Received August 22, 2015, accepted September 7, 2015, date of publication September 22, 2015, date of current version October 1, 2015.

Digital Object Identifier 10.1109/ACCESS.2015.2480422

A New Transient Attack on the Kish Key Distribution System

LACHLAN J. GUNN, (Student Member, IEEE), ANDREW ALLISON, AND DEREK ABBOTT, (Fellow, IEEE)
School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia
Corresponding author: L. J. Gunn (lachlan.gunn@adelaide.edu.au)

ABSTRACT The Kish Key Distribution (KKD) system has been proposed as a classical alternative to quantum key distribution, making use of temperature-matched thermal noise. Previous analyses assume instant propagation of signals along the cable connecting the two users. We describe a new attack that takes an advantage of propagation delays. At the start of each bit period, the noise temperature will then be increased from zero to its final value. During this process, the noise temperature variation will take time to propagate along the line, resulting in a temperature mismatch. We analyze the information leak due to this effect and consider several potential mitigation schemes.

INDEX TERMS Electromagnetic propagation, cryptography protocols, channel capacity, cryptography, communication system security.

I. INTRODUCTION

Ronald Rivest, of RSA fame, once remarked [1] "Calling a bit-string a 'secret key' doesn't actually make it secret … Rather, it just identifies it as an interesting target for the adversary." Key distribution forms a vital part of modern cryptography, and the holy grail for the cryptographer is to be able to distribute a key with *unconditional* [2] or *information-theoretic security*. The development of quantum cryptography [3] has heralded a golden age for information-theoretic security, motivating the development of a plethora of techniques, such as privacy amplification and information reconcilliation [4], with the aim of extracting a shared secret key from correlated random variables. A wide variety of classical systems have been proposed to take advantage of these tools, whose application is not limited merely to quantum cryptography; some are based on wireless fading [5], others on artificial signals—we consider the Kish Key Distribution (KKD) system [6], which uses artificially-generated noise mimicking a pair of hot resistors attached to a transmission line. This purely classical system can be implemented inexpensively, allowing it to be used in a far wider range of devices than QKD; requiring neither expensive optics or a wireless link, it is one of the few forms of physical-layer cryptography that is applicable to fixed industrial sensor networks, for which cost and reliability are of vital importance.

Whether purely classical key distribution systems can match or outperform quantum key distribution systems is hotly debated. Moreover, KKD is an elegant classical scheme whose study potentially brings us a step closer to understanding the essential differences in security between quantum and classical cryptosystems. It is of great general interest as the study of KKD is wide-ranging and brings together information theory [7], thermodynamics [6], [8], statistical physics [9], probability theory [10], [11], and electromagnetism [7], [12], [13] to bear in explaining its subtle properties.

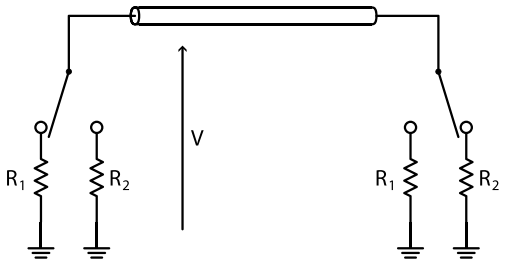

FIGURE 1. The idealized Kish Key Distribution system. The two switches are set randomly, and the noise voltage is measured on the line. Alice and Bob can determine the value of each others' resistors from the mean-square voltage on the line and the known values of their own resistors. Because the switches are randomly selected, a sequence of these states forms a random key that Alice and Bob effectively share. There are four resistor combinations in total, two of which are indistinguishable to Eve. Thus, to maintain secrecy, Alice and Bob maintain a simple protocol of agreeing to drop insecure bits from the key.

The Kish Key Distribution system, shown in Figure 1, is purely classical and its principles brilliantly simple; in its simplest form, each endpoint is composed of two resistors and a switch used to connect one of them to the line.

IEEE Access
The journal for rapid open access publishing

The mean-square voltage on the line is given by

$$\langle V^2 \rangle = 4kTB(R_1||R_2), \tag{1}$$

where R_1 and R_2 are the resistances selected at the left and right ends of the system, whose owners we denote Alice and Bob respectively. If R_1 and R_2 are both large, then $\langle V^2 \rangle$ will be correspondingly large. Conversely, if R_1 and R_2 are both small, $\langle V^2 \rangle$ will be correspondingly small. An eavesdropper measuring the line's noise voltage can thus determine the resistor values in these two cases.

However, when $R_1 = R_a$ and $R_2 = R_b$, or vice-versa, the magnitude of the line voltage will take an intermediate value that is independent of which end possesses which resistor. In this case, an eavesdropper cannot determine which of the two states was chosen; Alice and Bob declare a key bit of zero for one of these states, and a key bit of one for the other, as shown in Figure 2.

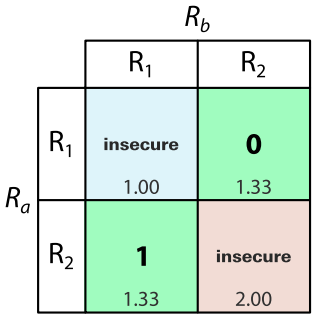

FIGURE 2. The four possible resistor states. Each time the protocol is run, the two switches are set at random, placing the system into one of the four states shown; at the bottom of each square is the mean-square line voltage for $R_a = 1\ \Omega$, $R_b = 2\ \Omega$, and $4kTB = 2$; this is only for illustrative purposes, and in practice the resistors will be of the order of several kilo-ohms. Two of the states are indistinguishable by an eavesdropper measuring only $\langle V^2 \rangle$, while Alice and Bob, who know their own selected resistor values, and so which row and column respectively the true state is in, can distinguish all four states. When running the protocol, Alice and Bob simply agree to drop any insecure bits from the generated random key.

