ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2020, том 84, № 3, с. 377–381

УДК 535.8,519.161

ПОЗИЦИОННО-ЗАВИСИМАЯ КРИПТОГРАФИЯ НА ОСНОВЕ КВАНТОВЫХ И КЛАССИЧЕСКИХ СХЕМ, ИСПОЛЬЗУЮЩИХ МНОГОЗНАЧНО-ЛОГИЧЕСКИЕ ВЫЧИСЛЕНИЯ

© 2020 г. А. Ю. Быковский*

Федеральное государственное бюджетное учреждение науки
"Физический институт имени П.Н. Лебедева Российской академии наук", Москва, Россия
**E-mail: bykovskiyay@lebedev.ru*

Поступила в редакцию 20.09.2019 г.
После доработки 15.11.2019 г.
Принята к публикации 27.11.2019 г.

Для верификации посещения мобильным агентом контрольных точек на маршруте следования предлагается использовать комбинацию квантового протокола Д. Унру и схемы случайного предсказателя, выполняемой на базе многозначно-логических функций со случайно заданными параметрами. Такая методика не позволяет добиться безусловной криптостойкости, но дает возможность наращивать относительный уровень защиты схем позиционно-зависимой криптографии, в которых злоумышленник использует ложные сигналы.

DOI: 10.31857/S0367676520030084

ВВЕДЕНИЕ

В обзоре [1], посвященном математическим аспектам квантовой криптографии, было показано, что к настоящему времени средствами квантовой оптики так и не удалось решить ряд важных для криптографии проблем, в число которых входят:

- позиционно-зависимая криптография (position-based cryptography),
- случайный предсказатель (random oracle),
- невозможность отказа от обязательств (bit commitment).

Актуальность указанных выше задач обусловлена разработками сетей КРК для глобальных сетецентрических систем [2, 3], объединяющих космические аппараты, вычислительные центры, людей и различные типы беспилотных устройств в единые коммуникационные сети. В настоящее время такие проекты представлены разработками защищенной сети управления критической структурой стационарных объектов электроэнергетики [3]. Однако сетецентрические системы проектируются как одноранговые сети, где возможна связь для любой пары стационарных и мобильных абонентов. При этом необходимо контролировать местоположение мобильных устройств и синхронизовать их работу со стационарными узлами. В глобальных сетецентрических системах востребованы космические линии связи и, в том числе, линии КРК для связи спутников с наземными станциями [4], также требующие синхронизации и контроля местоположения абонентов. Более того, актуальными гражданскими версиями сетецентрических систем являются сети беспилотного транспорта и логистики, для которых оценка местоположения имеет ключевое значение.

Указанные выше проблемы в общем виде можно представить как задачу позиционно-зависимой криптографии (ПЗК) [1, 2, 5, 6], (рис. 1), смысл которой заключается в конфиденциальной передаче закодированного сообщения (или ключа для схем

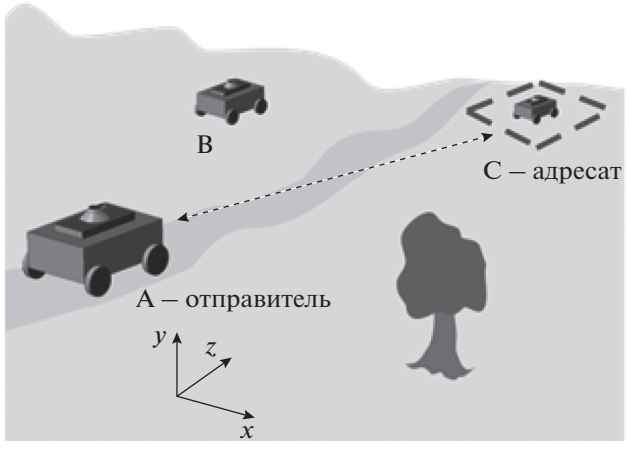

Рис. 1. Принцип работы систем позиционно-зависимой криптографии.

