

УДК 621.391 : 530.145 : 512.624.95 : 629.783

© 2023 г. А. В. Миллер

СИНХРОНИЗАЦИЯ ВРЕМЕНИ В СПУТНИКОВОМ КВАНТОВОМ РАСПРЕДЕЛЕНИИ КЛЮЧЕЙ

Временная синхронизация является одной из ключевых проблем, которые должны быть решены в процессе создания системы квантового распределения ключей (КРК). Точная синхронизация времени позволяет не только правильно присвоить порядковый номер каждому событию детектирования, но также увеличивает соотношение сигнал/шум. В спутниковой связи временная синхронизация затруднена особенно, ввиду таких факторов как высокие потери, замирание сигнала и эффект Доплера. В данной статье приводится описание простого, эффективного и надежного алгоритма для синхронизации времени. Алгоритм был протестирован в ходе реальных экспериментов по КРК между *Micius*, первым в мире спутником для квантовой связи, и приемной наземной станцией, расположенной на территории России. Полученная точность синхронизации лежит в диапазоне от 467 до 497 пс. Автор сравнивает свой алгоритм с использовавшимися ранее методами. Предлагаемый подход может применяться и для наземных систем КРК.

Ключевые слова: квантовая криптография, квантовое распределение ключей, спутниковая квантовая связь, синхронизация времени.

DOI: 10.31857/S0555292323040022, **EDN:** RHSP7P

§ 1. Введение

В основе квантовой криптографии лежит не вычислительная сложность используемых математических алгоритмов, а законы физики. Впервые эта идея была представлена в 1984 г. Чарльзом Беннетом и Жилем Брассаром, которые предложили первый протокол квантового распределения ключей [1]. В 1989 г. была продемонстрирована первая экспериментальная реализация квантового распределения ключей (КРК) [2]. В этом эксперименте кубиты были закодированы в поляризации фотонов, которые передавались через открытое пространство на оптическом столе на расстояние 32,5 см. С тех пор технология КРК претерпела существенное развитие. Расстояние между квантовым передатчиком и приемником существенно увеличилось. Так, в 2006 г. международная коллаборация ученых провела КРК между островами Пальма и Тенерифе в Атлантическом океане на расстояние 144 км с использованием протокола BB84 с состояниями-ловушками [3]. Недавно исследователи из Китая продемонстрировали КРК через оптоволокно на дистанции 1002 км с использованием протокола *Twin-field* [4]. Хотя полученный результат и является выдающимся для наземной системы КРК, скорость генерации секретного ключа на данном расстоянии составила около 10^{-11} бит на импульс, что едва ли можно считать удовлетворительным с точки зрения практического применения. Единственным разумным способом создать по-настоящему глобальную, межконтинентальную квантовую сеть видится использование искусственных спутников Земли: например, в качестве доверенных узлов между удаленными друг от друга наземными станциями. В 2016 г.

на орбиту был выведен первый такой спутник, Micius, и вскоре после этого были проведены эксперименты по КРК со спутника на Землю [5–7], распределению квантовой сцепленности [8], КРК на основе квантовой сцепленности [9] и квантовой телепортации [10].

Синхронизация времени является одним из наиболее важных аспектов в квантовом распределении ключей. Она позволяет Алисе и Бобу присвоить каждому событию детектирования правильный порядковый номер, что дает им возможность корректно выполнить согласование базисов. Кроме того, точная синхронизация времени позволяет существенно увеличить соотношение сигнал/шум. В спутниковом КРК синхронизация затруднена особенно, ввиду таких факторов как замирание сигнала, высокие потери и эффект Доплера. В системах КРК синхронизация может осуществляться, например, с помощью электрического сигнала [11] или глобальной навигационной спутниковой системы [3]. Однако наиболее распространенным методом является синхронизация с помощью излучения, что подразумевает передачу интенсивных оптических импульсов на той же [12] или другой [5, 13–16] длине волны. Также есть элегантное решение, основанное на анализе зарегистрированного квантового сигнала, которое не требует какого-либо дополнительного оборудования [17]. Недавно этот подход был с успехом адаптирован к реальному КРК со спутника на Землю [18]. Похожий метод использовался ранее другой группой исследователей [19], хотя стоит отметить, что интенсивность оптического сигнала в этом эксперименте на несколько порядков превышала интенсивность, соответствующую однофотонному уровню. В настоящей статье предлагается альтернативный подход, который более прост в реализации и не требует каких-то сложных математических вычислений. Данный подход, при обработке данных сразу со всего сеанса связи, показывает точность по крайней мере в 1,5 раза лучше, чем любой другой из ранее использовавшихся методов.

Структура этой статьи следующая: в § 2 даны общее описание проблемы синхронизации и детальное описание предлагаемого алгоритма; в § 3 представлены экспериментальные данные, полученные в ходе КРК между Micius и приемной наземной станцией на территории Звенигородской обсерватории; наконец, в § 4 даны некоторые выводы.

§ 2. Теория

2.1. Постановка задачи. Пусть Алиса отправляет квантовые состояния с периодом T_q , так что фотон с номером i испускается в момент времени $T_q \cdot i$. Поскольку часы Алисы могут спешить или отставать, реальное время испускания фотона составляет $\frac{\nu_0}{\nu_A} \cdot T_q \cdot i$, где ν_A – частота часов Алисы, а ν_0 – частота абсолютно точных часов. В общем случае также может быть некоторая задержка t_0^A , и тогда время испускания t_i должно быть записано как

$$t_i = t_0^A + \frac{\nu_0}{\nu_A} \cdot T_q \cdot i. \quad (1)$$

Следует отметить, что в уравнении (1) подразумевается, что частота часов ν_A не зависит от времени. В общем случае ν_A может быть функцией времени: $\nu_A = \nu_A(t)$. Тогда вместо (1) следует записать

$$\frac{1}{\nu_0} \int_{t_0^A}^{t_i} \nu_A(\eta) d\eta = T_q \cdot i. \quad (2)$$

Аспекты, связанные с дрейфом частоты, обсуждаются в этой статье далее. Пока что, если не оговорено иное, будем полагать, что частоты часов Алисы и Боба меняются

настолько медленно, что этими изменениями можно пренебречь на рассматриваемых временных интервалах.

Поскольку Алиса и Боб разделены пространством, есть некоторое ненулевое время распространения сигнала t_p . Соответственно, Боб принимает фотоны в моменты времени t_i^R , определенные следующим образом:

$$t_i^R = t_0^A + \frac{\nu_0}{\nu_A} \cdot T_q \cdot i + t_p. \quad (3)$$

Боб использует свои собственные часы, которые имеют частоту ν_B и временную задержку t_0^B , поэтому он ожидает принять фотон с номером i в момент времени

$$t_i^{R,EXP} = t_0^B + \frac{\nu_0}{\nu_B} \cdot T_q \cdot i. \quad (4)$$

Очевидно, что разница между $t_i^{R,EXP}$ и t_i^R не должна превышать по крайней мере $\frac{T_q}{2}$. В противном случае Боб будет некорректно присваивать порядковые номера тем фотонам, которые он получает.

