DOI: https://doi.org/10.30898/1684-1719.2025.2.10

УДК: 621.391

СИМУЛЯЦИЯ АЛГОРИТМА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ББ84 НА ПЛИС

А.М. Шерстобитов

Институт оптики атмосферы им. В.Е. Зуева Сибирского отделения РАН
634055, Россия, г. Томск, площадь Академика Зуева, 1

Статья поступила в редакцию 7 ноября 2024 г.

Аннотация. В работе представлен новый метод симуляции протокола квантового распределения ключа ББ84 и его реализация на программируемой логической интегральной схеме (ПЛИС). Состояние поляризации фотона задается с помощью двух тактовых сигналов, создаваемых во внутреннем генераторе ПЛИС. Процесс измерения состояния поляризации фотона моделируется с помощью детектора на основе «Исключающего ИЛИ». Результаты тестирования реализации данного метода на ПЛИС показывают хорошее согласие с теорией.

Ключевые слова: протокол квантового распределения ключа, ББ84, ПЛИС, аналоговые вычисления.

Автор для переписки: Шерстобитов Артем Михайлович, shrarm@yandex.ru

Введение

Спустя более 40 лет с момента публикации протокола ББ84[1] технологии квантового распределения ключа широко распространились [2-4]. Однако элементная база для их физической реализации все еще остается малодоступной [5].

Передачу одного бита сообщения по протоколу ББ84, в пренебрежении эффектами распространения сигналов в канале связи, можно рассматривать как простой пример квантовых вычислений: задание состояния кубита (передатчиком Алисы) и его измерение в одном из двух случайно выбранных неортогональных базисов (приемником Боба). Перехват сообщения (приемо-передатчиком Евы) с точки зрения квантовых вычислений – измерение части задаваемых Алисой кубитов и их подмена на результат измерений Евы. Состояние кубита при численном моделировании квантовых вычислений на персональном компьютере, или на программируемой логической интегральной схеме (ПЛИС) обычно задается с использованием модели сферы Блоха. Численное моделирование хорошо согласуется с экспериментальными данными и просто реализуемо. Однако, численная модель не такая наглядная, как физическая. Поэтому, для задач обучения и демонстрации, имеет смысл моделировать физический уровень протокола ББ84 с помощью классических объектов.

Классические аналоги квантовой двухуровневой системы (кубита) хорошо известны, например [6-11]. Так, в работе [6] используют механическую модель двух связанных пружинных маятников. В [7] используются оптические сигналы. В нашем случае более интересны модели с использованием электрических сигналов [8-11], так как они позволяют передавать данные на высоких скоростях, такие модели недороги и при этом просты в изготовлении. В работе [10] предлагается универсальный вариант симуляции квантового компьютера на основе аналоговых блоков. Входные параметры задаются начальными условиями дифференциальных уравнений. Для симуляции

процедуры измерения предлагается с помощью аналоговых блоков умножать полученную волновую функцию на базисные функции и усреднять во времени.

В [8, 9, 11] предлагается несколько иной подход: волновая функция, описывающая состояние кубита, симулируется помощью двух синусоидальных сигналов, по аналогии с квадратурами из радиотехники. Квантовые вентили в таких симуляциях строятся из сумматоров и умножителей, так же используются фильтры низких частот, они необходимы для фильтрации сигналов высоких частот, появляющихся на умножителях. Симуляция процедуры измерения осуществляется, как и в [10], умножением на базисную функцию и усреднением.

Таким образом, моделей протокола ББ84 созданных на основе электрических сигналов в ПЛИС в открытой печати нет, однако можно использовать известные подходы, применяемые для моделирования квантовых вычислений. В данной работе предлагается по аналогии с [8,9,11] симулировать состояние поляризации фотона двумя периодическими электрическими сигналами. Для удобства реализации в ПЛИС симуляция измерения состояния поляризации осуществляется с помощью фазового детектора по схеме «Исключающее ИЛИ». Ниже представлен принцип симуляции, его реализация на ПЛИС, а далее результаты тестирования.

