On Perfect Reconstruction in Critically Sampled Frequency-Domain Scrambler

J. A. Apolinário Jr.[†‡] apolin@coe.ufrj.br
M. R. Petraglia[‡] mariane@coe.ufrj.br
R. G. Alves[‡] guedes@coe.ufrj.br

[†]Instituto Militar de Engenharia
Depto. Eng. Elétrica
Pça Gal. Tiburcio, 80
Praia Vermelha, Rio de Janeiro, RJ
22.290-270 — Brazil

[‡]Universidade Federal do Rio de Janeiro
COPPE - Programa de Engenharia Elétrica
P. O. Box 68504
Rio de Janeiro, RJ
21945-970 — Brazil

Abstract

Spectrum scrambling schemes have been widely used in voice privacy systems. Those using modern digital filter banks concepts have reported the appearance of aliasing in the reconstructed speech. Such undesirable effect has encouraged designers to use filters with longer impulse response in order to obtain sharper frequency responses and thus minimize the aliasing in the reconstructed signal. This paper presents the condition to obtain a frequency scrambler allowing perfect reconstruction of the speech signal without the need for high order filter banks. The effects of residual channel distortion (not compensated by the equalizer) as well as the selectivity of the filter banks in the frequency-domain scrambler scheme are investigated.

1 Introduction

The basic idea of a frequency scrambler using critically sampled FIR filter banks is depicted in Fig. 1. The descrambler is similar to the scrambler but uses an inverse permutation matrix (P^{-1}). A communication system formed by a scrambler (TX), an ideal channel and a de-scrambler (RX) would contain aliasing at its output even if Perfect Reconstruction QMF (PR-QMF) filter banks [1] were employed. Such aliasing effects have been minimized by using Pseudo QMF (P-QMF) filter banks [2] with sharper prototype lowpass filter [3], [4]. We illustrate, in Fig. 2, these effects on a 17 channel frequency-scrambler, where we show the magnitudes of the FFTs of a test speech signal, and of the signals after TX/RX using order 101 PR-QMF filter banks and using order 159 P-QMF filter banks.

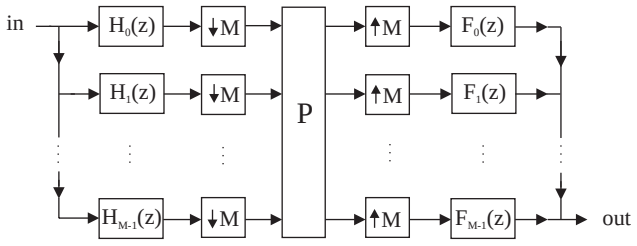

Figure 1: Basic frequency scrambler using filter banks.

In this work, the main "cause" of non-perfect reconstruction in frequency domain scramblers is addressed and perfect-reconstruction schemes are described. The channel equalization problem is then discussed and a solution is presented. Next, we deal with residual channel distortion and consider the possibility of varying the permutation matrix in time. Finally, simulations results and some conclusions are presented.

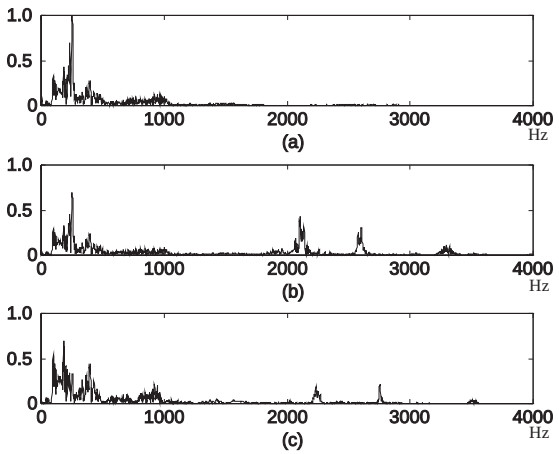

Figure 2: Output of a conventional privacy communication system based on frequency scramblers: (a) Original spectrum of the speech. (b) Output after order 101 PR-QMF TX/RX. (c) Output after order 159 P-QMF TX/RX.

