EECT Automation

Design of a Programmable SAW Correlator Using Binary Phase Shift Key Encryption for Wireless Network Security

Mr. John R. Haughery, Iowa State University, Department of Agricultural and Biosystems Engineering, 1340 Elings Hall , Ames, IA 50011-3270, (717) 587-6506, jhaughery@iastate.edu

Dr. William R. Grisé, Morehead State University, Department of Applied Engineering and Technology, 105B Lloyd Cassity Building, Morehead, KY 40351, (606) 783-2424, w.grise@moreheadstate.edu

Dr. Robert Mertens, University of Central Florida, College of Engineering and Computer Science, HEC 406, 4000 Central Florida Blvd., Orlando, FL 32816, (407) 694-4929, quarkmaster@gmail.com

Abstract

A Programmable Surface Acoustic Wave (PSAW) correlator pair using Binary Phase Shift Key (BPSK) modulation and an 11-bit Barker code sequence is proposed to increase the security levels of wirelessly transmitted network data in the 2.45 GHz WiFi frequency band. Due to the unique properties of SAW correlator's interdigital transducer (IDT) fingers, their orientation, and the alternating polarity between sets of IDT fingers, they are well suited for BPSK encoding applications. This encryption is made possible with the use of well-matched PSAW correlator pairs that encode RF burst signals to produce a high auto-correlation vs. cross-correlation signal. This encrypted signal is then decoded by passing it through a reverse coded PSAW correlator to remove the modulation encryption, leaving the original data signal. The critical parameters of the author's proposed design are presented, including the piezoelectric substrate material selection, relevant equations for critical parameter, and the final proposed design.

Introduction

IEEE 802.11 Security Issues

Amid the exponential growth of WiFi, it has become increasingly apparent that security levels have lagged behind transmission speeds and connectivity (Ramakrishna & Ravi, 2011). Even in spite of the rapid growth of this technology, there are growing concerns about how secure data really is when transferred over a WiFi network. A common concern is the prevalence of rogue access points (APs), which present themselves as trusted routers but in reality snoop the transmitted data in an attempt to obtain sensitive information (i.e. usernames, passwords, personal information). These rogue APs are hard to patrol and pose real security concerns for WiFi users (Park & Kim, 2013). Therefore, stronger data encryption techniques are needed that keep pace with the growth of this technology and the increasing prevalence of security attacks from rogue APs.

Purposed Solution to IEEE 802.11 Security Issues

This paper proposes the use of a Programmable Surface Acoustic Wave (PSAW) correlator with Binary Phase Shift Key (BPSK) encoding to increase the security levels of wirelessly transmitted network data in the 2.45 GHz WiFi frequency band. Similar work by NASA has been completed in which a PSAW was used for low-power communication links between ground and space transceivers (Elkordy, Elsherbini, & Gomaa, 2013). Additionally, Gallagher, Malocha, Puccio, and Saldanha (2008) have completed research using SAW correlators in wireless spread-spectrum and RFID applications to increase date rates and increase code encryption diversity. Also, a patent filed by Edmonson and Campbell (2012), has proposed the use passive SAW correlators for wireless communications in the 2.45 GHz Bluetooth spectrum. It is clear therefore that the author's proposed design is consistent with current work related to wireless network security.

Overview of Surface Acoustic Waves and SAW Correlators

Surface acoustic waves are produced by means of the electrometrical conversion process of a special type of transducer. This transducer, called a SAW transducer, converts electrical waves to mechanical surface acoustic waves by stimulating interdigital transducers (IDTs) etched onto a piezoelectric substrate with electrical radio frequency (RF) signals, as depicted by Figure 1. The IDTs are thin film metal electrodes, with a frequency dependent width ranging from a few micrometers to a few hundred nanometers. The IDTs act like antennas, launching the electrical signals onto the piezoelectric substrate between the IDTs. These launched signals are then converted into mechanical surface acoustic waves that propagate across the substrate and back onto the IDTs where they are converted back to electrical signals. ST Quartz is commonly used as the piezoelectric substrate because of its relatively slow acoustic wave velocity (~3,158 m/s), which enables the SAW device to produce large delays in the electrical to mechanical signal conversion process. These delays enable encoding of RF electrical signal with either frequency shift or phase shift chips (Token, 2010). These chips can be configured in such a way as to emulate a Barker code sequence, which can be used to encrypt RF burst signals (Malocha, Puccio, & Gallagher, 2004).

