Analog Hardware Trojan Vulnerability in the Analog Signal Chain

Kwabena Oppong Banahene, Matthew R. Strong, Bryce Gadogbe, Degang Chen, Randall L. Geiger
Department of Electrical & Computer Engineering
Iowa State University
Ames, IA, USA

***Abstract*— Hardware security vulnerabilities to hardware Trojans in widely used filter structures are identified. The widely used two-integrator loop filter architecture known as the Kerwin-Huelsman-Newcomb (KHN) Biquad is used to demonstrate the vulnerability. It is shown that the relationship between the passive component values and the nonlinear amplifier parameters, the slew rate and the output saturation voltages, determine the presence or absence of a stationary nonlinear undesired oscillatory mode of operation. Experimental results obtained from a discrete component filter demonstrate the vulnerability to the Trojan mode of operation in this filter structure.**

I. Introduction

Though there is considerable research focused on hardware security in large and complex digital systems, little attention is paid to security vulnerabilities in the analog signal chain. This may be, in part, due to the observation that the analog signal chain is often comprised of a small number of basic components that are well-understood by most engineers and that with so few components, it would be difficult to embed a hardware Trojan in the analog circuitry that would go unnoticed in peer design reviews and go undetected with the basic simulation and verification tools that are available today.

In this work, it will be shown that hardware Trojans can be embedded in some of the most basic filter structures. In contrast to most digital hardware security concerns where the focus of the adversary is on embedding additional components or altering the basic mode of operation, the vulnerability that will be explored in this paper is attributable to the potential presence of an undesired triggerable mode of operation that can be inserted without including any additional components and without altering what are widely recognized as well-known and widely used filter structures. Furthermore, it will be shown that the trigger can be applied at the normal input to the filter thereby giving an adversary direct access to a trigger input. Cover for this type of Trojan is provided by the observation that there are no known methods for finding all solutions of a set of nonlinear differential equations in finite time. Thus, the vulnerability that will be explored in this paper is at the interface between the linear operation of a filter and the nonlinearities inherent in any active device.

Two integrator loop filters are often used to realize second-order transfer functions. The KHN biquad filter [1], the Tow-Thomas Biquad [10]-[11] and the Åkerberg-Mossberg filter [2] are well known and widely used structures. The KHN biquad is the architecture of choice in the UAF42 (Universal Active Filter) by Texas Instruments [7] and the 2005 paper by Ibrahim [8] with almost 300 citations is based on the KHN biquad as well.

Though these filters have excellent sensitivity properties to the gain bandwidth products of the operational amplifiers and perform very well as filters, they are vulnerable to an unstable nonlinear oscillatory mode of operation [2]. The existence of this oscillatory mode cannot be detected by a standard linear analysis or simulation. It is caused by the nonlinearities [2] in the operational amplifiers used in these filters. Two of these non-linearities, slew rate limitations and saturation voltages of the amplifiers, will be discussed in this paper.

The instability associated with the nonlinear oscillatory modes in this paper should not be confused with the potential linear instability of a filter structure. Most authors focus on the instabilities caused by the gain bandwidth limitations of the operational amplifiers which can cause poles to shift into the right half-plane [3]-[5] or by additional parasitic poles [9] attributable to the reactive elements in the operational amplifiers. The oscillations caused by the nonlinearities (slew rate and saturation limits) will not be seen when performing analysis in the frequency domain. Slew rate and saturation voltages effects are usually restricted to what impact they have on distortion of the filter output signal [6].

In Section II, the linear operation of the KHN Biquad is briefly reviewed. In Section III the nonlinear oscillatory mode of the filter is discussed. A phase plane plot showing the unstable oscillatory mode, the stable operating mode, and the boundary between the two modes is shown in Section IV. Experimental results for a discrete implementation of the KHN biquad are presented in Section V. An analytical formulation of the relationship between oscillation frequency and the nonlinear amplifier characteristics comprises Section VI. A brief discussion of the vulnerability of filter structures to analog hardware Trojans comprises Section VII and VIII.

II. The KHN Biquad Filter

The KHN biquad shown in Fig.1 is a three operational amplifier active filter that can achieve band-pass, high-pass, and low-pass transfer functions simultaneously. It is obvious from the diagram where the "two-integrator" name comes from. The transfer functions of the band-pass, high-pass, and low-pass filters are shown in (1), (2), and (3) respectively. A more general version of the filter is described in [1] that realizes more general second-order transfer functions.

