О поляризационном разнесении в метеорном радиоканале при генерации ключей шифрования

А. И. Сулимов, А. В. Карпов
Кафедра радиофизики, Институт физики
Казанский (Приволжский) федеральный университет
420008, Российская Федерация, г. Казань, ул. Кремлевская, д.18
asulimo@gmail.com, arkadi.karpov@kpfu.ru

***Аннотация* — Природная случайность метеорного канала, образующегося при пролете быстрых метеорных частиц в верхних слоях атмосферы, может использоваться для генерации и распределения секретных ключей шифрования. С целью повышения скорости генерации ключа, предлагается новый метод считывания двух независимых значений фазы сигнала с одного метеорного радиоотражения. Метод основан на временном мультиплексировании поляризации зондирующего сигнала. Путем имитационного моделирования, основанного на строгом численном решении задачи дифракции радиоволн на метеорном следе, впервые выполнены оценки интервала поляризационной когерентности метеорного радиоканала. В работе получены корреляционные функции фазы при поляризационном разнесении зондирующих сигналов как для горизонтально, так и для вертикально поляризованных антенн. Показано, что использование временного мультиплексирования поляризации в метеорном канале позволяет сгенерировать два независимых секретных ключа шифрования вместо одного ключа, как было в предыдущих исследованиях. Тем не менее, предложенный метод генерации дополнительного ключа требует высокой точности установки поляризационных характеристик антенн, что затрудняет его реализацию на практике.**

Ключевые слова — метеорное распространение радиоволн; дифракция радиоволн; метеорное радиоотражение; невзаимность канала; ключ шифрования; поляризационное разнесение сигналов; корреляция; интервал когерентности канала

I. Введение

Мелкие метеорные частицы со случайной массой и вектором скорости непрерывно вторгаются в атмосферу Земли. Сгорая на высотах 80-120 *км*, метеоры оставляют протяжённые ионизированные следы. Такие следы способы ретранслировать радиосигналы между двумя пунктами связи, что используется для создания систем метеорной радиосвязи [1][2]. Характеристики метеорного канала распространения случайны в силу его астрономической и геофизической природы. Образующиеся метеорные следы имеют случайную локализацию, пространственную ориентацию, длину, степень ионизации и атмосферную высоту. Случайная траектория распространения сигнала в комплексе с непредсказуемыми характеристиками среды обуславливают случайность параметров метеорных радиоотражений (МРО), регистрируемых на выходе канала. На основе этой случайности два пункта связи (*A* и *B*) могут создать два экземпляра секретного ключа шифрования путем обмена серией зондирующих сигналов и регистрации их параметров при приеме [3]. Измеряя случайные характеристики принимаемого сигнала (например, фазу), каждый из пунктов накапливает вектор случайных чисел, который затем преобразует в двоичную строку. Если канал взаимный, то пункты *A* и *B* формируют одинаковые случайные последовательности, которые используют в качестве ключа шифрования.

Основной проблемой метеорных систем генерации ключей шифрования (систем МГКШ) является низкая скорость генерации ключа, которая не превосходит 160 *бит/час* [4]. В связи с этим актуальна проблема повышения их производительности. Главным ограничивающим фактором является малое количество метеорных регистраций, обычно составляющее 50-350 регистраций в час. В [3][4] для генерации ключа использовали лишь одно измерение случайной фазы несущей с каждого регистрируемого МРО. Это объясняется тем, что все остальные измерения фазы в пределах одного и того же МРО демонстрируют неприемлемо высокую корреляцию. С другой стороны, в [5] было показано, что метеорный канал чувствителен к поляризации зондирующих сигналов. При этом два зондирующих сигнала, разнесенных по поляризации, могут иметь на выходе канала некоррелирующие фазы. Это позволило бы снимать с каждого МРО не одно, а два независимых измерения фазы сигнала, что удвоит скорость генерации ключевой последовательности.

Целью данного исследования является обоснование возможности генерации двух независимых ключевых последовательностей путем поляризационного разнесения зондирующих сигналов в метеорном радиоканале. В работе будут представлены результаты имитационного моделирования корреляционной функции фазы при поляризационном разнесении зондирующих сигналов. Будут впервые представлены оценки интервала поляризационной когерентности метеорного канала. Путем бинарного квантования смоделированных фазовых

Работа выполнена при поддержке Программы Повышения Конкурентоспособности Казанского Федерального Университета.