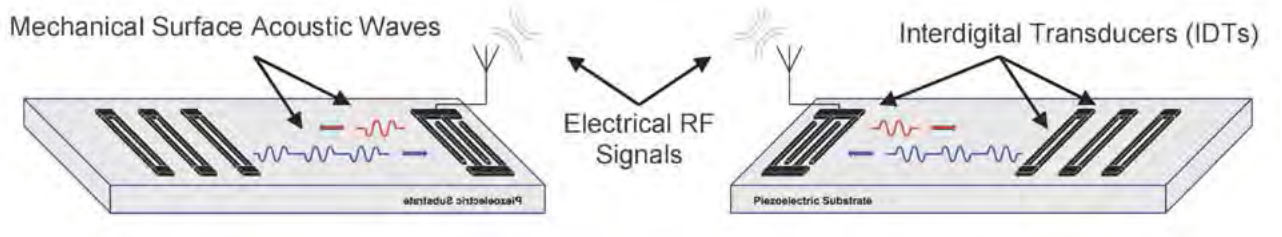


Figure 1. SAW transmitter (left) and receiver (right) correlator pair.
(Source: Malocha, Puccio, & Gallagher, 2004)

Decryption of this coded RF burst signal is easily accomplished by passing the encrypted signal back through a matched SAW receiver correlator. If the receiver correlator has an identical IDT structure design, the output signal will have a high auto-correlation to the input signal, meaning the original RF burst will be decoded with high accuracy. If the receiver correlator is not well matched (i.e. the IDTs do not have the same structural design), its output signal will be cross-correlated and resemble white noise similar to the side lobes of the auto-correlated output signal, as established by Malocha et. al. (2004). Figure 2 illustrates this contrast between auto and cross-correlated signals. Therefore, with a well-matched SAW correlator transmitter/receiver pair, an RF burst signal can be encoded in such a way as to produce a high auto-correlation vs. cross-correlation encryption scheme. It is also important to note that increasing the number of coded chips included in the SAW correlator will increase its encryption strength.

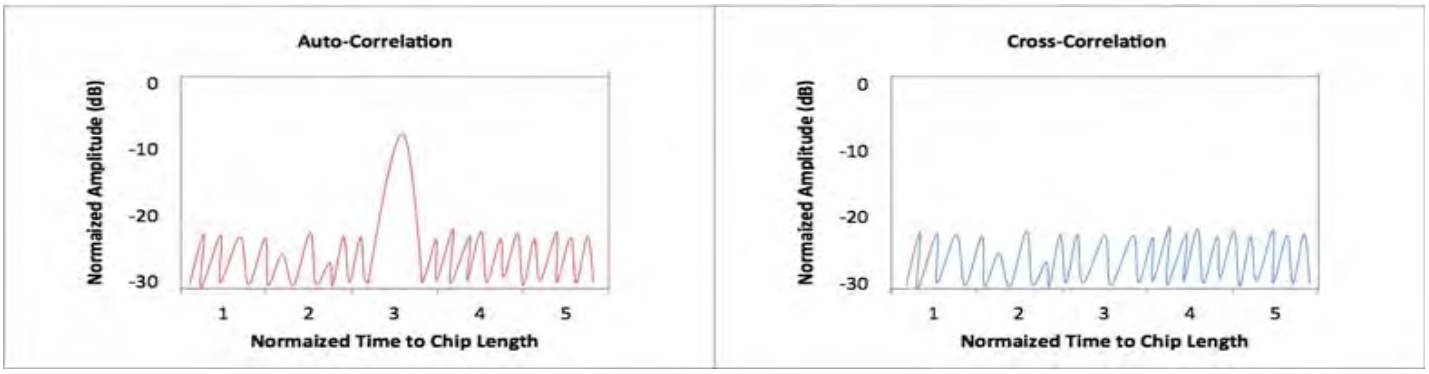


Figure 2. Auto-correlation vs. cross-correlation of SAW encoded signal.