The goal of an attacker, whom we denote Eve, is to exploit the simplifications inherent in this lumped model to differentiate the two spatially-mirrored configurations for which Alice and Bob declare a key bit.

We note that, in practice, a simple resistor does not provide enough noise—typically only a few nanovolts RMS per root-Hertz at room temperature. It is therefore necessary [6] to increase the apparent temperature of the resistances by artificial means. To do this, we place a source of Gaussian noise in series with each resistor, their powers proportional to the resistance in question. Practical values on the order of 1 V RMS correspond to noise equivalent temperatures of approximately 1×10^{18} K.

II. QUANTIFICATION OF ATTACK EFFECTIVENESS

In order to quantify the effectiveness of the attack, we must choose a suitable figure of merit. Previous work has either failed to provide a measure or used bit-error-rates either directly or with the assumption of a binary symmetric channel [13]–[15]; this latter approach, while providing a rough indication of the information available to Eve, does not provide a directly meaningful quantity. Another work [16], claiming to prove the unconditional security of the system, considers only asymptotic behaviour. We discuss this proof and its relevance to the present attack in the appendix. We adopt a more general approach, taking account of the asymmetry of the channel and computing bounds on the secrecy rate for each given attack. This is particularly important for the attack that we introduce in Section IV, as its error rates are highly asymmetric.

A. ATTACK CONSTRUCTION

As all the signals in the KKD system are zero-mean Gaussian, we describe the available measurement variables of the system using a multivariate Gaussian model, the covariance matrix conditioned upon the state of the two resistors, which may be swapped. We denote these two covariance matrices $\mathcal{C}_1$ and $\mathcal{C}_2$, the indices denoting whether Alice has chosen R_1 or R_2 respectively. The measurements in state i thus have a probability density function

$$f_i(\mathbf{x}) = (2\pi)^{-\frac{n}{2}} |\mathcal{C}_i|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}\mathbf{x}^t \mathcal{C}_i^{-1}\mathbf{x}\right], \tag{2}$$

where n is the number of measurement variables in the model. However, in many cases Bob and Eve make different measurements and thus see different covariance matrices $\mathcal{C}_{i,b}$ and $\mathcal{C}_{i,e}$, each containing a subset of the elements of $\mathcal{C}_i$. We showed in [13] that the Bayesian estimate for state S is given by the maximum-likelihood estimator,

$$\mathbf{x}^t \left(\mathcal{C}_q^{-1} - \mathcal{C}_p^{-1}\right)\mathbf{x} \underset{q}{\overset{p}{\lessgtr}} \log_e \frac{|\mathcal{C}_p|}{|\mathcal{C}_q|}, \tag{3}$$

for two arbitrary states p and q with corresponding covariance matrices $\mathcal{C}_p$ and $\mathcal{C}_q$ respectively.

However, a rigorous treatment of the system requires that we consider also the insecure states. In this case, we actually desire not the exact state of the system, but the resistance that was chosen by the sending party, since this is what will be used to determine the key bit. That is to say, if Alice is sending a message, the (R_1, R_1) state must be interpreted as a zero, since it lies within the $R_a = R_1$ row of Figure 2. Conversely, if Bob is the sender, a mistakenly-accepted (R_1, R_1) state will result in a one being used for the encryption, it falling within the same column as the true state.

Thus, while Alice and Bob—who need only distinguish between two states—can use the simple estimator above, Eve's maximum-likelihood estimator for the key bit used by Alice is

$$\begin{aligned} &|\mathcal{C}_{00}|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}\mathbf{x}^t \mathcal{C}_{00}^{-1}\mathbf{x}\right] \psi_{00}(\mathbf{x}) \\ &+ |\mathcal{C}_{10}|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}\mathbf{x}^t \mathcal{C}_{10}^{-1}\mathbf{x}\right] \psi_{10}(\mathbf{x}) \\ &\underset{R_2}{\overset{R_1}{\lessgtr}} \\ &|\mathcal{C}_{11}|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}\mathbf{x}^t \mathcal{C}_{11}^{-1}\mathbf{x}\right] \psi_{11}(\mathbf{x}) \\ &+ |\mathcal{C}_{01}|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}\mathbf{x}^t \mathcal{C}_{01}^{-1}\mathbf{x}\right] \psi_{01}(\mathbf{x}), \end{aligned} \tag{4}$$

where

$$\psi_{ab}(\mathbf{x}) = u\left(\mathbf{x}\left(\mathcal{C}_{ab}^{-1} - \mathcal{C}_{a(1-b)}^{-1}\right)\mathbf{x} - \log_e \frac{|\mathcal{C}_{ab}|}{|\mathcal{C}_{a(1-b)}|}\right) \times u\left(\mathbf{x}\left(\mathcal{C}_{ab}^{-1} - \mathcal{C}_{(1-a)b}^{-1}\right)\mathbf{x} - \log_e \frac{|\mathcal{C}_{ab}|}{|\mathcal{C}_{a(1-b)}|}\right) \quad (5)$$

is the indicator function for the set of measurements $\mathbf{x}$ that results in the bit being kept. That is to say, if a bit is kept, the likelihood is zero for any state that results in it being dropped. With this estimator, we may now simulate the system as a whole, allowing us to estimate the secrecy rate of the system. If Bob is the sender, the terms involving $\mathcal{C}_{00}$ and $\mathcal{C}_{11}$ are be swapped.