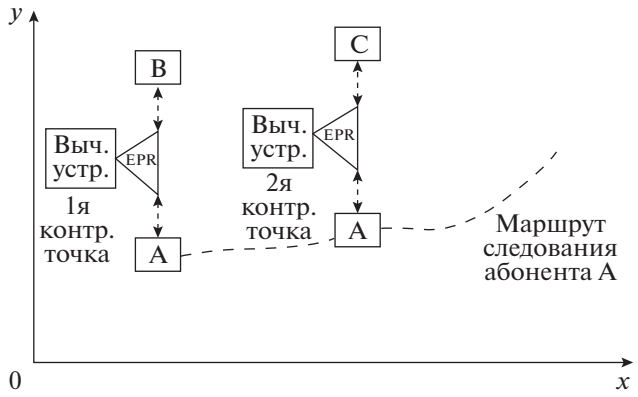

Рис. 2. Процедура формирования массива проверочных данных в процессе посещения абонентом А доверенных контрольных точек 1, 2, ... Обозначения: Выч. Устр. – доверенные вычислительные устройства, EPR – модули генерации запутанных фотонных пар, B, C... – доверенные устройства памяти.

КРК) от произвольного абонента А к абоненту С, расположенному в строго определенном месте (обозначенном пунктиром), исключив при этом расшифровку сообщения любым абонентом В с иным местоположением.

Схемы ПЗК наиболее подробно изучены [1, 5] для метода триангуляции в мобильной телефонии, в котором несколько проверяющих узлов совместно оценивают расстояние до проверяемого узла, измеряя временные задержки его ответного отклика на тестовые сигналы. Однако нечестный проверяемый абонент всегда может обмануть проверяющие узлы, разместив между ними и собой дополнительные источники ложных сигналов. Как показано в [1, 5], в известных схемах квантовой криптографии также не удается достичь безусловной криптостойкости, не зависящей от вычислительных и технических ресурсов злоумышленника. Нечестный абонент может обмануть проверяющих, если его источники ложных сигналов будут генерировать в случайные моменты времени достаточно большое число ложных кубитов. Но в статье Д. Унру [5] было теоретически обосновано, что наибольший уровень защиты обеспечивается для протокола со случайным предсказателем, т.е. использующим идеальный “черный ящик”, воспроизводящий идеальную случайную хэширующую функцию. Поскольку реализовать на практике идеальную хэш-функцию в принципе невозможно, в обзоре [1] обсуждаемый протокол был охарактеризован как интересная, но чисто теоретическая разработка, далекая от реальной жизни.

Чтобы практически воспользоваться протоколом верификации [5], в работе [6] автором на базе алгоритмов дискретной многозначной логики был предложен способ реализации аппаратного устройства случайного предсказателя. Для указанной методики в качестве сравнительного критерия качества можно непосредственно использовать показатели статистических тестов для так называемых криптографических хэширующих функций.

Цель данной работы – разработка схемы верификации следования по маршруту на базе квантового протокола [5], позволяющего увязать процедуру верификации абонента с предшествующей траекторией его движения. Предлагаемый вариант схемы ПЗК базируется на использовании проверочных данных, нарабатываемых для абонента доверенными устройствами в контрольных точках маршрута.

МЕТОДИКА ВЕРИФИКАЦИИ МАРШРУТА АБОНЕНТА

Предлагаемая методика дополняет протокол [5] и выборочно использует его отдельные процедуры. На рис. 2 показан процесс следования мобильного абонента А по заданному маршруту, где абонент посещает набор доверенных контрольных точек (1-я, 2-я...). Для верификации прохождения маршрута абонентом А в конечной точке назначения проводится независимая процедура сопоставления данных, либо запускается квантовый протокол [5], использующий в качестве проверочных данных случайные числа, сгенерированные в контрольных точках маршрута.

Алгоритм сбора проверочных данных

1. В контрольных точках маршрута размещены доверенные вычислительные устройства, управляющие устройствами памяти (B, C...) и источниками запутанных фотонных пар, обозначенными EPR.