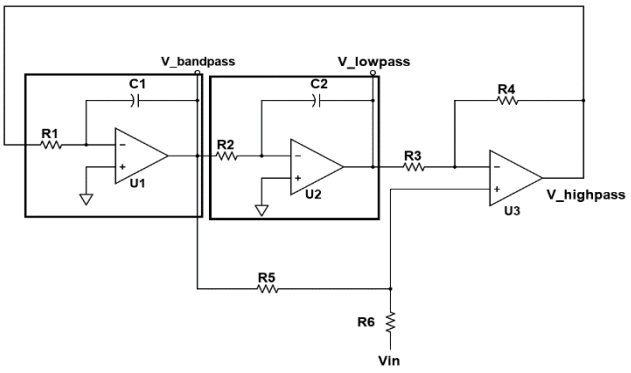


Fig. 1. KHN biquad

$$\frac{V_{bandpass}(s)}{Vin(s)} = \frac{-s\frac{R_5(R_3+R_4)}{C_1R_1R_3(R_5+R_6)}}{s^2+\frac{R_6(R_3+R_4)}{C_1R_1R_3(R_5+R_6)}s+\frac{R_4}{C_1C_2R_1R_2R_3}} \quad (1)$$

$$\frac{V_{highpass}(s)}{Vin(s)} = \frac{s^2\frac{R_5(R_3+R_4)}{R_3(R_5+R_6)}}{s^2+\frac{R_6(R_3+R_4)}{C_1R_1R_3(R_5+R_6)}s+\frac{R_4}{C_1C_2R_1R_2R_3}} \quad (2)$$

$$\frac{V_{lowpass}(s)}{Vin(s)} = \frac{\frac{R_5(R_3+R_4)}{C_1C_2R_1R_2R_3(R_5+R_6)}}{s^2+\frac{R_6(R_3+R_4)}{C_1R_1R_3(R_5+R_6)}s+\frac{R_4}{C_1C_2R_1R_2R_3}} \quad (3)$$

Pole frequency: $\omega_o = \sqrt{\frac{R_4}{C_1C_2R_1R_2R_3}}$ (4)

Quality factor: $Q = \frac{(R_5+R_6)}{R_6(R_3+R_4)}\sqrt{\frac{C_1R_1R_3R_4}{C_2R_2}}$ (5)

III. Unstable Oscillatory Mode

The KHN filter is known to support both a stable filtering mode and an undesired nonlinear oscillatory mode of operation [2] for some implementations of the filter. Recovery from the oscillatory mode generally requires recycling the power source to the filter. Though the nonlinear oscillatory mode of operation has been reported primarily based upon experimental evidence, there has been little discussion about what conditions must exist to create this vulnerability nor how to recognize that it is a problem in this or other filters during the design phase.

During the nonlinear oscillatory mode, it will be assumed that the two integrators in Fig.1 are operating normally and that amplifiers U1 and U2 are neither saturating nor slewing. It will also be assumed that the amplifier U3 in Fig.1 behaves as a comparator with a finite slew rate and symmetric saturation voltages of VDD and VSS. The effects of the nonlinear operation of U3 on the nonlinear oscillation will now be considered. With these assumptions, consider the block diagram of the filter shown in Fig.2 where V3 is the output of the comparator and V1 and V2 are the outputs of the integrators. Assuming some initial voltage at the outputs of V1 and V2, a sketch of the time-dependent output voltages is shown in Fig.3. In Fig. 3(a) the comparator is assumed to have infinite slew rate whereas Fig. 3(b), U3 has a finite slew rate.

In Fig. 3(a), at time t1, the output of the comparator flips and causes V1 to integrate in the opposite direction. When this occurs, V2 will still be integrating V1. Because V1 changes directions immediately the comparator flips its output, and there will be eventual settling so no oscillations will occur.

In contrast, in Fig. 3(b) at time t1, the output of the comparator begins to transition to VSS but V1 continues to integrate downward until U3 slews long enough to force V3 to cross the zero-volt line. This causes a buildup in the voltage difference between V1 and V2 which can lead to a sustained oscillation.

