ИССЛЕДОВАНИЯ БЕСКЛЮЧЕВОЙ КРИПТОСИСТЕМЫ ДИНА–ГОЛДСМИТА

А.С. Герасимович[1*], **В.И. Коржик**[1], **В.С. Старостин**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: alexgera93@gmail.com

Информация о статье
УДК 004.725.5
Язык статьи – русский

Ссылка для цитирования: Герасимович А.С., Коржик В.И., Старостин В.С. Исследование бесключевой криптосистемы Дина-Голдсмита // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 43–50.

Аннотация: *Представляются теоретические и экспериментальные исследования криптосистемы, предложенной двумя учеными из Стэнфордского университета – Т. Дином и А. Голдсмитом. Данная криптосистема в одной публикации о ней, выпущенной в журнале «Проблемы информационной безопасности», претендовала на «революцию в криптографии». В настоящей статье показывается, что данное позиционирование неправомерно, по крайней мере, в практических приложениях криптографии.*

Ключевые слова: *физический уровень секретности, замирающий канал, криптосистема, MIMO-система, сингулярное матричное разложение.*

I. Введение

Криптосистема, предложенная в 2013 году Т. Дином и А. Голдсмитом в работе [1] (далее – DG-криптосистема), могла бы претендовать, на первый взгляд, на звание «Революции в криптографии». Действительно, она не требует какого-либо предварительного распределения ключей и обеспечивает *доказуемую секретность*, поскольку ее криптоанализ сводится к решению вычислительно трудной задачи на решетке [2]. Правда, DG-криптосистема могла бы использоваться только при передаче зашифрованной информации по радиоканалам с замираниями. Заметим, что такой вид обеспечения безопасности называется в современной научно-технической литературе секретностью на *физическом уровне* (*Physical-Layer-Security* [3]). Однако, даже такое ограничение применения криптографии, не может еще отменить ее претензии на «революцию в криптографии», поскольку, в отличие от других методов «обеспечения секретности на физическом уровне», DG-криптосистема требует лишь единственного и вполне естественного условия – расположения приемника легального пользователя и перехватчика в несовпадающих точках пространства. Более того, предполагается даже, что перехватчик в точности знает расположение передатчика и приемника легальных пользователей.

В работе [4] DG-криптосистема была впервые проанализирована с точки зрения секретности и практической реализуемости. В частности, там было показано, что при одинаковом количестве приемных антенн у легального пользователя (n_r) и перехватчика (n_r'), а также при одинаковых (в среднем) свойствах легального канала и канала перехвата, легальные пользователи могут обмениваться достаточно надежной информацией, тогда как перехватчик, используя подоптимальные методы приема (из-за нереализуемой сложности оптимальных методов), получает недопустимо большую вероятность ошибочного приема информации. Сомнительность допустимости условия $n_r' = n_r$, была впервые отмечена в работе двух австралийских ученых [5]. В частности, они показали, что при прочих равных условиях, неограниченное возрастание отношения n_r'/n_r приводит к убыванию вероятности ошибки перехватчика к нулю, а следовательно и к компрометации DG-криптосистемы. Однако, поскольку в работе [5] были получены асимптотические результаты, которые не подтверждались каким-либо моделированием, то представляет интерес восполнить эти пробелы, что мы и пытаемся сделать в статье.

В разделе II производится моделирование DG-криптосистемы и делаются некоторые выводы, поясняющие ее свойства при условии, что $n_r' > n_r$. В разделе III выводятся приближенные теоретические формулы для расчета вероятности ошибки при оптимальной обработке сигналов легальным пользователем и подоптимальной обработке перехватчиком. Полученные результаты и дополни-

тельное моделирование поясняют кажущиеся парадоксы, которые были описаны в разделе II. Раздел IV содержит выводы относительно основных результатов работы и представляет направление дальнейшего возможного исследования DG-криптосистемы.

II. Моделирование DG-криптосистемы при условии $n_r' \geq n_r$

Напомним сначала точные условия, необходимые для функционирования DG-криптосистемы, описанные в оригинальной работе [1] и повторенные в [4]. Легальные пользователи A и B связаны каналом с замираниями, математическая модель которого имеет вид:

$$z = Ay + e, \quad (1)$$

где $y \in R^{n_r}$ – вектор, передаваемый от A к B; $A \in R^{n_t x n_r}$ – матрица, описывающая распространение сигнала по легальному каналу связи, причем $A = (a_{ij})$, $i \in (1, \dots, n_t)$, $j \in (1, \dots, n_r)$, где a_{ij} – взаимонезависимые гауссовские случайные величины с нулевыми средними и с одинаковыми дисперсиями σ^2 (физически, элемент a_{ij} матрицы A представляет собой коэффициент передачи сигнала от i-передающей антенны на j-приемную антенну); $e \in R^{n_r}$– вектор шума приемника легального пользователя B, элементы которого взаимонезависимые гауссовские случайные величины с нулевыми средними и одинаковыми дисперсиями $\sigma_e{}^2$; $z \in R^{n_r}$ – вектор полезного сигнала, принимаемого B.