2. По запросу прибывшего в контрольную точку 1, 2 абонента А, модуль EPR генерирует пары фотонов, идентичные с точностью до знака. Квантовые состояния пар фотонов измеряют в устройствах абонента А и в измерительном устройстве контрольной точки.

3. В результате измерений в памяти контрольной точки и в памяти абонента А формируют идентичные случайные битовые последовательности, маркируемые номером (меткой) контрольной точки $N_{\text{контр. точки}}$, временем сеанса связи $t_{\text{посещения}}$, и GPS-координатами абонента. Вектор с такими данными будем называть идентификатором посещений μ_N, а структура его имеет вид:

$$\mu_N = \{N_{\text{контр. точки}}, \text{GPS}_{\text{коорд.}}, \text{байт(ы) со случайными данными...}\}. \quad (1)$$

4. Для сравнения данных, записанных в памяти проверяемого абонента и контрольных точек, используется набор идентификаторов посещений μ_N.

Наиболее простым вариантом сопоставления данных проверяемого абонента и контрольных точек, является процедура верификации, не использующая напрямую протокол [5]. Прибыв в конечную точку назначения, абонент А направляет контрольному устройству запрос, содержащий список пройденных им контрольных точек (т.е. свою “предысторию”), в ответ на который вычислительное устройство точки назначения выбирает для проверки данных несколько контрольных точек, указывая их метки $N_{\text{контр. точки}}$. Далее вычислительное устройство в точке назначения запрашивает по сети доверенных узлов данные идентификаторов посещений μ_N в выбранных контрольных точках. Кроме того, вычислительное устройство точки назначения запрашивает аналогичные данные непосредственно у абонента А, сравнивает массивы и делает вывод относительно аутентичности абонента и целостности данных в его памяти.

Другой подход к построению процедур верификации может быть основан на альтернативной подстановке в процедуры протокола [5] массивов случайных данных, ранее записанных в контрольных точках и в проверяемом абоненте. Чтобы пояснить такой способ верификации, требуется дать описание процедур базового протокола [5].

БАЗОВЫЙ ПРОТОКОЛ ВЕРИФИКАЦИИ МЕСТОПОЛОЖЕНИЯ НА ОСНОВЕ СХЕМЫ СЛУЧАЙНОГО ПРЕДСКАЗАТЕЛЯ

Протокол Д. Унру был предложен и исследован в [5] для схем, основанных на оценке местоположения проверяемого с помощью измерений временной задержки отклика на тестовые сигналы проверяющих. При этом анализировалась так называемая игра (соревнование) проверяемых и проверяющих абонентов, в которой один и тот же случайный предсказатель используется всеми участниками сети в качестве идеального источника последовательностей случайных чисел. Протокол [5] для одномерного случая был представлен в виде схемы в [6] и упрощенно изображен на рис. 3. Основные процедуры выполняются (в одномерном случае) парой верификаторов V_1 и V_2 совместно с проверяемым абонентом P и состоят из 7 шагов, показанных ниже.

1) Верификаторы V_1 и V_2 выбирают случайные числа x_1 и x_2 для пересылки в классическом виде, а также случайное число $\hat{y}$ для передачи в виде кубита.

2) V_1 по секретному классическому каналу передает x_2 для V_2.

3) V_1 пересылает для P квантовое состояние $|\psi\rangle$ и классическое состояние x_1, одновременно V_2 передает x_2 для P. Здесь $|\psi\rangle := |\hat{y}\rangle_B$, где измерительный базис $B := H(x_1 \oplus x_2)$, $\oplus$ – булев оператор Искл.–ИЛИ. $|\hat{y}\rangle_B$ обозначает квантовое состояние, кодирующее $\hat{y}$ в базисе $B := \{0,1\}^n$.

