关于信息理论安全中的衰落生成密钥的注记

***摘要***—在这项工作中，我们探索通过无线衰落信道的电磁互易产生的密钥的安全性。我们确定一个新的复杂的密谋攻击，我们探索了这种密码的信息理论安全，这样的密钥存在于对方手中，是由量子力学的法则约束下驱动的。具体来说，我们计算了当一个具有无限计算和通信资源的对手在选定的位置放置定向天线拦截器时，发送方和接收方之间的条件相互信息的减少。这样的位置，在原则上，可以任意远离预期的接收者，但仍然会影响秘钥率。

**A Note on the Information-Theoretic-(in)Security of Fading Generated Secret Keys**

Robert Malaney ∗

*Abstract*—In this work we explore the security of secret keys generated via the electromagnetic reciprocity of the wireless fading channel. Identifying a new sophisticated colluding attack, we explore the information-theoretic-security for such keys in the presence of an all-powerful adversary constrained only by the laws of quantum mechanics. Specifically, we calculate the reduction in the conditional mutual information between transmitter and receiver that can occur when an adversary with unlimited computational and communication resources places directionalantenna interceptors at chosen locations. Such locations, in principal, can be arbitrarily far from the intended receiver yet still influence the secret key rate.

在实际通信系统中，信息理论安全密钥的快速生成。仍然是需要持续的努力。目前，几乎所有用于商业部署场景的密钥生成系统都是基于信息载体的量子力学特性的。然而，尽管在量子密钥分发(QKD)系统方面已经取得了很大的进展，但是在它们的部署变得无处不在之前仍然存在着重大的实际挑战(参见[1]最近的一篇回顾)。这种情况的技术原因是多种的，但它们确实导致了寻找其他共享随机性的来源，这些资源可以被用于秘密密钥生成。通过无线信道连接的无线电接收设备提供了一种可能性——通过纯粹的经典手段。[[1]](#footnote-1)

事实上，多年来人们都知道，一般无线环境中固有的随机衰落(加上电磁互惠)是秘密密钥生成的潜在来源(最近的一篇回顾参见4-7)。在合理的(和琐碎的验证)假设中，假设Eve(对手)不在附近(在GHz频率的几厘米)的Bob(合法的接收方)中，通常会说衰落会导致信息理论的安全密钥。这里我们澄清的是当 *Me* → ∞, *Me* 是指Eve所拥有的接收设备的数量。

在QKD系统1中几乎所有的安全分析中都使用了一个全能的对手，而它是对这个神秘的对手的保护，使基于量子系统的关键系统获得了他们的安全地位。这种受欢迎的安全是信息理论的安全(在传统的信道被验证的条件下)，即使*Me* → ∞，也能保持在适当的位置。

在这里，我们探讨了在无线衰落产生的关键系统上，一个全能的前夜的攻击。更具体地说，我们量化了这个Eve如何将定向天线接收器(例如光阑、线性阵列、相控阵等)放置在实字散射环境的多个位置，并且在主要驱动下，在任意的低水平上，Bob和Alice(发射机)之间的有条件的相互信息。讨论调用有限形式的攻击的实际场景，显示(至少)当前主流的密码系统是怎样在一定程度上受到攻击的。