Канал перехвата от A к перехватчику E описывается уравнением:

$$z' = By + e', \quad (2)$$

где $z' \in R^{n_r'}$ – вектор сигнала, принимаемый перехватчиком E на n_r' антенн; $B \in R^{n_t x n'r}$, $B = (b_{ij})$, $i \in (1, \dots, n_t)$, $j \in (1, \dots, n_r')$, где b_{ij} – взаимно независимые гауссовские величины с нулевыми средним и дисперсиями σ_w^2. $e' \in R^{n_r'}$ – вектор шума приемника перехватчика E, элементы которого взаимно независимые гауссовские случайные величины с нулевыми средними и с одинаковыми дисперсиями $\tilde{\sigma}_n^2$.

Предполагается, что все случайные элементы основного канала и канала перехвата статистически независимы друг от друга. Кроме того, предполагается что матрица A в точности известна легитимным пользователям, а матрицы A и B в точности известны перехватчику.

В работе [1] предлагаются следующий метод «модуляции» (шифрования) сигнала и его «демодуляции» (дешифрования).

Сначала производится преобразование:

$$y = Vx, \quad (3)$$

где $V \in R^{n_t x n_t}$ – квадратная матрица, входящая в *сингулярное (SVD) разложение* матрицы A легального канала, т.е. $A = USV^T$, $x \in R^{n_t}$, $x = (x_1, \dots, x_{n_t})$, $x \in (1, 2, \dots, M-1)$, M – целое число.

Подставляя (3) в (1), и учитывая ортогональность матриц U и V в *SVD*, получим:

$$z = Ay + e = USx + e. \quad (4)$$

Далее легальный пользователь B, пользуясь знанием матрицы A, выполняет следующее преобразование:

$$z'' = U^T z = U^T USx + U^T e = Sx + \tilde{e}. \quad (5)$$

Для ортогональной матрицы U^T случайный вектор z'' является достаточной статистикой относительно x и потому оптимальная оценка сообщения x будет иметь вид:

$$x' = argmin_x ||z'' - Sx||, \quad (6)$$

где ||...|| означает Евклидову норму.

Поскольку матрица S, взятая из *SVD*, имеет по определению диагональную форму, то дешифрование сообщения x по правилу (6) можно заменить эквивалентным выражением:

$$x_i' = argmin_{x_i} |z_i'' - s_i x_i|, \quad (7)$$

где $s = (s_1, \dots, s_{n_t})$ – диагональ матрицы S.

Из выражения (7) видно, что сложность решения задачи (6) оказывается линейной и пропорциональной количеству передающих антенн n_t.

Перехватчик E принимает вектор:

$$z' = By + e' = BVx + e' = U'S'^{(V')^T} Vx + e' = Cx + e', \quad (8)$$

где $C = U'S'(V')^T V$, *а* $U'S'(V')^T$ – результат *SVD* матрицы B канала перехвата.

Далее, следуя стратегии легитимного пользователя B, перехватчик E вычисляет:

$$z''' = (U')^T z' = (U')^T Cx + (U')^T e' = C'x + \tilde{e}, \quad (9)$$

где $C' = S'(V')^T V$, $\tilde{e} = (U')^T e'$.

Для гауссовского (по предположению) канала перехвата, оптимальной оценкой (дешифрованием) x является следующее выражение:

$$x'' = argmin_x \left||z''' - C'x|\right|. \quad (10)$$

Поскольку матрица C' в (10), вообще говоря, не является диагональной, то решение вышеприведенной задачи (10) представляет собой трудную проблему на решетке [2]. В работе [1] доказано, что решение этой проблемы имеет экспоненциальную сложность от количества передающих антенн n_t при выполнении следующего условия:

$$M\sigma_w\tilde{\sigma}_e^2 > \sqrt{n_t}. \quad (11)$$

Поскольку условие (11) достаточно просто выполняется (см. далее примеры), а количество передающих антенн n_t может быть выбрано достаточно большим, то отсюда авторы [1] делают вывод, что при условии расположения перехватчика E на расстоянии не меньшем, чем несколько длин волн связи от легального пользователя B (когда, в соответствии с результатами [6] элементы матриц A и B будут некоррелированными), сообщение x не может быть надежно расшифровано перехватчиком E.

Заметим, что вероятность ошибки символов дешифрованного перехватчиком сообщения на первый взгляд кажется непривычной характеристикой стойкости криптосистем, где типично использовать только сложность вычислений при криптоанализе. Однако это не всегда так. Например, вероятность ошибки, как характеристика стойкости шифра также фигурирует для таких, например, криптосистем с открытым ключом, как криптосистема на целочисленной решетке (LWE) [2].