B. COMPUTATION OF SECRECY BOUNDS

In order to provide concrete numbers, we consider the secrecy rate [4], [17] of the binary system formed by the application of this estimator to the variables $\mathbf{x}_b$ and $\mathbf{x}_e$ measured by Bob and Eve respectively. This is the maximum rate at which an arbitrarily-secret key can be generated by the system, and ranges from zero—where no security is available—to one—where a secret bit can be generated for every bit emitted by the system. This allows the security of an information-theoretic system to be evaluated independently of the available coding techniques, and in a fashion more directly applicable to the performance of the system. This is the first time that this has been evaluated for the KKD system, and so for reference we will apply the same technique to a number of previous attacks. In order to find this rate, the asymmetric error probabilities are computed by simulation, allowing mutual information and conditional mutual information to be estimated and thus the evaluation of the bounds from [4]:

$$S(X;Y|Z) \leq \min\{I(X;Y), I(X;Y|Z)\} \quad (6)$$

$$S(X;Y|Z) \geq \max\{I(X;Y) - I(X;Z), I(X;Y) - I(Y;Z)\}, \quad (7)$$

where X represents the variables available to Alice, Y those available to Bob, Z those available to Eve, and $I(X;Y|Z)$ the conditional mutual information of X and Y given Z. These results apply to arbitrary variables X, Y, and Z, not merely the wiretap channel. We denote $S(X;Y|Z)$ the secrecy rate of the channel with respect to an eavesdropper knowing Z. The error probabilities are calculated by generating, for each resistor configuration, an ensemble of random vectors of normal variables with the necessary covariance matrix and applying the state estimator being tested. Doing this simultaneously for Alice, Bob, and Eve provides us with the full joint probability distribution of X, Y, and Z, allowing computation of the secrecy rate bounds above from standard mutual information formulae. Increasing bit durations are modelled by adding additional independent steady-state samples; this enlarges the covariance matrix correspondingly.

It is important to note that in our analysis we use the binary variables X, Y, and Z produced by the bit estimation process. This is therefore not a canonical measure of security, but that of a hypothetical test setup. A bound on secrecy rate with respect to the raw measurements—as opposed to estimated resistor states—requires the consideration of more complex probability measures and is beyond the scope of this paper, and therefore only the upper bound on secrecy rate is directly meaningful, as it remains a possibility that a more sophisticated eavesdropper might use the raw analog measurements to glean further information from the system, for example by propagating reliability estimates through the decoding stages.

C. SYSTEM PARAMETERS

In order to provide a fair comparison, all of the attacks discussed will be considered with respect to the same system, described in Figure 3.

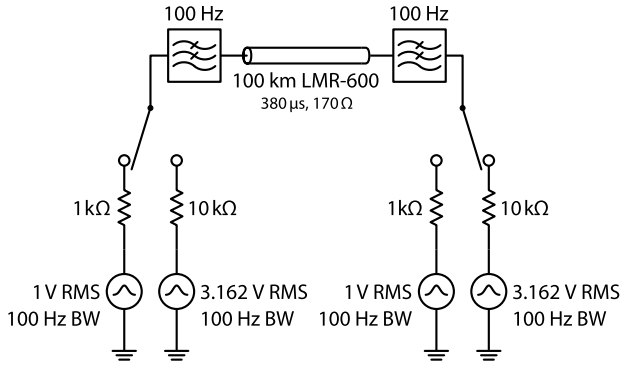

FIGURE 3. The KKD system under analysis, with component values included. We model a 100 km link constructed of low-loss LMR-600 [18] coaxial cable. This has a propagation velocity of 0.87c, and thus a 380 μs electrical length and half-wavelength frequency of 1300 Hz.

1) RESISTORS

We have chosen resistor values of 1 kΩ and 10 kΩ as in [13] and similarly to [19]. This choice will affect the security of the system against all types of attacks—resistors further apart in value allow the use of shorter bit periods and so make the task of the eavesdropper more difficult when carrying out steady-state attacks, however this makes certain transient attacks more efficient; we will introduce such an attack in Section IV.

2) TRANSMISSION LINE

The line is chosen to be 100 km long. This falls into the middle of the range proposed by [19], from chip-scale at the low end to 2000 km at the high end. This length is selected in order to achieve a cable resistance in line with the 200 Ω value considered in previous work [19]. The cable itself is low-loss LMR-600 [18], with a propagation velocity of $0.87c$ and core resistance of 1.7 Ωkm^{-1}.

3) SYSTEM BANDWIDTH

The propagation time of the line is 380 μs, and therefore has a half-wavelength frequency of 1300 Hz. We follow the

recommendation of [6] and limit the bandwidth to somewhat less than a tenth of this; we therefore use noise sources and line filters with a bandwidth of 100 Hz. Both are assumed to be perfect; that is, their frequency spectra and responses respectively are rectangular.

4) NOISE SOURCES

The noise sources themselves are assumed to be exactly Gaussian, with a linear ramp profile as used in [19]. The ramp lasts for 8% of the bit duration at both the beginning and the end of the cycle. The magnitudes of the voltages are chosen so that the 1 kΩ resistor has in series a noise voltage of 1 V RMS. This corresponds to a noise temperature of 1.8×10^{17} K.

III. NONIDEALITIES IN THE LUMPED MODEL

We begin by analysing the simple lumped model shown in Figure 3, modelling the transmission line as a resistor R_L. Let us denote the voltage sources of Alice and Bob $V_a(t)$ and $V_b(t)$ respectively, the voltage at Alice's end of the line $V_x(t)$, and the current through the line $I(t)$. Here, $V_x(t)$ and $I(t)$ are the measurement variables of the system, and are given by

$$\mathbf{x}(t) = \begin{bmatrix} V_x(t) \\ I(t) \end{bmatrix} \tag{8}$$

$$= \frac{1}{R_a + R_b + R_L} \begin{bmatrix} R_b + R_L & R_a \\ 1 & -1 \end{bmatrix} \begin{bmatrix} V_a(t) \\ V_b(t) \end{bmatrix} \tag{9}$$

$$= A\mathbf{V}(t). \tag{10}$$

From this we may compute the measurement covariance matrices $\mathcal{C}_x = A\mathcal{C}_v A^t$, where $\mathcal{C}_v$ is the covariance matrix of the noice sources of Alice and Bob and given by

$$\mathcal{C}_v = 4kT_{\text{eff}}B \begin{bmatrix} R_a & 0 \\ 0 & R_b \end{bmatrix}, \tag{11}$$

where T_{eff} is the noise equivalent temperature of the system.

