Channel Independent Cryptographic Key Distribution

Benjamin. T. H. Varcoe

Abstract—This paper presents a method of cryptographic key distribution using an ‘artificially’ noisy channel. This is an important development because, while it is known that a noisy channel can be used to generate unconditional secrecy, there are many circumstances in which it is not possible to have a noisy information exchange, such as in error corrected communication stacks. It is shown that two legitimate parties can simulate a noisy channel by adding local noise onto the communication and that the simulated channel has a secrecy capacity even if the underlying channel does not. A derivation of the secrecy conditions is presented along with numerical simulations of the channel function to show that key exchange is feasible.

Index Terms—Cryptography, secret key agreement, public discussion protocols, secrecy capacity, wire-tap channel, privacy amplification

I. INTRODUCTION

A fundamental aspect of cryptography is the ability to exchange information in perfect secrecy. However, almost all current forms of encryption rely on computational rather than information theoretic security. Computationally secure coding uses encryption techniques for which the known hacking algorithms require lengthy calculations and they therefore assume that the eavesdropper has a limited computational capability. Information theoretic security, on the other hand, makes no assumptions about an eavesdroppers capability. This is an important distinction because the computational difficulty can change with advances in algorithms and increased speed of calculation, leading to significant cryptographic breaks.

One solution to producing a perfectly encrypted message is the One Time Pad where the cryptographer has an infinite supply of symmetric key that is consumed as a resource in encrypting information. However, this creates the obvious problem of creating and securely distributing large amounts of symmetric key material. To address this problem several methods have been proposed for creating and agreeing on a perfectly secure key of arbitrary length under information theoretic security [1]–[8].

In particular, it has been shown [3], [4], [7], [9] that channel noise can be exploited to create and distribute symmetric key material in near perfect secrecy. The essential element is the use of feedback [5], [7]–[11], which exploits uncertainties in Eve’s (the eavesdropper’s) information, via a specially prepared sequence of messages, to generate random bit sequences known to the communicating pair, Alice and Bob, and unknown to Eve. Hence, the secrecy of the channel is given by the combination of information transmitted over both the noisy and noise-free channels.

The noisy channel model has been studied for several decades now (see for example [3], [4], [6]–[8], [10]) and it has been well established that when the mutual information between two distributions A and B exceeds the mutual information between A and E (that is $I(A; B) > I(A; E)$) it is possible to build a secret key from distributions A and B excluding E. Maurer [7] recognized that this condition was too strong and there are circumstances when $I(A; B) < I(A; E)$ and/or $I(A; B) < I(B; E)$ but secret key generation is still possible. In particular, feedback between Alice and Bob permits the generation of a sequence of messages $\hat{M}^t = [\hat{M}_1, \hat{M}_2, \ldots, \hat{M}_t]$ which can be used to generate $A = M^t A, \hat{B} = M^t \hat{B}$ and $\hat{E} = M^t E$ such that

$I(\hat{A}; \hat{B}) > I(\hat{A}; \hat{E})$.

The scenario works as follows, Alice and Bob first exchange symbols over the noisy channel. They then use feedback signals exchanged over an error-corrected channel to arrive at a secret key. Information Alice, Bob and Eve obtain about the secret key therefore comes from correlations in the signals and the joint information gained from the subsequent feedback messages.

The conditions of feedback are therefore an important aspect of distilling the secret key. The feedback must be constructed to allow Alice and Bob to use correlations in their data to exclude Eve. One way for them to do this is for Alice and Bob to reduce the errors in a subsequent communication channel. There are several codings that could be used for this purpose [12]. As Eve has errors in her knowledge of both Alice’s and Bob’s bit sequences, the coding only gives her partial information and she therefore receives the signals with errors cascaded over either Alice’s or Bob’s channel (depending on the nature of the reconciliation). It has been shown [7], [8], [12] that this gives Alice and Bob an advantage over Eve. This procedure can be cascaded to align their information while maintaining a well defined upper limit on Eve’s information. Moreover, knowing the upper limit on Eve’s information, Alice and Bob can subsequently use privacy amplification [5], [10] to reduce Eve’s information to an arbitrarily small level.

