Fluctuation and Noise Letters
Vol. 10, No. 3 (2011) 239–247

DOI: 10.1142/S0219477511000545

QUANTIZATION NOISE IN STATISTICAL KEY EXCHANGE

PAO-LO LIU and MADHUR S. JOSAN
Department of Electrical Engineering
University at Buffalo
The State University of New York
Amherst, NY 14260, USA

Received 14 February 2011
Accepted 1 March 2011

Communicated by Andras Der

Ideally, signals in statistical key exchange should be band-limited to prevent leak. During digitization, however, the broadband quantization noise gets incorporated. In this study, the security risk posed by the quantization noise is analyzed. The Savitzky–Golay filtering technique is used to reduce the quantization noise. Although the noise can be reduced, it cannot be eliminated. Legitimate users must take evasive measures. The adversary can perform exhaustive search. Once how signals are processed is identified, the security can be breached.

Keywords: Quantization error; random noise; signal processing; digital filter; information; security.

1. Introduction

Encryption and decryption using keys play crucial roles in secure communications [1]. There are a number of renowned techniques developed to generate and distribute keys [2–5]. Advances in quantum signals and information processing open opportunities and bring challenges. Quantum algorithms have the potential of cracking cryptography based on computational complexity [6]. Even the highly secure quantum key distribution method is subject to exploitation under real operating conditions [7]. Recently, several new approaches to establish the shared secret key have been reported [8–12]. In statistical key exchange two legitimate users try to establish correlated information by transmitting signals to each other in a public, authenticated channel. The process starts with generating band-limited random signals by legitimate users. The local random signal and a partial reflection of the received signal are added together to become the transmitted signal. The binary information is encoded on the sign of the feedback coefficient, positive for logic one and negative for logic zero. Legitimate users repeatedly transmit signals to each other to build up an ensemble. At the end of a symbol, statistical analysis

is performed to determine the binary information. Legitimate users decipher by correlating the locally generate random signal with the received signal. They enjoy a high success rate in determining the information. The adversary does not have access to the local random signal. Eavesdropping can only be performed by correlating two counter-propagating signals in the public. When legitimate users send binary complement information, i.e., Alice encodes with one and Bob zero or vice versa, the adversary faces uncertainty. There is only a very small signal buried in overwhelming fluctuations. The probability of getting the information is not much better than random guessing. After legitimate users establish a long sequence of highly correlated binary bits between them, they can perform sifting, distillation, and key agreement protocols to establish the shared secret key.

The protocol calls for band-limited signals. W represents the bandwidth, e.g., 5 kHz. The delay between two communicating parties, τ, must be small, for example, 4 μsec; therefore, τW is much less than unity. Otherwise, the adversary can exploit the difference between signals at two opposite terminals [12]. The duration of a symbol, T, should be sufficiently long, i.e., 5 msec, to build an ensemble for statistical analysis. The importance of bandwidth control is exemplified by an attempted attack [13]. If the spectrum of random signals is not band-limited but Lorentzian in shape, the adversary can extend the bandwidth by differentiating the signal. When the extended bandwidth becomes excessive, i.e., $\tau W \cong 1$, the adversary can easily determine the information. In the proposed protocol, the band-limited random signal is generated by passing a random Gaussian noise through an ideal, non-causal, low-pass filter. There is no Lorentzian tail to be extended.

Although signals start as band-limited, there is always a small, broadband component present. It results from the finite duration of signals, the quantization error in digitization, and the truncation error in computation [14]. The security risk during the transient turn-on has been addressed [15]. The truncation error can be arbitrarily small. The purpose of this study is to understand characteristics of the quantization noise and assess its security risk during the steady state.

