Письма в ЖЭТФ, том 105, вып. 12, с. 763 – 767

Квантовая запутанность и составные ключи в квантовой криптографии

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия Криптографии Российской Федерации, 121552 Москва, Россия

Факультет Вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 9 марта 2017 г.

После переработки 10 мая 2017 г.

Секретность протоколов квантовой криптографии после сеанса квантового распределения ключей (КРК) формулируется в терминах близости двух ситуаций – квантовых состояний, отвечающих реальной и идеальной ситуациям после КРК. Мерой близости является следовое расстояние. Более естественно формулировать секретность непосредственно в терминах малости вероятности успеха угадывания ключей подслушивателем после произвольного числа сеансов КРК. Возникает принципиальный вопрос, ответ на который заранее крайне неочевиден – достаточно ли критерия секретности в смысле близости реальной и идеальной ситуаций для одного сеанса КРК для того, чтобы гарантировать секретность ключей в смысле малости вероятности угадывания ключей подслушивателем для произвольного числа сеансов КРК? Показано, что ответ на данный вопрос оказывается положительным.

DOI: 10.7868/S0370274X17120116

Введение. Многие фундаментальные вопросы передачи и переработки информации в квантовой информатике сводятся к задачам различения квантовых состояний [1]. Вероятность различения квантовых состояний возникает в результате измерений. Имеется несколько мер, через которые выражается вероятность успеха различения квантовых состояний. Такими мерами являются следовое расстояние [1] и величина Холево [2–4].

Следовое расстояние возникает в задаче различения *пары квантовых состояний. Измерение имеет два исхода.* Для измерений предъявляется одно из состояний – ρ или σ. Один исход измерений интерпретируется как состояние ρ, второй как σ. Для пары квантовых состояний ρ и σ существует точное решение для максимальной вероятности успеха угадывания, которая выражается через следовое расстояние между матрицами плотности – $||\rho - \sigma||_1$ (см. далее).

Величина Холево ($\chi(\mathcal{E})$) возникает в задаче о различении максимально возможного числа последовательностей квантовых состояний ρ^x, эмитируемых источником в соответствии с распределением вероятностей $P_X(x)$. Здесь $\mathcal{E} = \{P_X(x), \rho^x\}$ – квантовый ансамбль, примем для определенности $x \in X = \{0,1\}^n$. Пусть классический источник генерирует классические символы из алфавита $x \in X = (x_1, x_2, \dots x_n)$ в соответствие с распределением вероятностей $P_X(x)$. Далее каждому классическому символу сопоставляется квантовое состояние ρ^x, которое предъявляется для измерений. Генерируется серия независимых состояний длиной M – $\rho^{x_{i_1}} \otimes \rho^{x_{i_2}} \otimes \dots \rho^{x_{i_M}}$. Цель измерений – различить последовательности состояний. *Измерение имеет* 2^{Mn} *исходов.* Величина Холево дает фундаментальную границу для максимального числа последовательностей $2^{M\chi(\mathcal{E})}$, которые могут быть различены из полного числа 2^{Mn} всевозможных последовательностей.

Квантовая механика допускает коллективные измерения с использованием запутанных состояний. Такие измерения сводятся к измерению всей последовательности. Один из фундаментальных результатов квантовой теории информации сводится к тому, что классическая информация, извлекаемая при таких измерениях, оказывается больше, чем сумма информаций при индивидуальных измерениях. Именно на таких измерениях достигается граница Холево [2–4].

Квантовая криптография на сегодняшний день, возможно, единственное из направлений квантовой теории информации, которое доведено до реальных практических применений. Целью квантовой криптографии является распределение секретных клю-

[1)]e-mail: sergei.molotkov@gmail.com

чей по открытым для прослушивания квантовым каналам связи. *Доказанный критерий секретности протоколов квантовой криптографии формулируется не в терминах различимости непосредственно самих ключей, а в терминах различимости пары квантовых состояний, отвечающих реальной и идеальной ситуациям* [5–7]. Кроме того, критерий секретности протокола квантовой криптографии формулируется для одного сеанса квантового распределения ключей (КРК), при этом возникают принципиальные вопросы о составных протоколах и составных ключах [6, 7].