характеристик метеорных радиоотражений будут сгенерированы две ключевые последовательности, соответствующие разным поляризациям зондирующего сигнала на входе канала. Будут выполнены оценки взаимной корреляции этих ключевых последовательностей, тем самым показана возможность генерации двух независимых секретных ключей шифрования (вместо одного ключа, как было в предыдущих исследованиях) путем временного мультиплексирования поляризации в метеорном канале.

II. Временное Мультиплексирование Поляризации Зондирующего Сигнала

В силу поляризационной восприимчивости метеорного канала, зондирующие сигналы с разными поляризациями γ_1 и γ_2 ($\gamma_i \in [0^\circ, 180^\circ], i = \{1,2\}$) приобретают при распространении отличающиеся сдвиги фазы φ_1 и φ_2, соответственно. Здесь и далее предполагается, что радиоволны имеют линейную поляризацию с угловой ориентацией плоскости поляризации γ. Эффект поляризационной восприимчивости канала можно использовать для генерации двух независимых ключей шифрования путем поляризационного разнесения сигналов, что позволит удвоить фактическую скорость генерации ключа в системах МГКШ. Традиционное поляризационное разнесение сигналов предусматривает их передачу и прием с одновременным использованием антенн, обладающих разной ориентацией поляризационного эллипса γ_1 и γ_2 [6]. В метеорном канале такая технология неосуществима. Из-за случайной ориентации метеорных следов в пространстве и случайного вращения плоскости поляризации радиоволн под воздействием эффекта Фарадея, при распространении сигнала происходит его деполяризация, и на выходе канала поляризация становится неопределённой [5]. Таким образом, два сигнала с разными поляризациями на входе канала становятся неразделимыми на его выходе.

В связи с этим, предлагается осуществлять поляризационное разнесение путем мультиплексирования поляризации зондирующего сигнала во временной области, как показано на рис. 1. Радиоотражение регистрируется на приемном конце до тех пор, пока не разрушится метеорных след. Длительность МРО T обычно варьируется в диапазоне от 10 *мс* до 10 *с* со средним значением порядка 300 *мс*. Согласно рис. 1, в некоторый промежуточный момент времени $t_{12} \in [0, T]$ происходит переключение поляризации зондирующего сигнала с γ_1 на γ_2, в результате чего фаза сигнала на приемном конце скачком изменяет значение с $\varphi_1 = \varphi(\gamma_1)$ на $\varphi_2 = \varphi(\gamma_2)$. Очевидно, что для генерации независимых ключей требуется найти такое разнесение поляризаций $\Delta\gamma = |\gamma_2 - \gamma_1|$, при котором коэффициент корреляции фазовых измерений $\rho = corr(\varphi_1, \varphi_2) \to 0$.

Ещё одной проблемой реализации этого метода является выбор момента переключения t_{12}. Особенности метеорного канала не позволяют выбирать этот момент произвольно. Одной из важных особенностей является неабсолютная взаимность метеорного канала, имеющая сложную электродинамическую природу [7]. При

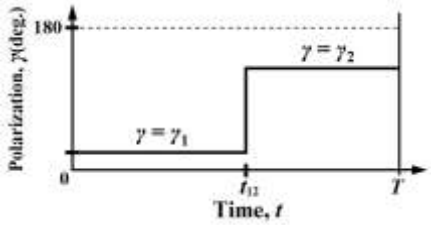

Рис. 1. Временная диаграмма мультиплексирования поляризации.