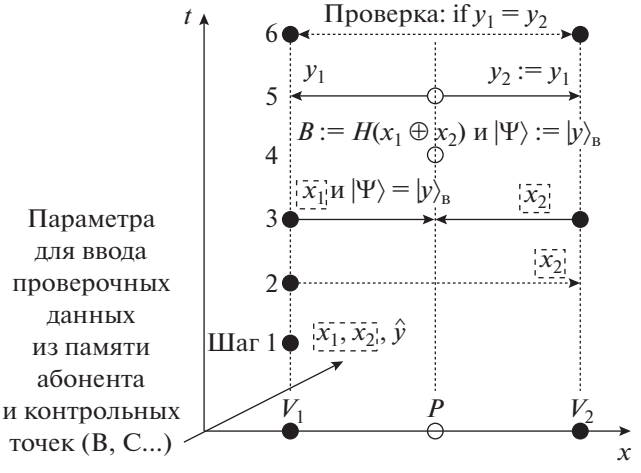

Рис. 3. Реализация протокола [3] (одномерный случай) в конечной точке назначения маршрута. Пунктирные прямоугольники указывают параметры протокола, пригодные для подстановки случайных данных, наработанных ранее при следовании по маршруту.

4) P вычисляет $B := H(x_1 \oplus x_2)$ и измеряет $|\psi\rangle$ в базисе B, получая y_1.

5) С помощью запутанной фотонной пары P одновременно передает y_1 для V_1 и $y_2 := y_1$ для V_2. (Детально этот шаг в работе [5] не регламентирован.)

6) V_1 и V_2 сравнивают по секретному классическому каналу, равны ли y_1 и y_2 (с точностью до знака).

7) V_1 и V_2 проверяют число ошибок $y_1 \neq y_2$, которое не должно превышать пороговое значение 3.5%.

Для представленного выше протокола [5] способы построения новых процедур верификации связаны с подстановкой в качестве x_1 или x_2 случайных данных, запрашиваемых непосредственно из идентификаторов посещений μ_N, хранящихся в памяти проверяемого абонента и контрольных точек. На рис. 3 параметры x_1 или x_2 обозначены пунктирными контурами. Например, на шаге 3) число x_1 вводится проверяющим узлом V_1 от случайного предсказателя, а число x_2 вводится проверяющим узлом V_2 в неявном виде, как указатель на случайное число, записанное ранее в идентификаторе посещения с номером N. Естественно, проверяющие узлы должны запрашивать эти данные по сети, и для выполнения указанных процедур требуется предусмотреть набор специальных команд.

Еще одна возможность для построения процедур верификации связана с шагом 4), где вместо одной операции Искл.–ИЛИ можно провести несколько операций с данными нескольких идентификаторов посещений.

Кроме того, шаг 5) в оригинальной работе [5] задан как одновременная передача классической величины y_1 двум проверяющим V_1 и V_2 с помощью запутанной фотонной пары. Фактически такая процедура, как минимум, требует отправки дополнительных сигналов, указывающих проверяющим, какие биты в полученной последовательности следует отбросить. Для такой процедуры можно использовать передачу кубитов и классических сигналов на нескольких несущих длинах волн, со сложным алгоритмом переключений, зависящим от результатов вычислений.