The essential element of secret key generation is that the noise channel is capable of generating a sufficient and predictable level of uncertainty in the information received by Eve. Quantum key distribution [1], [2] is one way of ensuring a guaranteed minimum level of channel noise and it comes with the added benefit that the security is protected by the physical limitations of quantum mechanical measurement.
However, as noted above, any noisy communications channel where Alice, Bob and Eve receive noisy copies of a signal, is also theoretically secure when it is assumed that each party receives uncorrelated noise.

Hence, an implementation of any cryptographic scheme will be strongly dependent on the specific properties of the channel and all of the apparatus surrounding it, because changes to the detectors, source or even medium (e.g. free space or waveguide) can change the noise and hence the secrecy conditions. Secrecy can even be removed entirely if the noise falls below a given threshold. Continuous variable quantum communication, for example, typically includes essential device calibration [13]. For this reason it is interesting to consider a method that would generate unconditional channel noise and therefore secrecy in key generation.

The current paper presents a method of applying unconditional noise to generate secrecy in a channel with no a priori secrecy capacity. Specifically it is found that if the signal is degraded locally (independent of transmission or detection noise) and by both Alice and Bob independently, the channel gains the ability to create a secret symmetric key even if it otherwise has no prior secrecy capacity.

II. SECRET KEYS FROM CHANNEL NOISE

It has been established that a noisy channel where, in particular, Eve and Bob both have reception errors is capable of secret communication while a perfect, noise-free communications channel has zero secrecy capacity [3], [4], [6]–[8], [10], [14]. However there are many channels in which noisy communication is not possible, or where an unconditionally noisy channel is not guaranteed. In such channels we propose that Alice and Bob use a local noise source to create an artificially noisy channel, simply by adding local noise after the transmission (Fig.1). Although Eve can receive a noiseless copy of the original data, it will now be shown that by altering their channel Alice and Bob have effectively simulated a noisy channel and can distill a correlated data set unknown to Eve. Alice and Bob have effectively generated a non-zero secrecy capacity at the expense of reducing the overall channel capacity.

In the arguments that follow it is assumed that Eve can detect all transmissions from Alice (and Bob) with no error and that she receives a signal that is identical to the receiver at all times. This represents the best possible case for Eve.

In this model (without loss of generality) Alice transmits a random number $R$ to Bob over an otherwise noiseless channel. Alice, Bob and Eve then use a local true random number generator to generate the random number sets $N_A$, $N_B$ and $N_E$ respectively, such that Eve cannot independently deduce the values $N_A$ or $N_B$ from her knowledge of $N_E$ and $R$. Alice and Bob and Eve use these to generate the variables

$$X_i = R_i \oplus N_i^A,$$ (1)

$$Y_i = R_i \oplus N_i^B$$ (2)

and

$$Z_i = R_i \oplus N_i^E$$ (3)

respectively. $N_i^A$, $N_i^B$ and $N_i^E$ are random biased bits with probabilities $P(N_i^A = 0) = 1 - \alpha$, $P(N_i^A = 1) = \alpha$, $P(N_i^B = 0) = 1 - \beta$, $P(N_i^B = 1) = \beta$ (where $0 < \alpha, \beta < 1$), $P(N_i^E = 0) = 1 - \gamma$ and $P(N_i^E = 1) = \gamma$ (where $0 \leq \gamma \leq 1$). The range of $\gamma$ expresses the fact that the value $N_i^E$ could contain any level of noise ranging from complete uncertainty to being an error free reception of $R_i$.

This effectively creates new binary symmetric channels between Alice and Bob and Alice and Eve shown in Fig.2. Where the bit flip probabilities $\alpha$, $\beta$ and $\gamma$ are related to the binary symmetric error rates $\epsilon$ and $\delta$ via $\epsilon = \alpha + \beta - 2\alpha\beta$ and $\delta = \alpha + \gamma - 2\alpha\gamma$. Importantly both $\delta > 0$ and $\epsilon > 0$ even if $\gamma = 0$ as long as both $\alpha > 0$ and $\beta > 0$.