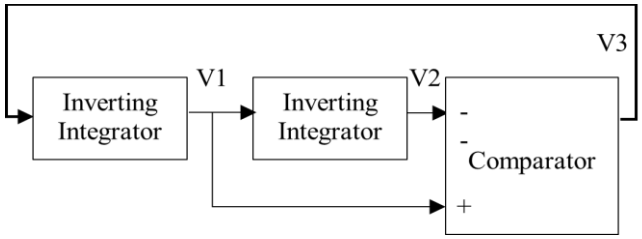


Fig. 2: Block diagram showing how the biquad is operating

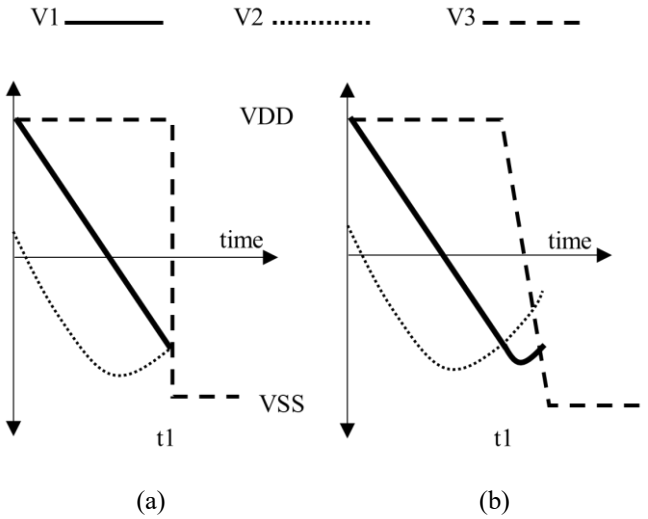


Fig. 3: Sketch of output of Fig.2

IV. Phase Plot

To better visualize the presence of the stable and unstable modes of operation in this filter, the phase portraits for an implementation of the KHN biquad shown in Fig. 4 are useful. In these phase portraits, the voltages on the two energy storage elements (capacitors of the integrators) are used as state variables. The output of the integrators can be initialized to any point in the phase plane. In these phase plots, the filter input is assumed to be zero (i.e., the system is unforced). After the initialization of these voltages, the system is allowed to settle to a stationary mode of operation. Depending on the initial values, the system may settle at either the stable dc operating point or a stationary nonlinear oscillatory mode of operation. The stationary operating point is at the origin. The nonlinear oscillatory mode of operation, if it exists, is characterized by the Oscillation Orbit shown in red in the Fig. 4(a). The arrows in the phase portrait show the direction of movement after initialization at each point in the phase plane. The trajectory the outputs follow is not shown. Also shown in the phase portrait is the Boundary of Attraction if it exists. If initial conditions are internal to the Boundary of Attraction, the outputs will settle to the stable dc operating point. If the initial inputs are outside of the Boundary of Attraction, the circuit will converge to the Nonlinear Oscillatory Mode of operation.

A. Model

The KHN filter was designed in MATLAB with the following conditions:

- All operational amplifiers were assumed to have infinite linear bandwidth
- The op amps in the integrators were modelled with symmetric saturation limits but with infinite slew rates.
- The operational amplifier U3 was modeled with a finite slew rate and the same saturation limits as the op amps in the integrators
- The filter input was set to ground potential.

The values of the resistors and capacitors used in this model are:

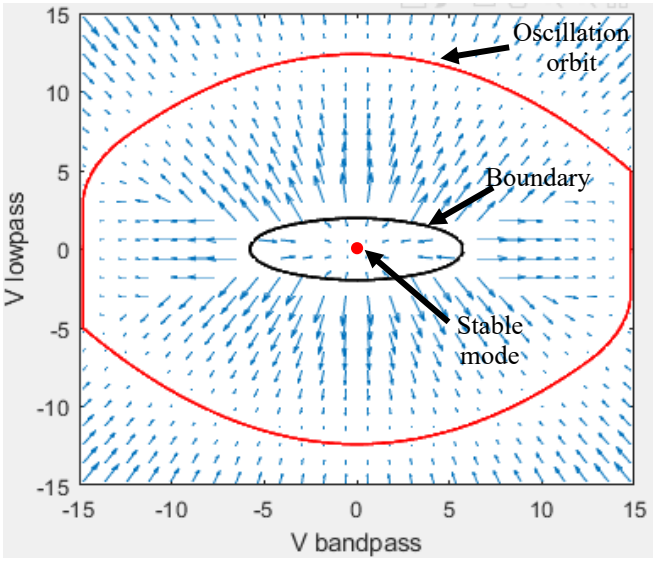
$$R_1 = R_2 = R_3 = R_6 = 10K\Omega$$

$R_4 = 100K\Omega$ $R_5 = 330K\Omega$ $C_1 = C_2 = 9.4nF$

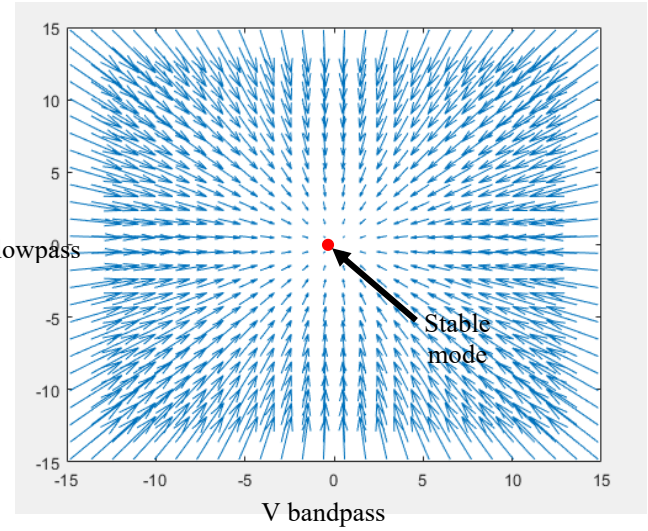
From (4) and (5) these values correspond to a pole Q of 9.77 and $f_o = 5.3542$ kHz, where $f_o = \omega_o/2\pi$. The saturation limits of the amplifiers were set at ±15V.

B. Phase Portrait

The distinction between the two-phase portraits in Fig. 4 are only the slew rates of the operational amplifier. The amplifier U3 corresponding to the plot in Fig.4(a) has a slew rate of 0.5V/µs. With this slew rate, the filter has both a stable operating point and a stationary nonlinear oscillatory mode with a Boundary of Attraction separating the two modes.



(a)



(b)

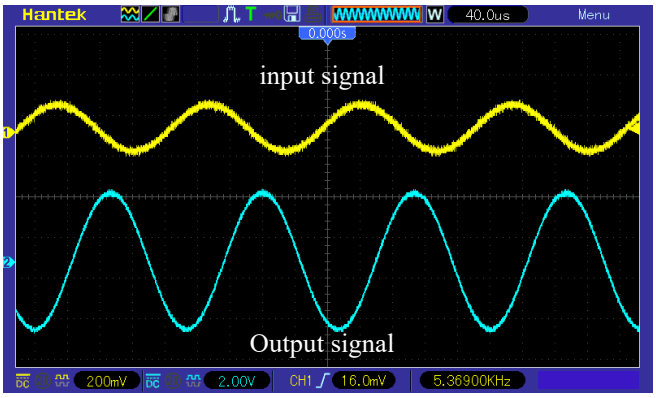
Fig. 4. Phase plot of filter with amplifier slew rate of (a) 0.5V/µs and (b) 2V/µs

When the slew rate of U3 is increased to 2V/µs, the phase plot of Fig. 4(b) is obtained. With this slew rate, it can be seen that the oscillatory mode disappears since for any excitation, the output will converge to the stable mode of operation.

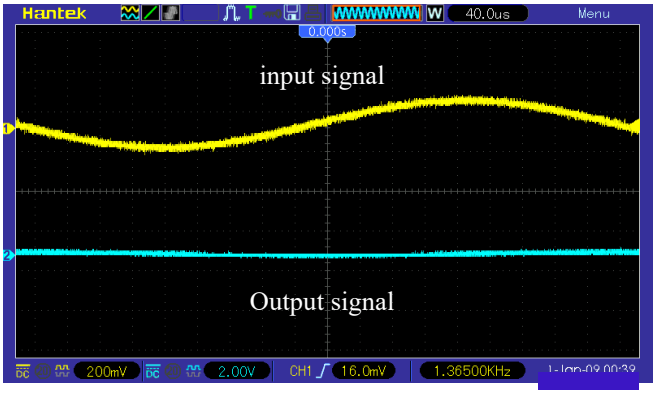
The relationship between the slew rate, the passive devices of the filter, and the saturation limits of the amplifiers will determine whether the undesired nonlinear oscillatory mode exists and, if it exists, how easy it is to trigger the circuit into the oscillatory mode. If used as a hardware Trojan, an adversary can manipulate the slew rate and saturation limits so that the Boundary of Attraction to the desired stationary operating point would be large so that it would be difficult to detect the presence of the undesired oscillatory mode during simulations or testing. For the KHN biquad, the Boundary of Attraction is a function of the SR and the saturation voltage limits of the operational amplifiers and for given filter specifications, the boundary of attraction can be designed to make the Trojan very stealthy while simultaneously having what appears to be a good design for normal operation of the filter.