1. Принцип симуляции протокола ББ84

Волновую функцию, описывающую поляризацию фотона обычно представляют следующим выражением [2-4]:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle. \quad (1)$$

Модели, предложенные в [6-11] позволяют полноценно симулировать квантовые вентили, как операции с (1). Однако для нашей задачи такие модели избыточны. Так как в протоколе ВВ84 измерение состояния фотонов происходит только в ортогональных базисах, можно в формуле (1) принять $\varphi = 90°$. Теперь состояние поляризации фотона может быть задано с использованием одного вещественного числа – угла θ:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + i\sin(\theta/2)|1\rangle. \quad (2)$$

Теперь по аналогии с [8,9 и 11] состояние поляризации фотона можно моделировать с помощью сигналов двух синусоидальных генераторов. Согласно (2) сигналы $S_1(t), S_2(t)$ должны иметь одинаковую амплитуду и частоту:

$$\begin{aligned} \psi(t) &= S_1(t) + iS_2(t); \\ S_1(t) &= A\cos(\theta/2)\cos(\omega t + \chi), \\ S_2(t) &= A\sin(\theta/2)\cos(\omega t + \chi). \end{aligned} \quad (3)$$

Далее, необходимо смоделировать процесс измерения состояния фотона в базисах ($|0\rangle, |1\rangle$) и $1/\sqrt{2}(|0\rangle + |1\rangle)$, $1/\sqrt{2}(|0\rangle - |1\rangle)$. Для этого был использован фазовый детектор на основе логического вентиля «Исключающее ИЛИ». Принцип работы данного детектора представлен на рисунке 1. К сигналам $S_1(t)$, $S_2(t)$ добавляется некоторое смещение $V_П$, соответствующее порогу срабатывания цифрового детектора, на рис. 1 $V_П$ = 2.5 В. Детектор состоит из двух однобитных АЦП(в реализации на ПЛИС их роль играют триггеры) D_1, D_2. В случайный момент времени *t* происходит оцифровка $S_1(t)$, $S_2(t)$, соответствующими триггерами, причем $D_i = 1, S_i(t) > V_П$; $D_i = 0, S_i(t) < V_П$. Рисунок 1 демонстрирует все возможные значения D_i, которые могут возникнуть при реализации протокола BB84: (1) – прием и передача в одинаковых базисах, передается «1»; (2) – прием и передача в одинаковых базисах, передается «0»; (3,4) –передача и прием «1» и «0» в разных базисах.