A. RESISTANCE ERRORS

The first nonideality that we consider is due to errors in the resistor values. These can be caused by manufacturing variations, but also by the resistance of the line itself—this can be interpreted as a known constant added to the resistors. With high-precision resistors available at low cost with tolerances less than 0.1%, it is the latter form of error that dominates, and so we focus our analysis there. By simulating the system in Equation 10, compute the secrecy rate of such a system, shown in Figure 4.

A characteristic shape is visible—at first the secrecy rate increases with bit duration, before peaking and slowly falling away. With very few samples, the error rate between Alice and Bob is so high as to render communication almost impossible; the secrecy rate is therefore very low in this regime. As the number of samples increases, Alice and Bob, whose state classification problem is very simple, quickly reduce their error rate. However, Eve's error rate falls in a similar way, albeit more slowly due to her relative lack of

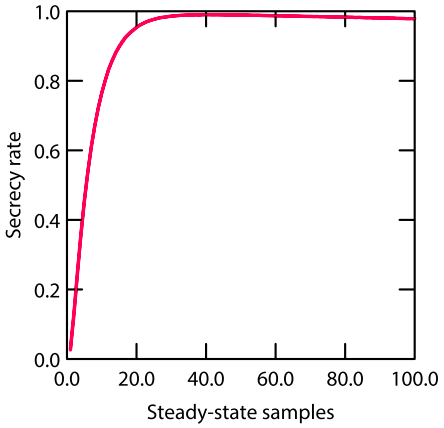

FIGURE 4. Secrecy rate as a function of steady-state averaging time in terms of equivalent independent samples, with 10^6 simulated bits per point. Upper and lower bounds are shown, though are not visible without magnification. Alice, Bob, and Eve make use of both voltage and current measurements. Note that the secrecy rate steadily increases as Alice and Bob reduce their error rate, eventually peaking as it approaches zero and so can no longer improve relative to Eve's performance.

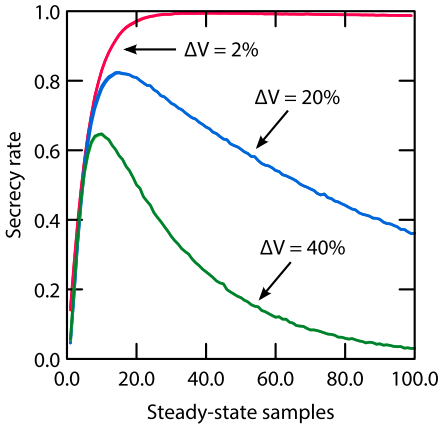

FIGURE 5. Secrecy rate of the ideal KKD system with various voltage mismatches and zero line resistance, with 10^5 simulated bits per point. We see that, even with a large mismatch of 2%, the effect on secrecy rate is slight; with calibration it will be almost negligible. Gross mismatch is necessary in order to substantially reduce the peak secrecy rate.

per-sample information, and eventually the additional information that Alice and Bob can squeeze from each sample falls below that which Eve can extract, resulting in a peak such as in Figures 4 and 5. The secrecy rate slowly approaches zero as the number of samples increase and the four states therefore become increasingly difficult to confuse.

We hasten to add that a countermeasure [8] is available that eliminates information leakage due to the line resistance. Briefly, when the system is in one of the two secure states, the line can be viewed as being part of the small resistor; by adjusting their mean-square voltages from $4kT_{\text{eff}}BR_1$ to $4kT_{\text{eff}}B(R_1 + R_L)$ the system becomes secure once more.

B. TEMPERATURE ERRORS

A related phenomenon is temperature error in the two terminals; if the voltages are not correctly calibrated,

the apparent temperatures of Alice's and Bob's resistors will differ, resulting in a net flow of power through the line [14]. This power flow manifests itself as a correlation between voltage and current, the sign depending upon its direction.

The effect is shown in Figure 5; we see that the effect is relatively small even with a pessimistic voltage error of 2%. In practice, one can regularly calibrate the noise temperatures, reducing the leak to a completely negligible level as seen experimentally in [19].

IV. TRANSIENT ATTACKS

In [13] we considered the use of directional measurements of the wave components travelling in each direction along the line; this is frustrated by the band-limited nature of the signals and the large reflection coefficients of typical endpoint designs. It was found that this model, while effective in the case of a resistive line, was unable to differentiate the zero- and one-states in the absence of propagation delays, though the general applicability of the attack proposed in [13] remains somewhat contentious [9], [20], [21]. This result has motivated us to consider the effect of propagation delays, with the goal of reconciling the non-constructive information-theoretic claims of [7]—which state that this type of system is inherently insecure—with the far less dire results found by analysis in the quasi-static limit.

V. PROPAGATION DELAYS AND TEMPERATURE MISMATCH

Irrespective of the veracity of the claims of [9] and [12], the signals injected onto the line by the endpoints must propagate at some finite sub-c speed; there must therefore be, even with perfect synchronisation, some finite period during which each point along the line experiences only a signal due to the closest endpoint.