В работе [4] был впервые поставлен вопрос о правомерности приведенного выше вывода авторов. Основанием для такой критики явился подоптимальный метод приема (дешифрования), предложенный в [4] и исследованный там при помощи моделирования. Действительно, рассмотрим выражение (8) и, предположим, что матрица C является несингулярной, т. е. $detC \neq 0$, что весьма вероятно. Умножая обе части (8) на C^{-1}, получим:

$$\tilde{z} = C^{-1}z' = x + C^{-1}e'. \qquad (12)$$

Поскольку матрица C^{-1} не обязательно будет ортогональной, то $C^{-1}e'$ – не обязательно гауссовский вектор с взаимно независимыми компонентами, для которого сложность декодирования оказывается линейной. Однако можно попытаться исследовать подоптимальный метод дешифрования:

$$x_i'' = argmin_{x_i}|\tilde{z}_i - x_i|, \qquad i = 1, 2, \dots, n_t. \qquad (13)$$

Очевидно, что сложность решения задачи (13) линейно зависит от количества передающих антенн n_t, а качество дешифрования будет определяться вероятностями ошибки, т. е. вероятностями событий $x_i'' \neq x_i$, $i = 1, 2, \dots, n_t$. Вероятности ошибок P легального пользователя при дешифровании по правилу (7) и для перехватчика – по правилу (13), были рассчитаны в работе [4] при помощи моделирования для частного случая $n_t = n_r = n_r' = n$.

Так, в частности, при n = 100, $\sigma^2 = \sigma_w^2 = 4$, $\sigma_e^2 = \tilde{\sigma}_e^2 = 7$, вероятность ошибки в канале легальных пользователей оказались P = 0,034, а в канале перехвата, при подоптимальном приеме, приемником реализованному по правилу (13), вероятность ошибки была P' = 0,3. В работе [4] было показано также, что при такой вероятности ошибки, невозможно корректно восстановить смысловой текст даже за счет его большой естественной избыточности. Поэтому, казалось бы, подтверждена практическая реализуемость DG-криптосистемы при выполнении, сформулированных выше условий, тем более что условие (11) выполняется «с запасом», т. к. для выбранных параметров левая часть этого неравенства равна ≈ 11,58, а правая часть равна 10.

Рассмотрим теперь сценарий, когда количество приемных антенн перехватчика n_r' больше, чем количество антенн легального приемника n_r.

Нами было проведено моделирование DG-криптосистемы при увеличении количества n_r' антенн перехвата. Результаты моделирования представлены в таблице 1.

ТАБЛИЦА 1. Расчет вероятностей ошибок P' для различных значений количества антенн перехватчика n_r'

n_r'	100	101	102	103	105	107	108	109	110	120	150
P'	0,31	0,22	0,16	0,12	0,07	0,048	0,039	0,03	0,024	0,003	$7 \cdot 10^{-6}$

Из данных, приведенных в таблице 1, видно, что при увеличении количества приемных антенн перехватчика от n_r' = 100 до n_r' = 109, т. е. всего на 9 %, вероятность ошибки перехвата, использующего подоптимальное правило (13) линейной сложности и вероятность ошибок легального пользователя при использовании оптимального приемника, совпадают. Это, очевидно, приводит к полной компрометации DG-криптосистемы, что, на первый взгляд, выглядит «парадоксом», поскольку интуитивно такое небольшое, в процентном отношении, увеличение количества приемных антенн перехвата, казалось бы, не должно приводить к «коллапсу» криптосистемы?

Для того, что бы проверить, не является ли полученный результат ошибочным, и в частности, не связано ли это с недостаточной обусловленностью матрицы B, рассмотрим в следующем разделе теоретические и более точные экспериментальные оценки вероятностей ошибок.

III. Теоретические и экспериментальные оценки вероятностей ошибочного приема сообщений легитимными пользователями и перехватчиком для DG-криптосистемы

Рассмотрим, не умаляя общности, при пояснении парадокса влияния n_r' на вероятность ошибки P', случай, когда элементы передаваемого сообщения $x_i \in (0,1)$ что аналогично использовались «амплитудной модуляции» в обычных системах связи. Тогда оптимальное правило решения (7) для легитимного пользователя будет эквивалентно следующему выражению:

$$x_i' = \begin{cases} 0, & \text{если } z_i'' \le \dfrac{S_i}{2} \\ 1, & \text{если } z_i'' > \dfrac{S_i}{2} \end{cases} \quad (14)$$

Для вероятности правильного приема по (14) двоичных символов x_i будем иметь нижнюю границу:

$$P\{x_i' = x_i\} \ge P\left\{|e_i| \le \frac{S_i}{2}\right\}, \quad (15)$$

где e_i– компоненты вектора шума e в (1).

Поскольку по нашему предположению, $e_i \in N(0, \sigma^2)$, то из (15) получим:

$$P\{x_i' = x_i\} \ge 2\Phi\left(\frac{S_i}{2\sigma_e}\right), \quad (16)$$

где

$$\Phi(a) = \frac{1}{\sqrt{2\pi}} \int_0^a exp(-\frac{t^2}{2})dt.$$

Следует отметить, что хотя (16) дает нижнюю границу для $P\{x_i' = x_i\}$ и не составило бы особого труда получить точное выражение для $P\{x_i' = x_i\}$, но это не имеет особого смысла, поскольку для интересующих нас параметров канала, при которых эта вероятность близка к 1, получаемые при такой замене, погрешность оказывается незначительной.