Предположим, что Алиса и Боб синхронизировали свои часы таким образом, что $t_0^B = t_0^A + t_p$, т.е. первый фотон ($i = 0$) приходит в точности в то время, когда Боб его ожидает. Тогда разница между $t_i^{R,EXP}$ и t_i^R запишется как

$$t_i^{R,EXP} - t_i^R = T_q \cdot i \cdot \nu_0 \cdot \left(\frac{1}{\nu_B} - \frac{1}{\nu_A} \right). \quad (5)$$

Принимая во внимание равенство (5) и тот факт, что $|t_i^{R,EXP} - t_i^R|$ должно быть меньше $\frac{T_q}{2}$, можно найти i_{MAX} – такой максимальный индекс i , при котором квантовое распределение ключа все еще возможно:

$$i_{MAX} \cdot \nu_0 \cdot \left| \frac{1}{\nu_B} - \frac{1}{\nu_A} \right| = \frac{1}{2}. \quad (6)$$

До сих пор мы не предполагали, что разница в частотах мала. Тем не менее в большинстве случаев относительная разница невелика. Если определить величины ε_A и ε_B следующим образом:

$$\nu_{A(B)} = \nu_0 \cdot (1 + \varepsilon_{A(B)}), \quad (7)$$

то

$$|\varepsilon_{A(B)}| \ll 1. \quad (8)$$

Величину i_{MAX} можно выразить из (6), и тогда, принимая во внимание (7) и (8), получим

$$i_{MAX} = \frac{1}{2|\varepsilon_A - \varepsilon_B|}. \quad (9)$$

Верхней оценкой для $|\varepsilon_A - \varepsilon_B|$ может служить точность часов, умноженная на 2. Таким образом можно оценить i_{MAX} . Например, точность лучших часов на основе кварцевого осциллятора составляет $\sim 10^{-7}$, и тогда соответствующий i_{MAX} равен $\sim 2,5 \times 10^6$. При частоте следования квантовых состояний 100 МГц, что имеет место на спутнике Micius [5], это соответствует отрезку времени ~ 25 мс. Это означает, что по крайней мере каждые 25 мс Алиса и Боб должны каким-то образом синхронизировать свои часы. Широко распространено использование для этой цели оптических импульсов [5, 12–16]. Так, например, Micius оснащен лазером-маяком,

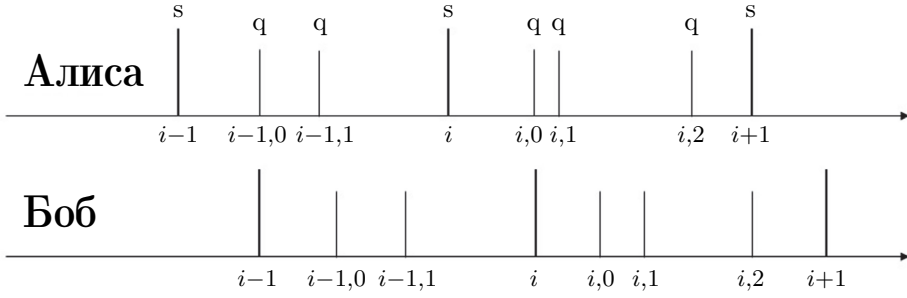


Рис. 1. Схематическое изображение синхроимпульсов (s) и квантового сигнала (q) на временной шкале

который генерирует световые импульсы длительностью 0,9 нс с частотой повторения ~ 10 кГц, которые также служат и целям синхронизации [5]. Гипотетически Алиса и Боб могли бы использовать атомные часы, которые намного более точны, и таким образом увеличить i_{MAX} на несколько порядков. Тем не менее в спутниковой связи в этом нет смысла из-за эффекта Доплера. Если спутник движется по своей орбите по скорости v_{SAT} , доплеровский сдвиг можно оценить как $\frac{v_{\text{SAT}}}{c}$, где c – скорость света в вакууме. Соответственно, нет смысла использовать часы, точность которых намного лучше, чем $\frac{v_{\text{SAT}}}{c}$, что для искусственных спутников Земли составляет $\sim 10^{-5}$. Хотя стоит отметить, что если траектория спутника известна с достаточной точностью, доплеровский сдвиг может быть скомпенсирован явным образом вычитанием рассчитанного t_p . В данной статье автор предлагает вниманию читателя альтернативный подход – простой и надежный алгоритм, который неявным образом одновременно учитывает как собственное смещение частоты, так и доплеровский сдвиг. При этом в данном подходе не требуется, чтобы траектория спутника была известна.

2.2. Предлагаемый подход.

Описание метода синхронизации. Допустим, есть последовательность из N синхроимпульсов, и пусть Алиса измеряет время каждого импульса t_{iA} , $i = 0, \dots, N-1$. Здесь и далее нижний индекс А (В) означает, что время измерено по часам Алисы (Боба). Боб принимает синхроимпульсы от Алисы и регистрирует их с помощью фотодетектора. Также Боб детектирует одиночные фотоны и присваивает каждому событию два индекса, i и j : i – это номер ближайшего предшествующего синхроимпульса, а j – порядковый номер среди всех событий, которые произошли между синхроимпульсами i и $i+1$ (см. рис. 1). Алиса отправляет Бобу значения t_{iA} по классическому открытому каналу связи. Теперь, если Бобу будут известны также значения $(t_{ij} - t_i)_A$, он сможет вычислить порядковые номера квантовых состояний n_{ij} , используя следующее выражение:

$$n_{ij} = \frac{t_{iA} + (t_{ij} - t_i)_A}{T_q}. \quad (10)$$

Таким образом, задачу синхронизации можно свести к задаче нахождения правильных значений $(t_{ij} - t_i)_A$.

Для начала рассчитаем время, когда Боб зарегистрирует синхроимпульс с номером i . Поскольку Алиса и Боб разделены в пространстве, есть некоторое ненулевое время распространения сигнала t_p , которое в спутниковой связи является функцией времени. Также есть некоторая случайная ошибка δt_i^{rand} , вызванная несовершен-

ством измерительного оборудования, в наибольшей степени – джиттером фотодетектора. Соответственно, время t_i^R , когда Боб регистрирует синхросигнал i , можно записать как

$$t_i^R = t_i + t_p(t_i) + \delta t_i^{\text{rand}}. \quad (11)$$

По аналогии с (11) время, когда Боб регистрирует квантовое состояние с индексами i, j , записывается как

$$t_{ij}^R = t_{ij} + t_p(t_{ij}) + \delta t_{ij}^{\text{rand}}. \quad (12)$$

Рассмотрим некоторую точку t_k , такую что все точки t_i и t_{ij} лежат в некоторой окрестности $(t_k - \delta t, t_k + \delta t)$ данной точки. Разложим функцию $t_p(t)$ в ряд Тейлора в окрестности точки t_k , удерживая квадратичные члены:

$$t_p(t_i) = t_p(t_k) + t'_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_i - t_k)^2, \quad (13)$$

$$t_p(t_{ij}) = t_p(t_k) + t'_p(t_k) \cdot (t_{ij} - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{ij} - t_k)^2. \quad (14)$$