Было бы естественней формулировать критерий секретности непосредственно для вероятности успеха угадывания самих ключей, которые имеют легитимные пользователи и подслушиватель после проведения им измерений над своей квантовой системой, коррелированной с ключами легитимных пользователей. При этом вероятность успеха угадывания можно было бы получить сразу для произвольного числа сеансов КРК с учетом коллективных измерений подслушивателя. Однако для формулировки критерия секретности в терминах вероятности угадывания подслушивателем непосредственно самих ключей нужно знать квантовые состояния. В этом случае можно было бы вычислить фундаментальную границу Холево и вероятность успеха угадывания ключей подслушивателем. Однако сами квантовые состояния подслушивателя неизвестны, а известно лишь, что они находятся ε-близко в смысле следового расстояния к состояниям для идеальной ситуации. Возникает принципиальный вопрос, достаточно ли следового расстояния, которое определяет вероятность различения пары состояний – ситуаций в одном сеансе – для того, чтобы гарантировать малость вероятности угадывания непосредственно для самих ключей в произвольном числе сеансов КРК? Прояснению этих вопросов посвящена данная заметка.

Критерий секретности в квантовой криптографии, основанный на следовом расстоянии. Рассмотрим критерий секретности протокола. основанный на следовом расстоянии [5–7]. Еще раз подчеркнем, что *данный критерий относится к различимости пары квантовых состояний, описывающих реальную и идеальную ситуации после КРК, а не к критерию различимости непосредственно самих ключей.* В результате сеанса КРК у легитимных пользователей возникает общий ключ $x \in X = \{0,1\}^n$ длины n; вероятность появления ключа $P_X(x)$. Подслушиватель имеет в своем распоряжении квантовую систему ρ_E^x, коррелированную с этим ключом, которую он может сохранять в квантовой памяти. Реальная ситуация после сеанса КРК описывается матрицей плотности ρ_{XE}. Идеальной ситуации отвечает состояние $\rho_U \otimes \rho_E$. Ключи в идеальной ситуации $x \in X = \{0,1\}^n$ равномерно распределены и некоррелированы с квантовой системой подслушивателя. Матрицы плотности, описывающие обе ситуации, имеют вид

$$\rho_{XE} = \sum_{x\in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x,$$
$$\rho_U = \frac{1}{N}\sum_{x\in X} |x\rangle\langle x|, \qquad (1)$$
$$\rho_E = \sum_{x\in X} P_X(x)\rho_E^x, \quad N = 2^n.$$

Критерий секретности [5, 6] дается в абстрактных терминах различимости *пары квантовых состояний* – малости следового расстояния между двумя ситуациями – квантовыми состояниями

$$||\rho_{XE} - \rho_U \otimes \rho_E||_1 = \frac{1}{2}\mathrm{Tr}\{|\rho_{XE} - \rho_U \otimes \rho_E|\} < \varepsilon.$$

При этом часто употребляется выражение, что ключи, полученные в таком протоколе, являются ε-секретными [5, 6], что может приводить к путанице. Правильнее говорить, что реальная ситуация после протокола ε-секретна. Параметр секретности ε выбирается легитимными пользователями "административно". Заданное значение ε достигается сжатием очищенных ключей до финального ключа x нужной длины. Очищенные ключи возникают после передачи квантовых состояний, измерений над ними и исправления ошибок в исходной битовой последовательности. Чем меньше ε, тем большей длины нужен очищенный ключ, соответственно, большее число исходно переданных квантовых состояний. *С операциональной точки зрения критерий секретности* [5, 6], *основанный на следовом расстоянии, относится, скорее, не к самим ключам, а к различимости реальной и идеальной ситуаций. Данный критерий дает вероятность успешного различения двух ситуаций.* Это означает, что если подслушиватель будет делать измерения с двумя исходами после КРК с целью различить в какой ситуации он находится – в ситуации с реальной матрицей плотности ρ_{XE} или идеальной с матрицей плотности $\rho_U \otimes \rho_E$, – то максимальная вероятность успеха различения этих двух ситуаций превышает вероятность простого угадывания не более, чем на $\varepsilon/2$:

$$\mathrm{Pr}_{\mathrm{Guess}}(\rho_{XE}, \rho_U \otimes \rho_E) =$$
$$= \frac{1}{2} + \frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \frac{1}{2} + \frac{1}{2}\varepsilon. \qquad (2)$$