2. Security Risk

The statistical key exchange protocol operates with two counter-propagating signals:

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

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

Alice is located at $x = 0$ and Bob at $x = L$. α and β represent reflection, i.e., feedback, coefficients, $|\alpha| = |\beta|$ with a nominal value of 0.2. τ is the delay between a signal transmitted by one user and then used in feedback by the other user. Here, V_+ and V_- represent analog signals. V_1 and V_2 are band-limited random signals generated locally. In digital communications, quantized signals are transmitted and

used in calculating the feedback.

$$V_{+q}(0,t) = Q\{V_1(t) + \alpha V_{-q}(L, t-\tau)\}, \tag{3}$$

$$V_{-q}(L,t) = Q\{V_2(t) + \beta V_{+q}(0, t-\tau)\}. \tag{4}$$

Q represents quantization. If the partial reflection is derived from the most recently sampled value, τ represents the sampling time. All parties, including legitimate users and the adversary, have full access to V_{+q} and V_{-q}. However, only Alice knows V_1 and Bob knows V_2, exclusively. The adversary has no information about them. Their accuracy is only limited by the truncation error in computation.

Quantized signals differ from analog signals by:

$$n_+(0,t) = V_+(0,t) - V_{+q}(0,t), \tag{5}$$

$$n_-(L,t) = V_-(L,t) - V_{-q}(L,t). \tag{6}$$

n_+ and n_- represent small deviations from analog signals. They are broadband. Strictly speaking n_+ and n_- are not exactly quantization errors according to the definition. They are not always smaller than $q/2$, where q represents the quantization step.

Quantization is a nonlinear process with thresholds. Often αn_- or βn_+ is too small to influence the outcome of digitization. The quantized value, V_{+q}, is determined by $V_1 + \alpha V_-$ alone. However, αn_- can influence the outcome when $V_1 + \alpha V_-$ is near the decision level of a quantization step. Although the αn_- term is small, it can play a role in determining whether the sum is above or below the threshold, hence, leak the information. In digitization, the addition of a large random signal to a small signal is called dithering. It is used in digitizing weak signals [16–18]. Here, $V_1 + \alpha V_-$ is the large dithering signal to carry the small αn$_-$ into the output. In this case, αn_- has a large bandwidth. $V_1 + \alpha V_-$ is a low frequency signal.

If V_+ and V_-, hence n_+ and n_-, are known to the adversary, the following correlation can be used to decipher the information:

$$\delta_q(t) = \langle n_+(0,t) \cdot n_-(L, t-\tau)\rangle - \langle n_+(0, t-\tau) \cdot n_-(L,t)\rangle. \tag{7}$$

The angled brackets represent ensemble average over the duration of a symbol. In reality, only quantized signals are transmitted. Neither legitimate users nor the adversary know V_+ and V_- directly. They must perform post processing after a symbol ends. If the duration of a symbol is sufficiently long, the low-pass filtered signal, LPF$\{V_{+q}\}$, is a good approximation of V_+; likewise LPF$\{V_{-q}\}$ for V_-. Hence, all parties can obtain approximations of n_+ and n_-; then δ_q. The procedure is equivalent to removing the low frequency components from V_{+q} and V_{-q} before calculating the correlation. It allows one to focus on the high frequency component. To subject the protocol to the most stringent challenge, we assume that the adversary can perform post filtering perfectly, i.e., LPF$\{V_{+q}\}$ equal exactly to the analog V_+.

Shown in Fig. 1 is the probability density function (PDF) of δ_q. The ensemble contains 10^4 symbols. The root-mean-square (RMS) amplitude of both V_1 and V_2 is

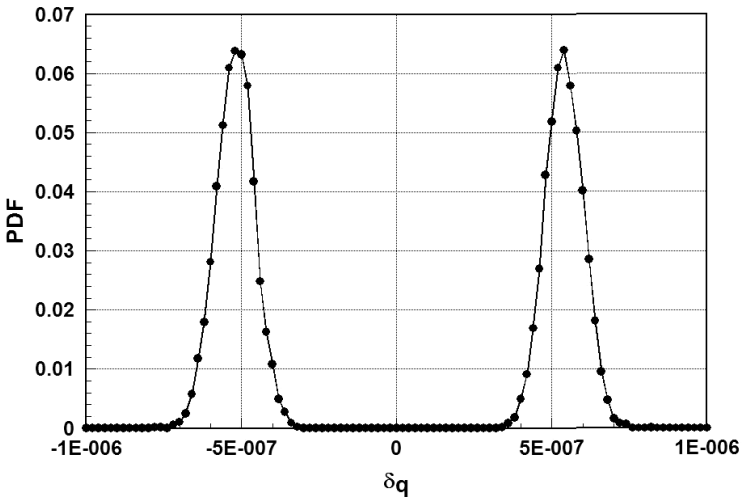

Fig. 1. PDF of δ_q. Data points are connected by line segments for viewing. There are two widely separated peaks corresponding to α equal to 0.2 and -0.2, respectively. One can easily determine the binary information according to the sign of δ_q.