Вычитая (11) из (12) и принимая во внимание (13) и (14), получаем

$$\begin{aligned} t_{ij}^R - t_i^R &= (t_{ij} - t_i) \cdot \left\{ 1 + t'_p(t_k) + t''_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{ij} - t_i) \right\} + \\ &+ \delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}. \end{aligned} \quad (15)$$

Очевидно, что если выполняется условие $t''_p \cdot \delta t \ll t'_p$, то третьим и четвертым членами в фигурных скобках можно пренебречь. Далее мы покажем, что это условие выполняется во время всего сеанса связи, за исключением короткого ($\lesssim 10$ мс) временного отрезка, внутри которого происходит изменение знака доплеровского сдвига. Стоит отметить, что вблизи точки изменения знака доплеровского смещения чрезвычайно мал и второй член в фигурных скобках t'_p . Это означает, что внутри данного интервала изменением t_p можно и вовсе пренебречь. Таким образом, квадратичные члены в (15) можно отбросить. Тогда, приняв также во внимание тот факт, что Алиса и Боб используют для измерения временных интервалов собственные часы, выражение (15) можно записать следующим образом:

$$\frac{\nu_0}{\nu_B} \cdot (t_{ij}^R - t_i^R)_B = \frac{\nu_0}{\nu_A} \cdot (t_{ij} - t_i)_A \cdot (1 + t'_p(t_k)) + \delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}. \quad (16)$$

Выражая $(t_{ij} - t_i)_A$ из (16), получаем

$$(t_{ij} - t_i)_A = \frac{\nu_A}{\nu_B} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (t_{ij}^R - t_i^R)_B + \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} (\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}). \quad (17)$$

Случайные ошибки δt_i^{rand} и $\delta t_{ij}^{\text{rand}}$ неизвестны, однако можно сделать разумное предположение, что математические ожидания этих величин равны 0. Тогда, если ввести обозначение

$$C_k = \frac{\nu_A}{\nu_B} \cdot \frac{1}{1 + t'_p(t_k)},$$

то (17) запишется в виде

$$(t_{ij} - t_i)_A = C_k \cdot (t_{ij}^R - t_i^R)_B. \quad (18)$$

По аналогии с (15) для двух соседних синхроимпульсов с номерами i и $i + 1$

$$t_{i+1}^R - t_i^R = \delta t_{i+1}^{\text{rand}} - \delta t_i^{\text{rand}} + (t_{i+1} - t_i) \cdot \left\{ 1 + t'_p(t_k) + t''_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{i+1} - t_i) \right\}. \quad (19)$$

Рассмотрим следующую сумму: $S_k = \sum_{i=0}^{N-2} (t_{i+1}^R - t_i^R)_B$. С одной стороны, очевидно, что

$$S_k = (t_{N-1}^R - t_0^R)_B. \quad (20)$$

С другой стороны, используя (19) и снова пренебрегая квадратичными членами, можно показать, что

$$S_k = \frac{\nu_B}{\nu_A} \cdot (t_{N-1} - t_0)_A \cdot (1 + t'_p(t_k)) + \frac{\nu_B}{\nu_0} \cdot (\delta t_{N-1}^{\text{rand}} - \delta t_0^{\text{rand}}). \quad (21)$$

Приравнявая (20) и (21), получим

$$(t_{N-1}^R - t_0^R)_B = \frac{\nu_B}{\nu_A} \cdot (1 + t'_p(t_k)) \cdot (t_{N-1} - t_0)_A + \frac{\nu_B}{\nu_0} \cdot (\delta t_{N-1}^{\text{rand}} - \delta t_0^{\text{rand}}). \quad (22)$$

Снова полагая, что математические ожидания случайных величин δt_0^{rand} и $\delta t_{N-1}^{\text{rand}}$ равны 0, ввиду того что

$$\frac{\nu_B}{\nu_A} \cdot (1 + t'_p(t_k)) \stackrel{\text{def}}{=} \frac{1}{C_k},$$

выразим C_k из (22):

$$C_k = \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B}. \quad (23)$$

Теперь, когда C_k найдены, можно рассчитать порядковые номера квантовых состояний n_{ij} , используя выражения (10) и (18). Таким образом, предлагаемый алгоритм чрезвычайно прост в реализации. Все, что необходимо сделать, – это разбить сеанс связи на короткие отрезки времени, внутри которых изменением доплеровского сдвига можно пренебречь. Затем для каждого временного интервала необходимо, используя (23), вычислить C_k . И наконец, используя формулы (10) и (18), нужно рассчитать порядковые номера квантовых состояний.

Точность синхронизации. Минимальное N . Точность синхронизации является статистической величиной и определяется как дисперсия величины $(t_{ij} - t_i)_A$. Если бы в (22) были известны реальные значения δt_0^{rand} и $\delta t_{N-1}^{\text{rand}}$, можно было бы рассчитать истинное значение C_k :

$$C_k^r = \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B + \frac{\nu_B}{\nu_0} \cdot (\delta t_0^{\text{rand}} - \delta t_{N-1}^{\text{rand}})}. \quad (24)$$

Аналогично, зная реальные значения случайных ошибок, из (17) можно было бы вычислить истинное значение $(t_{ij} - t_i)_A$:

$$(t_{ij} - t_i)_A^r = C_k^r \cdot (t_{ij}^R - t_i^R)_B + \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (\delta t_i^{\text{rand}} - \delta t_{ij}^{\text{rand}}). \quad (25)$$

Характерная величина случайной ошибки измерения намного меньше, чем все остальные временные интервалы. Если принять это во внимание, можно показать,

что разница между величиной $(t_{ij} - t_i)_A$, рассчитанной согласно выражению (18), и истинным значением $(t_{ij} - t_i)_A^r$ будет равна

$$\begin{aligned} & \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}) + \\ & + \frac{\nu_B}{\nu_0} \cdot \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B} \cdot (t_{ij}^R - t_i^R)_B \cdot (\delta t_0^{\text{rand}} - \delta t_{N-1}^{\text{rand}}). \end{aligned} \quad (26)$$

Как уже было сказано, в реальности сдвиг частоты достаточно мал: $|\varepsilon_{A(B)}| \ll 1$. Величина $|t'_p|$ не может превышать $\frac{v_{\text{SAT}}}{c}$, что составляет $\sim 10^{-5}$ для искусственных спутников Земли. Следовательно, множитель $\frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)}$ в первом слагаемом примерно равен 1. Множитель во втором слагаемом может быть записан как

$$\frac{\nu_B}{\nu_0} \cdot \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B} \times \frac{(t_{ij}^R - t_i^R)_B}{(t_{N-1}^R - t_0^R)_B}.$$