Рассмотрим теперь расчет вероятности правильного приема при принятии решения по правилу (13) в канале перехвата, причем, в том числе и для случая $n_r' > n_t$.

В этом случае подоптимальное правило решения (13) будет эквивалентно следующему выражению:

$$x_i'' = \begin{cases} 0, & \text{если } \tilde{z}_i \le \frac{1}{2} \\ 1, & \text{если } \tilde{z}_i > \frac{1}{2} \end{cases}, \quad (17)$$

где $\tilde{z}_i$ – координаты вектора $\tilde{z}$ из (12).

Из выражения (12) следует, что:

$$\tilde{z} = x + C^{-1}e',$$

где e' – вектор аддитивного шума приемника перехватчика, $C = BV = U'S'(V')^TV$, поскольку $B = U'S'(V')^T$ – это *SVD* разложение матрицы B канала перехвата.

Для вероятности правильного приема i-го символа сообщения x_i в канале перехвата получаем из (17) следующую нижнюю границу:

$$P\{x_i = x''_i\} \ge P\left\{|e_i''| \le \frac{1}{2}\right\}, \quad (18)$$

где e_i'' – координата вектора $e'' = C^{-1}e'$.

Поскольку $e_i' \in N(0, \tilde{\sigma}_e^2)$, то:

$$P\{x_i = x_i''\} \ge 2\Phi(\frac{1}{2 \cdot \sqrt{Var\{e_i''\}}}). \quad (19)$$

Для нахождения дисперсии σ_i'' выполним некоторые матричные преобразования:

$$C = BV = U'S'^{(V')^T}V,$$
$$C^{-1} = V^TV'^{(S')^{-1}(U)^T}.$$

Тогда:

$$e'' = C^{-1}e' = V^TV'(S')^{-1}(U')^Te'. \quad (20)$$

Из выражения (20), с учетом ортогональности матрицы U' и диагональности матрицы S', получаем, что:

$$Var\{e_i''\} = \tilde{\sigma}_e^2 \cdot \sum_{k=1}^{n_t} \frac{\upsilon_{ik}^2}{S_k'^2}, \quad (21)$$

где υ_{ik} – элементы матрицы V^TV', *а* S_k' – элементы диагонали матрицы S'.

Подставляя (21) в (19) получим:

$$\mathrm{P}\{x_i = x_i''\} \ge 2\Phi\left(\frac{1}{2\tilde{\sigma}_e\omega}\right), \quad (22)$$

где

$$\omega_i = \sqrt{\sum_{\mathrm{k}=1}^{\mathrm{n_t}} \frac{\upsilon_{ik}^2}{\mathrm{S_k'^2}}}.$$

Сравнивая вероятности правильного приема для легитимных пользователей (16) и для перехватчика (22) видим, что они отличаются коэффициентами s_i и величинами $1/2\tilde{\sigma}_e\omega_i$ в аргументах функции $\Phi(\cdot)$.

Для того, чтобы теоретически рассчитать средние величины вероятностей правильного приема, необходимо было бы усреднить (16) (22) по распределениям s_i *и* s_k', а также по элементам матрицы V^TV'. Это достаточно сложная задача и она связана с использованием значительных приближений.

Однако, уже из представления (22) мы сможем в дальнейшем убедиться в убывании дисперсии аддитивного шума e_i'' при увеличении количества приемных антенн перехватчика n_r', что, очевидно приведет к увеличению вероятности правильного приема перехватчиком при увеличении количества его приемных антенн.

В таблице 2 представлены полученные моделированием средние значения величин $P(x_i' = x_i)$ по (16), т. е. для легального пользователя и величины $P(x_i'' = x_i)$ по (22) для перехватчика при $n_t = n_r = 100$ и различных n_r' для $\sigma_w^2 = \sigma^2 = 7$, $\sigma_n^2 = \tilde{\sigma}_n^2 = 4$.

Как видно из данной таблицы, увеличение количества n_r' приемных антенн перехватчика всего лишь до 105 по сравнению со 100 приемными антеннами легальных пользователей, приводит даже к небольшому преимуществу перехватчика по сравнению с легитимными пользователями, не смотря на то, что последние выполняют оптимальный прием, а перехватчик – подоптимальный.