unity while the quantization step is 1/256 V. The ensemble only contains symbols with complementary information, i.e., $\alpha = -\beta$. α varies randomly between two possible values, 0.2 and -0.2. Correspondingly, β varies randomly between -0.2 and 0.2. Data points appear in two well separated peaks. One peak corresponds to $\alpha = 0.2$, the other -0.2. The quantization step and $|\alpha|$ determine the location of the peak. Since two peaks do not overlap, there exists a definitive correlation between the sign of δ_q and the sign of $\alpha - \beta$, i.e., the binary complement information. There is a security risk.

Let us take a closer look at the quantization process. Both Alice and Bob perform digitization. Their respective quantization errors are:

$$n_1(0,t) = V_1(t) + \alpha V_{-q}(L, t-\tau) - Q\{V_1(t) + \alpha V_{-q}(L, t-\tau)\}, \tag{8}$$

$$n_2(L,t) = V_2(t) + \beta V_{+q}(0, t-\tau) - Q\{V_2(t) + \beta V_{+q}(0, t-\tau)\}. \tag{9}$$

n_1 is known to Alice and n_2 to Bob, exclusively. From Eqs. (1)–(6), (8) and (9), we obtain:

$$n_+(0,t) = n_1(0,t) + \alpha n_-(L, t-\tau), \tag{10}$$

$$n_-(L,t) = n_2(L,t) + \beta n_+(0, t-\tau). \tag{11}$$

Equations (10) and (11) have exactly the same format as Eqs. (1) and (2). However, the spectral characteristics of n_1 and n_2 are very different from those of V_1 and V_2. Quantization noise is broadband. It has an auto-correlation like the δ-function [16]. Even though legitimate users know n_1 or n_2, they have no advantage over the adversary in deciphering the information [12]. As long as approximate values

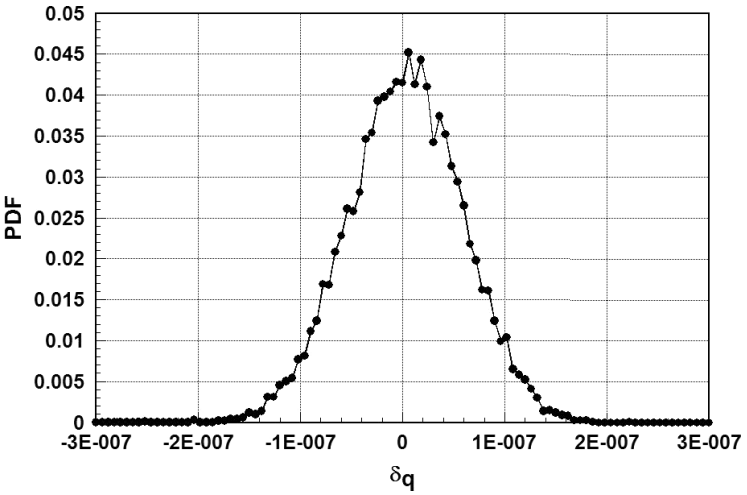

Fig. 2. PDF of δ_q when the quantization error is not incorporated into feedback. There is only one peak for both α equal to 0.2 and -0.2. No information can be deciphered.

of n_+ and n_- obtained from low-pass filter in post processing are accurate, the adversary can use δ_q to decipher the information.

To clarify the role of quantization noise, let us consider the following experiment. If legitimate users know and use analog signals, V_+ and V_-, in calculating reflected signals, the quantization errors of transmitted signals become

$$n_1'(0,t) = V_+(0,t) - Q\{V_+(0,t)\}, \tag{12}$$

$$n_2'(L,t) = V_-(L,t) - Q\{V_-(L,t)\}. \tag{13}$$

Shown in Fig. 2 is the PDF of δ_q, calculated from n_1' and n_2', for an ensemble of 10^4 symbols. Indeed, there is just one peak around zero. The adversary cannot determine the sign of $\alpha - \beta$ from δ_q. Quantization itself is not an issue. Only when the quantization error gets incorporated into feedback, the leak appears.