Ввиду сказанного выше первая часть множителя также примерно равна 1. Вторая часть не превышает величину, примерно равную $\frac{1}{N}$. Таким образом, если N достаточно велико, вторым слагаемым в (26) можно пренебречь. С практической точки зрения $N = 10$ является достаточным, поскольку в этом случае множитель во втором слагаемом уже на порядок меньше, чем в первом. Далее, если мы предположим, что $\delta t_{ij}^{\text{rand}}$ и δt_i^{rand} – это две независимые нормально распределенные случайные величины с математическими ожиданиями, равными 0, тогда $\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}$ также является нормально распределенной случайной величиной с математическим ожиданием, равным 0, и дисперсией $\sigma^2 = \sigma_i^2 + \sigma_{ij}^2$, где σ_i определяется джиттером фотодетекторов, которые используются для регистрации синхроимпульсов на спутнике и наземной станции, в то время как σ_{ij} определяется конечной шириной лазерных импульсов и джиттером детекторов одиночных фотонов, которые используются для регистрации квантового сигнала. Таким образом, наилучшая точность синхронизации, которую можно получить при использовании нашего метода, равна

$$\sqrt{\sigma_{\text{PD,SAT}}^2 + \sigma_{\text{PD,OGS}}^2 + \sigma_{\text{SPD}}^2 + \sigma_L^2}, \quad (27)$$

где $\sigma_{\text{PD,SAT}}$ и $\sigma_{\text{PD,OGS}}$ характеризуют джиттер фотодетекторов, которые используются для регистрации синхросигнала на спутнике и на приемной наземной станции соответственно, σ_{SPD} характеризует джиттер детекторов одиночных фотонов, а σ_L – ширину оптических импульсов, формирующих квантовый сигнал.

Максимальное N и δt . Как было показано выше, область, которая содержит в себе N синхроимпульсов, должна быть достаточно малой – такой, чтобы в пределах данной области мы могли пренебречь изменением величины доплеровского сдвига:

$$\delta t \ll \frac{t'_p}{t''_p}. \quad (28)$$

Для вычисления t'_p/t''_p используется простая модель. Во-первых, предполагается, что спутник движется по окружности (эксцентриситет = 0). Вращение Земли вокруг своей оси также не учитывается: скорость движения точки на поверхности Земли даже на экваторе на порядок меньше, чем скорость движения спутника. Наконец, рассматривается только пролет через зенит. Рассчитанная согласно этой модели зависимость t'_p/t''_p от времени представлена на рис. 2, а). Если рассмотреть

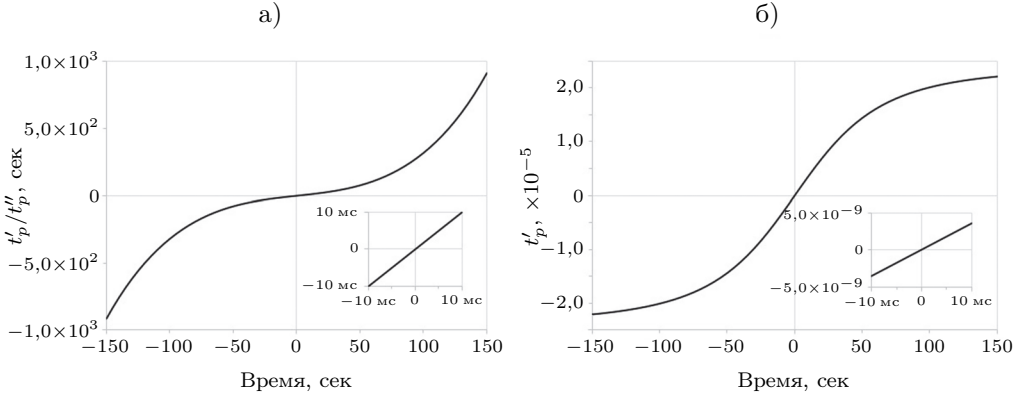


Рис. 2. Рассчитанные временные зависимости $\frac{t'_p}{t''_p}$ (а) и t'_p (б) во время пролета спутника через зенит. Здесь t'_p и t''_p – первая и вторая производные времени распространения сигнала. Высота 500 км, эксцентриситет 0. Вращение Земли вокруг своей оси не учитывается.

последовательность минимальной длины ($N = 10$), то при частоте следования синхрои́мпульсов 10 кГц это будет соответствовать $\delta t = 1$ мс. Тогда (28) выполняется для всего пролета, кроме небольшой области (± 10 мс) вблизи зенита – точки, в которой доплеровский сдвиг меняет свой знак. Однако, как можно видеть на рис. 2, б), доплеровское смещение в этой области чрезвычайно мало ($\lesssim 10^{-9}$), и поэтому его можно вовсе не принимать во внимание.

Физический смысл величины C_k . До сих пор мы не предполагали малости смещения частоты. Тем не менее в большинстве практических случаев отклонение частоты относительно мало. Модуль первой производной t'_p , которая с точностью до знака является доплеровским смещением, не превышает $\sim 10^{-5}$ для искусственных спутников Земли – т.е. это тоже малое возмущение. Таким образом, C_k можно разложить в ряд Тейлора вблизи 0. Удерживая только линейные члены, получаем

$$C_k = 1 + \varepsilon_A - \varepsilon_B - t'_p(t_k).$$

Таким образом, при малых отклонениях $C_k - 1$ характеризует то, насколько часы Алисы спешат относительно часов Боба, включая доплеровский сдвиг.

Сведение к оригинальному методу USTC. Минимальное возможное N для приведенного выше алгоритма равно 2. При $N = 2$ величина C_k определяется как $\frac{(t_1 - t_0)_A}{(t_1^R - t_0^R)_B}$. Соответственно, (18) запишется как

$$(t_{0j} - t_0)_A = \frac{(t_1 - t_0)_A}{(t_1^R - t_0^R)_B} \cdot (t_{0j}^R - t_0^R)_B,$$

что тождественно методу, который изначально применяли сотрудники Научно-технического университета Китая (USTC) [15]. Следует отметить, что при $N = 2$ множитель во втором слагаемом в (26) становится соизмерим с множителем в первом слагаемом, и поэтому второе слагаемое уже нельзя исключить из рассмотрения. Соответственно, выражение для теоретически достижимой точности синхронизации в этом случае будет отличаться от выражения, полученного для больших N .