ТАБЛИЦА 2. Зависимость вероятности правильного приема в легальном и канале перехвата от количества антенн n'_r

n'_r / $P; P'$	100	101	102	103	104	105
$P(x'_i = x_i)$	0,9498	0,9489	0,9488	0,9492	0,9460	0,9376
$P'(x''_i = x_i)$	0,71	0,7	0,8	0,87	0,9	0,95
n'_r / $P; P'$	106	107	108	109	110	
$P(x'_i = x_i)$	0,9478	0,9492	0,9462	0,9413	0,9469	
$P'(x''_i = x_i)$	0,96	0,97	0,98	0,985	0,99	

Это, в свою очередь объясняется тем обстоятельством, что сингулярные числа s_{ij} для *SVD*-матрицы легального канала практически не зависит от n'_r и убывают лишь с ростом i, тогда как величины ω_i слабо зависят от k и увеличиваются с ростом n'_r. Типичное поведение первых $i = \overline{1,40}$ сингулярных чисел s_{ij} и величин ω_{ij} (n_t = 100), $k = \overline{1,40}$ для пяти ($j = \overline{1,5}$) реализаций, показано в таблицах 3, 4 и 5, 6 соответственно.

ТАБЛИЦА 3. Случайные величины s_{ij} для $i = \overline{1,40}$ и пяти различных реализаций $j = \overline{1,5}$ при n'_r = 100

i \ j	s_{i1}	s_{i2}	s_{i3}	s_{i4}	s_{i5}
1	53,1421	51,2926	52,7574	51,2378	51,3030
2	49,0113	49,2300	51,3601	49,0261	50,5698
3	47,7710	48,9185	49,0998	48,8155	48,5014
4	46,4833	47,3819	48,5190	47,3624	47,7105
5	45,9201	47,0209	47,2610	46,5177	46,5155
6	44,5610	45,5884	45,7601	45,9859	45,6272
7	44,3215	44,4919	45,2538	45,4024	45,0222
8	43,7468	44,3907	44,9980	44,3537	44,0759
9	43,0688	43,3646	42,8331	43,1716	43,6774
10	42,1501	42,7447	42,5853	42,4437	43,0632
11	41,9077	41,8793	41,7970	41,5423	42,4033
12	41,0089	41,1890	41,5498	40,5631	41,6160
13	40,0538	40,2417	40,9805	40,1696	41,5232
14	39,3225	39,2230	40,4994	39,6923	40,4332
15	38,9847	38,9259	40,2919	39,0572	39,2452
16	38,6270	38,5469	39,4584	38,6847	38,6931
17	37,9362	37,6582	38,8286	37,7011	37,9846
18	37,4425	36,6192	37,8178	37,4408	37,7040
19	37,2768	35,5700	37,2773	36,6693	37,0888
20	36,8424	35,4713	36,6765	35,7515	36,8850
21	35,2984	34,9491	36,4558	35,5875	35,7610
22	34,9989	34,7923	35,7722	35,1888	35,3799
23	34,6652	33,7961	35,1258	34,4821	34,8883
24	34,0018	33,5146	35,0249	34,1817	34,3303
25	33,2964	31,9934	34,3889	33,7225	33,7744
26	32,7586	31,9353	34,1112	33,5202	33,1398
27	32,5421	31,5150	33,2352	32,8792	32,9256
28	32,3027	31,2458	32,7062	31,8925	32,2116
29	31,8145	30,8377	32,2890	31,1338	31,9206
30	30,4265	30,5690	32,0480	30,8268	31,4086
31	30,0797	30,0090	31,3032	30,5448	30,9605
32	29,5904	29,3225	30,5034	29,7901	30,4697
33	29,2897	28,9221	29,6564	28,8425	29,9553
34	28,7577	28,7277	28,9913	28,6074	28,8208
35	28,0603	27,5379	28,3158	28,3992	28,5650
36	27,5106	27,2784	27,7745	27,5041	28,5623
37	27,1995	26,6448	27,0441	27,0669	28,0026
38	26,5540	26,4751	26,7987	26,7708	27,2946
39	26,2846	26,0195	26,2976	26,0360	27,0040
40	26,0488	25,4953	26,0027	25,7208	26,8097

ТАБЛИЦА 4. Случайные величины s_{ij} для $i = \overline{1,40}$ и пяти различных реализаций $j = \overline{1,5}$ при n'_r = 105

i \ j	s_{i1}	s_{i2}	s_{i3}	s_{i4}	s_{i5}
1	51,0525	52,4051	50,7671	50,9304	53,3030
2	50,1215	50,1651	49,8737	49,9729	51,9680
3	49,0182	48,7795	47,3157	48,1872	50,3994
4	47,6980	47,7254	46,2905	47,2354	48,8838
5	45,9271	46,7796	45,6912	46,7631	47,6098
6	45,6491	45,9614	45,6158	46,3825	46,7328
7	44,4314	45,0383	44,2227	44,3765	45,7012
8	43,6762	44,4048	43,5531	43,9086	44,4846
9	43,0767	43,4138	43,1271	43,8365	43,9982
10	42,2469	42,8153	41,9297	42,5838	43,5527
11	41,7005	42,1903	41,7961	42,2480	43,3056
12	40,3599	41,6170	41,1772	41,4343	42,5701
13	40,1258	41,3271	40,6395	41,1894	41,2485
14	39,2298	40,6084	40,0972	39,9136	40,2877
15	38,7502	40,4165	39,3049	38,7834	40,2442
16	37,9958	39,5256	39,1801	38,4859	39,7597
17	37,5404	39,1158	38,3658	38,1844	39,1178
18	37,2299	38,4101	37,8458	36,5435	37,8485
19	36,4555	37,7388	37,3191	36,3994	37,6625
20	36,0850	37,1429	36,2638	35,5926	36,5804
21	35,5125	35,7764	35,9380	35,3538	36,0237
22	34,9910	35,3590	35,2148	34,3229	35,6984
23	34,7023	35,0952	34,9277	34,1906	35,5144
24	33,8417	34,9278	34,5666	33,7256	35,1886
25	33,5916	34,1016	33,8895	32,7836	34,5603
26	33,1604	33,0011	33,5583	32,4151	33,7950
27	32,4448	32,6937	33,1395	32,2744	33,2186
28	32,2882	32,3002	32,6185	32,0008	32,6310
29	31,8583	32,0213	31,9431	31,7464	32,0468
30	30,5857	31,5666	31,2539	31,1378	31,8992