Критерий секретности, основанный на вероятности угадывания ключей для произвольного числа сеансов КРК. Любое измерение в квантовой механике дается разложением единицы. Подчеркнем еще раз, что измерение, которое приводит к вероятности успеха по отличению одного из двух состояний – ситуаций ρ_{XE} и $\rho_U \otimes \rho_E$, содержит два исхода. Разложение единицы в этом случае имеет вид

$$I_{XE} = \mathcal{P}_0 + \mathcal{P}_1, \quad 0 \to \rho_{XE}, \quad 1 \to \rho_U \otimes \rho_E, \qquad (3)$$

где $\mathcal{P}_0$ и $\mathcal{P}_1$ – положительные операторно-значные меры, I_{XE} – единичный оператор для пространства состояний в одном сеансе КРК, соответственно в M сеансах $I_{XE}^{\otimes M}$.

Более естественно использовать критерий секретности непосредственно при вероятности угадывания ключей для произвольного числа сеансов. Пусть проведено M сеансов, в каждом из которых получен ключ x_{i_1}, x_{i_2}, и т.д.; x_{i_M}, $x_{i_k} \in X = \{0,1\}^n$, $k = 1, 2, \dots M$. Подслушиватель имеет последовательность квантовых состояний, коррелированных с данными ключами $\rho_E^{x_{i_1}}, \rho_E^{x_{i_2}}, \dots, \rho_E^{x_{i_M}}$, над которыми он может делать коллективные измерения сразу над всей последовательностью. В результате измерений сразу над всей последовательностью подслушиватель получает единую битовую последовательность $(\hat{x}_{i_1}, \hat{x}_{i_2}, \dots, \hat{x}_{i_M}) \in Y^M = \{\{0,1\}^n\}^M$. Вероятность того, что данная последовательность совпадает с ключами по всем сеансам, следующая:

$$\overline{\Pr}_{\text{Guess}}(M) = \qquad (4)$$

$$\sum_{x_i = \hat{x}_i \in (X,Y), i=1,2,\dots M} P_{X^M Y^M}(x_1, x_2, \dots x_M, \hat{x}_1, \hat{x}_2, \dots \hat{x}_M).$$

Измерение, в результате которого подслушиватель отличает последовательности квантовых состояний, коррелированных с ключами, дается разложением единицы вида

$$I_{XE}^{\otimes M} = \sum_{\hat{i} \in (i_1, i_2, \dots i_M)} \mathcal{M}_{\hat{i}}, \quad \hat{i} = 1, 2, \dots 2^{Mn}, \qquad (5)$$
$$i_k = 1, 2, \dots 2^n, \quad k = 1, 2, \dots n,$$

где $\mathcal{M}_{\hat{i}}$ – положительные операторно-значные меры, которые отличаются от мер в (3). Измерения имеют 2^n исходов для одного сеанса, и 2^{Mn} исходов для M сеансов. *Заранее неочевидно и ниоткуда заранее не следует, что из малости вероятности успеха различения двух состояний ρ_{XE} и $\rho_U \otimes \rho_E$, будет следовать малость вероятности различения самих ключей.*

Наша дальнейшая задача будет сводиться к нахождению верхней границы для вероятности угадывания по ключам по всевозможным измерениям. Как будет показано далее, верхняя граница по коллективным измерениям сразу над всей последовательностью квантовых состояний длины M для всех сеансов КРК будет выражаться через фундаментальную величину Холево, которую, как окажется, можно мажорировать следовым расстоянием для одного сеанса КРК.

Запутанные коллективные измерения и граница Холево для M сеансов КРК. В этом разделе будет получена верхняя граница вероятности угадывания непосредственно для самих ключей для произвольного числа сеансов с учетом коллективных измерений подслушивателя. Для вычисления величины Холево требуется знать непосредственно сами квантовые состояния подслушиателя в каждой посылке. Однако сами состояния неизвестны, гарантируется лишь их близость в следовой метрике к состояниям для идеальной ситуации. Заранее неочевидно, что этого достаточно. Покажем, что величина Холево, дающая вероятность успеха при угадывания самих ключей в произвольном числе сеансов, может быть ограничена сверху следовым расстоянием в одном сеансе.