We demonstrate this phenomenon in Figure 6. At time $t = 0$, the noise temperature of each endpoint begins to rise. However, this rise is invisible to the majority of the line—the increasing potential of the fluctuation is retarded, to use the terminology of [9]. In the middle of the line, the signals are retarded by equal amounts, and thus the apparent temperature profiles remain constant. Away from the centre of the line, however, the retardation times differ, resulting in an apparent temperature mismatch. This temperature mismatch allows a Hao-type attack [14] to be performed without relying on errors of calibration. We note that the temperatures involved here are of the sources and not of the transients themselves.

Let L be the length and v the speed of propagation of the line. We first consider a linear temperature profile, ramping from 0 to 1 in time t_r. The temperature of each source is at time t given by

$$T(t) = r(t/t_r) - r(t/t_r - 1), \tag{12}$$

where r denotes the unit ramp function. At a distance x from Alice, the apparent temperatures are given by

$$T_a(t) = T(t - x/v) \tag{13}$$

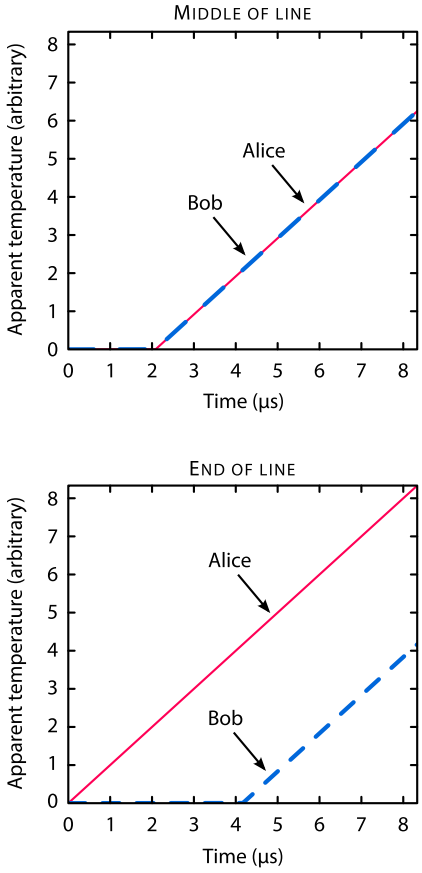

FIGURE 6. The effect of propagation on apparent noise temperatures with a linear profile. Parameters chosen are $L = 1$ km, $v = 2 \times 10^8$ ms^{-1} $t_r = 1$ ms. In the top graph, the apparent temperatures are shown from the perspective of a point equidistant between the two endpoints. As the signals from both endpoints are equally retarded, the apparent temperatures are equal. The bottom graph shows the apparent temperatures at one end of the line; one endpoint suffers no retardation, while the other experiences that by the full length of the line. This results in a temperature imbalance during the ramp-up time.

$$T_b(t) = T(t - (L - x)/v), \tag{14}$$

resulting in a temperature ratio of

$$\frac{T_a(t)}{T_b(t)} = \frac{r\left(\frac{t-x/v}{t_r}\right) - r\left(\frac{t-x/v}{t_r} - 1\right)}{r\left(\frac{t-(L-x)/v}{t_r}\right) - r\left(\frac{t-(L-x)/v}{t_r} - 1\right)}. \tag{15}$$

Supposing without loss of generality that $x > L/2$,

$$\frac{T_a(t)}{T_b(t)} = \begin{cases} 0, & (L-x)/v < t \le x/v \\ \dfrac{t - x/v}{t - (L-x)/v}, & x/v < t \le t_r + (L-x)/v \\ \dfrac{t - x/v}{t_r}, & t_r + (L-x)/v < t \le t_r + x/v \\ 1, & t > t_r + x/v, \end{cases}$$

shown in Figure 7.

VI. LEAK ANALYSIS

The non-ergodic nature of the modulated noise process prevents the Hao attack from being used directly over the entire

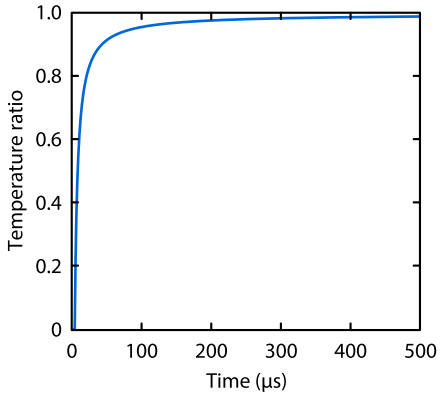

FIGURE 7. The ratio of apparent temperatures at one end, using a linear temperature profile. Parameters are identical to those described in Figure 6. With careful examination, the ratio is seen to remain at zero some time after $t = 0$.

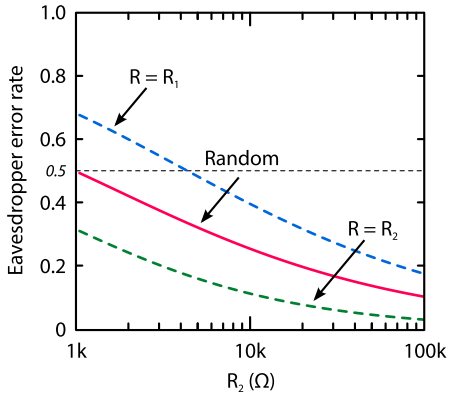

FIGURE 8. Resistor-estimation error rates for an eavesdropper using the attack discussed with $R_1 = 1$ kΩ. We show error rates for R_1 always chosen, R_2 always chosen, and for the resistor being chosen at random. Interestingly, the error rates are not symmetric with respect to the resistor actually chosen. The overall bit-error-rate approaches 0.5 as $R_2 \to R_1$; large gains in security are therefore possible if R_2 and R_1 are chosen to be similar. Note that these error rates are for estimation of a single resistor; by performing the attack at two points on the line, an eavesdropper may further reduce her bit error rate.