i \ j	s_{i1}	s_{i2}	s_{i3}	s_{i4}	s_{i5}
31	30,3614	31,0349	30,9671	30,0685	31,0186
32	29,9107	30,2961	30,4434	29,7443	30,7447
33	29,1624	30,0768	30,3460	29,2628	30,4146
34	28,0804	29,8380	29,6397	28,4758	29,4452
35	27,8688	28,7883	28,7459	28,0159	29,2755
36	27,5767	28,2542	28,5769	27,6436	28,7508
37	27,0264	27,8458	27,6775	27,4557	27,8893
38	26,5485	27,4480	27,3608	27,0286	27,1623
39	26,0338	26,4308	26,8501	26,5306	27,0440
40	25,9308	26,2616	26,6310	25,9455	26,6097

ТАБЛИЦА 5. Случайные величины ω_{kj} (n_t = 100) для $k = \overline{1,40}$ и пяти различных реализаций при n'_r = 100

k \ j	1	2	3	4	5
1	1,9846	0,5222	3,2900	4,6527	2,0207
2	3,4308	1,2298	2,5761	1,6060	2,4357
3	3,3587	1,5144	2,8048	3,7926	2,6829
4	6,6143	1,1309	1,0924	0,6373	1,3335
5	2,8218	0,5050	1,6004	1,6562	2,5735
6	2,8608	2,0991	3,4095	0,5823	2,0196
7	3,6834	3,2847	3,2654	0,5395	3,9628
8	4,4297	0,4656	1,1136	3,3682	5,2492
9	4,4331	0,6591	3,9570	0,7569	4,1201
10	3,1958	0,7685	3,1320	0,8674	3,6958
11	3,4283	2,7693	2,1594	1,1643	1,4124
12	4,0915	0,8224	2,8227	0,5428	3,3620
13	3,1960	2,0685	2,7783	1,0022	2,2754
14	5,6759	1,9221	3,1338	1,4704	2,4892
15	1,8939	1,9314	1,7613	4,6215	2,6918
16	3,0903	1,7260	5,8338	0,4706	1,9392
17	1,8665	0,8096	1,8194	4,1651	1,7015
18	2,3706	0,9222	3,6568	4,5733	5,1911
19	1,9215	2,4882	4,0727	0,6510	5,1157
20	2,8299	0,6427	5,7474	1,3071	2,1649
21	1,8476	1,1147	3,4409	0,3493	5,6532
22	2,7517	0,5247	3,7741	0,6099	3,2229
23	4,4024	0,5002	3,8064	0,5944	6,2287
24	2,7851	1,1352	5,4927	2,7942	1,7500
25	3,3366	0,4097	4,6385	0,3326	4,2765
26	2,6730	0,9086	2,0913	2,8262	2,3091
27	3,8579	0,8057	1,4655	1,1352	3,8464
28	2,3699	0,4921	4,0721	0,6573	1,8491
29	5,2229	0,7782	2,8351	0,6173	2,9256
30	1,1227	0,7285	1,6397	0,9779	4,5044
31	3,3540	0,7621	2,1291	0,9221	3,1184
32	3,0100	1,6583	3,1495	0,5934	1,9128
33	4,3621	3,7209	3,4513	1,4781	3,6105
34	1,9256	1,5865	2,5176	1,2569	3,7876
35	1,3389	0,9054	1,5619	1,1241	1,9794
36	2,4892	1,9327	4,8578	0,3260	1,3820
37	2,0796	1,4055	3,2001	3,2078	1,9919
38	1,9362	2,5563	5,2230	0,3634	1,4959
39	3,1184	1,1876	1,3201	0,5969	1,4720
40	4,9434	0,7916	4,8323	1,9655	2,7303