我们将把“信息理论安全”这个术语具体化为以下内容。将一些明确的假设条件（或限制）的做为系统模型参照，但由于独立的对方的能力（而不是由自然法的约束），对攻击者访问关键信息可以被缩小到任意范围的水平，可以适当的使用一些系统资源。具体来说，我们考虑一些系列的随机变量的观测*X* = (*X*1*,X*2*,...Xn,*), *Y* = (*Y*1*,Y*2*,...Yn,*), 和*Z* = (*Z*1*,Z*2*,...Zn,*) 是由分别是由Alice，Bob和Eve所共享的随机资源。 分别的，我们使用无限方案并假设Alice和Bob之间的消息交换(对Eve来说是用的),对于一些足够大n密钥计算Alice和Bob(分别KA和KB)是用来满足以下要求一些ǫ > 0, (i) Pr(K A 6= K B ) ≤ε, (ii) n −1 I(K A ;Z) ≤ ε, (iii) n −1 I(K A ) ≥ r K − ε, 并且 (iv) n −1 log|C| ≤ n −1 H(K A ) + ε, H (·)是两个随机变量之间的互信息，并且(·;\* | \*)是两个随机变量之间的互信息条件，则\*在另一个随机变量C中，而 C| |的基数是另一个密钥的字母(C)和rK。rK则是一个可以实现的密钥的方案。一般来说，因为密匙率是未知的，但是由于上限可以由8,9 rK min(I(X，Y)，I(X，Y Z)即可给出。在这里，X和Y之间的相互信息可以被写入*I* (*X*; *Y* |*Z*) = *H*(*X,Z*) + *H*(*Y,Z*) − *H*(*Z*) − *H*(*X,Y,Z*), H(，…)是一系列随机变量的联合熵。如果我们引入了两种概率质量函数p(w)和q(w)之间的信息散度的信息散度，即样本空间w和viz，D(pkq)== E，然后通过离散的公式来估计=*, p(x)*是概率*x=x，p(，…)*对应的关节概率。

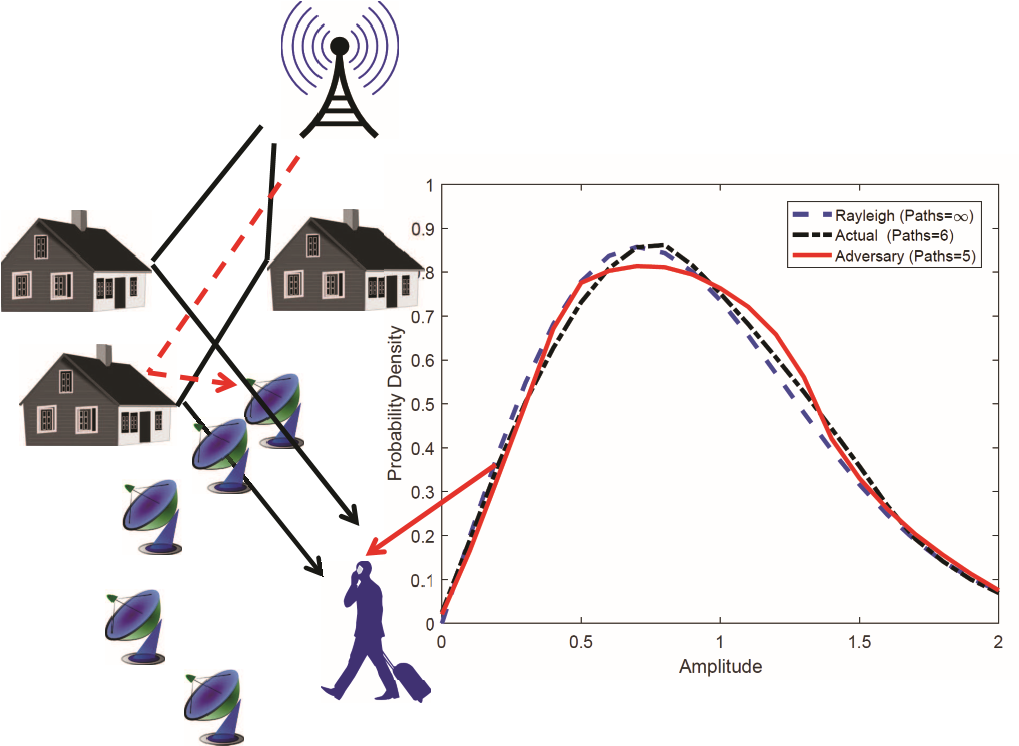
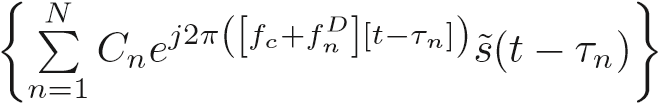
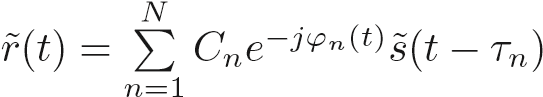
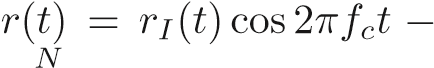