V. Experimental Plots

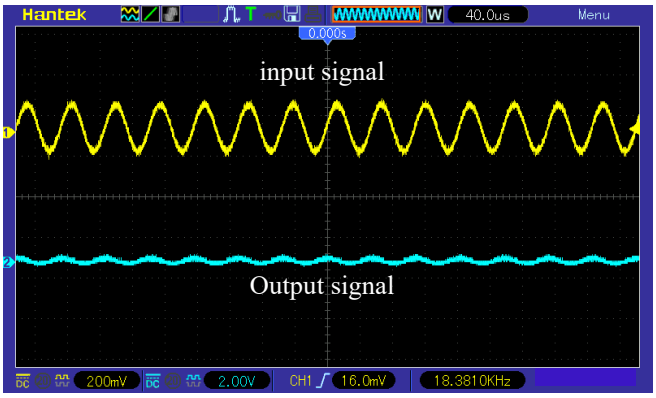
The KHN filter using the component values given in Section IV was built with discrete components. The amplifier used was the LM741. The gain bandwidth product of the operational amplifier is typically 1.5MHz and the slew rate is around 0.5V/µs. Experimental results are shown in Fig. 5 and Fig. 6. In Fig. 5, a low frequency input of 1.3kHz, a mid-band input of 5.3kHz, and a high-frequency input of 18.3kHz was applied. This filter is operating normally as shown in Fig.5. By applying extreme inputs, the oscillatory mode of operation can be triggered and is shown in Fig.6 where the input was set to 0V after triggering.



(a)



(b)



(c)

Fig. 5. KHN filter bandpass output: (a) operation at in-band frequency, (b)operation at low frequency (c)operation at high frequency

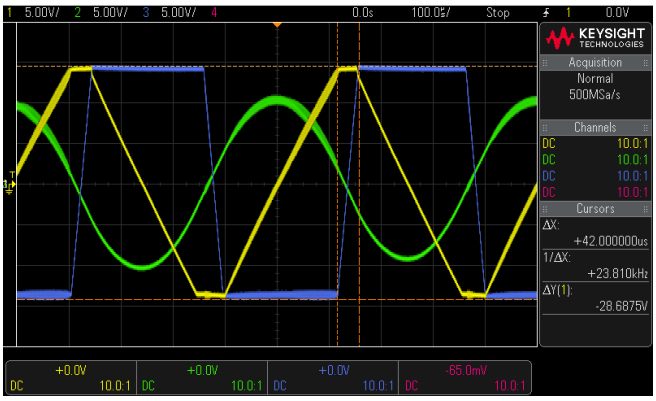


Fig. 6. Outputs of all operational amplifiers in oscillatory mode: Band-pass output(yellow), High-pass output (blue), Low-pass output (green)

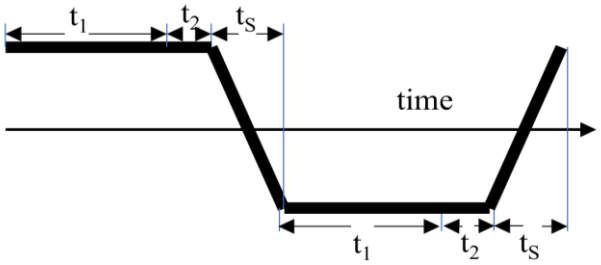


Fig. 7. A single period of the output of the comparator

VI. Anaysis of Oscillatory Mode

Using a steady-state nonlinear analysis, we will now attempt to develop an analytical expression for the oscillation frequency of the KHN biquad if an oscillatory mode of operation exists. This will be based upon a piecewise analysis of the unforced system. There may be several different conditions that can occur that will support oscillation depending upon the relationship between the RC time constants of the integrators, the slew rate of the operational amplifiers, and the saturation limits of all devices. In the experimental results presented in the previous section, U1 saturates before U3 slews so we will make this assumption.