ТАБЛИЦА 6. Случайные величины ω_{kj} (n_t = 100) для $k = \overline{1,40}$ и пяти различных реализаций при n'_r = 105

k \ j	1	2	3	4	5
1	6,2679	5,7891	7,2672	5,3831	5,9682
2	3,7038	3,6270	4,8018	5,3113	5,0838
3	4,3658	7,6600	8,0046	7,3262	5,0549
4	4,8616	9,5016	6,8342	6,1170	5,8418
5	4,2510	5,5914	7,5223	5,3520	6,6236
6	5,9091	8,1895	5,4094	5,4328	4,8303
7	4,6049	5,5495	4,8075	10,5884	6,5329
8	6,4248	8,6097	7,4937	6,0501	5,8135
9	3,6786	5,2058	5,0351	3,0167	7,0902
10	5,6959	8,3521	7,5842	4,5017	5,0697
11	5,5613	5,6151	4,8692	5,6888	6,5788
12	6,9997	4,7204	3,8405	7,7850	6,9683
13	5,1010	4,8062	5,2455	10,1494	4,5532
14	5,2678	7,2805	5,9596	5,5409	3,7928
15	5,6089	6,9313	6,2117	5,7224	6,6978
16	5,7201	5,5132	7,0248	3,9900	7,1515
17	3,9158	7,1903	5,3712	5,3842	7,2660
18	5,4469	8,9754	10,3433	7,4300	6,3544
19	7,2746	6,2582	7,0232	5,4671	7,4671
20	8,0872	7,9586	6,7233	4,6033	6,0726
21	6,8778	4,9960	5,2627	5,1678	7,3263
22	3,6874	5,9936	3,2304	8,4734	4,5826
23	7,3758	5,6581	6,5649	5,8878	8,8896
24	3,5204	7,1738	6,4555	7,2639	7,7913
25	4,5306	8,3439	8,0531	5,9445	7,7517
26	5,2706	5,1339	6,7258	6,7226	6,2229
27	7,2363	6,8404	7,3249	7,2963	3,9436
28	7,7720	6,9914	6,0754	6,2912	7,1116
29	7,1064	6,8517	5,3435	5,5372	7,3255
30	6,4529	12,3479	4,7709	4,5910	6,0625
31	5,7347	4,9199	6,8339	4,2195	6,6362
32	3,5772	6,2352	4,3817	7,1693	5,6378
33	4,0619	5,5543	7,7146	6,3833	3,9807
34	5,2881	3,7907	6,3661	9,9999	5,6802

k \ j	1	2	3	4	5
35	4,4696	4,5214	5,6794	9,5892	6,1307
36	4,3246	6,1177	4,7823	3,7072	8,8412
37	3,8956	5,5797	6,9569	6,1384	5,9812
38	7,2877	10,0537	7,7241	4,8599	6,0950
39	5,2380	3,1328	5,5268	6,5845	8,1906
40	5,1080	3,8480	8,4157	4,0010	7,3393

ПРИМЕЧАНИЕ. Заметим, что пять реализаций приведены здесь лишь из-за ограниченности объема статьи. В действительности нами получен значительно больший массив данных.

Таким образом, даже небольшое в процентном отношении увеличение количество антенн перехватчика приводит к полной компрометации DG-криптосистемы. С другой стороны, легальные пользователи DG-криптосистемы не могут, конечно, обеспечить выполнение условия $n_r' < n_r$ при котором эта система оказывается работоспособной.

В уже упоминавшейся статье [5] предлагалось изменить «предобработку» или «предкодирование» сигнала, которое ранее задавалось выражением (3), где V матрица SVD – разложения канальной матрицы A. В частности авторы [5] исследовали кодирование сигнала матрицей $V_0 = A^{-1}$ и показали, что в этом случае определяемое в некотором смысле числовое преимущество легального пользователя перед перехватчиком, возрастает пропорционально n^2, если $n_t = n_r = n_r' = n$.

Однако, во-первых, это представляет интерес при одинаковом количестве приемных антенн у легального пользователя и перехватчика, что не может быть практически гарантировано. Во-вторых, выбор предкодирования $V = A^{-1}$ означает, что фактически тривиально «отменяются» замирания канала, так как вместо выражения (4) для описания легального канала мы получаем модель этого канала в виде:

$$z = x + e.$$

Однако препятствием применения данного метода предкодирования является то обстоятельство, что требуемая мощность передатчика легального пользователя оказывается равной тогда $P = \|xA^{-1}\|^2$, что может значительно превысить его энергетические ресурсы.

Заметим здесь, что при прежнем методе предкодирования $y = Vx$, средняя мощность сигнала передатчика легального пользователя была равной n_t^2.

В таблице 7 приведены результаты моделирования случайных реализаций P_i, где $i \in \overline{1,12}$ средней мощности передатчика легального пользователя.