SAW Correlator Design Considerations

Piezoelectric Substrate

As indicated above, a SAW device's ability to encode a signal is related to the propagation delays produced by the piezoelectric substrate material. As the alternating electrical signals are launched off the IDTs, they are converted to mechanical waves and propagate through the substrate at a reduced velocity. As previously mentioned, ST Quartz is a common substrate used in SAW devices and has an acoustic velocity of ~3,158 m/s. Other materials are available with their own unique velocities that affect the propagation speeds of surface acoustic waves. In addition to substrate material, Morgan (2007) indicates that temperature changes also have an effect on surface acoustic waves. Table 1 lists some of the common piezoelectric substrate materials used in SAW devices, and indicates the velocity [vf (m/s)] and temperature [TDC (ppm/°C)] affects of these substrate materials, as well as some advantages, disadvantages and suitability considerations of various substrate materials. This table has been adapted from Morgan's text titled Surface Wave Acoustic Filters (2007).

Table 1. Common piezoelectric substrate materials used in SAW device

	Y–Z lithium niobate ($LiNbO_3$)	128°Y–X lithium niobate ($LiNbO_3$)	ST–X quartz (SiO_2)	36°Y–X lithium tantalate ($LiTaO_3$)
***vf* (m/s)**	3488	3979	3158	4212
TCD (ppm/°C)	94	75	0	32
Advantage	Low diffraction, strong coupling	Low bulk waves, strong coupling	Small TCD	Strong coupling, moderate TCD
Disadvantage	Large TCD, strong bulk waves	Large TCD	Weak coupling	-
Suitability	Wide-band filters, RACs, convolvers	Wide-band filters	Narrow-band filters, resonators, pulse compression	Low-loss filters, RF filters

IDT Design for BPSK

BPSK is a common modulation scheme used in digital communications systems to encrypt binary data, especially in WiFi communication networks. The prevalence of BPSK can be attributed to two facts, 1) Phase Shift Key (PSK) encryption has higher signal to noise ratios (SNR) compared to other modulation schemes, and 2) BPSK is the simplest form of PSK and lends itself readily to WiFi communication scenarios (Elkordy, Elsherbini, & Gomaa, 2013).

With BPSK encoding, a signal is encrypted into a binary code by modulating the original signal between 0° and 180° phase shifts. In this scheme a 0° phase shift may indicate a digital 1 bit while a 180° phase shift indicate a digital 0 bit. By shifting the phase of an RF signal between these two phase angles in a specific sequence (code) the signal is encrypted with a cipher key. This encrypted signal can be decoded by passing it through a reverse coded phase shift sequence key to remove the modulation encryption leaving only the original data. Due to the physical properties of SAW device's IDT fingers, their orientation, and the alternating polarity between sets of IDT fingers, they are very well suited for BPSK coding applications (Campbell, 1989).

The BPSK encoding scheme described above is easily achieved with specific design configurations of a SAW device's IDT fingers. These fingers can be arranged in such a way as to emulate a Barker code sequence, which is preferable due to reduced power requirements in the side lobes of the auto-correlated signal. A simplified IDT finger arrangement design to achieve a 5-bit Barker code sequence of + + + − + for BPSK encryption is depicted in Figure 3. As illustrated, the phase shift, and thus the encoding, is accomplished by alternating the arrangement of IDT finger pairs (chips). The relative polarity of the finger pairs stays constant as long as the arrangement is constant. When the arrangement is flipped, as seen in the 2nd IDT finger pair from the left, the polarity changes. This change in polarity causes a 180° shift in the phase angle of the signal passing through the SAW correlator, which corresponds to a change in the binary code (Elkordy, Elsherbini, & Gomaa, 2013). In this manner, an RF burst signal can be easily encoded with a Barker code sequence.