The output signal for one period of the oscillatory waveform is shown in Fig. 7 under the assumption that the positive and negative slew rates are the same. The piecewise modes of operation can be characterized by:

- During interval t_1, Integrator 1 integrates
- During interval t_2, the output of U1 saturates
- During interval t_s amplifier U3 is slewing

Under these assumptions, it can be shown that

$$t_1 = \frac{4C_1R_1 \times SR - V_{DD}}{2 \times SR} \tag{6}$$

$$t_2 = \frac{36C_1R_1R_4(SR)V_{DD}(R_5+R_6) - R_4V_{DD}^2(R_5+R_6)}{24R_4 \times C_1R_1 \times (R_6+R_5) \times SR^2} - \frac{48C_1C_2R_1R_2(SR)^2(R_3R_5+2R_3R_6+R_4R_6)}{24R_4 \times C_1R_1 \times (R_6+R_5) \times SR^2} \tag{7}$$

$$t_s = \frac{2 \times V_{DD}}{SR} \tag{8}$$

$$\text{period} = 2(t_2 + t_1 + t_s) \tag{9}$$

where

slew rate =SR

V_{DD} = saturation limits (same magnitude since supplies are symmetrical)

Using the component values in the design from Section IV, the measured slew rate of 0.447V/µs and saturation voltage of 13.9V for the operational amplifiers, the predicted frequency of oscillation is 1.95kHz, and the measured frequency of oscillation was 1.98kHz.

VII. Hardware Trojans in Filter Structure

The Stationary Nonlinear Mode of Operation in the KHN biquad can serve as a hardware Trojan. The Trojan can be triggered by applying a particular input into the normal filter input port of the filter. By judicious selection of the relationship between the components of the filter, the SR of the operational amplifiers, and the saturation limits of the operational amplifiers, the oscillatory mode of operation can be forced to exist or forced to vanish. Standard analysis and design tools will not detect the presence of the oscillatory mode of operation. It is not known how prevalent this vulnerability is in other filter structures but there are other well-known filter structures that are widely used that can support a nonlinear oscillatory mode of operation, yet the vulnerabilities have not been reported in the literature.

VIII. Triggering of Trojan Bearing Filter Circuits

As discussed earlier, there exists the possibility to trigger the non-linear oscillatory mode of operation through the input of the filter. In this section, simulation results are shown on using some forcing input signal to trigger the filters into the Trojan mode.

The operation of this Trojan can be explained with the simulated phase plots shown in Fig. 10. The boundary of attraction is the blue orbit. Fig. 10(a) shows the stationary oscillatory mode of operation and Fig. 10(b) shows the output orbit with a specific input forcing function. If the input is taken to 0 when the forced output is between points A and B, the circuit will operate in the oscillatory mode. If the input is taken to 0 when the input is between points C and D, the filter will return to normal operation. The adversarial designer can design the circuit to make the distance between nodes A and B very small making it unlikely that the oscillatory mode

would be detected during design, testing, or verification yet the adversary would have complete control of the mode of operation through the input trigger.

A. KHN Biquad

In the simulation results shown in Fig. 8(a), the input is set to zero when the forced output falls outside the boundary of attraction. As a result, the filter enters the undesired Trojan mode. In Fig. 8(b), the input is set to zero when the forced output falls within the boundary of attraction which causes the system to return to normal operation. The nature of the forcing signal required to trigger into or out of the Trojan mode depends on how the Trojan is designed into the filter.

B. Other structures with non-linear oscillatory mode – Tow-Thomas Biquad

Another popular filter structure known as the Tow-Thomas Biquad [10]-[11] or the State Variable Filter also has the unstable oscillatory mode. It is comprised of an inverting and a noninverting integrator connected in a feedback loop with one of the integrators being lossy. A lowpass version of this filter is shown in Fig. 9.

Fig. 11(a) shows simulation results for an implementation of this filter where the input is set to zero when the forced output falls outside the boundary of attraction. This triggers the filter into the undesired Trojan mode. Correspondingly, Fig. 11(c) shows the scenario where the input is set to zero when the forced output falls within the boundary of attraction which causes the system to return to normal operation. The nature of the forcing signal required to trigger into or out of the Trojan mode depends on how the Trojan is designed into the filter just as in the KHN biquad. Fig. 11(b) shows an example of what appears to be a trigger signal that fails to trigger the Trojan because the forced output is not between points A and B on the Boundary of Attraction locus when the trigger is applied.