图1. 不同路径设置的概率密度函数(pdf)。上图显示了Bob的概率密度函数，其中有无数条路径(虚线)、6条路径(点虚线)，以及一个被完全拦截(见文本)5条路径(固态)的合谋者。左边的示意图说明了共谋攻击的性质，在这里，固体(黑色)线表示了一些可能的射线，而这条线是在伊芙所拦截的，而(红色)虚线表明了一个潜在的“干扰”路径，其中一条是由Eve所持有的定向天线。

我们采用窄带的平衰落信道，并利用在平面几何上的波传播的远场近似。我们假设电场矢量是正交于平面的，并且在各向同性增益的天线由爱丽丝和鲍勃持有。如果我们考虑，在载波频率fc(波长c)，一个带通信号传输信号, 且*s*˜(*t*) 是复杂的包络线，接收到的带通信号可以被写入(如10)，r(t)=Re, *r*(*t*) = Re. 这里的*N* 传播路径到达接收器，Cn和n的传播路径分别是振幅和时间延迟，并且 *fnD* 是多普勒频率(n表示第n条路径)。 后一种量可以表示为*fnD* = (*v/λc*)cos*αn*, *v* v是接收方的速度，n是在接收方的第n条路径到达(AoA)角度，上不封相对于速度速度矢量。类似于传输信号，接收到一个复杂的包络线上，并且信号是可以被写入的。，

当。 因此，就得条件有 。在传输单音的情况下就可以写成

*n*P=1 *rQ*(*t*)sin2*πfct*, where *rI*(*t*) = *Cn*(*t*)cos*ϕn*(*t*) 并且

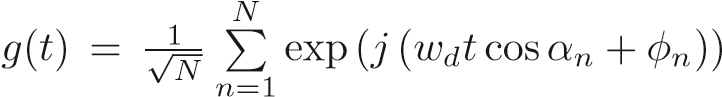
*N*

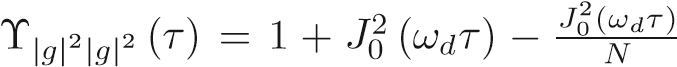
*rQ*(*t*) = *Cn*(*t*)sin*ϕn*(*t*). In the Rayleigh channel these quadratures are independent Gaussian processes. Writing

*n*P=1

|*A*| = q*rI*(*t*)2 + *rQ*(*t*)2 and *ϑ* = arctan(*rQ*(*t*)*/rI*(*t*)) we then have *r*(*t*) = |*A*|cos(2*πfct* + *ϑ*), where |*A*| is Rayleigh distributed and *ϑ* is uniformly distributed. In such a channel, |*A*| and/or *ϑ* can be used for secret key construction.

Ultimately the secret key is dependent on movement in the scattering environment, and it this movement that sets the channel coherence time (and therefore the key rate). The movement within the scattering environment ultimately manifests itself at the receiver through variation in received amplitudes and delays. However, to enable clarity of exposition, we will make some simplifications to our scattering model - noting that the attack we describe can in fact be applied to any scattering environment scenario. The simplifications are that we assume equal amplitudes for all received signals, and adopt random uniform distributions for all AoA and all phases as measured by the receiver. This is in fact the celebrated 2D isotropic scattering model of Clarke [11]. Moving to the baseband signal henceforth for convenience, we note in Clarke’s model the signal of a transmitted symbol can be

written as *,* where *wd* is now the maximum Doppler frequency in rad/s, and *φn* is the phase of each path. Assuming both *αn* and *φn* are independent and uniformly distributed in [−*π,π*), then in the limit of large *N* the amplitude of the signal *g*(*t*) is distributed as a Rayleigh distribution.