генерации ключей невзаимность канала приводит к низкой корреляции двусторонних измерений фазы ($\varphi_A \neq \varphi_B$), вследствие чего генерируемые сторонами экземпляры ключа имеют некоторое рассогласование ($Key_A \neq Key_B$). Из-за постепенного разрушения метеорного следа, характеристики канала (включая его невзаимность) изменяются во времени. Поэтому для каждого МРО существует момент t^* с минимальной невзаимностью. Именно в этот момент целесообразно снимать измерения фазы для генерации ключа [3]. Невзаимность канала также имеет поляризационную зависимость, поэтому для каждой поляризации зондирующего сигнала момент $t^*(\gamma)$ различен. Это обстоятельство не препятствует реализации временного мультиплексирования поляризации, поскольку всегда можно выбрать момент переключения как наибольшее время достижения минимума невзаимности: $t_{12} = \max\{t^*(\gamma_1); t^*(\gamma_2)\}$. Таким образом, выбор момента t_{12} имеет строгое обоснование, обусловленное физическими особенностями метеорного канала.

В рамках данного исследования будет выполнена оценка необходимого поляризационного разнесения $\Delta\gamma$, а также проведены исследования по оценке различия моментов минимальной невзаимности канала $\Delta t^* = |t^*(\gamma_1) - t^*(\gamma_2)|$ для обоснования возможности временного мультиплексирования поляризации сигнала. В силу сложной многофакторной природы метеорного канала, указанные исследования целесообразно проводить с помощью имитационного моделирования. План моделирования и описание параметров модели рассматриваются в следующем разделе.

III. План Имитационного Моделирования

Случайность поляризации зондирующего сигнала на выходе метеорного канала [5] значительно усложняет экспериментальные исследования его поляризационной когерентности. Такие исследования, вероятно, потребовали бы кодового разделения сигналов с различными поляризациями. Насколько известно авторам, подобных исследований до сих пор не проводилось. Теоретические исследования корреляционной функции фазы при поляризационном разнесении $\rho(\Delta\gamma)$ требуют учета всей цепочки поляризационных преобразований при метеорном распространении, включая рассмотрение процессов дифракции радиоволн на метеорном следе.

Однако, большинство существующих математических и имитационных моделей метеорных систем связи не обладают такими возможностями, что ограничило и проведение теоретических исследований по данному вопросу.

В данном исследовании имитационное моделирование метеорного канала выполнялось по методу [7]. В настоящее время лишь модель [7] позволяет корректно имитировать невзаимные свойства и поляризационные характеристики метеорного канала. В качестве тестовых использовались две линии метеорной связи разной протяженности, что позволило исследовать влияние длины радиолинии на интервал поляризационной когерентности канала. Первая радиолиния Москва (55.75° с.ш., 37.60° в.д.) – Санкт-Петербург (59.95° с.ш., 30.30° в.д.) имела протяжённость 635 *км*, в то время как вторая радиолиния Санкт-Петербург – Казань (55.75° с.ш., 49.10° в.д.) имела протяжённость 1200 *км*. Технические характеристики тестовых радиолиний представлены в Табл. 1.

Модель имитировала двустороннее распространение зондирующих сигналов, излучаемых одновременно с обоих концов радиолинии во встречных направлениях. Для каждой радиолинии было смоделировано 10000 метеоров. В отличие от реальной практики, при моделировании можно безошибочно разделить на выходе канала два сигнала, имевших разные поляризации на его входе. Последнее позволяло моделировать для каждого метеора одновременное сосуществование двух параллельных каналов распространения, разнесенных по поляризации антенн. Таким образом, никакого мультиплексирования поляризации по времени в ходе моделирования не выполнялось. Вместо этого, моделировалось одновременное распространение двух сигналов с разной поляризацией. Первый канал создавался с использованием на обоих концах радиолинии антенн почти линейной поляризации, поляризационный эллипс которых имел наклонение γ_1. Второй канал создавался аналогичными антеннами, но с поляризацией γ_2. Отметим, что на практике близкое размещение антенн разной поляризации могло бы вызвать их взаимное влияние и искажение поляризационных характеристик. Однако при моделировании взаимное влияние антенн не учитывалось, что позволяло наблюдать объективную картину поляризационной когерентности канала.