§ 3. Эксперимент и результаты

3.1. Эксперимент. Представленный в данной статье алгоритм применяли в ходе экспериментов по КРК между спутником *Micius* и приемной наземной станцией, расположенной на территории Звенигородской обсерватории ($55^{\circ}41'56''$ с.ш., $36^{\circ}45'32''$ в.д., 180 м над уровнем моря). *Micius* был запущен в 2016 г., после чего были проведены эксперименты по КРК со спутника на Землю [5–7], распределению квантовой сцепленности [8], КРК на основе квантовой сцепленности [9], квантовой телепортации [10] и некоторые другие [20]. Спутник оснащен лазером-маяком, работающим на длине волны 530 нм, который генерирует оптические импульсы длительностью 0,9 нс с частотой повторения ~ 10 кГц, которые также служат целям синхронизации. Наземная станция представляет собой телескоп с апертурой 0,6 м, который сопряжен с остальной оптикой: в основном это телескоп-гид и камера с широким полем зрения, которые нужны для грубого контура наведения, пьезозеркало и камера с узким полем зрения для тонкого контура наведения, дихроичное зеркало, спектральный фильтр и собственно квантовый приемник с пассивным выбором базиса. Для детектирования четырех возможных состояний поляризации используются четыре детектора одиночных фотонов, характеризующиеся джиттером 350 пс FWHM. Более подробное описание оптической наземной станции можно найти в предшествующих публикациях [21–24].

3.2. Полученные результаты. На рис. 3 приведена типичная зависимость $C_k - 1$ от времени в ходе пролета спутника (нижняя серая кривая). Полученные коэффициенты C_k используются для вычисления $(t_{ij} - t_i)_A$ (18). Соответствующее распределение срабатываний детектора по времени приведено на рис. 4. В экспериментах по КРК точность синхронизации варьируется от 536 пс 1 марта 2022 г. до 593 пс 10 марта 2022 г. Как было показано выше (27), наилучшая точность синхронизации, которую можно получить при использовании нашего алгоритма, равна $\sqrt{\sigma_{PD,SAT}^2 + \sigma_{PD,OGS}^2 + \sigma_{SPD}^2 + \sigma_L^2}$. Поскольку в нашем случае квантовый и синхросигнал регистрировали на Земле детекторами одиночных фотонов, причем одного и того же типа, это выражение можно записать как

$$\sqrt{\sigma_{PD,SAT}^2 + 2\sigma_{SPD}^2 + \sigma_L^2}. \quad (29)$$

Джиттер детекторов одиночных фотонов, которые использовались в данной статье, составляет 350 пс FWHM. Ширина лазерных импульсов, формирующих квантовый сигнал, составляет 200 пс [5]. Если пренебречь джиттером фотодетектора на спутнике, то из (29) получается, что наилучшая точность синхронизации, которую можно достичь, – около 230 пс. Как можно заметить, точность, полученная в реальном эксперименте, существенно хуже. По всей видимости, это расхождение вызвано конечной шириной синхроимпульсов (0,9 нс) и ограниченной мощностью синхросигнала: как результат, детектор не всегда срабатывает в точности по переднему фронту синхроимпульса – есть значительная вероятность срабатывания позже. Действительно, ранее было показано, что при определенных условиях флуктуации интенсивности оптического сигнала в атмосфере могут приводить к значительной ошибке синхронизации [25]. Второй возможной причиной ухудшения точности синхронизации может быть временная различимость квантовых состояний: на *Micius* поляризационные состояния формируются различными лазерными диодами, и гипотетически, если не проводить точную подстройку, между временами срабатывания лазерных диодов могут быть ненулевые задержки, что может приводить к кажущемуся ухудшению точности синхронизации. Детальное исследование флуктуаций интенсивности из-за мерцания в атмосфере и временной различимости квантовых состояний выходит за рамки данной статьи – это может быть темой отдельного исследования.

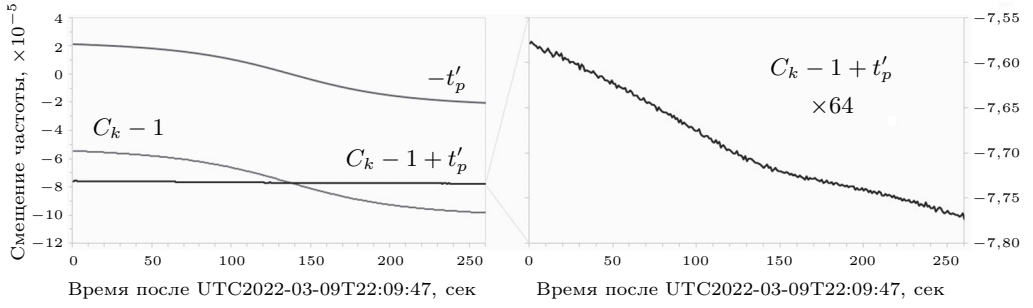


Рис. 3. Сеанс КРК 9 марта 2022 г. Разница (относительная) между частотами часов передатчика и приемника: верхняя серая кривая – доплеровский сдвиг из траектории спутника, рассчитанной с помощью модели SGP4; нижняя серая кривая – это $C_k - 1$ из анализа синхросигнала; черная кривая получена вычитанием доплеровского смещения из $C_k - 1$.

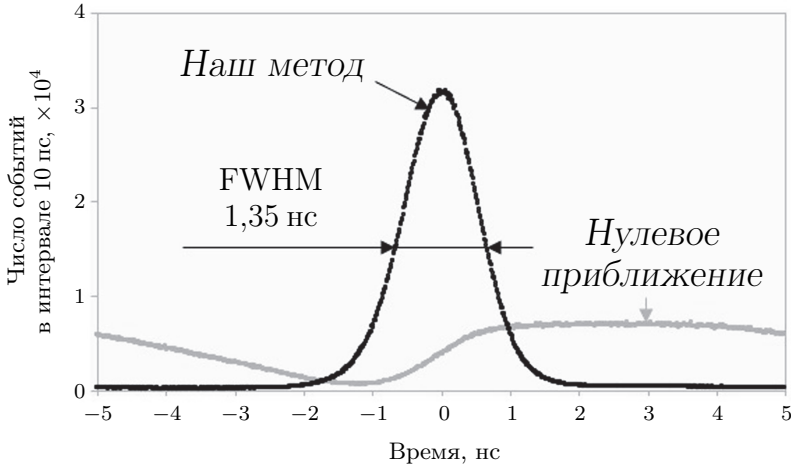


Рис. 4. Сеанс КРК 9 марта 2022 г. Распределение событий по времени, $\text{gem}\left(t_{iA} + (t_{ij} - t_i)_A + \frac{T_q}{2}, T_q\right) - \frac{T_q}{2}$. Серые точки – нулевое приближение: $(t_{ij} - t_i)_A = (t_{ij}^R - t_i^R)_B$. Черные точки – рассматриваемый метод синхронизации. Учитываются все события детектирования между UTC2022-03-09T22.09.47 и UTC2022-03-09T22.14.08 (261 сек).

