ЖЭТФ, 2019, том 156, вып. 2 (8), стр. 379–380

ПОПРАВКА К СТАТЬЕ «ДОСТАТОЧНО ЛИ СОСТОЯНИЙ ЛОВУШЕК (DECOY STATE-МЕТОДА) ДЛЯ ГАРАНТИИ СЕКРЕТНОСТИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ?»

С. Н. Молотков, К. С. Кравцов, М. И. Рыжкин

(ЖЭТФ, 2019, том **155**, вып. 4, стр. 636)

Поступила в редакцию 29 апреля 2019 г.

Изначально Decoy state-метод был предложен для противодействия атаке с расщеплением по числу фотонов (PNS-атака). Кратко идея Decoy state-метода исходит из следующих посылок. Поскольку фаза самого когерентного состояния в каждой посылке случайна, в канале присутствует не чистое состояние, а статистическая смесь фоковских состояний с разным числом фотонов, распределение числа фотонов является пуассоновским. Консервативно считается, что подслушиватель может измерять число фотонов непосредственно на выходе из передающей станции. Вероятность обнаружить состояния с числом фотонов $|k\rangle\langle k|$ зависит от среднего числа фотонов в состоянии — $e^{-\mu}\mu^k/k!$, если посылалось когерентное состояние со средним числом фотонов μ. При этом, обнаружив данное число фотонов k, подслушиватель принципиально не может узнать, из какого когерентного состояния, с каким средним числом фотонов μ, ν_1 или ν_2 происходит состояние $|k\rangle\langle k|$. Далее консервативно считается, что длина секретного ключа определяется долей однофотонной компоненты в состоянии. Считается, что из всех посылок с числом фотонов $k \geq 2$ подслушиватель получает достоверную информацию о передаваемом бите ключа. Для оценки наблюдаемой доли однофотонной компоненты посылаются состояния с разным средним числом фотонов. Из темпа отсчетов состояний с разным средним числом фотонов происходит оценка доли однофотонной компоненты и ошибки в ней.

Decoy state-метод изначально был разработан для детектирования изменения пуассоновской статистики состояний. При некоторых атаках (атака со светоделителем) пуассоновская статистика состояний не меняется. Поэтому заранее неочевидно, что Decoy state-метод не будет завышать длину секретного ключа при такой атаке.

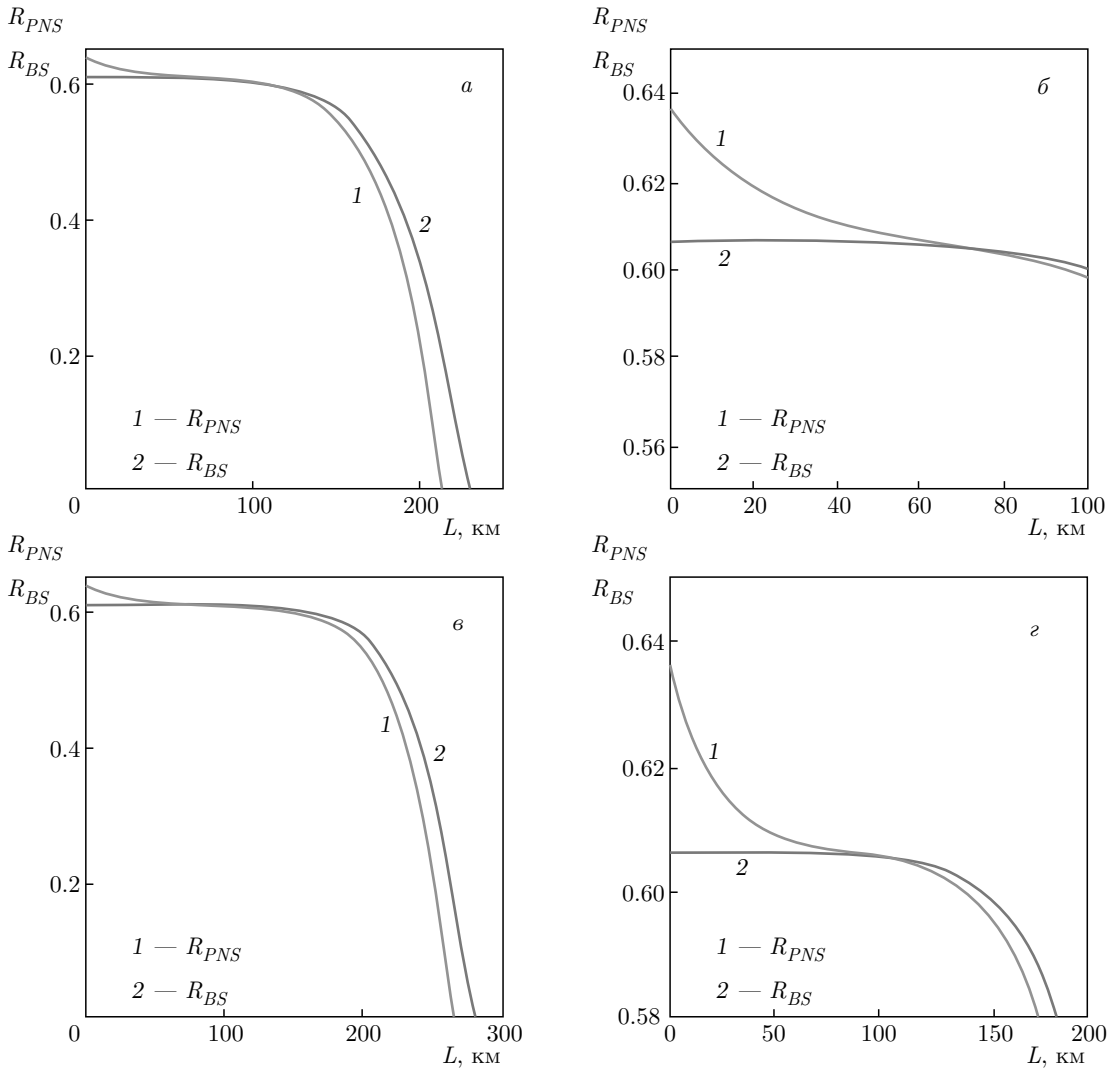
Этому была посвящена работа [ЖЭТФ **155**, 636 (2019)]. Однако при вычислениях была сделана переоценка длины ключа при Decoy state-методе по сравнению с атакой со светоделителем из-за пропущенного при вычислениях сомножителя $e^{-\mu}$ в формуле (30). Формула (30) должна выглядеть следующим образом:

$$R_{PNS} - R_{BS} =$$

$$= \left\{ \frac{e^{-\mu}\mu(p_d + \eta T(L))}{p_d + 1 - e^{-\mu\eta T(L)}} \left[1 - h\left(\frac{0.5p_d}{p_d + \eta T(L)} \right) \right] - h\left(\frac{0.5p_d}{p_d + 1 - e^{-\mu\eta T(L)}} \right) \right\} -$$

$$- \left\{ e^{-\mu(1-T(L))} - h\left(\frac{0.5p_d}{p_d + 1 - e^{-\mu\eta T(L)}} \right) \right\}.$$

Здесь имеет смысл отметить, что нехватка информации Евы о ключе при атаке со светоделителем (слагаемое $e^{-\mu(1-T(L))}$) не является консервативной в пользу Евы. При консервативной оценке следует заменить $e^{-\mu(1-T(L))} \to e^{-\mu}$. Величина $e^{-\mu}$ представляет собой $1 - \chi(\mu) = e^{-\mu}$, $\chi(\mu)$ — фундаментальная величина Холево, она имеет смысл верхней границы количества информации, которая может быть получена из ансамбля квантовых состояний непосредственно на выходе источника квантовых состояний. Данная граница включает в себя информацию от всех компонент состояния: однофотонных, двухфотонных и т. д. Причем



Зависимости длины секретного ключа в пересчете на зарегистрированные посылки как функции длины линии связи. Кривые *1* и R_{PNS} относятся к оценкам по Decoy state-методу, кривые *2* и R_{BS} — к консервативным оценкам для атаки со светоделителем. Параметры: среднее число фотонов $\mu = 0.5$, квантовая эффективность детектора $\eta = 0.2$, одинаковы для всех рис. *а–г*. Вероятность темновых шумов $p_d = 10^{-6}$ (*а,б*), 10^{-7} (*в,г*)

данная консервативная оценка информации подслушивателя, в отличие от Decoy state-оценок, не содержит никаких модельных предположений о параметрах канала и детекторов (квантовой эффективности η, вероятности p_d темновых шумов).

Зависимости длины секретного ключа при консервативных оценках, основанных на границе Холево, при атаке со светоделителем и по Decoy state-методу приведены на рисунке. Как видно из рисунка, при определенных длинах линии связи консервативная оценка, основанная на фундаментальной величине Холево, является более жесткой.

Как следует из сказанного и из рисунка, возможны различные консервативные оценки длины ключа, которые дают хотя и близкие, но разные результаты в различных областях длины канала связи. На наш взгляд, получение универсальных плотных оценок для длины секретного ключа, особенно для комбинации различных атак, без использования модельных предположений является на сегодняшний день не до конца решенной задачей.