Kish's key exchange scheme is insecure

F. Hao

Abstract: Kish proposed a scheme to exchange keys between two parties under the concealment of thermal noise. We show that the theoretical model in the scheme implicitly assumes thermal equilibrium throughout the communication channel. This assumption, however, is invalid in real communication systems. A slight temperature difference in the channel, as demonstrated in the paper, will lead to security failure.

1 Kish's system

Kish proposed a classic communication system, using only resistors, wires and Johnson noise, to replace quantum communication [1] (also featured in [2]). Fig. 1 shows the system design, in which there are two resistors R_1 and R_2 at each end, with $R_1 \ll R_2$. E_{s1}, E_{s2}, E_{r1} and E_{r2} are the resistors' Johnson-noise RMS (root mean square) voltages, due to the thermal agitation of electrons [3].

The two communicating parties, Alice and Bob, randomly select one resistor during each synchronised clock cycle. If they choose different resistances, an eavesdropper could not tell which side has the smaller resistance, giving Alice and Bob a 1-bit shared secret [1].

Let us first consider the case that Alice chooses R_1 and Bob R_2. We have the noise sources: $E_{s1} = \sqrt{4kT_s\Delta f_s R_1}$ and $E_{r2} = \sqrt{4kT_r\Delta f_r R_2}$ (see [3]), where k is Boltzmann's constant, T_s and T_r are the absolute temperatures at the sending and the receiving ends, respectively, and Δf_s and Δf_r are the corresponding noise bandwidths at two ends. Let E_t be the RMS voltage measured by an eavesdropper (see Fig. 1). Using superposition [3], we obtain:

$$E_t = \sqrt{\left(E_{s1}\frac{R_2}{R_1+R_2}\right)^2 + \left(E_{r2}\frac{R_1}{R_1+R_2}\right)^2} = \frac{\sqrt{4kR_1R_2(T_s\Delta f_s R_2 + T_r\Delta f_r R_1)}}{R_1+R_2} \qquad (1)$$

On the other hand, if Alice chooses R_2 and Bob R_1, we obtain the voltage expression E_t' by simply exchanging R_1 and R_2 in (1).

In [1], Kish simplifies the above calculations by assuming 'thermal equilibrium' in the circuit with equal temperature and noise bandwidth. Essentially, he assumes $T_s = T_r = T$, $\Delta f_s = \Delta f_r = \Delta f$, and obtains $E_t = E_t' = \sqrt{4kT\Delta f R_1R_2/(R_1+R_2)}$. Thus, Kish claims that an eavesdropper cannot tell whether Alice chose a bigger resistance or a smaller one, and that the system is 'totally secure'.

2 Design flaw

Scheuer and Yariv proposed two passive attacks against Kish's scheme [4]. In their threat model, an eavesdropper has access to two distant points on the transmission line, say one near Alice and the other near Bob. The first attack exploits the finite propagation time of signal waves. When a resistor is switched on at one end, the abrupt change of voltage generates voltage (and current) waves, propagating toward the other end. An eavesdropper could uncover the secret bits by measuring the time delay of the waves travelling between the two points on the line. The second attack exploits the finite resistance of the transmission line. This is done by comparing the voltages measured at the two distant points. More details are found in [4].

Our work shows that the problem with Kish's scheme is more fundamental. The theoretical model, which underpins the proposed system, is based on 'thermal equilibrium' [1]. However, absolute thermal equilibrium could never be achieved in real communication systems, which have to span a distance and endure different conditions. Any power flow from high temperature to low in the channel will leak the secret bits, as we demonstrate below.

First, we consider the impact due to the temperature difference at two ends (i.e. $T_s \neq T_r$), while still treating $\Delta f_s = \Delta f_r = \Delta f$ as in [1]. As an example, we use $R_1 = 1\ \Omega$, $R_2 = 100\ \Omega$. Let $\beta = \sqrt{4kT_s\Delta f}$ be a reference value. Figure 2 shows the voltages (RMS) measured on the wire (e.g. by an eavesdropper).

In Fig. 2, the two curves are indistinguishable only when the two endpoint temperatures are exactly the same. However, a slight temperature difference would tip the balance, rendering the communication vulnerable to eavesdropping.