Спутник и наземная станция были оснащены приемниками GPS, которые могли выдавать точные метки времени – сигнал “Pulse-per-second”, или сокращенно “PPS”. Это давало возможность отслеживать смещение частоты часов напрямую, путем анализа временного сдвига меток PPS. Максимальные скорости дрейфа часов Алисы и Боба ε'_A и ε'_B , обнаруженные во время сеансов квантовой связи, приведены в табл. 1. Как можно видеть, частота часов Алисы меняется как минимум на порядок быстрее, чем частота часов Боба. Кроме того, часы Алисы всегда дрейфуют в одном направлении – их частота уменьшается. По всей видимости, генератор опорной частоты на спутнике не термостабилизирован и начинает нагреваться после включения электроники. Тем не менее даже для часов на спутнике максимальная скорость ухода частоты, которую обнаружили в экспериментах, все еще как минимум на порядок ниже, чем скорость изменения доплеровского смещения,

Обзор экспериментов по КРК между спутником *Micius* и наземной станцией в Звенигородской обсерватории

Дата	Время начала сеанса квантовой связи, UTC+0	Время КРК, сек	Угол восхождения ^a , °	Макс. $ \varepsilon'_A $, сек ⁻¹	Макс. $ \varepsilon'_B $, сек ⁻¹	Точность синхронизации, пс
1 марта 2022 г.	UTC2022-03-01T22.12.28	222	28,5 / 23,0	$7,3 \times 10^{-9}$	$2,0 \times 10^{-10}$	536
9 марта 2022 г.^b	UTC2022-03-09T22.09.47	261	20,8 / 23,2	$7,4 \times 10^{-9}$	$7,7 \times 10^{-11}$	571
10 марта 2022 г.	UTC2022-03-10T21.46.26	249	25,6 / 23,6	$7,3 \times 10^{-9}$	$4,6 \times 10^{-10}$	593

^a Угол восхождения, при котором начинался/прекращался прием квантового сигнала.

^b Вместо истинно-случайной последовательности квантовые состояния фотонов модулировались заранее известной последовательностью длиной в 42 949 672 960 состояний.

которая составляет $\sim 10^{-7}$ сек⁻¹. Как было показано выше, первая производная доплеровского сдвига, равная второй производной времени распространения сигнала t''_p , достаточно мала, и соответственно, квадратичными членами в (15) и (19) можно пренебречь. Следовательно, ввиду того что скорость дрейфа часов составляет $\lesssim 10^{-8}$ сек⁻¹, в данном случае мы тем более можем не рассматривать соответствующие квадратичные поправки.

Помимо описанного выше способа определения смещения частоты мы также используем другой подход, основанный на анализе синхросигнала. Как было показано выше, для малых возмущений

$$C_k = 1 + \varepsilon_A - \varepsilon_B - t'_p(t_k).$$

Таким образом, $\varepsilon_A - \varepsilon_B$ можно вычислить как $C_k - 1 + t'_p(t_k)$. Коэффициенты C_k находятся из анализа синхросигнала описанным выше способом. Доплеровское смещение $-t'_p$ можно рассчитать из известной траектории спутника. В данной статье траекторию *Micius* рассчитывали с помощью модели SGP4 на основе данных TLE, взятых из открытых источников. В качестве примера на рис. 3 приведены временные зависимости $C_k - 1$ (нижняя серая кривая) и $-t'_p$ (верхняя серая кривая), полученные 9 марта 2022 г. После вычитания $-t'_p$ из $C_k - 1$ получается черная кривая, которая отображает совокупный дрейф часов Алисы и Боба относительно друг друга. В наших экспериментах максимальное расхождение между найденной таким образом величиной $\varepsilon_A - \varepsilon_B$ и той же величиной, найденной путем анализа сигнала PPS, не превышает 5% в течение всего сеанса связи.

Следует отметить, что рассматриваемый в данной статье алгоритм синхронизации не предполагает того, что траектория спутника известна. Использование приемников GPS также не является обязательным. Единственной целью представленных выше рассуждений является доказательство справедливости предположения, сделанного в начале статьи, – о том, что частоты часов Алисы и Боба можно рассматривать как константы, не зависящие от времени.

3.3. Сравнение с другими методами. В более ранних экспериментах со спутником *Micius* при использовании первоначального метода USTC точность синхронизации лежала в диапазоне 854–1041 пс, а при использовании метода “Qbit4Sync” – 711–988 пс [18]. Поскольку в тех экспериментах использовали детекторы одиночных фотонов того же самого типа, результаты можно сравнивать напрямую. В среднем по всем пролетам спутника наш алгоритм показывает точность синхронизации

Таблица 2

Прямое сравнение предлагаемого метода (МЦКТ) с методом “Qubit4Sync” (USTC) на интервалах 1 сек.

Дата	Время начала интервала 1 сек, UTC+0	Точность синхронизации, пс		Скорость просеянного ключа, кбит/с		
		МЦКТ	USTC	МЦКТ ^a	USTC ^{a,b}	Максимум ^b
1 марта 2022 г.	UTC2022-03-01T22.14.40	467	373	13,4	14,1	15,7
9 марта 2022 г.^c	UTC2022-03-09T22.12.36	480	369	8,58	9,08	10,1
10 марта 2022 г.	UTC2022-03-10T21.48.55	497	380	17,2	18,3	20,4

^a Применяется временная фильтрация с окном 2 нс.

^b Рассчитано в предположении нормального распределения ошибки по времени.

^c Вместо истинно-случайной последовательности квантовые состояния фотонов модулировались заранее известной последовательностью длиной в 42 949 672 960 состояний.

лучше в 1,7 и 1,5 раза, чем оригинальный метод USTC и метод “Qbit4Sync” соответственно.

Кроме того, было проведено прямое сравнение нашего алгоритма с методом “Qbit4Sync” на временных интервалах длительностью 1 сек. Реализация алгоритма “Qbit4Sync” была выполнена на стороне USTC. Обзор полученных результатов сравнения приведен в табл. 2. Как можно заметить, во-первых, точность синхронизации на интервале 1 сек значительно лучше, чем при обработке данных всего сеанса связи. Для нашего метода синхронизации она в среднем лучше на 15%. В случае метода USTC относительное изменение намного более существенное – на порядок больше. Во-вторых, если сравнивать два метода между собой на интервале 1 сек, “Qbit4Sync” показывает точность в 1,3 раза лучше, чем наш алгоритм.

Мы провели оценку, в какой степени разница в точности между двумя методами синхронизации влияет на скорость генерации секретного ключа. Для данной оценки мы делаем два предположения. Первое предположение – случайная ошибка измерения подчиняется нормальному распределению по времени. Второе – применяемое во временной фильтрации окно не меняется и составляет 2 нс. Согласно расчетам, при использовании в наших экспериментах с Micius алгоритма USTC скорость генерации просеянного ключа увеличилась бы не более чем на 6%: точные значения приведены в табл. 2. Помимо скорости генерации просеянного ключа необходимо принять во внимание и изменение уровня квантовых ошибок – “quantum bit error rate”, или “QBER”: на скорость генерации секретного ключа влияют оба параметра. Например, QBER, полученный 9 марта 2022 г. на интервале 1 сек с UTC2022-03-09T22.12.36, составляет 1,18%. Из них только 0,54% вызваны шумовыми срабатываниями детектора. Остальные ошибки, 0,64%, возникают вследствие конечного коэффициента поляризационной экстинкции из-за несовершенства оптических компонентов. Поэтому соотношение сигнал/шум, а следовательно, и точность синхронизации, на эти ошибки не оказывают никакого влияния.