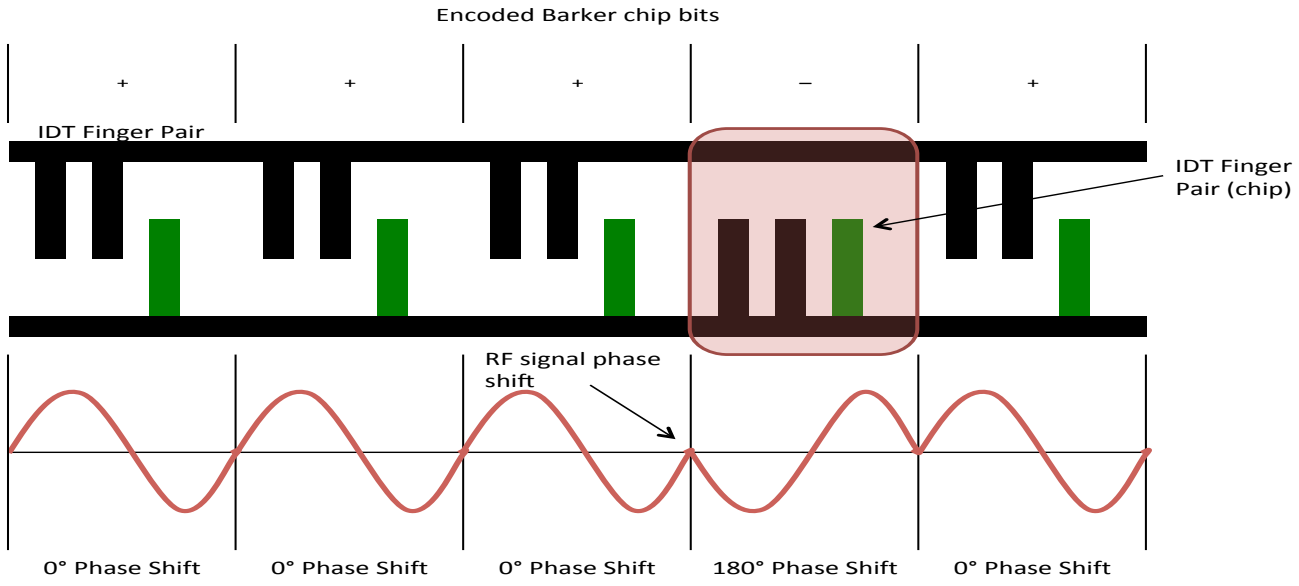


Figure 3. BPSK encoding by means of IDT finger pair arrangement

Physical Design Parameters

When determining the specific design dimensions of a BPSK SAW correlator, the first parameter to consider is the total length (LT) of the correlator's coded IDT pairs. As indicated by Malocha et. al. (2004), this length is contingent on the bit period () of the RF burst signal being imposed on the correlator. The relationship between these two variables is depicted in Equation 1 and 2, where (v) is the velocity of the piezoelectric substrate of the SAW correlator.

$$L_T = v \cdot \tau_B \quad (1)$$

$$\tau_B = \frac{1}{Bit\ Rate} \quad (2)$$

The next dimensional consideration is that of the number of IDT chips and their individual lengths. The number of chips is simply based on an integer number of Barker code bits desired in the encryption scheme. The length of each of these chips is determined by first determining the period of each chip (τ_C), which is found with Equation 3, where the number of chips (j) is an integer number based on the desired Barker code (Malocha, Puccio, & Gallagher, 2004). Once the chip period is determined, the length of each chip (LC) is then found with Equation 4,

$$\tau_C = \frac{\tau_B}{j} \quad (3)$$

$$L_C = v \cdot \tau_C \quad (4)$$

The dimensional relationships between Equations 1 – 4 are depicted in Figure 4.