2 Perfect Reconstruction Frequency-Domain Scramblers

For the rest of the paper we will assume that the filter banks used in the frequency scrambler satisfy the perfect reconstruction property. It means that if the analysis and synthesis filters are written in terms of their polyphase components, that is, $H_k(z) = \sum_{l=0}^{M-1} z^{-l} E_{kl}(z^M)$ and $F_k(z) = \sum_{l=0}^{M-1} z^{-(M-1-l)} R_{lk}(z^M)$, respectively, then the M $\times$ M matrices $\boldsymbol{E}(z) = [E_{kl}(z)]$ and $\boldsymbol{R}(z) = [R_{kl}(z)]$ (polyphase component matrices) are such that $\boldsymbol{E}(z)$ is lossless[1] and

[1]Stable and satisfying $\tilde{\boldsymbol{E}}(z)\boldsymbol{E}(z) = \boldsymbol{I}_M$ where $\tilde{\boldsymbol{E}}(z) = \boldsymbol{E}_*^T(z)$ [1]

$\boldsymbol{R}(z) = \tilde{\boldsymbol{E}}(z)$, which results in perfect reconstruction for the conventional filter banks applications.

We are now able to redraw Fig. 1 in terms of these polyphase component matrices as can be seen in Fig. 3, where the down-samplers and up-samplers were moved to the extremities. Again the RX diagram is similar to that of Fig. 3 but with P^{-1} instead of P. Let us call $\boldsymbol{X}_{TXin}$ the vector containing the signals between the down-samplers and $\boldsymbol{E}(z)$, and $\boldsymbol{X}_{TXout}$ the vector after $\boldsymbol{R}(z)$ and before the up-samplers. Analogously, we have $\boldsymbol{X}_{RXin}$ and $\boldsymbol{X}_{RXout}$ for the de-scrambler.

Using the above definitions, we show next that a signal passing through the scrambler and immediately followed by the de-scrambler would have perfect reconstruction if $\boldsymbol{X}_{RXin} = \boldsymbol{X}_{TXout}$. Since $\boldsymbol{X}_{TXout} = \boldsymbol{R}(z)P\boldsymbol{E}(z)\boldsymbol{X}_{TXin}$ and $\boldsymbol{X}_{RXout} = \boldsymbol{R}(z)P^{-1}\boldsymbol{E}(z)\boldsymbol{X}_{RXin}$, if $\boldsymbol{X}_{TXout} = \boldsymbol{X}_{RXin}$, then

$$\boldsymbol{X}_{RXout} = \boldsymbol{R}(z)P^{-1}\boldsymbol{E}(z)\boldsymbol{R}(z)P\boldsymbol{E}(z)\boldsymbol{X}_{TXin} = \boldsymbol{X}_{TXin}$$

and perfect reconstruction would be achieved.

However, Fig. 4 illustrates what happens to $\boldsymbol{X}_{TXout}$ and $\boldsymbol{X}_{RXin}$ for an arbitrary M: the elements of these vectors differ by a circular shift. In order to make $\boldsymbol{X}_{RXin} = \boldsymbol{X}_{TXout}$ we need to add a simple delay (z^{-1}) between TX and RX. This simple procedure, already used in transmultiplexers [1], shows the shift-variant nature of the problem: perfect reconstruction is obtained only if we have a constant delay of $rM+1$, with r a non-negative integer, between TX and RX. With the introduction of such a delay, perfect reconstruction filter banks designed by well-known techniques [5]-[7] can be used in the frequency-domain scrambler resulting in a perfect-reconstructed original signal in the absence of channel distortion. In this way, special filter bank design procedures for the frequency-scrambler, such as that developed in [9], are not needed.

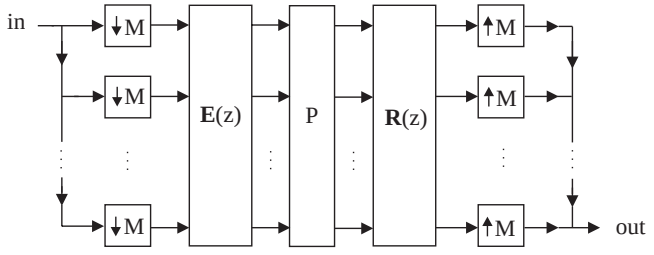

Figure 3: TX in terms of the polyphase matrices $\mathbf{E}(z)$ and $\mathbf{R}(z)$.