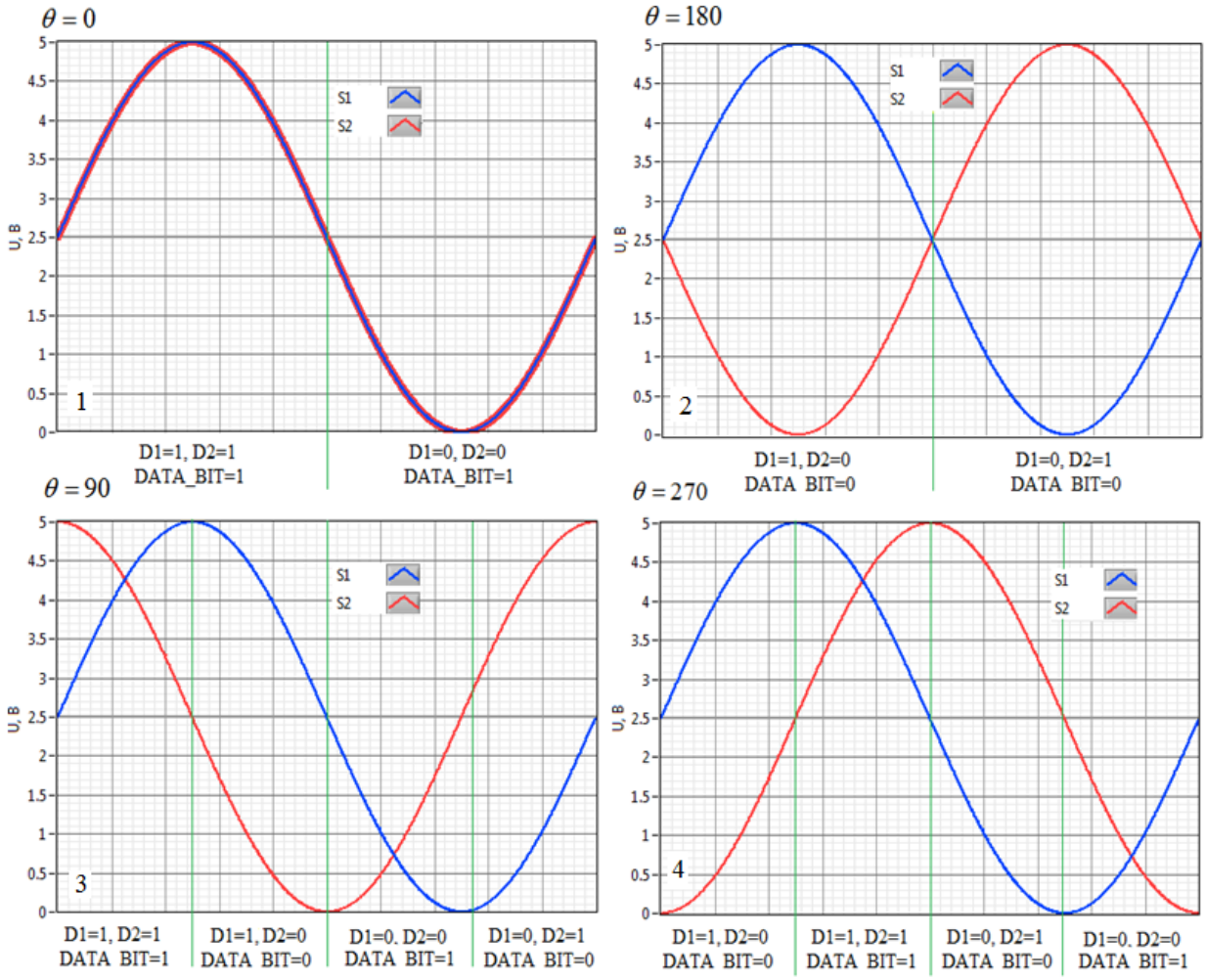

Рис. 1. Принцип работы детектора.

Такая симуляция имеет много общего с фазовыми алгоритмами ББ84[12]. Однако, у данной симуляции и [12] имеются и существенные различия: в качестве носителя в данной симуляции используются электрические колебания, различаются и фазовые детекторы: в предложенной реализации разность фаз детектируется без усреднения.

2. Реализация на ПЛИС

Для генерации сигналов $S_1(t)$, $S_2(t)$ использовался встроенный в ПЛИС генератор тактовых сигналов на основе блока автоподстройки частоты (PLL). Следует отметить, что генерируемые сигналы существенно отличаются по форме от синусоидальных (их форма приближена к меандру), это не должно существенно сказаться на статистике принимаемых детектором данных. Сдвиг фаз осуществлялся также путем прохождения сигнала через PLL.

Схема реализации блоков передатчика (Алисы), приемника (Боба) и приемо-передатчика (Евы) показана на рисунках 2 и 3. Алгоритм работы прошивки ПЛИС следующий:

1) Алиса случайно выбирает базис (0, 180), или (90, 270) и кодирует в одном из этих базисов бит передаваемых данных. Данное событие происходит по фронту тактового сигнала sys_clock.

2) Боб выбирает базис, и проводит «измерение». Выбор базиса, в котором будет проходить измерение, осуществляется путем добавки фазового сдвига 90°. Процесс измерения происходит при низком уровне сигнала sys_clock.

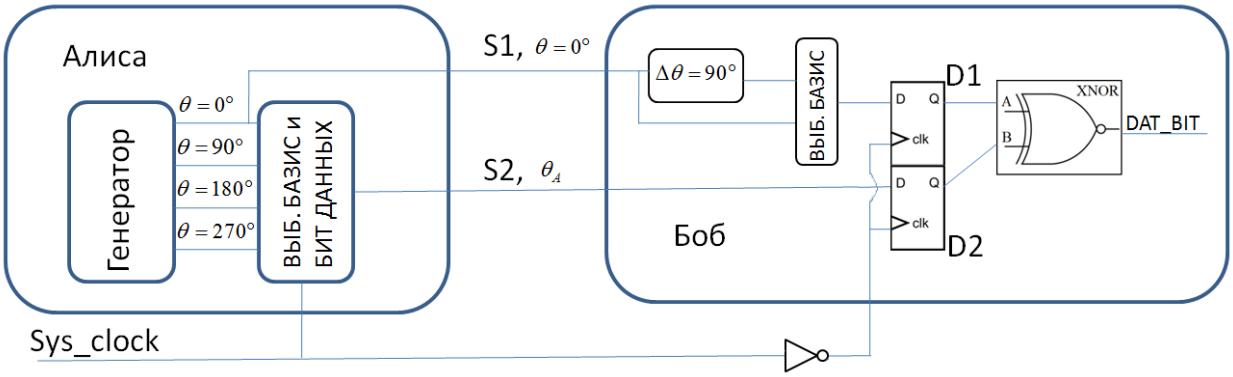

Рис. 2. Схема симуляции протокола ББ84 на ПЛИС.