3. Low-Pass Filter

Clearly, legitimate users must control the quantization noise in real time. It may seem like a straight forward task for the low-pass, line filter [9, 10]. However, a causal filter introduces a delay [19]. Delay is a security risk in statistical key exchange. A non-causal filter does not introduce any delay. However, there is a transient component at the edge of the sampling window [14]. We have adapted the Savitzky–Golay polynomial smoothing technique [20, 21]. In statistical key exchange, signals are over sampled to ensure short delay. Therefore, the quantization error is not completely random [16]. To improve the accuracy, following adjustments are implemented. The sampling time is reduced to τ'. This enables legitimate users to derive the reflection from earlier signals without getting into excessive delay. In the mean time, Alice

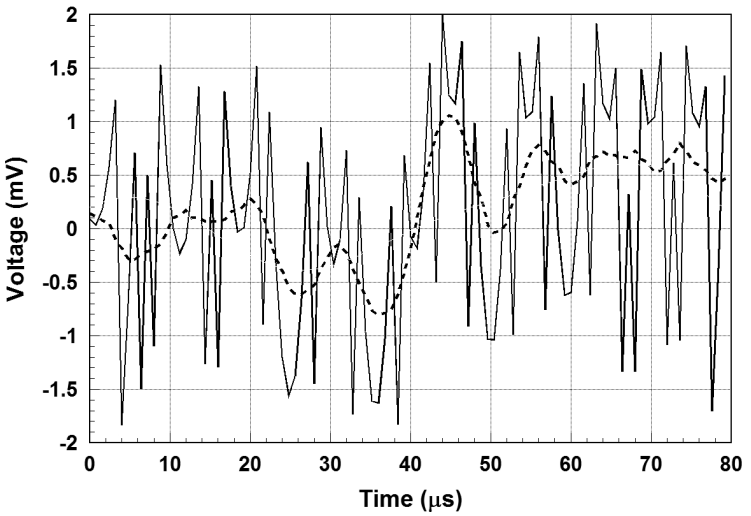

Fig. 3. High frequency noise resulting from quantization and its filtered waveform. The solid curve represents the difference between the quantized signal and its analog value, i.e., $V_{+q}(t) - V_{+}(t)$. After the polynomial filter, the noise is reduced to form the dashed curve.

and Bob can take advantages of few additional points indicating the trend of signal. We use the second-order polynomial to find the filtered value of $V_{-qF1}(t-3\tau')$ from a moving window of quantized data, $V_{-q}(t-n\tau')$, where $1 \leq n \leq 12$. Then, we use the third-order polynomial to find the filtered $V_{-qF}(t-5\tau')$ from $V_{-qF1}(t-m\tau')$, where $3 \leq m \leq 14$. In other words, we apply polynomial filters twice. Feedback at time t is derived from the filtered signal at $t-5\tau'$. τ' has a nominal value of $0.8\,\mu$sec.

Shown in Fig. 3 are deviations of signals from the analog signal in the steady state. They include the quantized signal, V_{-q}, and the smoothed signal generated by the polynomial filter, V_{-qF}. The mean-square (MS) deviation of V_{-q} from the analog V_{-} normalized by the quantization step of 1/256 V is 8.39×10^{-2}. The MS deviation of V_{-qF} from V_{-} is 1.09×10^{-2}. Although a polynomial filter can substantially reduce the quantization error it cannot completely eliminate it.