Всего имеется $2^{M \cdot n}$ последовательностей, с которыми ассоциированы последовательности квантовых состояний. Каждый ключ возникает с вероятностью $P_X(x)$. Пусть выбрана определенная случайная кодовая таблица. Неформально это означает, что сделано сопоставление каждой битовой последовательности квантовых состояний, $\hat{x}^l = (x_{i_1}^l, x_{i_2}^l, \dots x_{i_M}^l) \to$ $\to (\rho_E^{x_{i_1}^l}, \rho_E^{x_{i_2}^l}, \dots \rho_E^{x_{i_M}^l})$. Ошибка за счет коллективных запутанных измерений по всем кодовым словам в данной таблице определяется как

$$\overline{\Pr}_{\text{Guess}}(M, l) = 1 - \frac{1}{2^{M \cdot n}} \sum_{j=1}^{2^{M \cdot n}} \text{Tr}\{\rho_E^{\hat{x}^l} \mathcal{M}_j^l\}, \qquad (6)$$
$$\hat{x}^l = (x_{i_1}^l, x_{i_2}^l, \dots x_{i_M}^l),$$

где измерение дается разложением единицы вида (5). Средняя ошибка по всем случайным кодовым таблицам, сгенерированным в соответствии с распределением вероятностей $P_X(x)$, определяется как (см. детали в [2–4, 8–10], идея вычисления ошибки восходит к работам Шеннона, Галлагера, Аримото для классических каналов [9, 10], затем идея была перенесена на квантовые каналы [2–4, 8]):

$$\overline{\Pr}_{\text{Guess}}(M) = \mathbf{E}\left(\overline{\Pr}_{\text{Guess}}(M, l)\right),$$

$$\mathbf{E}(\ldots)=\sum_{x_{i_1}\in X}\sum_{x_{i_2}\in X}\ldots \tag{7}$$

$$\ldots\sum_{x_{i_M}\in X}P_X(x_{i_1})P_X(x_{i_2})\ldots P_X(x_{i_M})(\ldots),$$

где усреднение проводится по распределению вероятностей $P_X(x)$. Для ошибки может быть получено неравенство – сильное обращением теоремы кодирования (см. детали в [8, 10]):

$$\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M)>1-\exp\{-M(-s\cdot n+E_0(s,P_X))\}, \tag{8}$$

$$E_0(s,P_X)=-\log\left(\mathrm{Tr}\left(\sum_{x\in X}P_X(x)(\rho_E^x)^{\frac{1}{s+1}}\right)^{s+1}\right),$$

где параметр s – произвольное число в интервале $-1<s<0$. Из (8) следует, что

$$E_0(0,P_X)=0,\quad \frac{\partial E_0(s,P_X)}{\partial s}|_{s=0}=$$
$$=S(\overline{\rho}_E)-\sum_{x\in X}P_X(x)S(\rho_E^x)=\chi(\mathcal{E}), \tag{9}$$

где $S(\rho)=-\mathrm{Tr}\{\rho\log(\rho)\}$ – энтропия фон Неймана, $\chi(\mathcal{E})$ – величина Холево для квантового ансамбля $\mathcal{E}=\{P_X(x),\rho_E^x\}$. Из (9) следует, что при $-s\cdot n+$ $+\chi(\mathcal{E})>0$ (для $-1<s<0$) ошибка будет экспоненциально мала. Далее требуется установить связь между следовым расстоянием и границей Холево $\chi(\mathcal{E})$.

Секретность для различения пары состояний. Секретность в смысле следового расстояния для различения пары состояний в одном сеансе гарантирует секретность в смысле малости вероятности успеха угадывания ключей для любого числа сеансов КРК. Теперь покажем, что критерия секретности в смысле следового расстояния для одного сеанса КРК оказывается достаточным для произвольного числа сеансов КРК. Покажем, что следовое расстояние мажорирует информацию Холево, $\chi(\mathcal{E})<2\varepsilon\cdot n$. Откуда будет следовать, что из полного числа $2^{M\cdot n}$ последовательностей подслушиватель сможет различить не более $2^{M\cdot n2\varepsilon}$ битовых последовательностей, т.е. лишь экспоненциально малую долю $2^{-M\cdot n(1-2\varepsilon)}$. Для этого потребуется несколько вспомогательных величин, связанных с асимметричной относительной квантовой энтропией (см. детали в [11–13]]). Определим отображение для положительных операторов $\Lambda_\rho(\sigma)$,

$$\Lambda_\rho(\sigma)=\frac{d}{dt}\log(\rho+\sigma t)|_{t=0}=$$
$$=\int_0^\infty ds(\rho+sI)^{-1}\sigma(\rho+sI)^{-1},\quad \Lambda_\rho(\rho)=I, \tag{10}$$

