

PREDICTION ACCURACY OF BAND-RESTRICTED RANDOM SIGNALS AND SECURITY RISK IN STATISTICAL KEY EXCHANGE

PAO-LO LIU

*Department of Electrical Engineering, University at Buffalo
The State University of New York
Amherst, NY 14260, USA*

Received 7 June 2010

Accepted 22 August 2010

Communicated by Mark Dykman

Statistical key exchange relies on signals with irreducible randomness to covertly transmit information. Because of causality, there may be disturbances during the transient turn-on, which can pose as a security risk. Linear prediction and the Gerchberg–Papoulis methods are used to analyze the risk quantitatively. With properly generated signals, the probability of leak during the transient turn-on is found to be comparable to that of the steady state. The transient signal does not pose as an additional security risk.

Keywords: Random noise; signal processing; prediction; information; security.

1. Introduction

Key exchange plays an important role in secure communications [1]. It enables legitimate users to share a common secret key for encryption and decryption. Once encrypted, the information is only legible to the legitimate user. If the key is only used once as in the one-time pad or Vernam cipher, the adversary cannot get any information [2]. Recently, a new key exchange method based on random signals was introduced [3]. It shares certain features with the Kirchhoff’s loop, Johnson-noise circuit cipher [4,5]. Like in quantum key distribution, the key is not generated unilaterally but jointly by two parties in two-way communications [6, 7]. Distillation ensures that the secret keys are identical. Privacy amplification denies the adversary any useful information [8, 9]. Signals involved are classical, random, band-restricted, and digitized. Such signals possess statistical fluctuations. The security is granted and guarded by the irreducible randomness intrinsic to such signals. Therefore, the method is identified as the statistical key exchange protocol. Statistically, even the adversary can obtain some information. However, legitimate users enjoy a much higher probability in getting the information. The difference in probabilities determines the information capacity [10]. The protocol is compatible with digital

communication systems. As long as a reliable digital link can operate, there is no additional distance limit imposed by the protocol. It may facilitate key exchange at a rate of Mbit/sec over a distance of thousands of kilometers in broadband optical communication systems.

To familiarize readers with the protocol, a brief introduction is provided. In the statistical key exchange, the operation and the security risk are governed by two signals propagating in the channel:

$$V_+(0, t) = V_1(t) + \alpha V_-(L, t - \tau), \quad (1)$$

$$V_-(L, t) = V_2(t) + \beta V_+(0, t - \tau). \quad (2)$$

$V_+(0, t)$ is the signal transmitted by Alice who is located at $x = 0$. Her information is encoded on the signal originated from Bob at an earlier time, $t - \tau$, and different location, $x = L$. τ is the signal transit time. A small reflection coefficient, α , positive for logic one and negative for logic zero, is used to encode her binary information. The encoded information is added to a locally generated random signal, $V_1(t)$. Once added, values of individual terms at any given moment cannot be separated [11, 12]. $V_1(t)$ is obtained by truncating a long span of band-limited Gaussian random signal to a short duration. The spectrum of the band-limited Gaussian random signal is square. There is no residual signal beyond the band limit, W . It is obtained by filtering a white noise with an ideal, non-causal low pass filter [13]. One cannot use a random signal with Lorentzian spectrum. The Lorentzian spectrum has a tail extending beyond the band limit, therefore, is subject to the inverse filter attack [14]. The inverse filter attack turns the random signal into a broadband white noise. With a broadband signal, there is no security [4]. After truncation, the duration of signal becomes finite. The spectrum of the truncated signal is given by the convolution of the truncating window function and the band-limited Gaussian random signal. After truncation, the signal is no longer strictly band-limited. There is a residual spectrum beyond the band limit. How much signal exists beyond the band limit depends on how abrupt the truncating window function is, i.e., how fast the signal is switched between off and on states. It must be carefully controlled. Therefore, the signal is labeled as band-restricted. Alice transmits the combined signal, $V_+(0, t)$. Bob performs similar operations. He generates a band-restricted random signal $V_2(t)$ and transmits $V_-(L, t)$. His binary information is encoded in β . They transmit signals and communicate with each other until the end of a symbol with duration T is reached. The binary information of legitimate users varies randomly between zero and one from symbol to symbol. It remains constant during each symbol.