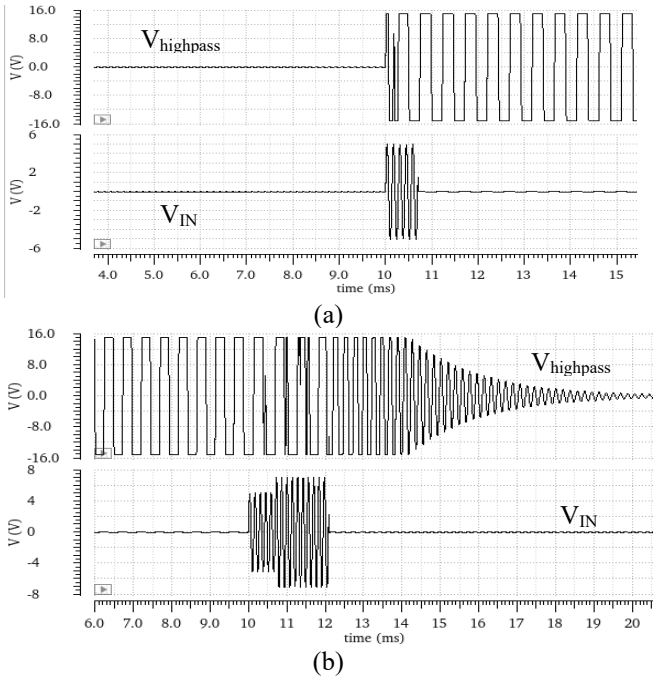


Fig. 8. Transient response of V_{OUT} and V_{IN} for KHN biquad using inputs as trigger: (a) input to trigger into Trojan mode, (b) input to trigger out of Trojan mode