The individual IDT finger width and inter-IDT spacing between adjacent fingers is the next critical parameter to consider. According to Satoh, Ikata, Miyashita, and Ohmori (2012), this dimension (W) is proportional to the wavelength (λSAW) of the piezoelectric substrate, as indicated by Equations 5,

$$W = \frac{\lambda_{SAW}}{4} \quad (5)$$

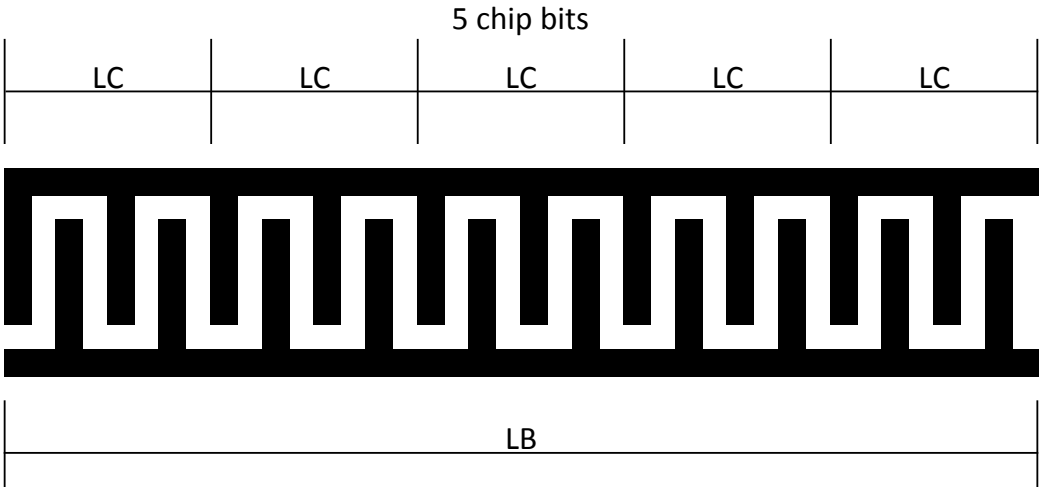


Figure 4. Coded IDT length relative to bit length, chip number and chip length

Equations 6 further defines the wavelength of the piezoelectric substrate, which is based on the acoustic velocity (v) of the SAW substrate and the frequency (f) of the RF signal being encrypted by the SAW correlator. Figure 5 illustrates the physical relationships of Equations 5 and 6.

$$\lambda_{SAW} = \frac{v}{f} \quad (6)$$

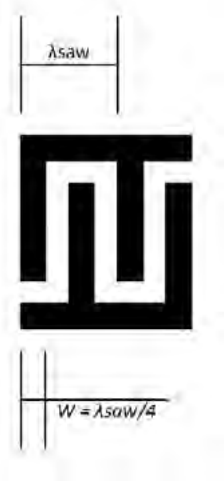


Figure 5. IDT finger width and inter-IDT spacing relationships

Calculating the number of IDT fingers in each chip (Fchip) is also necessary to calculate using Equation 7,

$$F_{chip} \approx \left(\frac{L_C}{W}\right) \cdot 0.5 \qquad (7)$$

This equation assumes that the chip length is filled with equally dimensioned IDT fingers and inter-IDT gaps. This assumption is not always necessary, but will be used in this design.

The IDT finger's apodization (overlap) can either be held constant or it can vary (Campbell, 1989). In this design, constant apodization (A) will be used for simplicity and can be calculated as proportional to IDT finger length (L) with Equation 8,

$$A = 0.75 \bullet L$$

Furthermore, with constant apodization, the finger length must be held constant as well and can be proportional to finger width (Campbell, 1989) as seen by Equation 9,

$$L = W \bullet 10$$

Another design consideration of a SAW correlator is the input/output IDT. This IDT serves the dual purpose as input for the RF signal and output for the encrypted signal. This paper proposes connecting the input/output IDT to a 2.45 GHz Tx/Rx antenna for wireless data transmission of WiFi data. The dimensions of this IDT may simply be a four-finger design, as shown in Figure 6, with dimensions identical to those of the coded IDT chips as calculated by Equations 5, 6, 8 and 9 (Campbell, 1989).