The eavesdropper can listen to communications in the channel. She can process intercepted signals in an attempt to decipher the binary information. For example, she can perform delayed correlation between two counter-propagating signals. However, she cannot access either one of the two local random signals generated by legitimate users. When both legitimate users transmit the same binary information,

the adversary is fully aware of the information. However, when two legitimate users transmit binary conjugate information, the adversary becomes confused [4, 15]. She cannot accurately determine which side sends binary one and which side transmits binary zero. Armed with the locally generated random signal, legitimate users have a substantially higher probability in correctly identifying the binary information. Such an advantage has been established when correlations of steady-state signals are used to determine the information [3]. Legitimate users can correctly determine the information with a probability of 91.7%. For the adversary, it is only 57.3%. Therefore, legitimate users can selectively keep the binary conjugate information forming the preliminary key. Subsequently, privacy amplification enhances the margin and establishes the shared secret keys.

In addition to correlations, the adversary can also examine the following two signals in an attempt to determine the binary information sent by Alice:

$$V_1(t) = V_+(0, t) - \alpha V_-(L, t - \tau), \quad (3)$$

$$V'_1(t) = V_+(0, t) + \alpha V_-(L, t - \tau). \quad (4)$$

Both signals are calculated from signals in the channel. One corresponds to the true random signal generated by Alice. The other is the false signal derived from using the wrong sign in the feedback coefficient. Likewise, there exist another pair of signals, $V_2(t)$ and $V'_2(t)$ involving β . Eve needs to identify which one is likely the true signal. If her probability of success is high, there is a leak. It turns out that these two signals are completely indistinguishable in the steady state. There are no differentiable features in spectra, mean-square fluctuations, or statistical distributions. If there is any differentiable feature, it only exists during the initial transient turn-on. The security risk during the transient stage was recognized in a prior publication [16]. However, the discussion was qualitative. There was no quantitative measure, such as the probability of leak. In this paper, signal processing techniques are used to analyze the probability of transient leak. How accurately band-restricted random signals can be predicted is evaluated. How prediction methods can be applied to reveal the transient disturbances is discussed. The probability of transient leak is determined quantitatively.

2. Transient Signals and Linear Prediction

At $t = 0$, Alice has no information about what Bob is doing because of causality. Signal transmitted by Bob takes time τ to reach Alice. Not only is τ the signal transit time, it is also the sampling time. Legitimate users digitize and transmit signals with interval τ . At $t = 0$, Alice sends the first value of her random signal alone. At the next moment in time, $t = \tau$, $V_-(L, 0)$ arrives. Alice starts encoding her binary information. There may exist discontinuities in $V_+(0, \tau)$ and its time derivatives contributed by the sudden turn-on of $\alpha V_-(L, 0)$ [16]. Such disturbances appear only in the false signal. They do not exist in naturally generated, band-restricted random signals. The true signal has only one discontinuity, namely, the

transition from $t < 0$ to $t = 0$. Any difference between the true and false signals is a security risk. If Eve can identify which is the true signal, she can get the binary information. The potential leak due to causality only appears during the turn-on. Even though there is also a turn-off transition at the end of a symbol, just like in the steady state, causality does not pose as a security risk as long as the product, τW , is small. Legitimate users can simply terminate the transmission of signals simultaneously.

To detect whether there is any disturbance at the beginning of a waveform, one can extrapolate the steady-state data towards $t = 0$. The well known backward linear prediction algorithm is given by [14, 17, 18]:

$$S(t) = \sum_{n=1}^{N/m} a_n \cdot S(t + n \cdot m\tau). \quad (5)$$

m indicates how far backward in time unit of τ to predict. For clarity, $m = 1$ is called 1τ prediction; $m = 2, 2\tau$ prediction, etc. The summation ends with $n = N/m$. In other words, the last data point employed in prediction is $N\tau$ away in time. $S(t)$ can be $V_1(t)$, $V'_1(t)$, or their time derivatives. The weighing coefficients are determined by minimizing the square deviations between the actual and predicted waveforms.