Of particular interest to us here will be the statistics of *g*(*t*) at low values of *N*, since in such circumstances the potential for an adversary to intercept all signals is larger. The higher order statistics of the distribution within Clarke’s model at finite *N* have been explored in [12], showing that the following autocorrelation functions are in place; Υ*gg* (*τ*) = *J*0 (*ωdτ*), and , where *J*0 (·) is the zero-order Bessel function of the first kind. For large *N* these functions approach those of the Rayleigh distribution. Importantly, the Υ *g*|2|*g*|2 function is well approximated by an

|

exponentiated sinc function at values of *N* ≥ 6, meaning that (as per the usual assumption for any fading generated key), Eve must be several wavelengths away from Bob for the secret key rate to be non-zero.[[2]](#footnote-2)

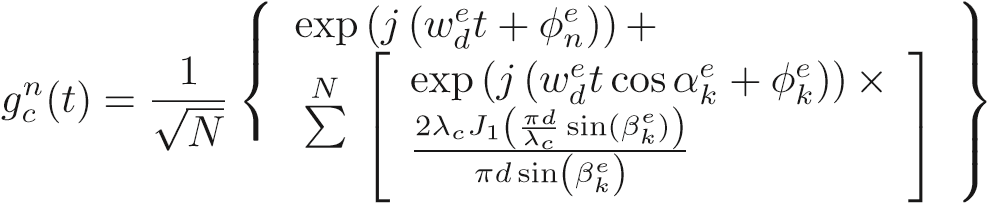
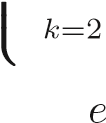
Many refinements on Clarke’s model exist with perhaps the most widely used being that of [12] in which the main differentiator is a constraint placed on the AoA, viz.,, where *θn* is independently (relative to *φn*) and uniformly distributed in [−*π,π*). This latter simulator is wide sense stationary, is more efficient, and has improved second-order statistics. In consideration of *all* statistical measures, it is noted that for this refined model any differences between *N* & 8 and the *N* = ∞ model (pure Rayleigh distribution) are largely

inconsequential [12].[[3]](#footnote-3)

In real-world channels, therefore, we have to be aware that even in cases where the channel appears to be consistent with a Rayleigh channel, the number of propagation paths contributing to the received signal can be relatively small. This can be seen more clearly from Fig. (1) where the probability density functions formed from six and five propagation paths are shown in comparison to the infinite path limit. The five path model corresponds to a case where Eve is missing one of the propagation paths used to construct Bob’s signal. For the cases shown the Kullback-Leibler divergence between the Rayleigh distribution and the lower-path models is very small.

Let us assume the communications obtained by Bob consist of the combined signals from *N* last-scattering events. We are interested in determining the effect, on some secret key generation scheme, caused by Eve’s interception of all (or some fraction of) the *N* last-scattered paths received by Bob. We assume Eve has *Me >> N* directional-antenna receivers, and has placed them at multiple locations with the aim of continuously intercepting all of the last-scattered signals towards Bob with high probability.[[4]](#footnote-4) We assume that these locations are much greater than *λc* from Bob.