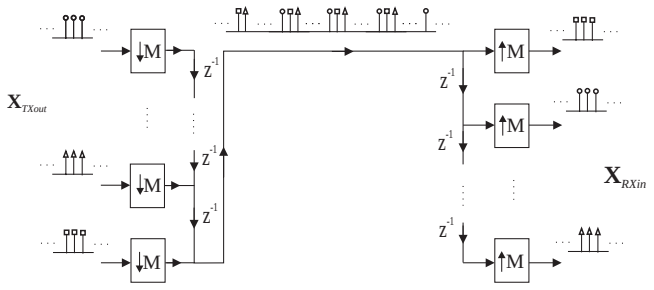

Figure 4: Circular shift effect between $\boldsymbol{X}_{TXout}$ and $\boldsymbol{X}_{RXin}$.

3 Channel Equalization

In order to have perfect or near-perfect reconstruction when transmitting the ciphered speech through a practical channel, such as a telephone line or a radio link, we need to equalize the channel to ensure a constant and proper delay. Figure 5 shows the classical approach of an adaptive digital equalizer where the adaptation algorithm can be a simple one (such as the LMS) when slow convergence is allowed or a more complex one (RLS type) when a shorter training sequence is needed. In this figure, L is the group delay in number of samples that should be chosen as stated in the previous section.

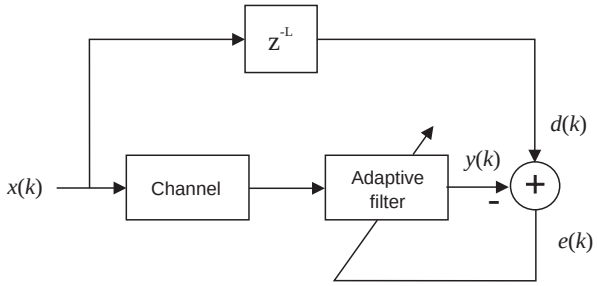

Figure 5: Channel equalization.

After the training period, the coefficients of the equalizer are frozen and the ciphered speech is transmitted. In our experiments we used a model of a telephone line as channel, obtaining very good equalization with a 141 coefficients adaptive filter (order N=140). Using M=16 subbands and assuming that the delay introduced by the channel and the equalizer is of 141 samples, the next integer L such that $L = rM+1$ is 145 ($9\times16+1$). It is shown in Fig. 6 the magnitude frequency response and group delay (in samples) of the channel used. Three other types of channels generated by a digital filter telephone line simulator were also used and the results obtained were similar.

Figure 7 shows the learning curves for the LMS and the RLS algorithms, as well as the impulse response and group delay of the channel followed by the equalizer after convergence.

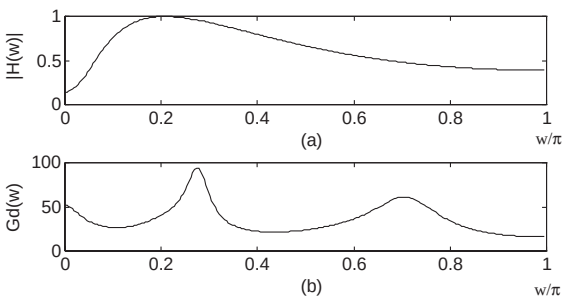

Figure 6: Simulated channel: (a) Magnitude frequency response. (b) Group delay.

4 Effects of Residual Channel Distortions and Time-Varying Key

In this section we examine the effects of poor equalization on the behavior of the whole system (TX+channel+equalizer+RX) and what happens when we change the key from time to time.

4.1 Residual Channel Distortion

We have simulated two different situations: freezing the equalizer coefficients before convergence (MSE in dB approximately half of its minimum value) and using an equalizer with 2/3 of the number of coefficients previously used ($N = 96$ and $L = 6 \times 16 + 1 = 97$). In both cases the results were considered acceptable as can be seen from the overall system impulse responses shown in Fig. 8.

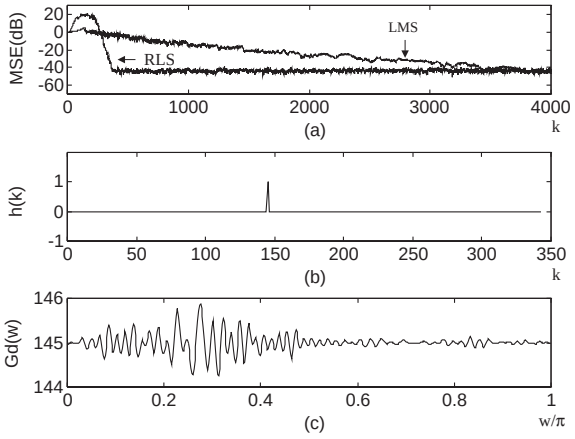

Figure 7: Behavior of the equalizer: (a) Learning curve (LMS and RLS). (b) Impulse response (channel+equalizer). (c) Group delay (channel+equalizer).