transient time; a full characterisation of the resulting information leak is therefore beyond the scope of this paper. Instead, we restrict ourselves to the time period $x/v < t \leq T + (L - x)/v$, during which the signal produced by only one endpoint is apparent. Because the correlation time of the system is required [6] to be substantially longer than the propagation time of the line, these measurements will contain little information beyond that of a single sample. The sample is distributed

$$X \sim \mathcal{N}(0, k\sigma_{\text{in}}^2), \tag{16}$$

where k is some constant that depends upon the choice of filter and temperature profile. We know [13] that

$$\sigma_{\text{in}}^2 = \frac{1}{2} kTBZ_0(1 - \Gamma^2), \tag{17}$$

where Γ is the reflection coefficient of the chosen resistance, and therefore this single sample provides us with enough information to estimate the choice of resistor. Values of $1-\Gamma^2$ for various choices of resistor are shown in Table 1.

TABLE 1. Values of $1 - \Gamma^2$ for various choices of resistor. A characteristic impedance of 50 Ω is assumed.

R	$1 - \Gamma^2$
1 kΩ	0.1814
10 kΩ	0.0198
100 kΩ	0.0020

It is therefore clear that substantially different resistors will result in substantially different variances, resulting in an information leak.

We plot the error rates for the estimation of a single resistor in Figure 8, which in the single-variable case can be calculated using Eqn. 3 as

$$E_{1\to 2} = F_{\chi^2}\left(\frac{\log \gamma}{\gamma - 1}\right) \tag{18}$$

$$E_{2\to 1} = 1 - F_{\chi^2}\left(\frac{\log \gamma}{1 - \gamma^{-1}}\right) \tag{19}$$

where

$$\gamma = \frac{1 - \Gamma_1^2}{1 - \Gamma_2^2}. \tag{20}$$

We see that the error rate of the eavesdropper falls towards zero as the difference in resistance increases. With currently-favoured component values—on the order of $R_1 = 1$ kΩ and $R_2 = 10$ kΩ—the error rate of the eavesdropper is approximately 25%. She can further reduce her error rate by making a similar measurement at the other end of the line, however doing so requires a multivariate estimator and so resists the calculation of error rates analytically by straightforward means.

We now proceed to calculate the secrecy rate. As the signals emitted by Alice and Bob are independent, the measurement covariance matrix is diagonal, with the two entries given by Eqn. 17. The effect of the attack upon the secrecy rate of the system is shown in Figure 9; the maximum secrecy rate is reduced by approximately one-third, and therefore this attack, if realised, has a significant effect upon security.

VII. COUNTERMEASURES TO THE TRANSIENT ATTACK

As noted previously, the error rate of the eavesdropper is substantial, even with current designs. It is therefore feasible to simply increase the level of privacy amplification. However, this comes at the cost of key rate, and it is therefore desirable to tackle the problem more directly.

It is proposed in [22] that the resistor values themselves vary during the equilibriation period, allowing the line to reach an approximate thermal equilibrium, however no implementation [13], [19] to date has been carried out. A time-varying resistance can be used to thwart our proposed attack by filling the line with noise before allowing the resistors to differ, thereby removing the period in which each resistor's final value can be probed separately. A similar

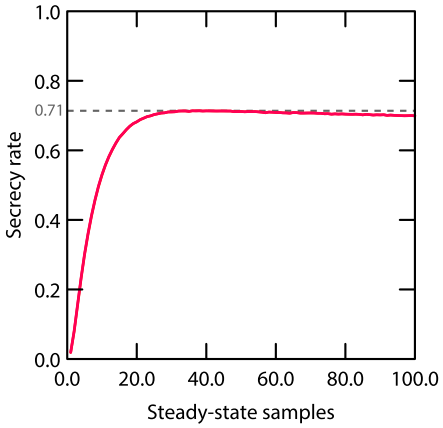

FIGURE 9. The secrecy rate of the system in the presence of an eavesdropper performing the described transient attack against both endpoints. We see that the plot is qualitatively similar to that of Figure 4, but reaching a maximum of only 0.71. Defending against this attack therefore requires substantial changes to the design parameters of the privacy amplification subsystem.

effect can be achieved by modifying the temperature profile according to the choice of resistor such that the injected signal $\frac{1}{2}kTBZ_0(1-\Gamma^2)$ is initially identical, irrespective of the resistance chosen. Combining these two approaches has the potential to further complicate further attempts at attack, at the very least in a practical sense. Eavesdropping on such systems will require a more general attack than that which we have proposed, taking advantage of the smaller imbalance that persists throughout the lengthy period of equilibriation.

VIII. CONCLUSION

We have discussed an attack against the Kish Key Distribution scheme based upon propagation delays between the two endpoints. This attack deviates from previous work in that it uses in a fundamental way the propagation delays of the line, putting it outside the class of temperature-resistance mismatch attacks that have dominated the literature on the scheme up to this point and opening the door to further discussion of the extent to which propagation-based effects determine the level of security of the system. Our analysis also provides a hitherto-unexplored connection between the choice of resistors and the degree of security, allowing this design decision to be made on a more informed basis.

APPENDIX

A paper [16] has been published claiming to prove the unconditional security of the a KKD system by an asymptotic argument. However, the assumptions made are overly severe and thus it fails to provide a meaningful demonstration of security—indeed, the actual proof of security is made without any reference to the physical system, and thus is equivalent to stating that any classical system, which can provide secure communication in an idealised setting, will provide unconditional security when subject to the nonidealities of the real world.

