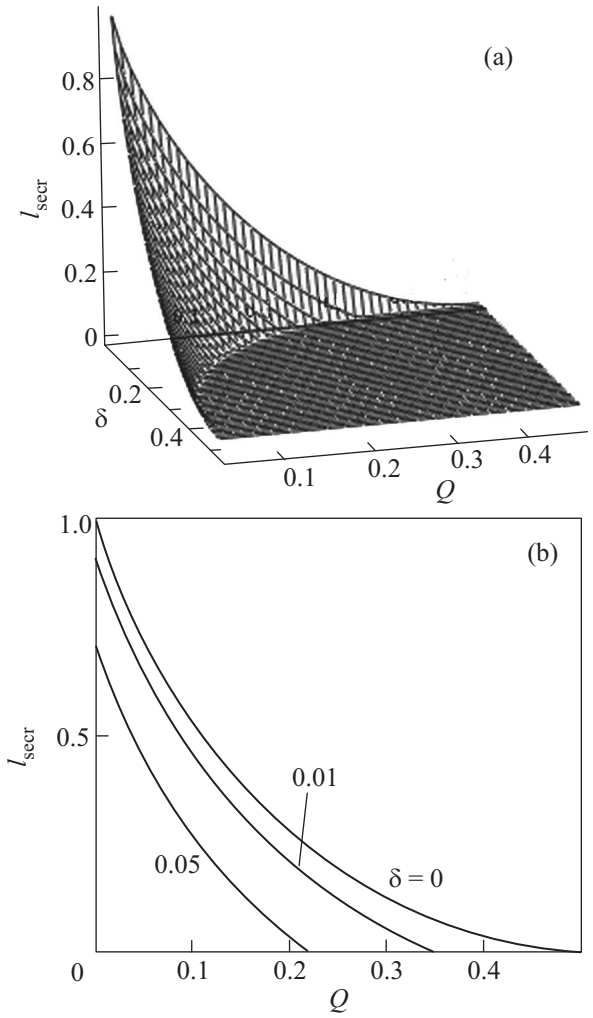

Рис. 2. Зависимости длины секретного ключа от параметров протокола Q и δ

ностей, кроме как регулировать ошибку Q, которая в этом случае может достигать $Q_c \to 50\%$. Это связано с тем, что Ева не может отличить достоверно состояния в базисах R и L, что *неизбежно будет приводить к отсчетам с вероятностью δ в контрольных временны́х окнах, которых не должно быть при совпадающих у Алисы и Боба базисах.*

Сравнение с протоколом BB84. Сравним критическую ошибку для протокола с фазово-временны́м кодированием с критической ошибкой для протокола BB84. В протоколе BB84 используется только один из базисов, $R^{+,\times}$ или $L^{+,\times}$, $|\overline{0}^{+}\rangle_A = (|1\rangle_A + |2\rangle_A)/\sqrt{2}$, $|\overline{1}^{+}\rangle_A = (|1\rangle_A - |2\rangle_A)/\sqrt{2}$ и $|\overline{0}^{\times}\rangle_A = (|1\rangle_A + i|2\rangle_A)/\sqrt{2}$, $|\overline{1}^{\times}\rangle_A = (|1\rangle_A - i|2\rangle_A)/\sqrt{2}$. Величина перекрытия состояний "+" и "×" из разных базисов в этом случае равна $c = |{}_A\langle\overline{0}^{+}|\overline{0}^{\times}\rangle_A| = |{}_A\langle\overline{0}^{+}|\overline{1}^{\times}\rangle_A| = |{}_A\langle\overline{1}^{+}|\overline{1}^{\times}\rangle_A| = 1/\sqrt{2}$. Согласно (14) получаем

$$H(X_A|E) \geq 2\log\frac{1}{c} - H(X_A|Y_B),$$
$$l_{\text{secr}} \approx 2\log\frac{1}{c} - 2H(X_A|Y_B) = 1 - 2h(Q), \tag{17}$$

что приводит к знаменитой критической ошибке $Q_c \approx 11\%$ $(1 = 2h(Q_c))$ [12, 16, 17] (в работе [18] критическая ошибка за счет модификации протокола увеличена до $\approx 20\%$).

Заключение. Таким образом, протокол с фазово-временны́м кодированием позволяет "дотянуться" по критической ошибке до величины $Q_c \to 50\%$, до которой гарантируется секретное распределение ключей. Величина $Q_c \to 50\%$ существенно превышает допустимую ошибку для всех известных протоколов и является теоретическим пределом.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа частично поддержана проектом РФФИ # 11-02-00455.

1. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397 (1948); **27**, 623 (1948).
2. R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, N.Y., 1968.
3. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India **175** (1984).
4. W. Heisenberg, Zeit. für Phys. **43**, 172 (1927).
5. H. P. Robertson, Phys. Rev. **34**, 163 (1929).
6. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
7. K. Kraus, Phys. Rev. D **35**, 3070 (1987).
8. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
9. J. M. Renes and J.-C. Boileau, Phys. Rev. Lett., **103**, 020402-1 (2009).
10. M. Berta, M. Chritlandl, R. Colbeck et al., arXiv/quant-ph: 0909.0950.
11. M. Tomamichel and R. Renner, arXiv/quant-ph: 1009.2015.
12. R. Renner, arXiv/quant-ph: 0512258.
13. С. Н. Молотков, ЖЭТФ **133**, 5 (2008); Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).
14. C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
15. D. Mayers, *Advances in Cryptology – CRYPTO LNCS*, Springer, **1109**, 343 (1996).
16. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
17. M. Koashi, J. Phys. (Conf. Ser.) **36**, 645 (2007).
18. D. Gottesman and H.-K. Lo, arXiv/quant-ph: 0105121.