Beyond our assumption of 2D geometry, and that the amplitude of each last-scattered ray entering any receiver is equal, we also assume that the number of paths reaching each of Eve’s antennas is equal to *N*.[[5]](#footnote-5) Extension of our analysis to cover these issues is cumbersome, but straightforward. To make our mathematical notation less unwieldy, we will artificially set *Me* = *N* in our equations, with the understanding that we are then simply ignoring all of Eve’s devices which (at any given time) are not intercepting any scattered rays towards Bob. For added focus, we will assume Eve uses circular apertures of diameter *d* as her directional receivers - the physics and properties of which can be found elsewhere, e.g. [14]. Eve configures her *n*th aperture at each location so as to maximize signal gain for the signal directed by the last scatterer in the direction of Bob (i.e. the *n*th of *N* rays reaching Bob is centered in the main lobe of Eve’s *n*th aperture). In such circumstances the signal collected by Eve’s *n*th receiver can be approximated as,

where the superscript applied to any previously used variable means it is now applied to Eve (but same meaning), where *βke* represents the angle between the *k*th propagation path (side lobe ‘interference’ path) arriving at Eve’s detector and ray *n* (i.e. *βne* = 0), and where *J*1 (·) is the Bessel function of the first kind of order one. Note that the maximum Doppler shift *wde* on Eve’s detector is included so as to cover the general case. However, for focus we will assume all of Eve’s detectors are stationary, and in the following always set . To reduce the mathematical complexity further we have not included in our analysis an obliquity factor (1 + cos*βke*)*/*2, which makes our calculations conservative (i.e. results in higher key rates).

Upon receipt of the signals *gcn*(*t*) Eve will adjust the signals for the known distance offset between each detector and Bob, and the known motion of Bob. This entails a phase adjustment at each detector which manifests itself as an ‘adjusting’ phase *φna*. The combined adjusted signal obtained by Eve after such signal processing, can then be written as

*N*

*g*(*t*) = *gcn*(*t*)exp(*jφna*). *n*P=1

Assuming Eve’s different apertures intercept all paths that are received by Bob, the above relations lead us to conclude that, in principle, by increasing her aperture size Eve can determine Bob’s received signal to arbitrary accuracy. In practice this accuracy will be limited by any receiver noise on Eve’s antennas, and error due to imprecise location information on Bob. However, with regard to these accuracy limitations (which we include in our Monte Carlo simulations below), we note the following two points that favor Eve. (i) Given her all-powerful status, Eve can set her noise to be at the quantumlimit (quantum noise). (ii) Beyond any other means available to her, an unlimited Eve can determine the location of Bob at time *t* to any required accuracy through signal acquisition. More specifically in regard to (ii), the minimum position error via signal processing varies as  - a result that holds even if some of Eve’s devices are affected by shadowing in which the path-loss exponents are unknown [15].

To make further progress we must introduce an actual scheme for generating a secret key. Although there are many such schemes (e.g. [4–7]) we will adopt here a generic formulation that covers the conceptual framework of the widely used signal threshold schemes. The basic concept of such schemes is to quantize a received signal metric, say amplitude, into a 1 or 0 value. For some parameter *T >* 0, and for some median value *m* of the expected amplitude distribution, the decision value can then be set dependent on whether the amplitude is below *m* − *T* or above *m* + *T*. Such schemes offer many pragmatic advantages and compensate to a large extent errors introduced through a lack of exact reciprocity between transceiver configurations. Assuming a given level of Gaussian noise at Bob and Eve’s receivers, an appropriate value of *T* can be chosen. Further, so as to maximize the entropy of the final key, we introduce an ‘entropy’ factor *s*. For a given *T* and probability density function *R*′(*r*) for the received amplitude *r*, the value of *s* can be determined through

. Note, in general *R*′ is the

distribution for the amplitudes in the presence of non-zero Gaussian receiver noise. When *r* is measured by Alice and/or Bob to be between the two ‘allowed’ regions, as defined by the integrals of this relation, it is agreed by both parties that the measurement be dropped.