Since the high frequency quantization noise cannot be completely eliminated, legitimate users must take evasive measures. They must perform filtering in private, i.e., without revealing the filter used. Each filter generates a unique sequence of quantization errors. They compose feedback signals with high frequency components different from those of received signals. The low-frequency feedback signals, however, are not altered. The following feedback signals represent one set of possible choices:

$$\beta V_{+q}(L,t) \to \beta\{V_{+qF}(L,t) + [V_{+qF}(L,t) - V_{+q}(L,t)]/k\},$$
$$\alpha V_{-q}(0,t) \to \alpha\{V_{-qF}(0,t) + [V_{-qF}(0,t) - V_{-q}(0,t)]/k\}.$$

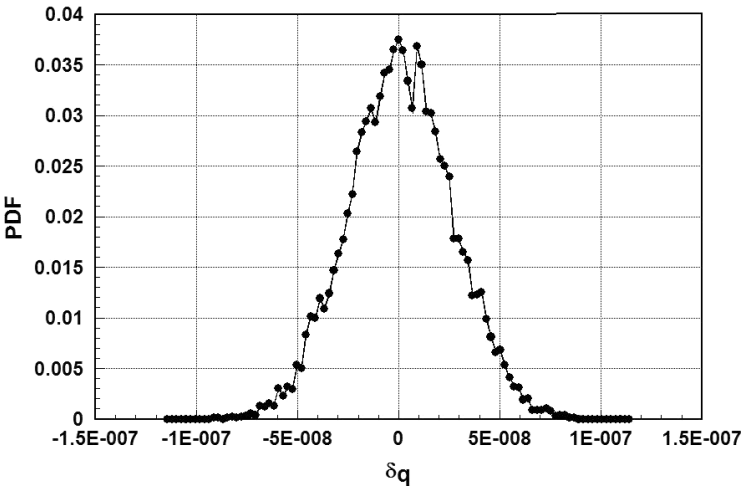

Fig. 4. PDF of δ_q when legitimate users take evasive measures while the adversary does not use any filter. There is only one peak for both α equal to 0.2 and -0.2. No information can be deciphered.

The primary component is V_{+qF} or V_{-qF}. The filtered signal contains less high frequency component. The amount of quantization noise going through reflection is reduced. k can be optimized so that δ_q is centered at zero. Its value depends on how effective the filter is in reducing the high frequency noise. When the filter is perfect, i.e., V_{-qF} approaches the analog V_-, k approaches infinity. For the above-mentioned polynomial filter, the value of k is 6.4. Shown in Fig. 4 is PDF of δ_q for an ensemble of 10^4 samples. There is just one peak. Furthermore, by varying k, legitimate users can even control the sign of δ_q making it independent of the information. The eavesdropper cannot rely on δ_q to decipher the information.

4. Exhaustive Search

Recognizing that legitimate users cannot eliminate the high frequency noise completely, the adversary knows that evasive measures have been taken. Although legitimate users implement filtering in private, the adversary can perform an exhaustive search. She can try each and every filter as well as different feedback signals. For example, the adversary can use V_{+qF} and V_{-qF} in calculating n_+ and n_-; then δ_q.

$$n_+(0,t) \to V_+(0,t) - V_{+qF}(0,t),$$
$$n_-(L,t) \to V_-(L,t) - V_{-qF}(L,t).$$

Here we assume that the adversary can obtain V_+ from LPF$\{V_{+q}\}$. We also assume that the exhaustive search will encounter filters used by legitimate users. When the adversary hits exactly the same filter used by legitimate users, the scatter plot of δ_q becomes what is shown in Fig. 5. There are two peaks, one for positive reflection coefficient and the other for negative coefficient. There is a strong correlation

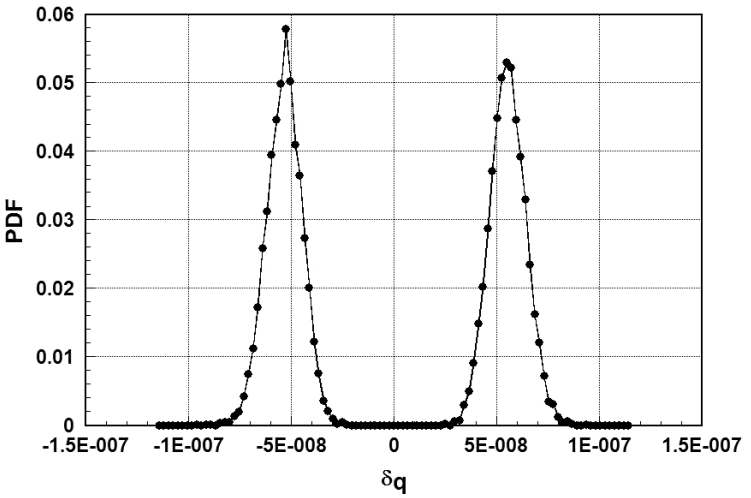

Fig. 5. PDF of δ_q when the adversary uses the same filter as legitimate users. There are two peaks, one for α equal to 0.2 and the other -0.2. Information can be deciphered.