Before applying the linear prediction method to detect disturbances in the waveform, one needs to quantify the prediction accuracy. The linear prediction method is applied to analyze band-restricted random signals with an average value of zero and a mean-square fluctuation of unity. Values of parameters used include: $\tau = 4 \mu\text{sec}$, $W = 5 \text{ kHz}$, $T = 5 \text{ msec}$, and the quantization step is $1/512$. τ is the transit delay as well as the sampling time. W is the bandwidth. T is the duration of symbols. During each symbol, one bit of secret key is exchanged. Appropriate values of these parameters are found in an earlier study analyzing the performance of the protocol using steady-state signals [3]. As shown in the earlier study, the product, τW , determines the leak, i.e., how much information the adversary can obtain. WT determines the amount of fluctuations. In statistical key exchange, the information is masked by fluctuations. Therefore, τ , W , and T are critical parameters. The sampling rate is well above the Nyquist rate. This is needed to avoid information leak due to causality in the steady state. Shown in Fig. 1 is the mean-square deviation, which reflects the prediction accuracy, as a function of N for 1τ and 2τ predictions. As expected, the accuracy of linear prediction improves rapidly as N is increased from unity. When $N \geq 90$, the mean-square deviations between the original waveform and prediction are 2.45×10^{-6} for 1τ prediction and 1.35×10^{-5} for 2τ prediction, respectively. The accuracy deteriorates rapidly when the number of steps involved in prediction increases. Only the one and two-step predictions can be used in detecting discontinuities in false signals.

From $V_1(t)$, the linear prediction produces $W_1(t)$. From $V'_1(t)$, it generates $W'_1(t)$. Discontinuities can produce large errors in linear prediction. Because of feedback, any initial discontinuity can produce gradually diminishing discontinuities at subsequent time moments. The dominant discontinuities are located at $t = 0$ and τ .

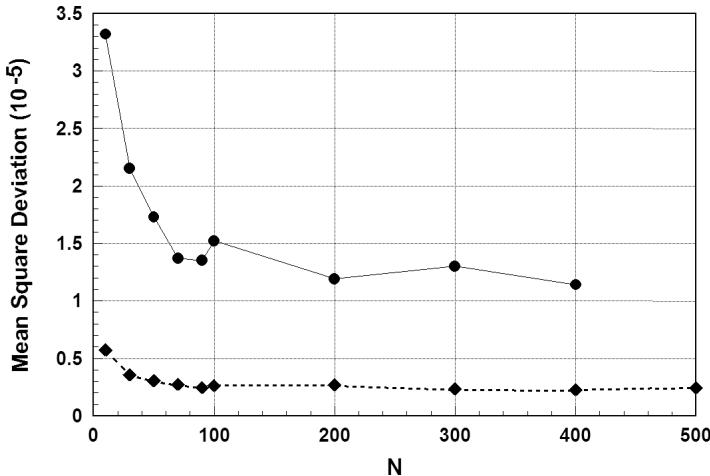


Fig. 1. The mean-square deviation as a function of the number of data points used in prediction. Circles are obtained from 2τ prediction. Diamonds are obtained from 1τ prediction. Data points are linked together by line segments shown as solid lines or dashed lines.

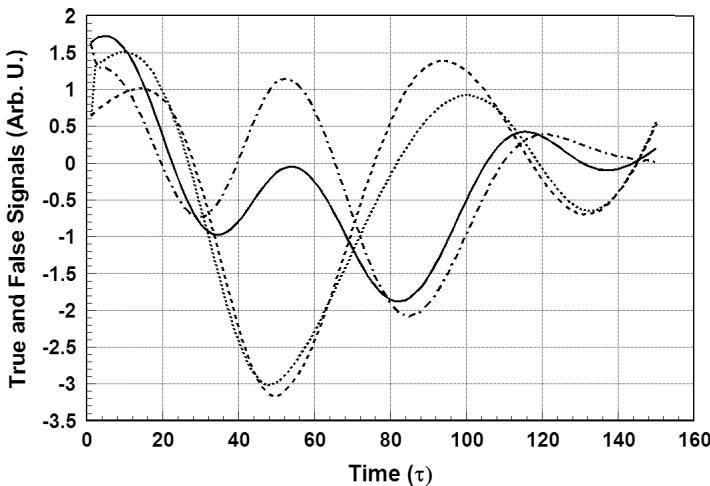


Fig. 2. Two sets of true and false signals corresponding to $V_1(t), V'_1(t)$ and $V_2(t), V'_2(t)$ in one symbol. They are shown as solid, chained, dashed, and dotted curves, respectively. False signals have discontinuities near $t = 0$. Linear predictions yield results in excellent match with waveforms except during the initial transient turn-on for false signals.