Принимая во внимание два предположения, сделанных выше, можно показать, что при использовании в эксперименте метода USTC уровень квантовых ошибок из-за шумовых срабатываний понизился бы с 0,54 до 0,51%. Соответственно, суммарный QBER снизился бы с 1,18 до 1,15%. Таким образом, изменение QBER было бы пренебрежимо малым и, следовательно, не оказало бы какого-либо существенного эффекта на скорость генерации секретного ключа. Как итог, улучшение точности в 1,3 раза в условиях данного эксперимента приводит к выигрышу в скорости генерации квантового ключа только в 6%.

§ 4. Заключение

В данной статье вниманию читателя предлагается к рассмотрению простой, эффективный и надежный алгоритм для синхронизации времени в спутниковом квантовом распределении ключей. Предлагаемый подход не предполагает того, что траектория спутника известна, и не требует сложных математических вычислений. Алгоритм был протестирован во время реальных экспериментов по квантовому распределению ключа между спутником *Micius* и приемной наземной станцией, расположенной на территории Звенигородской обсерватории. Во время этих экспериментов максимальное смещение частоты между передатчиком и приемником, включая доплеровский сдвиг, составляло около 10^{-4} . При этом полученная точность синхронизации не превышала 0,5 нс.

Результаты сравнения с другими методами синхронизации неоднозначны. На коротких (1 сек) временных отрезках метод “Qubit4Sync”, разработанный в USTC, показывает точность в 1,3 раза лучше, чем наш алгоритм. Однако при этом выигрыш в скорости генерации квантового ключа относительно небольшой – не более 6%. Если применять наш метод для обработки данных со всего сеанса связи, который длится несколько сотен секунд, то он показывает точность синхронизации по крайней мере в 1,5 раза лучше, чем любой другой из применявшихся ранее методов.

Предлагаемый подход не предполагает ни использования приемников GNSS, ни даже того, что синхроимпульсы и квантовый сигнал формируются на основе сигнала с одного генератора опорной частоты. Автор полагает, что предложенный метод может применяться не только в спутниковой квантовой связи, но также и в наземных системах КРК.

Автор благодарит Научно-технический университет Китая (USTC) и компанию “QSpace Technologies” за разрешение использовать данные, полученные в ходе совместных экспериментов. Автор выражает особенную благодарность д-ру Чао-Цзэ Вану из USTC за помощь, оказанную при обработке экспериментальных данных.

СПИСОК ЛИТЕРАТУРЫ

1. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc. Int. Conf. of Computers, Systems & Signal Processing. Bangalore, India. Dec. 9–12, 1984. V. 1. P. 175–179.
2. *Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental Quantum Cryptography // J. Cryptol. 1992. V. 5. № 1. P. 3–28. <https://doi.org/10.1007/BF00191318>
3. *Schmitt-Manderbach T., Weier H., Furst M., Ursin R., Tiefenbacher F., Scheidl T., Perdigues J., Sodnik Z., Kurtsiefer C., Rarity J.G., Zeilinger A., Weinfurter H.* Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km // Phys. Rev. Lett. 2007. V. 98. № 1. P. 010504 (4 pp.). <https://doi.org/10.1103/PhysRevLett.98.010504>
4. *Liu Y., Zhang W.-J., Jiang C., Chen J.-P., Zhang C., Pan W.-X., Ma D., Dong H., Xiong J.-M., Zhang C.-J., Li H., Wang R.-C., Wu J., Chen T.-Y., You L., Wang X.-B., Zhang Q., Pan, J.-W.* Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance // Phys. Rev. Lett. 2023. V. 130. № 21. P. 210801 (6 pp.). <https://doi.org/10.1103/PhysRevLett.130.210801>
5. *Liao S.-K., Cai W.-Q., Liu W.-Y., Zhang L., Li Y., Ren J.-G., Yin J., Shen Q., Cao Y., Li Z.-P., Li F.-Z., Chen X.-W., Sun L.-H., Jia J.-J., Wu J.-C., Jiang X.-J., Wang J.-F., Huang Y.-M., Wang Q., Zhou Y.-L., Deng L., Xi T., Ma L., Hu T., Zhang Q., Chen Y.-A., Liu N.-L., Wang X.-B., Zhu Z.-C., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W.* Satellite-to-Ground Quantum Key Distribution // Nature. 2017. V. 549. № 7670. P. 43–47. <https://doi.org/10.1038/nature23655>
6. *Liao S.-K., Cai W.-Q., Handsteiner J., Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M., Deng L.,*