ТАБЛИЦА 7. Расчет средней мощности передатчика легального пользователя P_i

i	1	2	3	4	5	6
P_i	$4{,}5\cdot10^5$	$1{,}2\cdot10^7$	$9{,}1\cdot10^5$	$2{,}1\cdot10^6$	$8{,}8\cdot10^4$	$5{,}9\cdot10^5$
i	7	8	9	10	11	12
P_i	$3{,}4\cdot10^4$	$5{,}2\cdot10^4$	$2{,}5\cdot10^5$	$1{,}08\cdot10^5$	$7{,}1\cdot10^5$	$3{,}8\cdot10^5$

Видно, что предкодирование при помощи обратной матрицы A^{-1} приводит к резкому возрастанию требуемой мощности по сравнению с мощностью при предкодировании матрицей V. (В последнем случае для n_t = 100, средняя мощность была бы равна 10000).

Расчет распределения мощности (гистограмм) показывает, что примерно на 9800 итерациях мощность оказывается менее 10^5, а на остальных итерациях она лежит в диапазоне от 10^5 до 10^{12}. Подобное свойство приводит к мысли, что легальный пользователь мог бы передавать информацию только в тех случаях, когда после предкодирования матрицей A^{-1}, требуемая мощность оказывается ниже некоторого допустимого порога (очевидно, что при знании обоими легальными пользователями матрицы канала передачи A, различение сеансов с передачей информации и без нее не составит проблемы).

Если же выбрать для кодирования произвольную матрицу V_0, которая обеспечивает ограничение средней мощности легального передатчика, то прием легальным пользователем по правилу (7) окажется невозможным, так как не выполняется равенство (5) при $V_0 \neq V$. Тогда остается лишь использовать для легального пользователя подоптимальное правило (12), пытаясь минимизировать при этом вероятность ошибки. Этот подход требует проведение дополнительных исследований.

IV. Заключение

Криптосистема, предложенная Дином и Голдсмитом в 2013 году, казалась на первый взгляд, новой революцией в криптографии, по крайней мере, для каналов с замираниями, поскольку она не требовала никакого предварительного распределения ключей и не предполагала наличия никаких преимуществ легальных пользователей перед перехватчиком, за исключением различного их положения в пространстве.

В работе [5] тезис «революционности» этой криптосистемы был впервые поставлен под сомнение при использовании перехватчиком бóльшего количества антенн, чем легальными пользователями. В настоящей работе приведено дальнейшее исследование данной криптосистемы, как в теоретическом, так и в экспериментальном плане. Было доказано, что даже небольшое в процентном отношении увеличение количества антенн перехватчика по сравнению с количеством

антенн легальных пользователей, приводит к полной компрометации данной криптосистемы.

Предположение, высказанное в работе [5] о возможности использования предкодирования в виде обратной матрицы к матрице легального канала, приводит, как показано в нашей работе, к нереализуемо большой мощности передатчика легальных пользователей. Метод работы сеансами с ограниченной мощностью (также предложенный в данной работе) требует, однако, дополнительного изучения.

Таким образом, можно сделать общий вывод, что DG-криптосистема не имеет в настоящем виде положительных перспектив для ее практического применения. Более предпочтительными представляются методы распределения ключей по радиоканалам с использованием MIMO-технологии. Один из примеров подобного подхода описан в работе [7].

Список используемых источников

1. Dean T., Goldsmith A. Physical-Layer Cryptography through Massive MIMO // Proceedings of the IEEE Information Theory Workshop. 2013.
2. Micciancio D., Regev O. Lattice-based Cryptography in Post-Quantum Cryptography. Springer. 2009. PP. 147–191.
3. Mukherjee A., Fakoorian S., Huang J., Swindlehurst A. Principle of Physical Layer Security in Multiuser Wireless Networks: A Survey. 2014. arXiv:1011.3754v3[csIT].
4. Коржик В.И., Яковлев В.А., Тихонов С.В. Вторая революция в криптографии: миф или реальность // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 79–89.
5. Steinfeld R., Sakad A. On Massive MIMO Physical Layer Cryptosystem. 2015. arXiv:1507.08015v1[csIT].
6. Tse D., Viswanath P. Fundamentals of Wireless Communication. Cambridge University Press. 2000.
7. Yakovlev V., Korzhik V., Mylnikov P., Morales-Luna G. Outdoor Secret Key Agreement Scenarios Using Wireless MIMO Fading Channels // International Journal of Computer Science and Applications. 2017. Vol. 14. Iss. 1. PP. 1–25.

* * *

INVESTIGATION OF KEYLESS CRYPTOSYSTEM PROPOSED BY DEAN AND GOLDSMITH

A. Gerasimovich[1], **V. Korzhik**[1], **V. Starostin**[1]

[1]The Bonch-Bruevich State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
Article in Russian

For citation: Gerasimovich A., Korzhik V., Starostin V. Investigation of Keyless Cryptosystem Proposed by Dean and Goldsmith // Proceedings of Telecommunication Univercities. 2017. Vol 3. Iss. 3. PP. 43–50.

Abstract: *Theoretical and experimental investigation of cryptosystem proposed by two scientists from Stanford University are presented. This cryptosystem has been called in one paper by "revolution" in cryptography. In the current paper it is shown that it is not the case at least in practical application.*

Keywords: *physical layer cryptography, fading channel, singular value decomposition, MIMO-systems.*