Поляризация антенн задавалась угловой ориентацией плоскости их полотна относительно земли путем вращения этой плоскости вокруг оси антенны. Горизонтальной поляризации соответствовали ориентации $\gamma = 0°$ и $\gamma = 180°$. Ориентация полотна антенны под углом $\gamma = 90°$ задавала вертикальную поляризацию. Первый канал считался опорным, поэтому поляризация его антенн γ_1 оставалась фиксированной. Рассматривались случаи как горизонтальной ($\gamma_1 = 0°$), так и вертикальной ($\gamma_1 = 90°$) поляризации опорного канала. Поляризация второго канала γ_2 свободно варьировалась для изменения поляризационного разнесения $\Delta\gamma$ и наблюдения функции поляризационной когерентности $\rho(\Delta\gamma)$.

Для каждого сгенерированного метеора синтезировались четыре фазово-временные характеристики $\{\varphi_A(t,\gamma_1);\varphi_B(t,\gamma_1);\varphi_A(t,\gamma_2);\varphi_B(t,\gamma_2)\}$ МРО, синхронно регистрируемых на обоих концах

ТАБЛИЦА I ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ ТЕСТОВЫХ РАДИОЛИНИЙ

Технические параметры	**Москва – Санкт-Петербург**	**Санкт-Петербург – Казань**
Протяженность, L(*км*)	635	1200
Несущая частота, f_0 (*МГц*)	50	
Мощность передатчика, P_T (*Вт*)	2000	
Порог регистрации, P_0 (*дБм*)	-116	
Тип антенн	5-элементный «волновой канал»	
Высота подвеса антенн, h_a(*м*)	4,4	13,9
Поляризация антенн, γ (*град.*)	$\gamma_1 = 0$ (горизонтальная, фиксированная), $\gamma_1 = 90$ (вертикальная, фиксированная), $\gamma_2 = 0 – 180$ (варьируемая)	
Дата и время сеанса связи	15 июня, 6 часов утра	
Объём выборки, N	10 000 метеорных радиоотражений	

радиолинии. Анализ этих данных позволял находить для каждого метеора моменты минимальной невзаимности канала $t^*(\gamma_1)$ и $t^*(\gamma_2)$. Таким путем определялось минимально допустимое разнесение каналов по времени мультиплексирования Δt^*. Для оценки интервала поляризационной когерентности канала строилась корреляционная функция фазы сигнала путём вычисления коэффициента линейной корреляции $\rho(\Delta\gamma) = corr\{\varphi_A(t,\gamma_1),\varphi_A(t,\gamma_2)\}$, причем усреднение проводилось как по времени $t \in [0,T]$, так и по выборке радиоотражений ($i = 1..N$). Несмотря на невзаимность канала, усреднённые характеристики для пунктов A и B имели близкие значения, что позволяло анализировать результаты только для пункта A. Для генерации двух независимых ключей формировались отсчёты фазы в моменты минимальной невзаимности канала $\varphi_1 = \varphi_A(t^*(\gamma_1))$ и $\varphi_2 = \varphi_A(t^*(\gamma_2))$. Такие операции выполнялись для всех смоделированных метеоров, что позволило накопить необходимую выборку измерений.

IV. ОЦЕНКА ИНТЕРВАЛА ПОЛЯРИЗАЦИОННОЙ КОГЕРЕНТНОСТИ МЕТЕОРНОГО КАНАЛА

Результаты моделирования корреляционной функции фазы сигнала при поляризационном разнесении представлены на рис. 2 для обеих тестовых радиолиний при двух различных поляризациях опорного канала. Полученные кривые несимметричны, что обусловлено асимметрией распределения направлений прихода

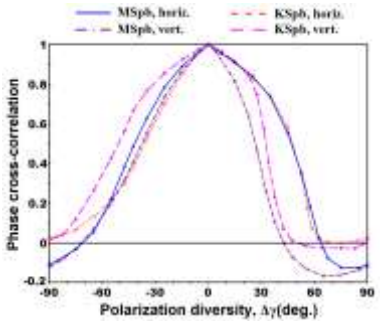

Рис. 2. Корреляциионная функция фазы сигнала при поляризационном разнесении $corr\{\varphi_A(t,\gamma_1), \varphi_A(t,\gamma_2)\}$.