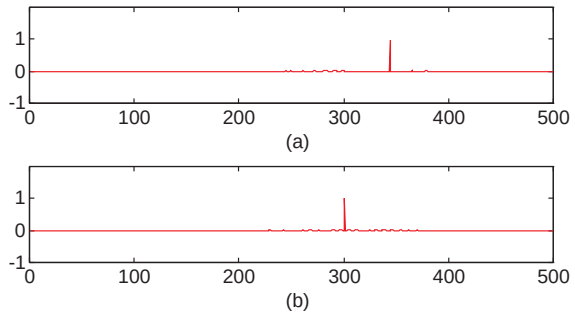

Figure 8: Impulse response of the overall system in case of poor equalization: (a) Convergence not reached. (b) Insufficient number of coefficients.

4.2 Variable Key

With the purpose of increasing the resistance to an eventual cryptanalitic attach, the scramblers are usually designed to change the key periodically according to a pseudo-random number generator. In the frequency-domain scheme, such changes in the key cause disturbances in the recovered speech signal because the subband filters use samples of two different signals during an interval following transition between keys. Therefore, the changing period of the key can not be very small or the speech quality would be severely degraded. As a rule of thumb one can change the key around ten times per second. Because the above transient is proportional to the length of the filters in the filter banks, the use of reduced order filters would allow us to change the key more frequently while keeping the degradation of the speech signal within acceptable levels. This indeed can be done since the perfect reconstruction property stated in Section II is not related to the filter bank order (N_{FB}). Therefore, one can use a relatively small N_{FB} and have a higher rate of key-change while enjoying other benefits such as lower delay, lower computational complexity and lower residual intelligibility of the ciphered speech. Figure 9 shows this transient when the key changes for the cases of filter orders $N_{FB} = 63$ and $N_{FB} = 101$.

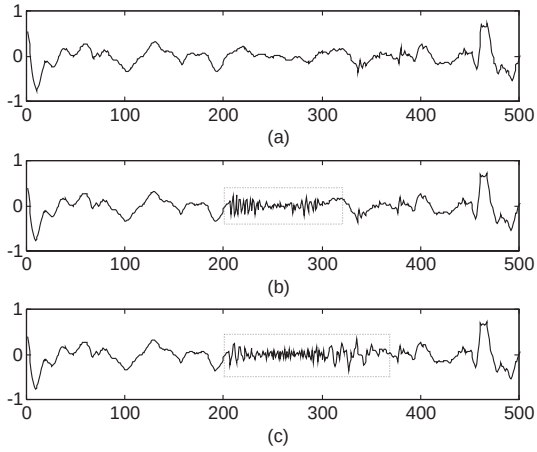

Figure 9: Transient effect when the key is changed: (a) Original signal. (b) $N_{FB} = 63$. (c) $N_{FB} = 101$.

5 Experimental Results

In this section, we compare the results of the frequency-domain scrambler scheme with different filter banks and filter lengths. In the simulations presented in this paper, we have used three distinct filter banks:

- P-QMF with $N_{FB} = 159$ given in [2]
- PR-QMF with $N_{FB} = 101$ given in [5]
- PR-QMF with $N_{FB} = 63$ given in [6],[7]

Figure 10 shows the original signal as well as the time-domain outputs (deciphered speech) of the first and last cases. The output of the second case ($N_{FB} = 101$ PR-QMF) is not shown here since it is identical to that of the third case except for a delay. From this figure, we can see that using a PR-QMF with a proper delay in the proposed scheme, the reconstructed signal is a replica of the original one; the same observation does not apply to the P-QMF scrambler.