It is worth noting that Eve might tamper with the initial transmission of $R$, which effectively amounts to creating a new variable $T_i$, where $P(T_i = 0) = 1 - \tau$, $P(T_i = 1) = \tau$. This would lead to Bob receiving a new variable $Y'_i = Y_i \oplus T_i$. This has the same effect as transmission noise and may make key agreement between Alice and Bob more difficult, but it is not impossible as long as $I(Y;Y') \neq 0 \neq I(X;Y')$ [7]. Tampering is considered in more detail below.

$$X = R \oplus N_A$$
$$Y = R \oplus N_B$$
$$Z = R \oplus N_E$$

It is therefore proposed that for $\alpha > 0$, $\beta > 0$ and $\gamma \geq 0$ a channel has been created with a capacity for secrecy, irrespective of the properties of the underlying channel. This is a new condition introduced in this paper that does not match the conditions established previously [7]–[9]. It is therefore...
are left with, of 1s and 0s (that is, Eve has a 50% transmission error), we sequence and the sequence decoded by Eve has equal numbers and

Bob calculates the sequence \( C \) using the sequence \( Y \) via

\[ X_i \oplus C \oplus Y_i, X_{i+1} \oplus C \oplus Y_{i+1}, \ldots, X_{i+N-1} \oplus C \oplus Y_{i+N-1} \]

and accepts the value of \( C' \) only when he has obtained the vectors \([0, 0, \ldots, 0]\) or \([1, 1, \ldots, 1]\). This encoding therefore creates a new binary symmetric channel between Alice and Bob with error probability, \( \epsilon_N \), given by

\[ \epsilon_N = \frac{P_{\text{Error}}}{P_{\text{Correct}} + P_{\text{Error}}} = \frac{\epsilon^N}{1 - \epsilon^N} \]  

(4)

where \( P_{\text{Error}} \) is the bit calculated by Bob that is not equal to the bit encoded by Alice and \( P_{\text{Correct}} \) is the probability that the two are equal. Eve can also calculate ‘\( C' \)’ using her variables \([Z_i, Z_{i+1}, \ldots, Z_{i+N-1}]\), however, it is assumed that Eve takes a more sophisticated approach than Bob and calculates the value of ‘\( C' \)’ based on the most likely value. Errors in Eve’s calculation are therefore determined by the number of sequences with \( N/2 \) errors or more, given that the sequence has been accepted by Bob. Eve’s error in the \( N \)-fold virtual channel is \( \delta_N \), assuming Eve adds no noise (i.e. \( \gamma = 0 \)). Hence, the best match that Eve can achieve to Bob’s data is given by the binomial probability \([7], [8]\).

\[ \delta_N = \frac{1}{P_{\text{Total}}} \sum_{w=N/2}^{N} \binom{N}{w} (1 - \epsilon)^{N-w} \epsilon^w \]  

(5)

where, \( P_{\text{Total}} \) is the total number of states accepted by Bob, \( p_{\text{hit}} \) is the probability that when the result of Alice’s calculation \((R + \text{Noise}) = 0\), Bob’s result is \( n \) and Eve’s result is \( m \). In this specific case their values are given by,

\[ P_{\text{Total}} = P_{\text{Correct}} + P_{\text{Error}} = (1 - \epsilon)^N + \epsilon^N \]

\[ p_{00} = (1 - \alpha)^2, \]

\[ p_{01} = \alpha^2, \]

and

\[ p_{10} = p_{11} = \alpha(1 - \alpha). \]

Considering only the special case that Bob has accepted a sequence and the sequence decoded by Eve has equal numbers of 1s and 0s (that is, Eve has a 50% transmission error), we are left with,

\[ \delta_N > \frac{1}{P_{\text{Total}}} \binom{N}{N/2} (2(\alpha - \alpha^2)^N). \]