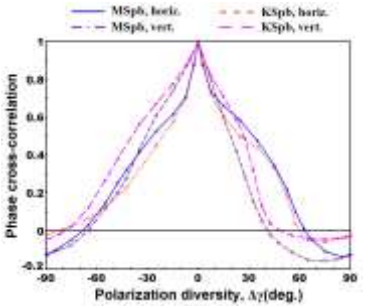

Рис. 3. Корреляциионная функция фазовых отсчетов при поляризационном разнесении $corr\{\varphi_A(t^*(\gamma_1),\gamma_1), \varphi_A(t^*(\gamma_2),\gamma_2)\}$.

метеорных радиоотражений. Из рис. 2 видно, что при определённых разнесениях $\Delta\gamma_0$ корреляция фазовых измерений исчезает. Физически, это объясняется тем, что изменение поляризации зондирующего сигнала на $\Delta\gamma_0$ в среднем сдвигает фазу принимаемого сигнала на $\pi/2$. Разнесение более чем на $\Delta\gamma_0$ сдвигает фазу более чем на $\pi/2$, что приводит к отрицательной корреляции измерений. Наличие точек нулевой корреляции имеет важное значение для генерации независимых ключей шифрования. В то же время из рис. 2 следует, что применение взаимоортогональных поляризаций не позволяет устранить корреляцию фазовых измерений. В зависимости от параметров радиолинии, интервал поляризационной когерентности канала варьировался в пределах от 40° до 90° и более, в среднем составляя около 65°.

Анализ результатов, представленных на рис. 2, показывает, что на коротких радиолиниях интервал поляризационной когерентности канала уже, чем на длинных. Вероятно, это объясняется более высоким разбросом точек отражения сигнала на коротких радиолиниях [8]. При высокой дисперсии характеристик метеоров малые изменения поляризации зондирующего сигнала вызывают большие изменения фазы. На длинных радиолиниях характеристики всех регистрируемых метеоров близки, что сохраняет высокую корреляцию измерений. Кроме того, на длинных радиолиниях слабее выражен эффект отрицательной корреляции, что говорит о том, что рассеянные с разной поляризацией сигналы редко имеют рассогласование по фазе более чем на $\pi/2$.

На рис. 2 была показана корреляционная функция мгновенной корреляции фазовых измерений с нулевым сдвигом по времени. Однако для генерации независимых ключей будут использованы отсчёты фазы $\varphi_1 = \varphi_A(t^*(\gamma_1))$ и $\varphi_2 = \varphi_A(t^*(\gamma_2))$, взятые в разные моменты времени. Учёт дополнительной декорреляции измерений из-за сдвига по времени на Δt^* может уменьшить интервал поляризационной когерентности канала. Чтобы проверить это предположение, была построена функция корреляции фазовых отсчётов, соответствующих моментам минимальной невзаимности канала при различных поляризациях сигнала $\rho(\Delta\gamma, \Delta t^*) = corr\{\varphi_A(t_1^*,\gamma_1), \varphi_A(t_2^*,\gamma_2)\}$. Полученные результаты представлены на рис. 3. Сравнение их с рис. 2 показывает, что эффект дополнительного сдвига по времени заметно

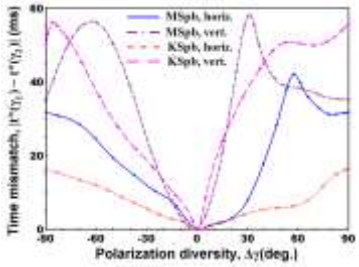

Рис. 4. Рассогласование моментов достижения минимальной невзаимности канала при поляризационном разнесении сигналов.

снижало корреляцию фазы лишь при малых разнесениях $\Delta\gamma$. Наиболее сильно этот эффект проявлялся при вертикальной поляризации опорного канала, сокращая интервал когерентности канала в среднем на 10°.