МЕТОДИКА РЕАЛИЗАЦИИ СЛУЧАЙНОГО ПРЕДСКАЗАТЕЛЯ

Случайный предсказатель [1], необходимый для реализации протокола [5], представляет собой идеальный “черный ящик”, реализующий идеальную случайную хэширующую функцию. По запросу любого абонента, т.е. при вводе произвольного набора из n бит, он выдает случайный набор из m бит, имеющий строго равномерное распределение 0 и 1. Существенно, что случайный предсказатель воспроизводит хэш при повторном вводе данных, т.е. обладает памятью и его нельзя заменить генератором случайных чисел. По сути, случайный предсказатель [6] представляет собой схему записи данных от компактного квантового оптического генератора случайных чисел (например, производства IdQuantique). Как показано в [5], функции случайного предсказателя удобно представить в виде многозначно-логической (МЗЛ) функции со случайно заданными параметрами. Для ее реализации следует применить модифицированный алгоритм построения криптографической односторонней МЗЛ-функции, предложенный ранее в [7] для реализации аналога метода “одноразового шифроблокнота”. Здесь удобно использовать так называемую алгебру Аллена–Живона с числом дискретных уровней истинности от $k = 256$ и выше. При этом полная система логических операторов, не сводимых к операторам булевой логики, включает в себя константы $C = \{1,\ldots,k-1\}$ и операторы $MINIMUM\,(x_1,x_2)$, $MAXIMUM\,(x_1,x_2)$, а также оператор LITERAL, обозначаемый $X\,(a,b)$. Произвольная МЗЛ функция может быть задана в виде таблицы истинности, либо в виде эквивалентного выражения:

$$\begin{gathered} F\,(x_1,x_2,\ldots,x_n) = 1 * X_1\,(a_{11},b_{11}) *\times \\ \times X_2\,(a_{12},b_{12}) * \ldots * X_n\,(a_{1n},b_{1n}) + \\ + (k-1) * X_1\,(a_{k-1,1},b_{k-1,1}) *\times \\ \times X_2\,(a_{k-1,2},b_{k-1,2}) * \ldots * X_n\,(a_{k-1,n},b_{k-1,n}), \end{gathered} \tag{2}$$

где * обозначает *MINIMUM* и + обозначает *MAXIMUM**. Но для реализации процедур ПЗК удобнее записывать МЗЛ-функцию в виде индексированных констант c и пар параметров (a,b):

$$A_u = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{k-1,1} & \ldots & a_{k-1,n} \end{pmatrix},\quad B_u = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{k-1,1} & \ldots & b_{k-1,n} \end{pmatrix},$$
$$C = \begin{pmatrix} c_{11} & \ldots & c_{1q} \\ \ldots & \ldots & \ldots \\ c_{k-1,1} & \ldots & c_{k-1,q} \end{pmatrix}. \tag{3}$$

Для создания аппаратных версий случайного предсказателя применимы два подхода [5], первый из которых основан на формальном описании отклика генератора случайных чисел и последовательном добавлении к имеющейся МЗЛ-функции (1) соответствующих логических выражений. Этот способ требует затратной минимизации логических выражений. Второй, более сложный метод не требует логической минимизации и предполагает заполнение случайными данными набора матриц (3).

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА СЛУЧАЙНОГО ПРЕДСКАЗАТЕЛЯ

Поскольку идеальная хэширующая функция случайного предсказателя с точки зрения математики в принципе является недостижимым объектом [1], то обсуждаемые процедуры направлены на сравнение и выбор более предпочтительного варианта из двух и более аппаратных версий. Прежде всего необходимо подобрать квантовый генератор случайных чисел [2], демонстрирующий лучшие результаты прохождения тестов NIST и ряда других известных алгоритмов. Далее выбранное устройство (при заданном значении k) используется для формирования необходимого набора логических констант и пар параметров (a, b) для операторов Literal. На этой стадии целесообразно проводить промежуточный тест на равномерность распределения получаемых значений a и b.

После отладки алгоритма вычислений хэширующей МЗЛ-функции на базе ПЛИС/FPGA, приемлемой для установки в устройствах контрольных точек и мобильных агентов, с помощью внешнего PC необходимо провести окончательное тестирование случайного предсказателя с помощью известных тестов для так называемых

криптографических хэширующих функций [6]. Все вышеуказанные процедуры являются достаточно сложными, однако именно последний этап оценивается как наиболее затратный и трудоемкий. В целом оценка качества и описание способов тестирования случайного предсказателя заведомо выходит за рамки данной работы.