где производная понимается в смысле Фреше. Далее введем полуторалинейную форму, которая может рассматриваться как метрика:

$$M_\rho(\sigma,\tau)=\mathrm{Tr}\{\sigma\Lambda_\rho(\tau)\},\quad M_\rho(\sigma,\sigma)\geq 0. \tag{11}$$

Дифференциал от асимметричной относительной энтропии

$$D_\alpha(\rho||\sigma)=\alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\}=$$
$$=-\alpha\frac{d}{d\alpha}S(\rho||\alpha\rho+(1-\alpha)\sigma), \tag{12}$$

где относительная $S(\rho||\sigma)$ и асимметричная $S_\alpha(\rho||\sigma)$ энтропии соответственно равны

$$S(\rho||\sigma)=\mathrm{Tr}\{\rho(\log(\rho)-\log(\sigma))\},$$
$$S_\alpha(\rho||\sigma)=-\frac{1}{\log(\alpha)}S(\rho||\alpha\rho+(1-\alpha)\sigma). \tag{13}$$

Асимметричная энтропия в отличие от относительной является непрерывной и связана с дифференциалом следующим соотношением:

$$S_\alpha(\rho||\sigma)=-\frac{1}{\log(\alpha)}\int_0^{-\log(\alpha)}D_\alpha(\rho||\sigma)d(-\log(\alpha')). \tag{14}$$

С учетом (10)–(14) дифференциальная энтропия явно ограничивается сверху следовым расстоянием

$$D_\alpha(\rho||\sigma)=\alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\}=$$
$$=\alpha\mathrm{Tr}\{(\rho-\sigma)\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\}\leq$$
$$\leq\alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\}\leq$$
$$\leq\alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\alpha\rho+(1-\alpha)\sigma)\}=$$
$$=\mathrm{Tr}\{(\rho-\sigma)_+\}=\delta(\rho,\sigma), \tag{15}$$

где $(\rho-\sigma)_+$ – проекция на подпространство, отвечающая положительным собственным числам.

Остается связать величину Холево с относительной энтропией, а относительную энтропию с дифференциальной энтропией, которая ограничена следовым расстоянием. Величина Холево по определению [2–4] имеет вид

$$\chi(\mathcal{E})=S(\overline{\rho}_E)-\sum_{x\in X}P_X(x)S(\rho_E^x),\quad \overline{\rho}_E=\sum_{x\in X}P_X(x)\rho_E^x. \tag{16}$$

Величина Холево выражается через относительную энтропию

$$\chi(\mathcal{E}) = \sum_{x\in X} P_X(x) S(\rho_E^x||\overline{\rho}_E) =$$
$$= -\sum_{x\in X} P_X(x)\log(P_X(x)) S_{P_X(x)}(\rho_E^x||\overline{\rho}_E^x) \le$$
$$\le -\sum_{x\in X} P_X(x)\log(P_X(x))\delta(\rho_E^x,\overline{\rho}_E^x) \le$$
$$\le -\sum_{x\in X} P_X(x)\log(P_X(x)) \times$$
$$\times \sum_{x\ne x'\in X} \frac{P_X(x')}{1-P_X(x)}\delta(\rho_E^x,\rho_E^{x'}). \qquad (17)$$