Beyond $t = 2\tau$, the discontinuity is minimal. To maximize the accuracy of prediction, 2τ prediction is used to predict $W_1(0)$. 1τ prediction is used to predict $W_1(\tau)$. Shown in Fig. 2 are the true and false waveforms. Results of linear prediction match extremely well with signals except for the false signal during the initial turn-on.

Since there are disturbances in the false signal initially, $|V'_1(t_0) - W'_1(t_0)| > |V_1(t_0) - W_1(t_0)|$. t_0 is either zero or τ . In other words, the false signal has a larger prediction error than the true signal. Using this initial prediction error as an indicator, the probability for the adversary to correctly decipher the information can be quantified by using the Monte Carlo method. With $|\alpha| = |\beta| = 0.2$, the probability of leak is 98% using the prediction error at $t_0 = 0$ or 95% using the prediction error at $t_0 = \tau$. The linear prediction algorithm can detect the initial disturbance and differentiate the true signal from the false signal. The adversary can identify the information with almost full certainty. To avoid detection, legitimate users must eliminate transient disturbances and reduce the correlation between the transient and steady-state signals to render prediction ineffective.

3. Ramping of Signals

One method to prevent the waveform discontinuity is to ramp up the reflection coefficient [16]. The reflection coefficient increases from zero to full value according to the ramp-up function:

$$R(t) = [1 + \sin(t - T_R/2) \cdot \pi/T_R]/2, \quad 0 \leq t < T_R \\ 1. \quad T_R < t \quad (6)$$

T_R is the period during which the ramp-up takes place. Since the reflection coefficient starts from zero, $V'_1(0) = V_1(0)$. The true and false signals start with identical value. They gradually and smoothly become different. There is no abrupt discontinuity in the time-domain waveform. Since legitimate users depend only on steady-state signals for deciphering the information, they can intentionally reduce the correlation between the initial signal and the steady-state signal. The locally generated, band-restricted signal is given by:

$$V_1(t) = 0, \quad t < 0 \\ [1 - R(t)] \cdot U_1(t) + R(t) \cdot U_2(t), \quad 0 \leq t < T_R \\ U_2(t), \quad T_R \leq t < T \\ 0. \quad T \leq t \quad (7)$$

$R(t)$ is the same ramp-up function used in ramping up the reflection coefficient. $U_1(t)$ and $U_2(t)$ are uncorrelated, band-limited random signals. T is the full duration of a symbol. The inclusion of $U_1(t)$ is a new feature implemented in the statistical key exchange. With ramping using $T_R = 50\tau$, i.e., $200\mu\text{sec}$, the probability for the adversary to correctly decipher the information according to the initial prediction error is reduced to 52% at $t = 0$ or 51% at $t = \tau$. Essentially, the ability of the adversary is reduced to random guessing. The linear predication method cannot breach the security.

4. Distributed Prediction Error and the Gerchberg–Papoulis Method

In linear prediction, signals are considered to be band-limited. Linear prediction is performed using only the time-domain data. Information in the frequency domain is not taken into account explicitly. The Gerchberg–Papoulis method which was developed for super resolution, extrapolation, and spectral estimation, however, operates in both the time and frequency domains [19, 20]. In the last step of iterations, the spectrum beyond the band limit is reduced to zero. Then, the inverse Fourier transform is performed on the truncated spectrum to obtain the calculated time-domain waveform. The adversary can compare the calculated signal to the actual signal and use the distributed prediction error as a measure to differentiate the true and false signals. The distributed prediction error is defined as:

$$\Delta = \sum_{n=0}^M [V_1(n\tau) - W_1(n\tau)]^2, \quad (8)$$

where $M = T_R/\tau$, truncated to an integer. Just like in the linear prediction, the false signal is expected to have a larger distributed prediction error. It is well known that the Gerchberg–Papoulis method can be slow to converge [21]. In this application, however, a large number of iterations are not necessary. The adversary can simply perform a small number of iterations, e.g., 20, and then calculate distributed errors. Iterations extend the waveform beyond $t < 0$. Instead of extrapolation, the purpose is to minimize the out-of-band spectrum due to the abrupt turn-on at $t = 0$. The remaining difference between the signal and the calculate result is contributed mainly by causality. In this application, the Gerchberg–Papoulis method is adopted to exploit the spectral difference between true and false signals beyond the band limit. Shown in Fig. 3 are the true waveform and the result calculated by the Gerchberg–Papoulis method. The difference exists primarily during the initial ramping.