Briefly, the argument is as follows. Let $Q = (x_1, x_2, \ldots)$ parametrise the system design parameters in such a way that they are all equal to zero for the mathematically-ideal system [6], which can be demonstrated to be unconditionally secure. Now suppose that the two legitimate parties have access to the same measurements as Eve, and define a score δ representing the clarity that these measurements provide; they reject all bits with δ greater than some threshold ω, thus reducing the effect of outliers.

We define a function $p_\delta(Q)$ representing the probability that an eavesdropper will correctly determine the bit. Perfect secrecy is achieved if $p_\delta(Q) = 0.5$, and unconditional security if—but not only if—$p_\delta(Q) < 1 - p_e$, where p_e is the error rate of the two legitimate parties. We note that the definition of unconditional security that we have used in our paper based on the secrecy rate is a quantitative version of the more common one by Diffie and Hellman [2], and differs from that used in [16], where it is erroneously defined to be the closest practical approximation to perfect secrecy. As Q was defined such that it was equal to zero in the idealised scenario, which achieves perfect secrecy, $p_\delta(\mathbf{0}) = 0.5$.

The paper then claims that as linear and stable nonlinear systems have variables described by continuous functions, the function $p_\delta(Q)$ must be continuous in $\{x_i\}$, and that therefore $p_\delta(Q)$ can be made arbitrarily close to 0.5 by setting the $\{x_i\}$ arbitrarily small, thereby demonstrating the system to be unconditionally secure.

However, these assumptions range from being overly strict to completely unjustified, as explained in the following.

A. PARAMETRISATION OF THE DESIGN PARAMETERS

The assumption that one can completely parametrise the system in advance is a very strict condition and not at all practical. There will inevitably be unmodelled effects due to environmental conditions, tampering by the eavesdropper, or simply unintentional omission by the designer of the system. Any claim that a system is secure based on such an assumption must by accompanied by incontrovertible proof that the parameters have been completely enumerated, in order that they can not only be controlled in practice, but in order to ensure that the other assumptions are indeed valid—neither of which have been attempted by [16].

It is further assumed that these parameters can all be varied towards their ideal values, something that is not true in practice. One example provided by [16] of such a parameter is the cable length, however this is manifestly invariant—it cannot be made arbitrarily small, as it must be sufficiently long to connect the two endpoints. This immediately disqualifies the proof from application to any practical system, and also to the attack presented in this paper, which relies upon the nonzero length of the transmission line.

B. CONTINUITY ARGUMENT

In addition, it is also claimed that linear systems and stable nonlinear systems produce variables that are continuous-valued, and in particular that this applies to

the probability of error. However this is emphatically not true, which we demonstrate using the DC resistive circuit in Figure 10 as a counterexample.

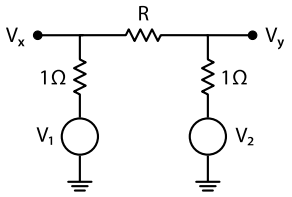

FIGURE 10. A resistive circuit containing two secret DC voltage inputs V_1 and V_2. An eavesdropper can measure the voltage at two points on the line, yielding voltages V_x and V_y, which determine V_1 and V_2 if and only if $R \neq 0$.

Figure 10 shows a KKD-like system that operates at DC. The two voltage sources are given a randomly-determined voltage—we assume some continuous distribution such as the Gaussian distribution in which all elements of the support are chosen almost never—and the eavesdropper is restricted to measuring the voltage at two points V_x and V_y. We may write this in matrix form as

$$\begin{bmatrix} V_x \\ V_y \end{bmatrix} = \frac{1}{R+2} \begin{bmatrix} R+1 & 1 \\ 1 & R+1 \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \end{bmatrix}. \tag{21}$$

This system is exactly soluble provided $R > 0$. However, when $R = 0$ the matrix is no longer invertible, and therefore Eve's estimate will be wrong almost surely, resulting in a probability of error equal to

$$p_e = \begin{cases} 1, & R = 0, \\ 0, & R > 0. \end{cases} \tag{22}$$

This function is not continuous, and thus the statement is disproven by contradiction.

Knowing that this type of behaviour is possible, it is therefore necessary to demonstrate that this continuity property exists on a case by case basis after having found a set of design parameters that can be made to approach their ideal while still representing a viable system. This is not carried out by [16], which simply assumes it to be so, rendering its argument invalid.

REFERENCES

[1] R. L. Rivest. *Illegitimi Non Carborundum*. [Online]. Available: http://iacr.org/conferences/crypto2011/slides/Rivest.pdf, accessed Sep. 17, 2015.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bengaluru, India, Dec. 1984, pp. 175–179.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[6] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," *Phys. Lett. A*, vol. 352, no. 3, pp. 178–182, 2006.

[7] C. H. Bennett and C. J. Riedel. (2013). "On the security of key distribution based on Johnson–Nyquist noise." [Online]. Available: http://arxiv.org/abs/1303.7435

[8] L. B. Kish and C.-G. Granqvist. (2014). "Elimination of a second-law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system." [Online]. Available: http://arxiv.org/abs/1406.5179

[9] H.-P. Chen, L. B. Kish, C.-G. Granqvist, and G. Schmera, "Do electromagnetic waves exist in a short cable at low frequencies? What does physics say?" *Fluctuation Noise Lett.*, vol. 13, no. 2, Jun. 2014, Art. ID 1450016.

[10] R. Mingesz, G. Vadai, and Z. Gingl, "What kind of noise guarantees security for the Kirchhoff-law–Johnson-noise key exchange?" *Fluctuation Noise Lett.*, vol. 13, no. 3, 2014, Art. ID 1450021.

[11] G. Vadai, R. Mingesz, and Z. Gingl, "Generalized Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system using arbitrary resistors," *Sci. Rep.*, vol. 5, Sep. 2015, Art. ID 13653.