The final dimension of a SAW correlator to calculate is the distance between the input/output IDT and the coded IDT. This is dimension is critical and is dependent on the wavelength of the acoustic waves (λSAW) propagating between these IDTs. To ensure resonance, the input/output IDTs must be spaced so that the waves arrive at the coded IDT at the correct phase (0° phase angle). Equation 10 illustrates this relationship between the wavelength and the spacing between the IDTs (d) to achieve resonance and proper phase angle of the signal (Morgan, 2007),

$$d = \frac{\left(\left[n+\left(\frac{\Delta\phi}{\pi}\right)\right]\lambda_{SAW}\right)}{2} \qquad (10)$$

where ($\Delta\phi$) is is the phase angle offset desired by the BPSK scheme.

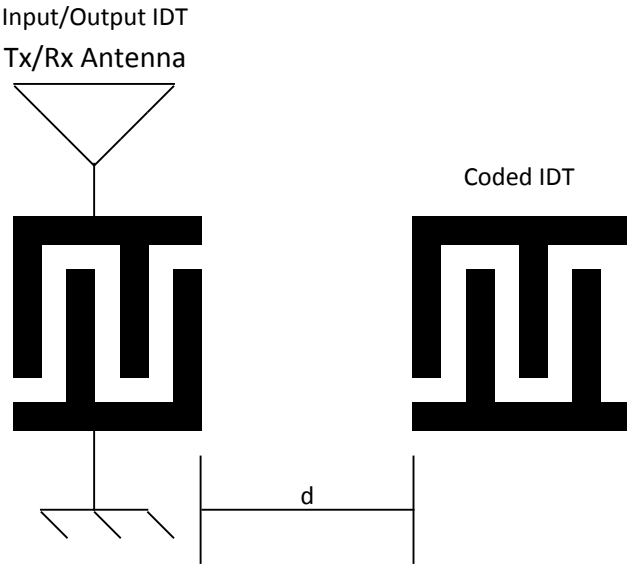


Figure 6. Input/Output IDT design and distance from coded IDT

PSAW Correlator Design

SAW correlators can be designed as either passive or dynamic. For a correlator to be dynamic, it must exhibit an ability to frequently re-arrange the coded IDT fingers as required by the communication system's encryption protocol. By inserting RF switches (i.e. BJTs or FETs) between the bus strips above and below the coded IDT fingers they can be dynamically rearranged as needed, as illustrated by Figure 7. It is important to note that in this design it is crucial that the RF switches be ganged according to chips so that all fingers associated with a single chip change arrangement together. Furthermore, the last finger of each chip can be permanently connected to the ground bus to mark a consistent end of each chip (Campbell, 1989).