Для моделирования прослушки канала связи, между передатчиком (Алисой) и приемником (Бобом) устанавливался еще один блок (Ева). Ева осуществляла прием данных Алисы и передачу принятых значений Бобу, имитируя транзакцию Алисы. Схема блока приемо-передатчика (Евы) показана на рисунке 3.

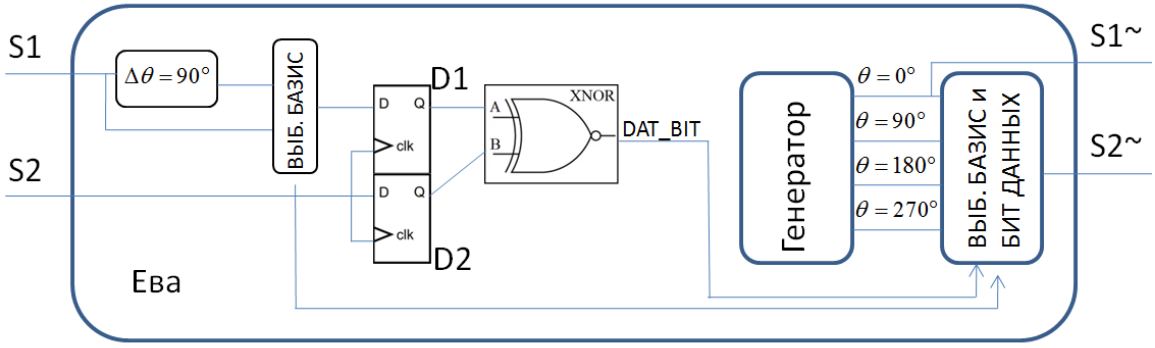

Рис. 3. Схема блока приемо-передатчика (Евы).

В качестве платформы была выбрана плата Max10dev board. Блоки передатчика (Алисы), приемника (Боба) и трансивера (Евы) реализованы на одном кристалле (ПЛИС MAX10M50DAF484C6GES). Данные передавались блоками по 8 бит. В ходе тестирования в программе на ПК задавались базисы Алисы, Боба, базис Евы и данные, передаваемые Алисой. Передача данных между ПК и ПЛИС осуществлялась по интерфейсу UART, через имеющийся на плате преобразователь USB-UART.

3. Результаты тестирования на ПЛИС

В таблице 1 приведены результаты тестирования на ПЛИС с использованием блоков Алисы и Боба, данные получены в ходе усреднения по 10^4 восьмибитных посылок. Тактовая частота sys_clock составляла 3 МГц, частота передаваемых Алисой сигналов составляла 77 МГц (генератор ФАПЧ подключен к тому же кварцевому резонатору, что и ФАПЧ sys_clk); 26 МГц (генератор ФАПЧ подключен к другому кварцевому резонатору). В первом случае (см. таблицу 1. пункт (а)) при совпадении базисов Алисы и Боба данные передаются корректно, что полностью согласуется с теорией. Причем за 10^4 посылок не произошло ни одной ошибки. Однако, при выборе Бобом неверного базиса, наблюдается существенное расхождение с теорией – вероятность приема значения, противоположного передаваемому, почти в два раза превышает вероятность приема правильных данных (66-67 и 33-34 %), в то время как теория предсказывает (50% и 50%). Во втором случае (таблица 1, пункт (б)), при совпадении базисов Алисы и Боба происходят ошибки передачи. В то же время, при выборе Бобом неверного базиса, согласование с теорией лучше (расхождение 5% и менее).

Таблица 1. Частота передаваемых сигналов: (а) – 77 МГц; (б)– 26 МГц.