ВОЗМОЖНОСТИ ЦИФРОВОЙ МЗЛ-КАРТЫ В ЗАДАЧАХ ПЗК

Ввиду недостижимости безусловной криптостойкости в известных схемах ПЗК в них следует дополнительно использовать классические приемы защиты, вынуждающие злоумышленника неприемлемо для него увеличивать частоту отправки ложных сигналов, варьировать длину волны передающего канала связи и временную сетку приема/передачи сигналов. Это усложняет сам алгоритм управления системой ПЗК и требует использования в наращиваемой многопараметрической МЗЛ-модели цифровой карты местности [8]. Удобство такого подхода заключается в возможности описать не только случайный предсказатель [6], но и при необходимости формализовать даже “прыгающие коды” со случайно изменяющимися в известном диапазоне параметрами передачи. Это обусловлено тем, что входными переменными МЗЛ-функции $F(x_1,\ldots,x_n)$ кроме координат и времени могут быть длины волн оптических сигналов λ, временные интервалы Δt, вспомогательные радиочастоты f и другие параметры.

Указанная логическая модель всегда позволяет добавить новые параметры, поскольку, по определению, любая МЗЛ-функция $F(x_1,\ldots,x_n)$ всегда может быть преобразована в функцию большей размерности $F(x_1,\ldots,x_n,x_{n+1})$ путем добавления во все ее логические выражения нового оператора $X_{n+1}(a,b)$ с соответствующими наборами параметров a,b.

ЗАКЛЮЧЕНИЕ

Квантовый протокол верификации местоположения мобильного абонента, разработанный Д. Унру [5], не обеспечивает безусловную криптостойкость, но теоретически позволяет реализовать максимально криптостойкий вариант путем подбора случайного предсказателя с наилучшими показателями прохождения криптотестов для хэширующих функций. Поэтому предложенный в [6] способ аппаратной реализации случайного предсказателя открывает возможность применить этот протокол на практике. Но для внедрения методов ПЗК в область сетецентрических систем требуется расширить существующий набор методик, добавив, в том числе, способ верификации следования по заданному маршруту.

Предложенный в данной работе метод верификации посещения контрольных точек на маршруте следования комбинирует алгоритмы квантового протокола [5] и случайного предсказателя [6] с процедурой сравнения массивов случайных данных, наработанных ранее при следовании по маршруту и хранящихся в памяти проверяемого абонента и контрольных точек. Вышеуказанные данные можно сопоставлять независимо от протокола [5], но, кроме того, их можно подставлять в качестве параметров данного протокола. Многозначно-логическая модель может быть использована не только для моделирования случайного предсказателя, но и для формирования наращиваемой многопараметрической модели местности и маршрута.

СПИСОК ЛИТЕРАТУРЫ

1. *Broadbent A., Fefferman B., Gagliardoni T. et al.* // Design. Codes. Cryptogr. 2016. V. 78. № 1. P. 351.
2. *Быковский А.Ю., Компанец И.Н.* // Квант. электрон. 2018. Т. 48. № 9. С. 777; *Bykovsky A.Yu., Kompanets I.N.* // Quant. Electron. 2018. V. 48. № 9. P. 777.
3. *Hughes R.J., Nordholt J.E., McCabe P.K. et al.* // Proc. 3d Int. Conf. Quantum Cryptography. (Waterloo, 2013). P. LA-UR-13-22718.
4. *Bedington R., Arrazola J.M., Ling A.* // NPJ Quant. Inform. 2017. № 3. P. 30.
5. *Unruh D.* // Proc. of EUROCRYPT-2014. (Copenhagen, 2014). P. 1.
6. *Bykovsky A.Yu.* // J. Russ. Las. Res. 2019. V. 40. № 2. P. 130.
7. *Antipov A.L., Bykovsky A.Yu., Vasiliev N.A. et al.* // J. Russ. Las. Res. 2006. V. 27. № 5. P. 492.
8. *Быковский А.Ю.* // Кр. сообщ. по физ. ФИАН. 2013. № 11. С. 9; *Bykovsky A.Yu.* // Bull. Lebedev Phys. Inst. V. 40. № 11. P. 310.