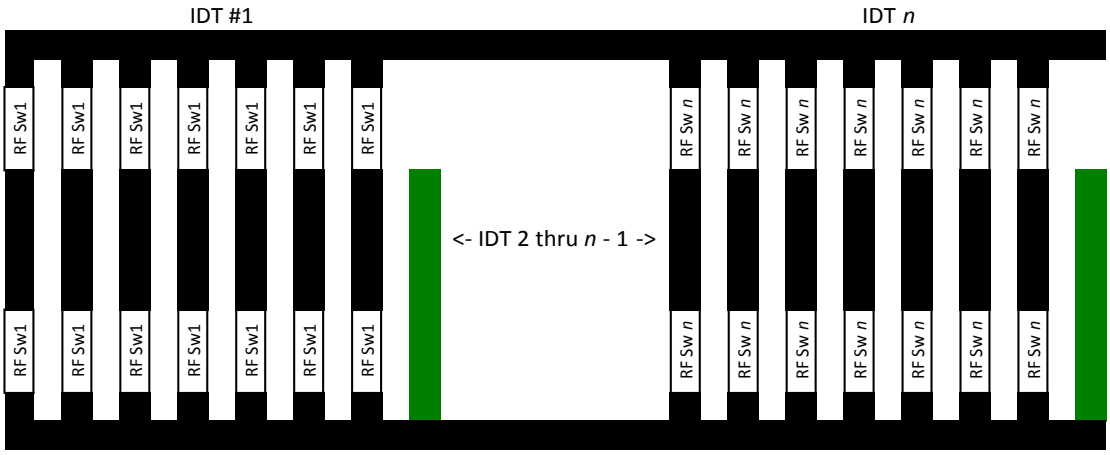


Figure 7. Coded IDT with RF switches enabling dynamic fingers re-arrangement

Proposed SAW Correlator Design

The purpose of this paper is to present a design solution to security issues related to IEEE 802.11 networks operating in the 2.45 GHz and 5.8 GHz frequency bands. To that end, this research proposed a PSAW design capable of operation in the 2.45 GHz band. This frequency band is chosen due to exponentially increasing limitations of SAW devices above 3 GHz (Morgan, 2007). Also, the proposed design will use a coded IDT with an 11-bit Barker BPSK code sequence, as is currently prevalent in IEEE 802.11 security protocols (Agilent Technologies, 2007). This 11-bit Barker code sequence will also have a maximum of 2,048 possible permutations (211 = 2,048).

As illustrated in Figure 1, the design will make use of one Tx PSAW correlator and one Rx PSAW correlator at each end of the transmission link. The Tx PSAW correlator will be used to encode a data bit stream before it is transmitted to the Rx PSAW correlator. This receiving correlator will have an identical, but reverse-oriented, coded IDT configuration for auto-correlation decoding of the data bit stream. It is proposed that the cipher key (IDT arrangement) of the Tx and Rx fingers be changed after a random number of data frames are sent. This random number will range from 0 – 10 and will be initiated by the Tx correlator and indicated to the Rx correlator by an 11-bit data stream piggybacked with the last transmitted frame sent. This 11-bit data stream will indicate the next 11-bit Barker code sequence that will be used by the Tx correlator. When the Rx correlator receives this cipher-change code it will send an ACK frame back to the Tx correlator, similar to a SSL cipher change confirmation procedure. Additionally, the Tx and Rx correlators will use timers to guard against lost or damaged cipher-change ACK frames. Once the cipher-change sequence is completed, both correlators will change their respective RF switches to the new cipher key configuration and resume encrypted data transfer.

The final parameters that must be clarified for the proposed PSAW correlator pair design is 1) substrate material, 2) the dimensions of the input/output IDTs, and 3) the dimensions of the coded IDTs. The proposed piezoelectric substrate will be ST-Quartz, based on its prevalence and suitability to pulse compression of bit streams per Table 1. Related to the last two parameters, Appendix A presents the dimensions of the proposed PSAW correlator pair design. The design dimensions depicted in this appendix are based on Equations 1 – 10 and presented in Appendix B.

Conclusion

Summary

This paper has presented an example of current security issues related to WiFi networks and proposed an encryption scheme to solve this problem. A brief review of acoustic surface waves, SAW transducers, PSAW devices and BPSK encoding were presented in order to lay a foundation for the proposed design solution of a PSAW correlator pair equipped with an 11-bit Barker code sequence for WiFi BPSK encryption applications. The critical parameters necessary in the design of this correlator pair were presented, including the selected substrate material, relevant equations, and the proposed design. At this stage of the author's research the design herein is only a proposed design. Further investigation is necessary to completely implement this design, as stated below.

Recommendations and Further Investigations

At this stage of the research, it is recommended that a more detailed investigation be made into the circuit requirements of the RF switches for dynamically re-arranging the coded IDT chips. This aspect of the design was not included in the research herein, but is necessary to implement the proposed design. This is recommended as a point of further investigation.

Additionally, it is recommended that the specific cipher-change protocol necessary for the proposed PSAW correlators be further investigated. This protocol is vitally important to the functionality of the proposed design. If this step of the data encryption process is flawed, the Rx PSAW correlator could lose the cipher key. This loss would be catastrophic and would inhibit accurate auto-correlation of the transmitted data.