The adversary can attribute the waveform with less distributed error to the locally generated random signal. Based on this criterion, the probability of success for the adversary is obtained by using the Monte Carlo method. With ramping implemented, the probability of success for the adversary is only 57%. It is comparable to her success rate using steady-state signals. The transient signals do not pose as an additional security risk.

The statistical key exchange operates with random signals. Each bit is transmitted with a unique set of signals. The time-domain waveform and the frequency-domain spectrum fluctuate from symbol to symbol. Similar to the keyed communication in quantum noise, there also exists unpredictable randomness in truncated, band-restricted, and quantized classical signals [22]. Both the time-domain waveform and the frequency-domain spectrum contain unpredictable randomness that cannot be filtered out or eliminated. With properly generated random signals, the irreducible randomness can mask any minute difference, if there is any,

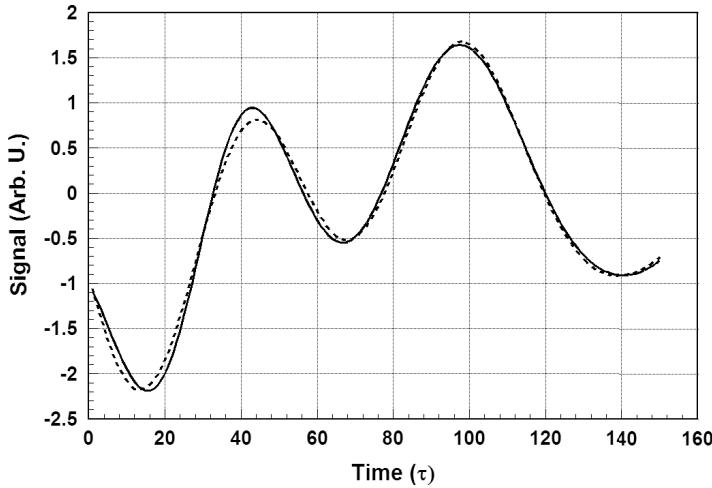


Fig. 3. The true signal shown as the solid curve and the calculated result of the Gerchberg–Papoulis method shown as the dashed curve. The horizontal axis is time in unit of τ , which is $4 \mu\text{sec}$. Ramping takes place during the initial 50τ .

between true and false signals. Signal processing techniques studied cannot reveal the identity of the true, locally generated, random signal. Therefore, the adversary cannot decipher the information.

5. Discussion

The risk of information leak during the transient turn-on has long been recognized. In the Kirchhoff's loop, Johnson-noise circuit cipher, the strength of random signals is ramped up from zero at the beginning of a symbol and ramped down at the end. Line filters are used at both ends to tightly control the bandwidth of analog signals propagating in the transmission line [4, 5]. In statistical key exchange, digital signals are used. Random signals operate at full strength during the symbol. Instead, the feedback coefficient is ramped up at the beginning of a symbol with no ramping down at the end [16]. One unique advantage of ramping the reflection coefficient is to prevent the adversary from performing reverse ramping. The adversary intercepts $V_+(t)$ and $V_-(t)$. However, $V_+(t)$ and $V_-(t)$ are composed of two terms, for example, $V_+(t) = V_1(t) + \alpha V_-(t - \tau)$. In the case of ramping the reflection coefficient, only α is multiplied by $R(t)$. The adversary cannot simply divide $V_+(t)$ or $V_-(t)$ by $R(t)$ to reverse the effect of ramping. In this paper, Eq. (7) involves ramping. However, it is completely different from ramping up $V_1(t)$. $V_1(t)$ operates with full strength from the beginning to the end of a symbol. In Eq. (7), two uncorrelated signals are added to form $V_1(t)$. $U_1(t)$ is at full strength at $t = 0$ while $U_2(t)$ is at full strength for $t > T_R$. The purpose is to destroy correlation between $V_1(0)$ and $V_1(t)$ in the steady state. Therefore, the adversary cannot use the steady-state signal to predict

the signal at $t = 0$. So far, the digital signal processing procedure corresponding to the analog line filter has not been implemented in the statistical key exchange protocol. It may be needed in the future to address information leak during the steady state.