Для реализации мультиплексирования поляризации согласно рис. 1 необходимо, чтобы моменты наименьшей невзаимности $t^*(\gamma_1)$ и $t^*(\gamma_2)$ двух разнесенных по поляризации каналов имели достаточное разнесение по времени. На практике промежуток времени Δt^* необходим для обнаружения метеора, настройки приемопередающего оборудования, снятия фазовых измерений в первом канале и для перестройки поляризации антенн. Результаты моделирования рассогласования моментов достижения минимальной невзаимности канала представлены на рис. 4. В зависимости от параметров радиолинии, величина Δt^* в среднем изменялась от 15 *мс* до 55 *мс*, что достаточно для выполнения всех необходимых операций. Величина Δt^* определяется корреляцией условий распространения сигналов в параллельных каналах. В частности, из рис. 2–4 видно, что локальные максимумы величины Δt^* соответствуют минимальной корреляции разнесенных каналов. Моделирование также показало, что знак Δt^* имеет систематическую зависимость от разнесения $\Delta\gamma$. Следовательно, можно предсказать для какой из двух поляризаций момент наименьшей невзаимности наступит раньше, что позволяет подобрать на практике корректные значения γ_1 и γ_2, согласующиеся с диаграммой на рис. 1.

Таким образом, полученные результаты подтверждают реализуемость предложенной в разделе II технологии временного мультиплексирования поляризации сигнала. Для полного обоснования предложенной технологии в

следующем разделе будет выполнена тестовая генерация двух независимых ключевых последовательностей с использованием фазовых отсчётов, соответствующих разным поляризациям зондирующего сигнала.

V. Анализ Коррелированности Ключей Шифрования

Выборки отсчётов фазы $\{\varphi_1\}_N$ и $\{\varphi_2\}_N$, сформированные путем обработки радиоотражений, были использованы для создания двух разных ключевых последовательностей K_1 и K_2. Примерно 3% из метеорных регистраций имели неприемлемо высокую невзаимность: $(|\varphi_A(t^*)-\varphi_B(t^*)|\geq \pi/2)$. Соответствующие им отсчёты фазы были исключены из выборки. Оставшиеся фазовые отсчёты были подвергнуты бинарному квантованию

ТАБЛИЦА II Корреляция Ключевых Последовательностей

Поляризационное разнесение		**Москва – Санкт-Петербург**	**Санкт-Петербург – Казань**
$\gamma_1 = 0°$	$\gamma_2 = 55°$	0.117	0.085
$\gamma_1 = 0°$	$\gamma_2 = 57°$	0.185	**0.010**
$\gamma_1 = 0°$	$\gamma_2 = 58°$	0.233	-0.058
$\gamma_1 = 0°$	$\gamma_2 = 60°$	0.076	-0.116
$\gamma_1 = 0°$	$\gamma_2 = 63°$	**0.011**	-0.133
$\gamma_1 = 0°$	$\gamma_2 = 65°$	-0.037	-0.144
$\gamma_1 = 0°$	$\gamma_2 = 90°$	-0.223	-0.141
$\gamma_1 = 0°$	$\gamma_2 = 118°$	**-0.018**	**0.009**
$\gamma_1 = 0°$	$\gamma_2 = 120°$	0.043	0.029
$\gamma_1 = 90°$	$\gamma_2 = 0°$	-0.233	-0.141
$\gamma_1 = 90°$	$\gamma_2 = 45°$	-0.107	-0.117
$\gamma_1 = 90°$	$\gamma_2 = 50°$	**0.001**	**0.002**
$\gamma_1 = 90°$	$\gamma_2 = 55°$	0.117	0.207
$\gamma_1 = 90°$	$\gamma_2 = 150°$	0.028	0.177
$\gamma_1 = 90°$	$\gamma_2 = 153°$	**-0.011**	0.111
$\gamma_1 = 90°$	$\gamma_2 = 154°$	-0.021	0.088
$\gamma_1 = 90°$	$\gamma_2 = 157°$	-0.060	0.022
$\gamma_1 = 90°$	$\gamma_2 = 158°$	-0.073	**0.001**
$\gamma_1 = 90°$	$\gamma_2 = 160°$	-0.099	-0.032
$\gamma_1 = 90°$	$\gamma_2 = 180°$	-0.231	-0.146

согласно методу [5], что позволило создать две ключевые последовательности K_1 и K_2 длиной 9700 *бит*. Далее вычислялся их коэффициент корреляции. Согласно [9], корреляция двух двоичных последовательностей указанного объёма считается пренебрежимо низкой, если её абсолютное значение не превосходит 0,02. Для проверки возможности генерации независимых ключевых последовательностей коэффициент корреляции $corr(K_1,K_2)$, вычисленный при нескольких различных разнесениях $\Delta\gamma$, сравнивался с предельно допустимым уровнем 0,02. Результаты проведенного анализа сведены в табл. 2.