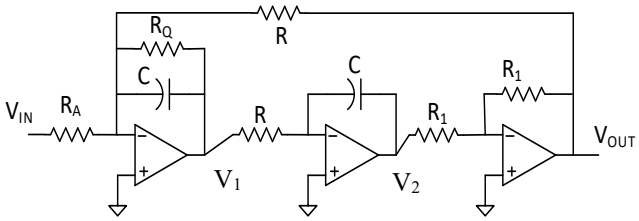


Fig. 9. Popular State Variable Lowpass Filter

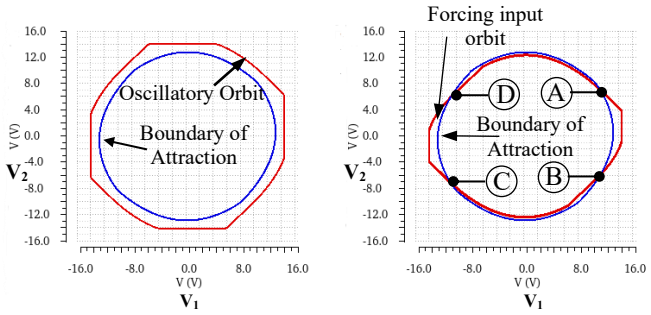


Fig. 10. Typical Phase Plane Orbits for State Variable Filter

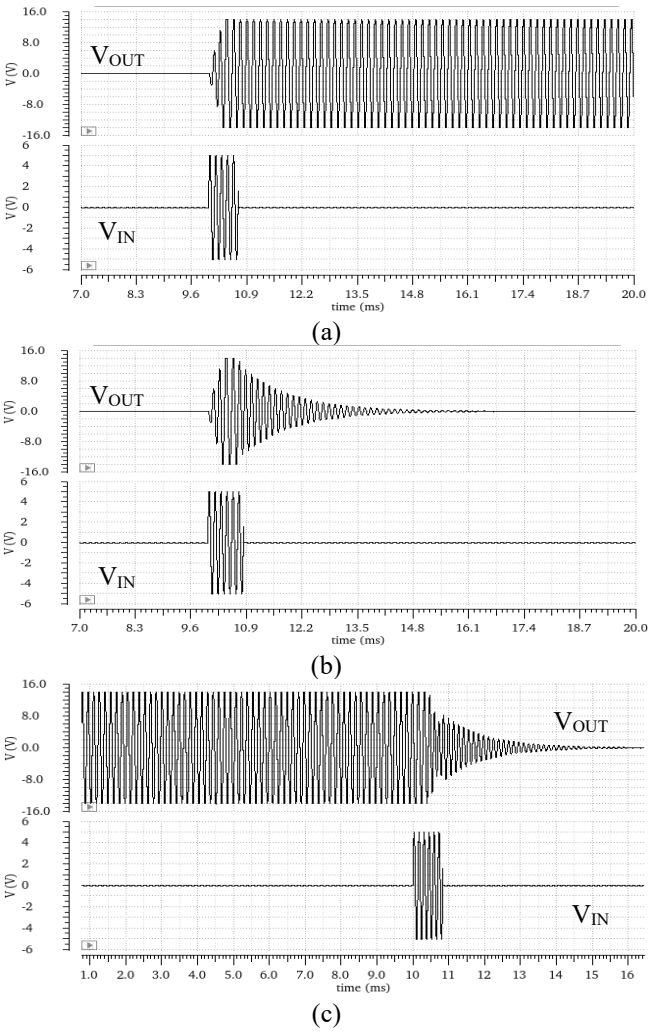


Fig. 11. Transient response of V_{OUT} and V_{IN}, for the Tow-Thomas biquad using inputs as trigger: (a) input to trigger into Trojan mode, (b) the return to normal mode when not triggered right, (c) input to trigger out of Trojan mode

IX. Conclusion

Methods for determining the presence or absence of stationary nonlinear modes of operation in the KHN biquad filter have been discussed. The nonlinear oscillatory mode of operation can serve as an analog hardware Trojan that can be stealthy yet easy to trigger through the normal input to the filter. The presence or absence of the Trojan mode of operation is strongly dependent upon the relationship between the component values used in the filter and the nonlinear properties of the amplifiers, specifically the slew rate and the saturation voltage limit.

Acknowledgment

This work was supported, in part, by the National Science Foundation (NSF) and the Semiconductor Research Corporation (SRC).

References

[1] W. J. Kerwin, L. P. Huelsman and R. W. Newcomb, "State-variable synthesis for insensitive integrated circuit transfer function", IEEE J. Solid-State Circuits, vol. SC-2, pp. 87-92, Sept. 1967.

[2] D. A kerberg and K. Mossberg, "A Versatile Active RC Building Block with Inherent Compensation for the Finite Bandwidth of the Amplifier", IEEE Transactions on Circuits and Systems, vol. 21, pp. 75-78, 1974.

[3] G. Hilber et al., "Stability analysis and design methodology for an Åkerberg-Mossberg filter," 2014 IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne VIC, 2014, pp. 2097-2100, doi: 10.1109/ISCAS.2014.6865580.

[4] A. Budak and D. Petrela, "Frequency limitations of active filters using operational amplifiers," in IEEE Transactions on Circuit Theory, vol. 19, no. 4, pp. 322-328, July 1972, doi: 10.1109/TCT.1972.1083470.

[5] P. Aronhime, "Effects of finite gain-bandwidth product on three recently proposed quadratic networks," in IEEE Transactions on Circuits and Systems, vol. 24, no. 11, pp. 657-660, November 1977, doi: 10.1109/TCS.1977.1084277.

[6] P. Allen, "A model for slew-induced distortion in single-amplifier active filters," in IEEE Transactions on Circuits and Systems, vol. 25, no. 8, pp. 565-572, August 1978, doi: 10.1109/TCS.1978.1084518.

[7] Texas Instruments, UAF42 Universal Active Filter . 1993, Jul. . Available from: http://www.ti.com/lit/ds/symlink/uaf42.pdf

[8] Muhammed A. Ibrahim, Shahram Minaei, Hakan Kuntman, "A 22.5MHz current-mode KHN-biquad using differential voltage current conveyor and grounded passive elements," AEU - International Journal of Electronics and Communications, Volume 59, Issue 5, 2005, Pages 311-318, ISSN 1434-8411, doi: 10.1016/j.aeue.2004.11.027.

[9] R. Geiger, "Parasitic pole approximation techniques for active filter design," in IEEE Transactions on Circuits and Systems, vol. 27, no. 9, pp. 793-799, September 1980, doi: 10.1109/TCS.1980.1084896.

[10] J. Tow, "Active RC filters—A state-space realization," in *Proceedings of the IEEE*, vol. 56, no. 6, pp. 1137-1139, June 1968, doi: 10.1109/PROC.1968.6502.

[11] L. Thomas, "The Biquad: Part I-Some practical design considerations," in *IEEE Transactions on Circuit Theory*, vol. 18, no. 3, pp. 350-357, May 1971, doi: 10.1109/TCT.1971.1083277.