between δ_q and the sign of the reflection coefficient. Although the search may require extensive efforts, the security can eventually be breached.

5. Conclusion

In summary, there is a security risk presented by the quantization noise in statistical key exchange. The quantization noise reflected is very small. Because of dithering, however, it can still carry information into the transmitted signal. The Savitzky–Golay polynomial smoothing technique can reduce the quantization noise but cannot eliminate it. Although legitimate users can implement evasive measures to hide information, the adversary can still obtain it through exhaustive search. The complexity of the task depends on diversity, i.e., how many filters with different characteristics can be deployed by legitimate users and how sophisticated the feedback signals are. Unless legitimate users can eliminate the quantization noise or, at least, perform real-time filtering with a performance rivaling that of the best low-pass filter in post processing, the security can be breached.

References

[1] H. Delfs and H. Knebl, *Introduction to Cryptography*, 2nd ed. (Springer-Verlag, Berlin, Germany, 2007).
[2] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Info. Theory* **IT-22** (1976) 644–654.
[3] R. L. Rivest, A. Shamir and L. M. Adleman, A method of obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21** (1978) 120–126.

[4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. IEEE Int. Conf. on Computers Systems and Signal Processing*, Bangalore India, (1984), pp. 175–179, http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.
[5] K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67** (1991) 661–663.
[6] W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, *Proc. 35th Annual Symp. Foundations of Computer Science*, Santa Fe, NM, (1994), pp. 124–134, http://www-math.mit.edu/∼shor/papers/algsfqc-dlf.pdf.
[7] F. Xu, B. Qi and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, *New J. Phys.* **12** (2010) 113026.
[8] H. P. Yuen, KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation (2004), http://arxiv.org/abs/quant-ph/0311061v6.
[9] L. B. Kish, Totally secure classical communication utilizing Johnson-like noise and Kirchhoff's law, *Phys. Lett. A* **352** (2006) 178–182.
[10] 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.
[11] J. Scheuer and A. Yariv, A classical key-distribution system based on Johnson (like) noise — How secure? *Phys. Lett. A* **359** (2006) 737–740.
[12] P.-L. Liu, A Key agreement protocol using band-limited random signals and feedback, *J. Lightwave Tech.* **27** (2009) 5230–5234.
[13] 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.
[14] P. Z. Peebles, Jr., *Probability, Random Variables, and Random Signal Principles*, 4th ed. (McGraw Hill, New York, USA, 2001).
[15] P.-L. Liu, Prediction accuracy of band-restricted random signals and security risk in statistical key exchange, *Fluctuation and Noise Letters* **9** (2010) 413–422.
[16] B. Widrow and I. Kollár, *Quantization Noise: Roundoff Error in Digital Computation, Signal Processing, Control, and Communications* (Cambridge University Press, Cambridge, UK, 2008).
[17] R. A. Wannamaker, The theory of dithered quantization, Ph.D. thesis, University of Waterloo, Waterloo, Ontario, Canada, (1997).
[18] L. Krause, Effective quantization by averaging and dithering, *Measurement* **39** (2006) 681–694.
[19] R. Cristi, *Modern Digital Signal Processing* (Brooks/Cole-Thomson Learning, Pacific Grove, CA, USA, 2004).
[20] A. Savitzky and M. J. E. Golay, Smoothing and differentiation of data by simplified least squares procedures, *Anal. Chem.* **36** (1964) 1627–1638.
[21] R. A. Leach, C. A. Carter and J. M. Harris, Least-squares polynomial filters for initial point and slope estimation, *Anal. Chem.* **56** (1984) 2304–2307.