[12] L. B. Kish, D. Abbott, and C. G. Granqvist, "Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme," *PLoS ONE*, vol. 8, no. 12, 2013, Art. ID e81810.

[13] L. J. Gunn, A. Allison, and D. Abbott, "A directional wave measurement attack against the Kish key distribution system," *Sci. Rep.*, vol. 4, Sep. 2014, Art. ID 6461.

[14] F. Hao, "Kish's key exchange scheme is insecure," *IEE Proc.-Inf. Secur.*, vol. 153, no. 4, pp. 141–142, 2006.

[15] J. Scheuer and A. Yariv, "A classical key-distribution system based on Johnson (like) noise—How secure?" *Phys. Lett. A*, vol. 359, no. 6, pp. 737–740, 2006.

[16] L. B. Kish and C. G. Granqvist, "On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator," *Quantum Inf. Process.*, vol. 13, no. 10, pp. 2213–2219, 2014.

[17] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[18] Times Microwave. *LMR-600 Datasheet*. [Online]. Available: http://www.timesmicrowave.com/documents/resources/LMR-600.pdf, accessed May 10, 2015.

[19] R. Mingesz, Z. Gingl, and L. B. Kish, "Johnson(-like)-noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line," *Phys. Lett. A*, vol. 372, no. 7, pp. 978–984, 2008.

[20] H.-P. Chen, L. B. Kish, C. G. Granqvist, and G. Schmera, "On the 'cracking' scheme in the paper 'a directional coupler attack against the Kish key distribution system' by Gunn, Allison and Abbott," *Metrol. Meas. Syst.*, vol. 21, no. 3, pp. 389–400, 2014.

[21] L. B. Kish, Z. Gingl, R. Mingesz, G. Vadai, J. Smulko, and C.-G. Granqvist, "Analysis of an attenuator artifact in an experimental attack by Gunn–Allison–Abbott against the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system," *Fluctuation Noise Lett.*, vol. 14, no. 1, 2015, Art. ID 1550011.

[22] L. B. Kish, "Enhanced secure key exchange systems based on the Johnson-noise scheme," *Metrol. Meas. Syst.*, vol. 20, no. 2, pp. 191–204, 2013.

LACHLAN J. GUNN (S'08) received the B.Eng. (Hons.) and B.Math. & Comp.Sc. (Pure) degrees from The University of Adelaide, Australia, in 2012. He is currently pursuing the Ph.D. degree under D. Abbott and A. Allison. He received the J. Mazumdar Prize in Engineering and Mathematic in 2012, four DSTO Scholarships in Radar Technology from 2009 to 2012, and the Australian Post-Graduate Award in 2013. In 2014, he also received an Endeavour Research Fellowship by the Australian Government in order to undertake research into stochastic phenomena at the University of Angers.

His research interests include information-theoretic security and the use of stochastic signal processing for characterization of nonlinear systems.

ANDREW ALLISON received the B.Sc. degree in mathematical sciences and the B.Eng. (Hons.) degree in computer systems engineering from The University of Adelaide, in 1978 and 1995, respectively, and the Ph.D. degree in electrical and electronic engineering from The University of Adelaide, in 2009, under D. Abbott and C. E. M. Pearce.

He was with Barrett Brothers, Adelaide, as a Laboratory Technician, performing chemical assays, from 1976 to 1977. From 1980 to 1981, he was with the Commonwealth Scientific and Industrial Organization, Urrbrae, Australia, where he was involved in the area of high-pressure liquid chromatography, analysis of infrared spectroscopy data, and analysis of radioactive assays of DNA recombination. From 1981 to 1995, he held various positions, mainly in the area of local area networks with Telstra Corporation, Australia. Since 1995, he has been with the School of Electrical and Electronic Engineering, University of Adelaide, as a Lecturer.

Dr. Allison's research interests include probability, statistics and estimation, control theory, communication theory, and diffusion processes.

DEREK ABBOTT (M'85–SM'99–F'05) was born in London, U.K., in 1960. He received the B.Sc. (Hons.) degree in physics from Loughborough University, U.K., in 1982, and the Ph.D. degree in electrical and electronic engineering from The University of Adelaide, Adelaide, Australia, in 1995, under K. Eshraghian and B. R. Davis. From 1978 to 1986, he was a Research Engineer with the GEC Hirst Research Centre, London. From 1986 to 1987, he was a VLSI Design Engineer with Austek Microsystems, Australia. Since 1987, he has been with The University of Adelaide, where he is currently a Full Professor with the School of Electrical and Electronic Engineering. He holds over 800 publications/patents and has been an invited speaker at over 100 institutions. He has co-edited the book entitled *Quantum Aspects of Life* (Imperial College Press) and co-authored the books entitled *Stochastic Resonance* (Cambridge University Press) and *Terahertz Imaging for Biomedical Applications* (Springer-Verlag). He is a fellow of the Institute of Physics (IOP). He has received a number of awards, including the South Australian Tall Poppy Award for Science (2004), the Premier's SA Great Award in Science and Technology for outstanding contributions to South Australia (2004), and the Australian Research Council Future Fellowship (2012). He has served as an Editor and/or a Guest Editor of a number of journals, including the JOURNAL OF SOLID-STATE CIRCUITS, the *Journal of Optics B* (IOP), the *Microelectronics Journal* (Elsevier), the PROCEEDINGS OF THE IEEE, the IEEE PHOTONICS JOURNAL, and *PLOSONE*. He is on the Editorial Boards of *Scientific Reports* (Nature), *Royal Society Open Science*, and IEEE ACCESS.

Prof. Abbott's interest is in the area of multidisciplinary physics and electronic engineering applied to complex systems. His research programs span a number of areas of stochastics, game theory, photonics, biomedical engineering, and computational neuroscience.