Из табл. 2 видно, что при определённых разнесениях $\Delta\gamma$ корреляция ключевых последовательностей K_1 и K_2 становится пренебрежимо низкой (соответствующие ячейки выделены жирным шрифтом), что подтверждает возможность генерации независимых ключей шифрования с использованием поляризационного разнесения сигналов. Отмеченные случаи хорошо согласуются с результатами на рис. 2 и рис. 3, поскольку соответствуют случаям нулевой корреляции фазовых измерений. Кроме того, из табл. 2 видно, что ортогональность поляризаций зондирующих сигналов не устраняет корреляцию ключей K_1 и K_2, так как не обеспечивает ортогональности принимаемых МРО по фазе. Серьёзным препятствием к реализации поляризационного разнесения на практике является сильная чувствительность корреляции ключей K_1 и K_2 к малым изменениям разнесения $\Delta\gamma$. Согласно табл. 2, погрешность в установке требуемого поляризационного разнесения всего на 1°–2° приводит к недопустимо высокой корреляции ключевых последовательностей. Техническая реализация столь точной установки поляризации антенн может оказаться сложной задачей.

VI. Заключение

В рамках проведенного исследования впервые рассматривалась возможность метеорной генерации статистически независимых ключей шифрования путем поляризационного разнесения зондирующих сигналов. Используя строгое решение задачи дифракции радиоволн на метеорном следе, впервые выполнены оценки интервала поляризационной когерентности метеорного канала, а также построены корреляционные функции фазы метеорных радиоотражений при поляризационном разнесении. Для реализации поляризационного разнесения с учетом сильной деполяризации сигнала при его распространении в канале предложена технология мультиплексирования поляризации по времени. Методом имитационного моделирования доказана её реализуемость. Путем бинарного квантования фазы смоделированных метеорных радиоотражений доказана возможность генерации независимых ключей шифрования, что являлось основной целью исследования. Основным препятствием к реализации предложенного технического решения на практике является сильная чувствительность корреляции генерируемых ключей к малым погрешностям установки требуемого поляризационного разнесения. Выполненные оценки показали, что допустимая погрешность установки наклона поляризационного эллипса антенн не должна превышать одного градуса.

Список литературы

[1] D. W. R. McKinley, "Meteor science and engineering," McGraw-Hill, 1961.

[2] J.D. Oetting, "An analysis of meteor burst communications for military applications," IEEE Trans. on comm, vol. COM-28, no. 9, pp. 1591-1601, 1980.

[3] A.I. Sulimov et al., "Secure key distribution based on meteor-burst communications," Proc. 11th Int. Conf. on Security and Cryptography (SECRYPT-2014), pp. 445-450, Vienna (Austria), Aug. 2014.

[4] A.I. Sulimov et al., "Performance evaluation of meteor key distribution," Proc. 12th Int. Conf. on Security and Cryptography (SECRYPT-2015), pp. 392-397, Colmar (France), Jul. 2015.

[5] A.I. Sulimov, "On possibility of using of measurements of random polarization of radio reflections from meteor trails for generating shared encryption keys," Proc. 2017 Int. Conf. on Radiation and Scattering of Electromagn. Waves (RSEMW-2017), pp. 146-149, Divnomorskoe (Russia), June-July 2017.

[6] S.R. Saunders, A. Aragon-Zavala, "Antennas and propagation for wireless communication systems," 2nd ed., John Wiley and Sons, 2007.

[7] A. I. Sulimov et al., "Analysis and simulation of channel nonreciprocity in meteor burst communications," IEEE Trans. Ant. and Prop., vol. 65, no. 4, pp. 2009-2019, Apr. 2017.

[8] J.A. Weitzen, "Performance of short- and long-range meteor scatter communication with different antennas," IEEE J. Sel. Areas Com., vol. 10., pp. 491-496, April 1992.

[9] D.E. Knuth, "The art of computer programming," vol. 2, 3rd ed., Addison Wesley Longman, 1998, 762 p.