- Xi T., Ma L., Hu T., Li L., Liu N.-L., Koidl F., Wang P., Chen Y.-A., Wang X.-B., Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang J.-Y., Zeilinger A., Pan J.-W. Satellite-Relayed Intercontinental Quantum Network // *Phys. Rev. Lett.* 2018. V. 120. № 3. P. 030501 (4 pp.). <https://doi.org/10.1103/PhysRevLett.120.030501>
7. Chen Y.-A., Zhang Q., Chen T.-Y., Cai W.-Q., Liao S.-K., Zhang J., Chen K., Yin J., Ren J.-G., Chen Z., Han S.-L., Yu Q., Liang K., Zhou F., Yuan X., Zhao M.-S., Wang T.-Y., Jiang X., Zhang L., Liu W.-Y., Li Y., Shen Q., Cao Y., Lu C.-Y., Shu R., Wang J.-Y., Li L., Liu N.-L., Xu F., Wang X.-B., Peng C.-Z., Pan J.-W. An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres // *Nature*. 2021. V. 589. № 7841. P. 214–219. <https://doi.org/10.1038/s41586-020-03093-8>
8. Yin J., Cao Y., Li Y.-H., Liao S.-K., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li B., Dai H., Li G.-B., Lu Q.-M., Gong Y.-H., Xu Y., Li S.-L., Li F.-Z., Yin Y.-Y., Jiang Z.-Q., Li M., Jia J.-J., Ren G., He D., Zhou Y.-L., Zhang X.-X., Wang N., Chang X., Zhu Z.-C., Liu N.-L., Chen Y.-A., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W. Satellite-Based Entanglement Distribution over 1200 Kilometers // *Science*. 2017. V. 356. № 6343. P. 1140–1144. <https://doi.org/10.1126/science.aan3211>
9. Yin J., Li Y.-H., Liao S.-K., Yang M., Cao Y., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li S.-L., Shu R., Huang Y.-M., Deng L., Li L., Zhang Q., Liu N.-L., Chen Y.-A., Lu C.-Y., Wang X.-B., Xu F., Wang J.-Y., Peng C.-Z., Ekert A.K., Pan J.-W. Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres // *Nature*. 2020. V. 582. № 7813. P. 501–505. <https://doi.org/10.1038/s41586-020-2401-y>
10. Ren J.-G., Xu P., Yong H.-L., Zhang L., Liao S.-K., Yin J., Liu W.-Y., Cai W.-Q., Yang M., Li L., Yang K.-X., Han X., Yao Y.-Q., Li J., Wu H.-Y., Wan S., Liu L., Liu D.-Q., Kuang Y.-W., He Z.-P., Shang P., Guo C., Zheng R.-H., Tian K., Zhu Z.-C., Liu N.-L., Lu C.-Y., Shu R., Chen Y.-A., Peng C.-Z., Wang J.-Y., Pan J.-W. Ground-to-Satellite Quantum Teleportation // *Nature*. 2017. V. 549. № 7670. P. 70–73. <https://doi.org/10.1038/nature23675>
11. Beveratos A., Brouri R., Gacoin T., Villing A., Poizat J.-P., Grangier P. Single Photon Quantum Cryptography // *Phys. Rev. Lett.* 2002. V. 89. № 18. P. 187901 (4 pp.). <https://doi.org/10.1103/PhysRevLett.89.187901>
12. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H. Quantum Key Distribution over 67 km with a Plug&Play System // *New J. Phys.* 2002. V. 4. P. 41 (8 pp.). <https://doi.org/10.1088/1367-2630/4/1/341>
13. Sasaki M., Fujiwara M., Ishizuka H., Klaus W., Wakui K., Takeoka M., Miki S., Yamashita T., Wang Z., Tanaka A., Yoshino K., Nambu Y., Takahashi S., Tajima A., Tomita A., Domeki T., Hasegawa T., Sakai Y., Kobayashi H., Asai T., Shimizu K., Tokura T., Tsurumaru T., Matsui M., Honjo T., Tamaki K., Takesue H., Tokura Y., Dynes J.F., Dixon A.R., Sharpe A.W., Yuan Z.L., Shields A.J., Uchikoga S., Legre M., Robyr S., Trinkler P., Monat L., Page J.-B., Ribordy G., Poppe A., Allacher A., Maurhart O., Langer T., Peev M., Zeilinger A. Field Test of Quantum Key Distribution in the Tokyo QKD Network // *Opt. Express*. 2011. V. 19. № 11. P. 10387–10409. <https://doi.org/10.1364/OE.19.010387>
14. Wang S., Chen W., Yin Z.-Q., Li H.-W., He D.-Y., Li Y.-H., Zhou Z., Song X.-T., Li F.-Y., Wang D., Chen H., Han Y.-G., Huang J.-Z., Guo J.-F., Hao P.-L., Li M., Zhang C.-M., Liu D., Liang W.-Y., Miao C.-H., Wu P., Guo G.-C., Han Z.-F. Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network // *Opt. Express*. 2014. V. 22. № 18. P. 21739–21756. <https://doi.org/10.1364/OE.22.021739>
15. Wang C., Li Y., Cai W., Yang M., Liu W., Liao S., Peng C. Robust Aperiodic Synchronous Scheme for Satellite-to-Ground Quantum Key Distribution // *Appl. Opt.* 2021. V. 60. № 16. P. 4787–4792. <https://doi.org/10.1364/AO.425085>
16. Shakhovoy R., Puplauskis M., Sharoglazova V., Maksimova E., Hydyrova S., Kurochkin V., Duplinskii A. Wavelength- and Time-Division Multiplexing via Pump Current Variation of a Pulsed Semiconductor Laser—A Method of Synchronization for Quantum Key Distribution // *IEEE J. Quantum Electron.* 2023. V. 59. № 1. Article No. 8000110 (10 pp.). <https://doi.org/10.1109/JQE.2023.3237265>

17. *Calderaro L., Stanco A., Agnesi C., Avesani M., Dequal D., Villoresi P., Vallone G.* Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution // *Phys. Rev. Appl.* 2020. V. 13. № 5. P. 054041 (9 pp.). <https://doi.org/10.1103/PhysRevApplied.13.054041>
18. *Wang C.-Z., Li Y., Cai W.-Q., Liu W.-Y., Liao S.-K., Peng C.-Z.* Synchronization Using Quantum Photons for Satellite-to-Ground Quantum Key Distribution // *Opt. Express.* 2021. V. 29. № 19. P. 29595–29603. <https://doi.org/10.1364/OE.433631>
19. *Takenaka H., Carrasco-Casado A., Fujiwara M., Kitamura M., Sasaki M., Toyoshima M.* Satellite-to-Ground Quantum-Limited Communication Using a 50-kg-Class Microsatellite // *Nat. Photon.* 2017. V. 11. P. 502–508. <https://doi.org/10.1038/nphoton.2017.107>
20. *Lu C.-Y., Cao Y., Peng C.-Z., Pan J.-W.* Micius Quantum Experiments in Space // *Rev. Mod. Phys.* 2022. V. 94. № 3. P. 035001 (46 pp.). <https://doi.org/10.1103/RevModPhys.94.035001>
21. *Хмелев А.В., Дуплинский А.В., Майборода В.Ф., Бахшалиев Р.М., Баланов М.Ю., Курочкин В.Л., Курочкин Ю.В.* Регистрация однофотонного сигнала от низколетящих спутников для целей спутникового квантового распределения ключей // *Письма в ЖТФ.* 2021. Т. 47. № 17. С. 46–49. <https://doi.org/10.21883/PJTF.2021.17.51387.18817>
22. *Khmelev A.V., Duplinsky A.V., Kurochkin V.L., Kurochkin Y.V.* Stellar Calibration of the Single-Photon Receiver for Satellite-to-Ground Quantum Key Distribution // *J. Phys.: Conf. Ser.* 2021. V. 2086. № 1. P. 012137 (5 pp.). <https://doi.org/10.1088/1742-6596/2086/1/012137>
23. *Khmelev A.V., Ivchenko E.I., Miller A.V., Duplinsky A.V., Kurochkin V.L., Kurochkin Yu.V.* Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers // *Entropy.* 2023. V. 25. № 4. P. 670 (14 pp.). <https://doi.org/10.3390/e25040670>
24. *Miller A.V., Pismeniuk L.V., Duplinsky A.V., Merzlinkin V.E., Plukchi A.A., Tikhonova K.A., Nesterov I.S., Sevryukov D.O., Levashov S.D., Fetisov V.V., Krasnopejev S.V., Bakhshaliev R.M.* Vector—Towards Quantum Key Distribution with Small Satellites // *EPJ Quantum Technol.* 2023. V. 10. Article No. 52 (20 pp.). <https://doi.org/10.1140/epjqt/s40507-023-00208-8>
25. *Wu Q.-L., Han Z.-F., Miao E.-L., Liu Y., Dai Y.-M., Guo G.-C.* Synchronization of Free-Space Quantum Key Distribution // *Opt. Commun.* 2007. V. 275. № 2. P. 486–490. <https://doi.org/10.1016/j.optcom.2007.03.068>

Миллер Александр Витальевич
 ООО “Московский центр квантовых технологий”
 avm@mcqt.ru

Поступила в редакцию
 15.11.2023
 После доработки
 08.02.2024
 Принята к публикации
 18.02.2024