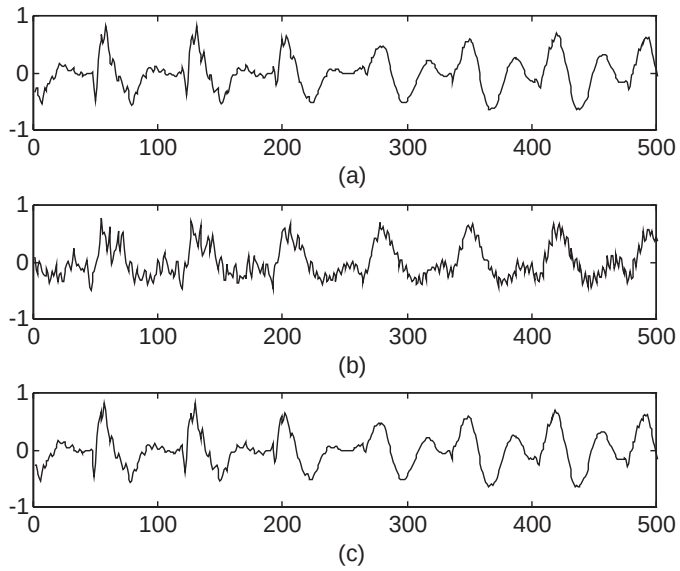

Figure 10: Deciphered speech: (a) Original Speech. (b) Output of the P-QMF system ($N_{FB} = 159$). (c) Output of the PR-QMF ($N_{FB} = 63$).

Next we can see in Fig. 11 the overall impulse responses of the three systems. All other results were already presented in previous sections. We could finally remark that it is possible to use PR FIR QMF banks designed without the minimization of the sum of stopbands energies [5]. This fact would allow very simple design procedures to obtain filter banks of arbitrary number of channels with different filter orders.

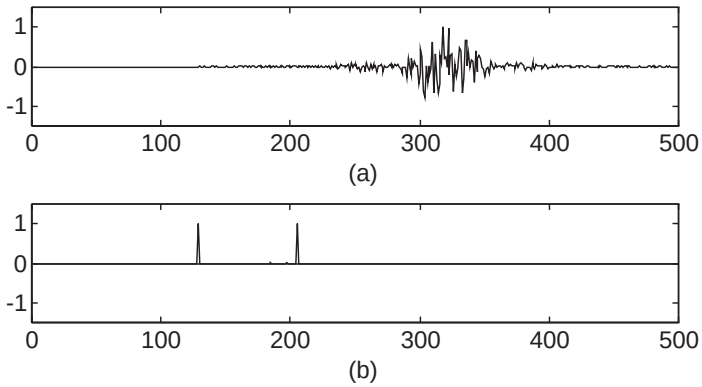

Figure 11: Impulse responses of the overall voice privacy system: (a) P-QMF ($N_{FB} = 159$). (b) PR-QMF ($N_{FB} = 101$ and $N_{FB} = 63$).

6 Conclusion

In this work, we have presented a frequency-domain scrambler which allows perfect reconstruction of the ciphered speech. The need of a constant and proper delay between scrambler and de-scrambler was addressed as well as the effects of poor equalization and the use of a time-varying key. Besides perfect reconstruction of the recovered speech, some other important features due to the possibility of using lower order filter banks were pointed out.

References

[1] P. P. Vaidyanathan, "Multirate Systems and Filter Banks." Englewood Cliffis, NJ: Prentice Hall, 1993.

[2] P. L. Chu, "Quadrature mirror filter design for an arbitrary number of equal bandwidth channels," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-33, no. 1, pp. 203-218, Feb. 1985.

[3] R . V. Cox et al., "The Analog Voice Privacy System," *AT&T Technical Journal*, vol. 66, no. 1, pp. 119-131, Jan./Feb. 1987.

[4] E. D. Re, R. Fantacci, G. Bresci and D. Maffucci, "A New Speech Signal Scrambling Method for Mobile Radio Applications," *Alta Frequenza*, vol. LVII, no. 2, pp. 133-138, Feb./March 1988.

[5] P. P. Vaidyanathan and R. D. Koilpillai, "Cosine-Modulated FIR Filter Banks Satisfying Perfect Reconstruction," *IEEE Trans. on Signal Processing*, vol. 40, no. 4, pp. 770-783, Apr. 1992.

[6] H. S. Malvar, "Modulated QMF filter banks with perfect reconstruction," *Electron. Lett.*, vol. 26, no. 13, pp. 906-907, Jun. 1990.

[7] H. S. Malvar, "Signal Processing with Lapped Transform." Artech House, Inc., 1992.

[8] L. S. Lee, G. C. Chou and C. S. Chang, "A New Frequency Domain Speech Scrambling System Which Does Not Require Frame Synchronization." *IEEE Trans. Communications*, vol. COM-32, no. 4, pp. 444-456, April 1984.

[9] C. W. King and C. A. Lin, "A Unified Approach to Scrambling Filter Design," *IEEE Trans. on Signal Processing*, vol. 43, no. 8, pp. 1753-1765, Aug. 1995.