Базис Алисы	Базис Боба	Бит данных Алисы	Вероятность приема «0», %	Вероятность приема «1», %
0	0	0	100(а); 99(б).	0(а); 1(б).
0	1	0	33(а); 51(б).	67(а); 49(б).
1	0	0	33(а); 55(б).	67(а); 45(б).
1	1	0	100(а); 95(б).	0(а); 5(б).
0	0	1	0(а); 2(б).	100(а); 98(б).
0	1	1	66(а); 49(б).	34(а); 51(б).
1	0	1	67(а); 45(б).	33(а); 55(б).
1	1	1	0(а); 5(б).	100(а); 95(б).

Далее было проведено тестирование с использованием модуля Евы (см. таблицу 2). После многочисленных экспериментов с разными прошивками ПЛИС для лучшей симметрии распространения сигналов и их захвата таковая частота sys_clk и способ оцифровки были немного изменены. Случайный базис Евы задавался с помощью встроенного в python модуля генерации псевдослучайных чисел random, данные усреднялись как и раньше по 10^4 посылок. Как видно из таблицы 2, результаты данного теста удовлетворительно согласуются с теорией: вероятность принять «1», или «0» при совпадении базисов Алисы и Боба теоретически должна составлять 75%, в то время как полученные значения составляют 74% и 73% соответственно.

Таблица 2. Ева выбирает случайный базис.

Базис Алисы	Базис Боба	Бит данных Алисы	Вероятность приема «0», %	Вероятность приема «1», %
0	0	0	73	27
0	1	0	45	55
1	0	0	46	54
1	1	0	73	27
0	0	1	26	74
0	1	1	54	46
1	0	1	53	47
1	1	1	26	74

Заключение

Таким образом, реализация предложенного способа на ПЛИС демонстрирует хорошее согласие с теорией. Расхождения не превышает 5%. Следует отметить, что в основе данного способа симуляции лежит реальный физический процесс, близкий по своей сути к фазовым алгоритмам BB84, что делает его удобным инструментом для демонстраций и обучения.

Литература

1. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Theoretical computer science. – 2014. – Т. 560. – С. 7-11.
2. Cao Y. et al. The evolution of quantum key distribution networks: On the road to the qinternet // IEEE Communications Surveys & Tutorials. – 2022. – Т. 24. – №. 2. – С. 839-894.
3. Nielsen M., Chuang I. Quantum Computation and Quantum Information. Cambridge University Press. – 2010. – 676 p.
4. Gisin N. et al. Quantum cryptography // Reviews of modern physics. – 2002. – Т. 74. – №. 1. – С. 145.
5. Xu F. et al. Secure quantum key distribution with realistic devices // Reviews of modern physics. – 2020. – Т. 92. – №. 2. – С. 025002.
6. Bernazzani L., Burkard G. Fluctuating parametric drive of coupled classical oscillators can simulate dissipative qubits // Physical Review Research. – 2024. – Т. 6. – №. 1. – С. 013284.
7. Spreeuw R.J.C. et al. Classical realization of a strongly driven two-level system // Physical review letters. – 1990. – Т. 65. – №. 21. – С. 2642.
8. La Cour B.R., Ott G.E. Signal-based classical emulation of a universal quantum computer // New Journal of Physics. – 2015. – Т. 17. – №. 5. – С. 053017.
9. Sundqvist K. et al. Exploring Analog Emulation of Quantum Computation Using Quadrature Modulation // ThinkMind (TM) Digital Library, IARIA. – 2020. – Т. 21.

10. Kish L.B. Quantum computing with analog circuits: Hilbert space computing // Smart Structures and Materials 2003: Smart Electronics, Mems, Biomems, and Nanotechnology. – SPIE, 2003. – Т. 5055. – С. 57-65.
11. La Cour B.R. et al. Classical emulation of a quantum computer // International Journal of Quantum Information. – 2016. – Т. 14. – №. 04. – С. 1640004.
12. Inoue K. Quantum key distribution technologies // IEEE journal of selected topics in quantum electronics. – 2006. – Т. 12. – №. 4. – С. 888-896.

Для цитирования:

Шерстобитов А.М. Симуляция алгоритма квантового распределения ключа ББ84 на ПЛИС // Журнал радиоэлектроники. – 2025 – № 2. https://doi.org/10.30898/1684-1719.2025.2.10