6. Conclusion

In summary, the risk of transient leak in the statistical key exchange protocol is analyzed quantitatively by using signal processing techniques. The linear prediction method and the Gerchberg–Papoulis method are used to determine the probability for the adversary to gain access to the information. Without ramping, the linear prediction method can identify the initial disturbance in signals and breach the security. With ramping, the probability for the adversary to obtain the information from transient signals is reduced to become comparable to that of steady-state signals. Legitimate users continue to enjoy a substantial advantage over the adversary. If future attacks originated from information theory, signal processing, and, possibly, quantum computing, cannot breach the security, the statistical key exchange protocol may provide a common platform for secure communications in digital systems.

Acknowledgments

Author thanks Prof. Ge Wang and Mr. Yang Lu for their efforts in evaluating the discrete cosine transform for use in the statistical key exchange.

References

- [1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theor.* **22** (1976) 644–654.
- [2] C. E. Shannon, Communication theory of systems, *Bell System Technical J.* **28** (1949) 656–715.
- [3] P.-L. Liu, A key agreement protocol using band-limited random signals and feedback, *J. Lightwave Technol.* **27** (2009) 5230–5234.
- [4] L. B. Kish, Totally secure classical communication utilizing Johnson-like noise and Kirchhoff's law, *Phys. Lett. A* **352** (2006) 178–182.
- [5] R. Mingesz, Z. Gingl and L. B. Kish, Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator demonstrated for ranges of two kilometers to two thousand kilometers, *Phys. Lett. A* **372** (2008) 978–984.
- [6] S. Wiesner, Conjugate coding, *ACM SIGACT News* **18** (1986) 48–51.
- [7] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. IEEE Int. Conf. Computers Systems and Signal Processing*, Bangalore, India (1984), pp. 175–179, <http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf>.
- [8] G. Brassard and L. Salvail, Secret key reconciliation by public discussion, *Advances in Cryptology: Eurocrypt 93 Proc.* (1993), pp. 410–423.
- [9] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, Generalized privacy amplification, *IEEE Trans. Inform. Theor.* **41** (1995) 1915–1923.

- [10] A. A. Bruen and M. A. Forcinito, *Cryptography, Information Theory, and Error-Correction, A Handbook for the 21st Century* (Wiley Interscience, Hoboken, New Jersey, USA, 2005).
- [11] A. J. Viterbi, *CDMA Principles of Spread Spectrum Communication* (Addison-Wesley, Reading, MA, USA, 1995).
- [12] R. M. Narayanan, J. Chuang and K. M. Mohan, Propagation effects on noise-modulated randomly polarized ultrawideband communication system, *IETE Tech. Rev.* **26** (2009) 303–308, <http://tr.ietejournals.org/text.asp?2009/26/4/303/52999>.
- [13] P. Z. Peebles, Jr., *Probability, Random Variables, and Random Signal Principles*, 4th edn. (McGraw Hill, New York, NY, USA, 2001).
- [14] L. L. Kish, M. Zhang and L. B. Kish, Cracking the Liu key exchange protocol in its most secure state with Lorentzian spectra, *Fluctuation and Noise Letters* **9** (2010) 37–45.
- [15] J. Muramatsu, K. Yoshimura, K. Arai and P. Davis, Some results on secret key agreement using correlated sources, *NTT Tech. Rev.* **6** (2008), https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200802rp1.pdf&mode=show_pdf.
- [16] P.-L. Liu, Security risk during the transient in a key exchange protocol using random signals and feedback, *Phys. Lett. A* **373** (2009) 3207–3211.
- [17] J. Makhoul, Linear prediction: A tutorial review, *Proc. of IEEE* **63** (1975) 561–580.
- [18] P. P. Vaidyanathan, *The Theory of Linear Prediction* (Morgan and Claypool, 2008).
- [19] R. W. Gerchberg, Super-resolution through error energy reduction, *J. Modern Optics* **21** (1974) 709–720.
- [20] A. Papoulis, A new algorithm in spectral analysis and band-limited extrapolation, *IEEE Trans. Circuits Syst.* **CAS-22** (1975) 735–742.
- [21] J. A. Cadzow, An extrapolation procedure for band-limited signals, *IEEE Trans. Acoust. Speech Signal Process.* **ASSP-27** (1979) 4–12.
- [22] H. P. Yuen, KCQ: A new approach to quantum cryptography i. General principles and key generation (2004), <http://arxiv.org/abs/quant-ph/0311061v6>.

Copyright of Fluctuation & Noise Letters is the property of World Scientific Publishing Company and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.