At this point a choice of coding is made, deciding on the specific value of \( N = 2 \). Under these conditions the errors in Eve’s calculation are given by

\[ \delta_{N=2} > \frac{4(\alpha - \alpha^2)^2}{P_{\text{Total}}}. \]

However, \( \epsilon_{N=2} \) shows that when \( N = 2 \) and \( \alpha = \beta \), Bob’s error is also given by

\[ \epsilon_{N=2} = \frac{\epsilon^2}{P_{\text{Total}}} = \frac{(2\alpha - 2\alpha^2)^2}{P_{\text{Total}}}. \]  

(6)

Hence, \( \delta_{N=2} \) is always strictly greater than \( \epsilon_{N=2} \). It follows that \( I(X;Y) > I(Y;\hat{Z}) \) and therefore \( S(X;Y||\hat{Z}) > 0 \) \([8]\). This is sufficient even if it is only true for the special case of \( N = 2 \).

This proposition is useful because it also provides a protocol with which a secret key can be established. Alice can repeat the exchange with same transmission steps (and different random variables \( C \)), knowing that Eve’s ability to calculate the value will be worse than Bob’s because Eve started with an imperfect code \( \hat{Z} \). This can be repeated until Alice and Bob have \( n \)-bit sets \( S_n \) and \( S'_n \), where \( \text{Prob}(S \neq S'_n) < \kappa \). Likewise Eve will have \( S''_n \) for which \( \text{Prob}(S = S''_n) < \lambda \), for some choice of \( \kappa \) and \( \lambda \).

For sufficiently small \( \kappa \) we have

\[ I(S_n; S'_n) - I(S_n; S''_n) \approx 1 - I(S_n; S''_n) \leq k, \]

indicating that Eve’s knowledge of \( S_n \) is upper bounded by \( k \). Therefore, privacy amplification \([11]\) can be used then be used to further reduce Eve’s information using a hash function \( F_{n,k} \) which performs a mapping from Alice and Bob’s \( n \) bit sequence to a sequence of length \( n(1-k) \) bits. This creates new \( n(1-k) \) length sets \( F_{n,k}(S''_n) \) and \( F_{n,k}(S') = F_{n,k}(S) \) such that \( I(F_{n,k}(S''_n); F_{n,k}(S)) \approx 0 \). If the hash function \( F_{n,k} \) is decided after the protocol has been completed, Eve cannot influence the exchanges in advance in order to create a favorable situation.

Figure 3 presents the results of a simulation of random data exchanged between Alice and Bob, followed by adding local noise (the first two steps in the protocol). The simulation modeled a real exchange, where bit strings and added noise were generated using a random number generator and the signal was sent virtually between analysis programs. In this case the random number generator fails a universal statistical test \([15]\) so this particular exchange has limited capacity for generating actual secrecy, however, it does allow us to investigate the statistical effects of added noise. The solid line is an evaluation of equations \([3] \text{ and } [5] \) and the open and closed circles are the results of the simulation for Bob and Eve respectively. This simulation shows that for all values of noise \( \alpha > 0 \) to \( \alpha < 1/2 \) (with \( \alpha = \beta \)) the noise in Eve’s channel exceeds the noise in Bob’s channel following the first exchange.

### III. EAVESDROPPING

It is also worth considering the type of eavesdropping attacks that might be expected and how they are thwarted. For this purpose, the system can be broken down into two
elements; the private channel in which the key material is exchanged and the public channel in which the two way communication used to distill the secret key takes place.

The private channel is always used for the exchange of random variables which will be unknown to Bob in advance of the exchange. Hence it is possible that Eve could tamper or otherwise interfere with these transmissions by removing, altering or inserting symbols without Bob knowing.

It is also assumed that Eve is only able to read but not modify messages in the authenticated public channel. Authentication in this case meaning that Alice and Bob are authenticated users rather than referring to the security of the connection itself.