Последнее слагаемое в цепочке неравенств (17) мажорируется следовым расстоянием

$$\frac{1}{2}\sum_{x\ne x'\in X}\frac{P_X(x')}{1-P_X(x)}|\rho_E^x-\rho_E^{x'}| \le$$
$$\le \frac{1}{2}\sum_{x\ne x'\in X}\frac{1}{1-P_X(x)} \times$$
$$\times\left(|P_X(x')\rho_E^{x'}-P_X(x)\rho_E^x|+|\rho_E^x(P_X(x')-P_X(x))|\right)\le$$
$$\le \frac{1}{2}\sum_{x\in X}\frac{2}{1-P_X(x)} \times$$
$$\times\left(|\frac{\overline{\rho}_E}{N}-P_X(x)\rho_E^x|+|\rho_E^x||P_X(x)-\frac{1}{N}|\right). \qquad (18)$$

Вычисляя след от (18) и учитывая, что максимальная вероятность не превышает $\max_{x\in X} P_X(x) < \frac{1}{N} + \varepsilon$, получаем

$$\frac{1}{1-(\frac{1}{N}+\varepsilon)} \times \qquad (19)$$
$$\times\left(\sum_{x\in X}\mathrm{Tr}\{|\frac{\overline{\rho}_E}{N}-P_X(x)\rho_E^x|\}+||P_X-\frac{1}{N}||_1\right) < \frac{2\varepsilon}{1-2\varepsilon}.$$

Для величины Холево приходим к неравенству $\chi(\mathcal{E}) < H(X)\frac{2\varepsilon}{1-2\varepsilon} \approx 2\varepsilon H(X) < 2\varepsilon\cdot n$. С учетом того, что параметр $0 < |s^*| < 1$ в (8), для вероятности правильного угадывания находим

$$\mathrm{Pr}_{\mathrm{Guess}}(M) < \frac{1}{2^{M\cdot n(1-2\varepsilon)}}. \qquad (20)$$

Заключение. Интерпретируем формулу (20). В идеальном случае, когда ключи строго равномерно распределены и подслушиватель может их только угадывать, вероятность равна $\mathrm{Pr}_{\mathrm{Guess}}(M) = \frac{1}{2^{M\cdot n}}$ обратной величине размерности ключевого пространства. В реальной ситуации вероятность (20) успеха различения ключей в M сеансах с учетом коллективных измерений имеет аналогичный вид, и можно думать, что вероятности успеха для отдельных сеансов КРК умножаются. Важно подчеркнуть, что данный результат не может быть получен перемножением вероятностей, вычисленных для отдельных сеансов КРК, поскольку подслушиватель использует коллективные измерения с проектированием на запутанные измеряющие состояния целой последовательности квантовых состояний для всех сеансов.

Таким образом, если протокол в одном сеансе КРК является ε-секретным в смысле различения двух ситуаций, то он является таковым и для произвольного числа сеансов КРК – гарантируется малость вероятности угадывания непосредственно самих ключей. При этом без ущерба для криптостойкости ключи из разных сеансов можно конкатенировать в единый ключ.

Выражаю благодарность И.М. Арбекову, А.Н. Климову, С.П. Кулику за многочисленные обсуждения, а также коллегам по Академии криптографии Российской Федерации за постоянную поддержку и обсуждения. Работа выполнена при поддержке гранта РНФ # 16-12-00015.

1. M. M. Wilde, *From Classical to Quantum Shannon*, arXiv: 1106.1445 [quant-ph].
2. A. S. Holevo, Probl. Inform. Transm. **9**, 177 (1973).
3. А. С. Холево, УМН **53** 193 (1998).
4. А. С. Холево, *Введение в квантовую теорию информации*, серия *Современная математическая физика*, вып. 5, МЦНМО, М. (2002).
5. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. (2005). arXiv/quant-ph: 0512258
6. C. Portmann and R. Renner, *Cryptographic Security of Quantum key Distribution*, arXiv: 1409.3525 [quant-ph].
7. J. Müller-Quade and R. Renner, *Composability in Quantum Cryptography*, arXiv: 1006.2215 [quant-ph].
8. T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory **45**, 2486 (1999).
9. R. G.Gallager, IEEE Trans. Inform. Theory **IT-11**, 3 (1965).
10. S. Arimoto, IEEE Trans. Inform. Theory **IT-19**, 357 (1973).
11. W. Roga, M. Fannes, and K. Zyczkowski, Phys. Rev. Lett. **105**, 040505 (2010).
12. K. M. R. Audenaert, J. Math. Phys. **54**, 073506 (2013).
13. K. M. R. Audenaert, J. Math, Phys. **55**, 112202 (2014).