Worse, an eavesdropper does not even have to know which side's temperature is higher. In Fig. 2, the voltage at the intersection point is $\sqrt{R_1R_2/(R_1+R_2)} = 0.995\,\beta$ [see (1)]. By examining the relative voltage difference to that intersection point, an eavesdropper could easily distinguish the two curves, hence uncover the secret bits. A similar attack is possible if $\Delta f_s \neq \Delta f_r$.

As a countermeasure, Alice and Bob might be able to adjust the difference in temperature (and noise bandwidth) at two ends to be as small as possible. However, this gives no security guarantee; an eavesdropper could still discern the difference merely by obtaining a voltage meter that is more accurate than the equipments used by Alice and Bob.

IEE Proceedings online no. 20060068
doi:10.1049/ip-ifs:20060068
Paper first received 11 April and in final revised form 12th September 2006

The author is with the Computer Laboratory, University of Cambridge, UK
E-mail: Feng.Hao@cl.cam.ac.uk

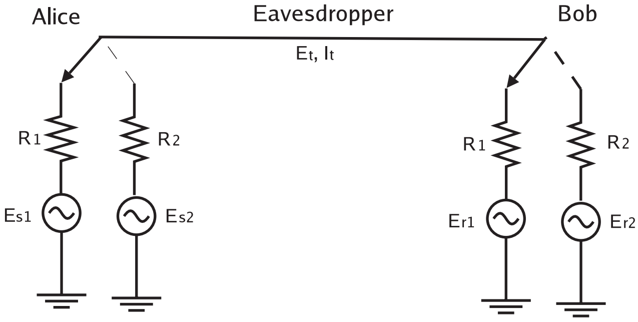

Fig. 1 *The proposed communication system*

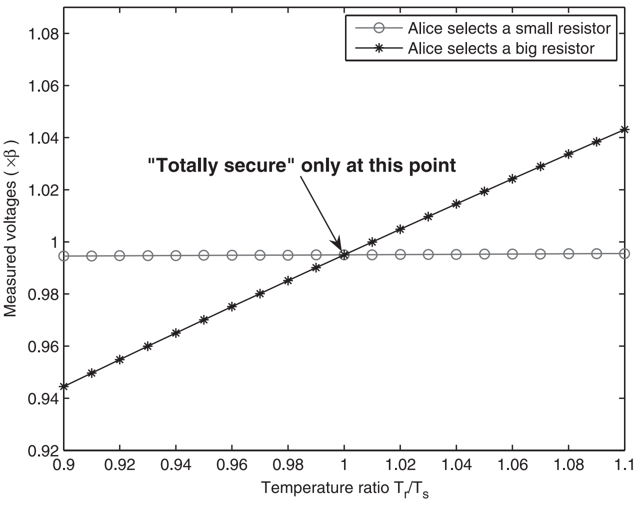

Fig. 2 *Voltages measured on the wire*

In addition, the transmission line must maintain the same temperature and noise bandwidth as the two ends to ensure 'thermal equilibrium', which is clearly impossible. Kish avoids this problem by assuming zero resistance in the transmission line [1].

3 Conclusion

In circuit analysis, it is common practice to make assumptions in order to simplify the calculation; the resultant discrepancy is usually well within the tolerable range. However, the design of a secure communication is very different, as a tiny discrepancy could severely compromise the system security. Basing security upon invalid assumptions is a fundamental flaw in the design of Kish's scheme.

4 Acknowledgment

We would like to thank the anonymous reviewers for their helpful comments.

5 References

1 Kish, L.B.: 'Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law'. *Physics Letters*, 2006, **352**, pp. 178–182. Available at http://www.arxiv.org/physics/0509136

2 Cho, A.: 'Simple noise may stymie spies without quantum weirdness'. *Science*, 2005, **309**, pp. 2148

3 Motchenbacher, C.D., and Connelly, J.A.: 'Low-noise electronic system design', John Wiley & Sons, 1993

4 Scheuer, J., and Yariv, A.: 'A classical key-distribution system based on Johnson (-like) noise – how secure?'. Available at http://www.arxiv.org/abs/physics/0601022