Eve has two possible attacks. Firstly she can look for correlations in the data exchanged and try to use this to gain insight into the final key (more than the insight she gains by simply following Alice and Bob’s protocol). Secondly, she can manipulate the symbols exchanged; for example, by performing selected bit flips in some of the data exchanged.

The first attack carries no additional information because the key is not sourced from the initial data but rather from the elements $C$ used in subsequent exchanges. Moreover the noise, $N^A$ and $N^B$ and the virtual channel value $C$ are chosen such that $I(X : C) = I(Y : C) = I(Z : C) = 0$, hence no information about $C$ can be gained from observations of the initial code $R$.

The second attack is somewhat more important because it can go unnoticed especially as Bob is already expecting unknown random data. However, as the statistics cannot be altered from the original and the number of bits must still be the same, Bob can perform local checks to ensure that the data is still random. Therefore the attack may be quite subtle. For example, it could be assumed that Eve’s goal in manipulating the data is not to reveal the secret key itself but rather to reveal a few additional bits of each exchange that will be unaccounted for in the privacy amplification. Eve may use this to gain a cryptographic break over the final key (Eve may, for example, wish to reduce the search space in a brute force key guessing attack). She may even consider an attack where small amounts of information accumulated over a very long period of time eventually reveals significant amounts of information (precisely how this is achieved is not considered here). A low level tampering attack is therefore an important consideration.

As noted above, any tampering attack would take the form of introducing the tamper variable $T$, to the message text via $R'_i = R_i \oplus T_i$ before it is sent on to Bob. Bob’s local variable therefore becomes

$$Y'_i = Y_i \oplus T_i = R_i \oplus N^B_i \oplus T_i.$$  

Eve cannot know $N^B$ therefore it is necessarily the case that $I(N^B; T) = 0$. The act of tampering modifies the binary symmetric channel between Alice and Bob (figure 2) changing the error rate from $\epsilon$ to $\epsilon'$. 

$$\epsilon' = (\beta + \tau) + \alpha - 2(\beta + \tau)\alpha = \epsilon + \Delta \epsilon$$

where $\Delta \epsilon = \tau(1-2\alpha)$. The result is an increase in the channel noise between Alice and Bob without changing the channel noise between Eve and Alice, assuming that Eve does not incorporate the tamper variable in her own data (if she does, her error actually exceeds Bob’s and secrecy is maintained). Figure 4 shows the impact of tampering attacks on the value of $P_{Total}$ for attacks modifying $0-5\%$ of the data. Hence, this particular tampering attack is detectable by examining $P_{Total}$ which reduces as a function of $\tau$. Alice and Bob can monitor $P_{Total}$, with any significant drop indicating a tampering attack. A $2-5\%$ attack is clearly detectable and is outside a standard deviation of variation of the untampered value.

This leaves a potential vulnerability to tampering attacks that introduce less than $2\%$ errors. The full protocol of key agreement now becomes important. It has already been shown that small amounts of tampering reduce Bob’s mutual information with Alice and hence $P_{Total}$ in the first exchange, however...
it also, simultaneously, reduces Eve’s mutual information with Bob.

In their exchange, and in the presence of tampering, Alice and Bob will arrive at the key source $S_F$ and $S'_F$ respectively which will have been reduced in size by Eve’s tampering. However, as key agreement is driven by Bob and not Alice, the final value of $I(S_F; S'_F)$ must therefore also be reduced, precisely because Eve has distanced herself from Bob. It remains the case that Eve’s best attack is to do nothing.

Finally in completing the protocol, Alice and Bob, unaware of the tampering, can always use a Hash code derived without knowing the details of the attack and assuming a perfect Eve. Figure 5 shows the final key agreed by Alice and Bob when Eve has tampered with the data. The key rate stays broadly flat with $I(S_n; S'_n) \approx 0$. This is true for small levels of tampering and the situation changes if the error is substantially above $5\%$, hence continual monitoring of $P_{total}$ is essential. Alice should therefore also keep track of the information that Eve would have at each level of the protocol.