Clearly, in practice larger values of *T* will minimize mismatches in the key at the cost of a reduced key generation rate. Ultimately, in any real scheme a period of reconciliation and privacy amplification will be pursued in order to obtain the final key. However, here we will simply investigate the upper limit of the key rate through a numerical evaluation

0

0.1

0.2

0.3

0.4

0.5

0.6

Diameter (m)

0

0.5

1

I(X;Y| Z)

Actual Paths=6 & Adversary Paths=4

Actual Paths=6 & Adversary Paths=5

Actual Paths=6 & Adversary Paths=6

0.4

0

0.1

0.2

0.3

0.5

0.6

Diameter (m)

0

0.5

1

I(X;Y| Z)

Actual Paths=20 & Adversary Paths=15

Actual Paths=20 & Adversary Paths=19

Actual Paths=20 & Adversary Paths=20

0

0.1

0.2

0.3

0.4

0.5

0.6

Diameter (m)

0

0.5

1

I(X;Y| Z)

Actual Paths=20 & Adversary Paths=15

Actual Paths=20 & Adversary Paths=19

Actual Paths=20 & Adversary Paths=20

Fig. 2. Change in the conditional mutual information between Alice and Bob as function of the diameter of Eve’s directional antenna (a circular aperture) for different path conditions. Six paths (top figure) and 20 paths (middle figure) are used to construct the approximate Rayleigh distribution. One calculation (bottom figure) on the 20 path scenario assumes zero receiver noise at Eve and zero location error on Bob. Results shown are for 1 million Monte Carlo runs.

of the conditional mutual information as defined earlier. We assume Eve’s strategy on detection is to decide on the binary number in the ‘disallowed’ region by setting *s* = *T* = 0. We also assume all issues on the decision strategy of the scheme and all communications between Alice and Bob (e.g. which measurements to drop) are available to Eve.

Fig. (2) (top) displays a calculation of the conditional mutual information as a function of aperture diameter (all of Eve’s circular apertures are assumed to be the same size) in which a receiver noise contribution (on all receivers) is set so that the signal-to-noise ratio (SNR) is equal to 17dB. The maximum Doppler shift of Bob is set to 10Hz, *λc* is set to 0.1m, and a Gaussian error on the pointing of Eve’s apertures (due to location error on Bob) is set to a standard deviation of 0.002 radians. The threshold is set at three times the receiver noise. We can see that if all signals are intercepted the key rate can be driven to almost zero over the range of aperture diameters probed. For fewer signals intercepted we see that useful key rates are still possible, albeit at significantly diminished values relative to a no-attack scenario. For comparison, Fig. (2) (middle) displays similar calculations but for 20 propagation paths forming the Rayleigh distribution, and Fig. (2) (bottom) shows the same calculation when Eve’s detectors are operating with zero receiver noise, and location errors on Bob are assumed to be zero.

The specific key scheme discussed here is limited in scope relative to the large number of possible key generation schemes available. More sophisticated schemes, such as those based on multi-antenna transceiver configurations, the use of optimal coding techniques, and the use of channel state information, are possible. However, straightforward extensions of the attack described here would still apply to all of these more sophisticated schemes - only the quantitative details on how the key rate is diminished under the attack will be different.

Indeed, we note the attack described here can be generalized further so as to *always* drive the secret key rate to zero, even if we relax the assumption that it is only the last-scattering rays that are intercepted. An all-powerful Eve, with *ME* → ∞, can intercept all propagation paths (of any energy) at all points in space, and in principal possess knowledge on all characteristics of all scatterers. With the unlimited computational resources afforded to her the classical Maxwell equations can then be solved exactly, thereby providing information on any of Bob’s received signals at an accuracy limited only by quantum mechanical effects. Of course, such an attack whilst theoretically possible, is not tenable. The calculations described here can be considered a limited form of such an attack, tenable in a real-world scattering environment.

In conclusion, we have described a new attack on classical schemes used to generate secret keys via the shared randomness inherent in wireless fading channels. Although the attack we have described will be difficult to implement in a manner that drives the secret key rate to zero, our work does illustrate how such a rate can at least be partially reduced. As such, all schemes for secret key generation via the fading channel must invoke a new restriction - a limitation on the combined information received by a colluding Eve.

1. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *npj Quantum Information*, 2, 16025, 2016.
2. C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, “Quantum cryptography approaching the classical limit,” *Phys. Rev. Lett.* 105, 110501, 2010.
3. N. Hosseinidehaj and R. Malaney, “Quantum entanglement distribution in next-generation wireless communication systems,” *IEEE VTC Spring*, Sydney, Australia (arXiv:1608.05188), 2017.
4. L. Lai, Y. Liang, H. V. Poor, and W. Du, “Key generation from wireless channels,” *Physical Layer Security in Wireless Comms.*, (CRC), 2014.
5. P. Narayan and H. Tyagi, “Multiterminal secrecy by public discussion,” *Found. and Trends in Comms. and Info. Theory*,” 13, pp. 129–275, 2016.
6. J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” *IEEE Access*, 10.1109/Access.2016.2521718, 2016.
7. H. V. Poor and R. F. Schaeferb, “Wireless physical layer security,” *PNAS*, vol. 114, no. 1, pp. 19-26, 2017.
8. U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory,* vol. 39, no. 3, pp. 733-742, 1993.
9. R. Ahlswede and I. Csiszar,“Common randomness in information theory and cryptography-Part I: Secret sharing” *IEEE Trans. Inf. Theory,* vol.

39, no. 4, pp. 1121-1132, 1993.

1. G. L. Stu¨ber, “Principles of Mobile Communication,” (Kluwer) 2002.
2. R. H. Clarke, “A statistical theory of mobile-radio reception” *Bell Syst. Tech. J.,* pp. 957-1000, Jul.-Aug. 1968.
3. C. Xiao,Y. R. Zheng, and N. C. Beaulieu, “Novel sum-of-sinusoids simulation models for Rayleigh and Rician fading channels” *IEEE Transactions on Wireless Communications*, vol. 5, no. 12, 2006.
4. X. He, H. Dai, W. Shen, and P. Ning,“Is link signature dependable for wireless security,” *in Proc. IEEE Infocom,* Turin, Italy, pp. 200–204, 2013. [14] S. J. Orfanidis, “Electromagnetic Waves and Antennas,” 2016.

[15] R. Malaney, “Nuisance parameters and location accuracy in log-normal fading models,” *IEEE Trans. Wireless Communications*, vol 6, issue 3, pp. 937–947, 2007.

1. 这条经典的路线尤其重要，因为QKD直接超过了在GHz范围内的无线信道，限制在短距离为 [2,3].

   . [↑](#footnote-ref-1)
2. A relaxation of this requirement may be obtained in specific correlated channel scenarios applicable to a distance of order 10 wavelengths (∼ meters at GHz frequencies) away from the receiver [13]. The attack we describe here is unrelated to the special case of correlated channels. It is a general attack. Eve’s receivers can in principal be positioned anywhere (e.g. kms away from the intended receiver) yet still mount a successful attack. [↑](#footnote-ref-2)
3. In the calculations to follow, we find that the key rates computed are, in effect, independent of whether this refined model or Clarke’s original model is the adopted Rayleigh simulator. [↑](#footnote-ref-3)
4. Such a possibility can be enhanced in some scenarios by additional actions on Eve’s part. For example, a scenario in which Eve has conducted an *a priori* ray-tracing measurement (or analysis) campaign between a given pair of transmit and receive locations thereby obtaining probabilistic information on likely last scattering points (for that given pair of locations). Of course in the limit *ME* → ∞ her probability of intercepting all paths approaches one in any case. [↑](#footnote-ref-4)
5. As an aside, we find a doubling of this number of paths at each of Eve’s detectors has negligible impact on the results. Also note, as the number of paths reaching Eve approach infinity, the size of her aperture must be made to approach infinity for the attack to remain viable. Neither limits are ever in place of course. [↑](#footnote-ref-5)