IV. CONCLUSION

This paper demonstrates the exchange of secret keys using an arbitrary communication channel with no a priori assumptions. This could therefore include channels such as the TCP/IP stack, or error corrected radio communication stacks. In this model Alice and Bob (the legitimate communicators) add noise to the data to simulate the action of a noisy channel. It has also been shown that a communication protocol exists that can be used to distill a secret key.

The nature of the noise is however key to the secrecy and therefore it must be unpredictable. Hence, the essential element is that the noise should be supplied by a truly random source. In practice this means that it should probably be sourced from quantum effects as these are both unpredictable and cannot, typically, be externally manipulated.

A feedback mechanism was also demonstrated where a new data set was constructed using a virtual error corrected channel exchanging data pairs. This was shown to be capable of enhancing the overlap between Alice and Bob while reducing the noise in Eve. A potential attack has been considered where Eve attempts to degrade her data. This attack has been shown to lead to increased secrecy.

The final step of extracting a key uses a two-way feedback protocol. Such a protocol has not been considered in any detail in the current paper, however there are many examples in the literature that can be followed (see for example [11], [12], [16]–[18]).

ACKNOWLEDGMENT

Thanks go to W. Munro, T. Spiller and M. Everett for useful feedback in assembling this paper.

REFERENCES

[1] F. Grosshans, G. Van Assche, J. Wenger, R. Brouil, N. J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states,” Nature, vol. 421, no. 6920, pp. 238–241, 2003.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, 2002.
[3] A. D. Wyner, “Wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.
[4] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. 24, no. 3, pp. 339–348, 1978.
[5] U. Maurer and S. Wolf, Privacy amplification secure against active adversaries in Cryptology CRYPTO ’87, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1997, vol. 1294, pp. 307–321.
[6] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175, 1984.
[7] U. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol. 39, no. 3, pp. 733–742, 1993.
[8] U. Maurer and S. Wolf, “Unconditionally secure key agreement and the intrinsic conditional information,” IEEE Trans. Inform. Theory, vol. 45, no. 2, pp. 499–514, 1999.
[9] R. Ahlswede and I. Csiszar, “Common randomness in information-theory and cryptography .1. secret sharing,” IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 1121–1132, 1993, mm075Times Cited:187Cited References Count:12.
[10] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” SIAM Journal on Computing, vol. 17, no. 2, pp. 210–229, 1988.
[11] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inform. Theory, vol. 41, no. 5, pp. 1915–1923, 1995.
[12] M. Van Dijk and H. Van Tilborg, “The art of distilling [secret key generation],” in Information Theory Workshop, 1998, pp. 158–159.
[13] S. Fossier, E. Diamanti, T. Debusschert, A. Villing, R. Tuaille-Brouil, and P. Grangier, “Field test of a continuous-variable quantum key distribution prototype,” New J. Phys., vol. 11, no. 4, p. 045023, 2009.
[14] U. Maurer, R. Renner, and S. Wolf, Unbreakable Keys from Random NoiseSecurity with Noisy Data. Springer London, 2007, pp. 21–44.
[15] U. Maurer, A Universal Statistical Test for Random Bit Generators, Advances in Cryptology-CRYPTO 90, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1991, vol. 537, pp. 409–420.
[16] C. Silberhorn, T. C. Ralph, N. Lekienhaus, and G. Leuchs, “Continuous variable quantum cryptography: Beating the 3db loss limit,” Phys. Rev. Lett., vol. 89, no. 16, p. 167901, 2002.
[17] G. Van Assche, J. Cardinal, and N. J. Cerf, “Reconciliation of a quantum-distributed gaussian key,” IEEE Trans. Inform. Theory, vol. 50, no. 2, pp. 394–400, 2004.
[18] G. Brassard and L. Salvail, Secret-Key Reconciliation by Public DiscussionAdvances in Cryptology EUROCRYPT 93, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1994, vol. 765, pp. 410–423.