References

Agilent Technologies. (2007, January 10). *RF Testing of WLAN Products: Application Note 1380-1*. Retrieved December 6, 2013, from Agilent Technologies Literature Website: http://cp.literature.agilent.com/litweb/pdf/5988-3762EN.pdf

ATMAE. (2013, January 1). *ATMAE Accreditation*. Retrieved June 19, 2013, from ATMAE: http://www.atmae.org/accred/2011OutcomesAssessmentModel01-14-13.pdf

Bari, J., & Ferdousi, B. J. (2012). Introducing Renewable Energy Courses in the Classroom and Online EECT Curriculum. *2012 ATMAE Conference Proceedings* (p. 73). Ann Arbor: ATMAE.

Campbell, C. (1989). *Surface Acoustic Wave Devices and Their Signal Processing Applications.* San Diego, CA, USA: Academic Press, Inc.

Constellation. (2013). *E2 Energy to EducateSM*. Retrieved July 6, 2012, from Constellation Energy Resources: http://www.constellation.com/community/pages/energy-to-educate-grants.aspx

Edmonson, P. J., & Campbell, C. K. (2012). *Patent No. US 8,099,048 B2.* USA.

Elder, J. L. (2009, October 30). *Higher Education and the Clean Energy, Green Economy*. Retrieved June 21, 2013, from Educause Web site: http://www.educause.edu/ero/article/higher-education-and-clean-energy-green-economy#

Elkordy, M. F., Elsherbini, M. M., & Gomaa, A. M. (2013). A comparative study of surface acoustic wave correlators . *African Journal of Engineering Research , 1* (1), 6-16.

Gallagher, D. R., Malocha, D. C., Puccio, D., & Saldanha, N. (2008). Orthogonal Frequency Coded Filters for use in Ultra-Wideband Communication Systems. *Ultrasonics, Ferroelectrics and Frequency Control, IEEE Transactions on , 55* (3), 696-703.

Malocha, D. C., Puccio, D., & Gallagher, D. (2004). Orthogonal frequency coding for SAW device applications. *Ultrasonics Symposium, 2004 IEEE , 2*, 1082-1085.

Morgan, D. (2007). *Surface Acoustic Wave Filters with Applications to Electronic Communications and Signal Processing.* (2nd, Ed.) Oxford, UK: Academic Press, Inc.

NREL. (2012, September 19). *MapSearch.* Retrieved June 19, 2013, from National Renewable Energy Laboratory: http://www.nrel.gov/gis/images/eere_pv/national_photovoltaic_2012-01.jpg

O'Toole, M. (2002). The relationship between employees' perceptions of safety and organizational culture. *Journal of Safety Research , 33* (2), 231-243.

Park, B., & Kim, N. (2013). A Study of Secure Communications in WiFi Networks. *The 2nd International Conference on Software Technology. 19*, pp. 35-37. ASTL.

Perahia, E., Yee, J., & Cordeiro, C. (2012, July). *Status of Project IEEE 802.11ad: Very High Throughput in 60 GHz.* Retrieved December 6, 2013, from http://www.ieee802.org/11/Reports/tgad_update.htm

President's Climate Commitment. (2013). *Home*. Retrieved June 21, 2013, from American College & University President's Climate Commitment Web site: http://www.presidentsclimatecommitment.org

Ramakrishna, H., & Ravi, K. (2011). A Study on Multi Wireless Technologies – Architectures and Security Mechanisms . *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives"* , 96-103.

Satoh, Y., Ikata, O., Miyashita, T., & Ohmori, H. (2012, March). RF SAW Filters. *International Symposium on Acoustic Wave Devices for Future Mobile Communication Systems* , 125-132.

Seybert, T. A. (2010). Using An Industrial Advisory Council For Student Outcomes Assessment: A Work In Progress. *The Technology Interface International Journal , 11* (1), 53-59.

Token. (2010). *Build a Custom Saw Component*. Retrieved December 6, 2013, from Token Passive Components Website: http://www.token.com.tw/saw/saw-devices.htm

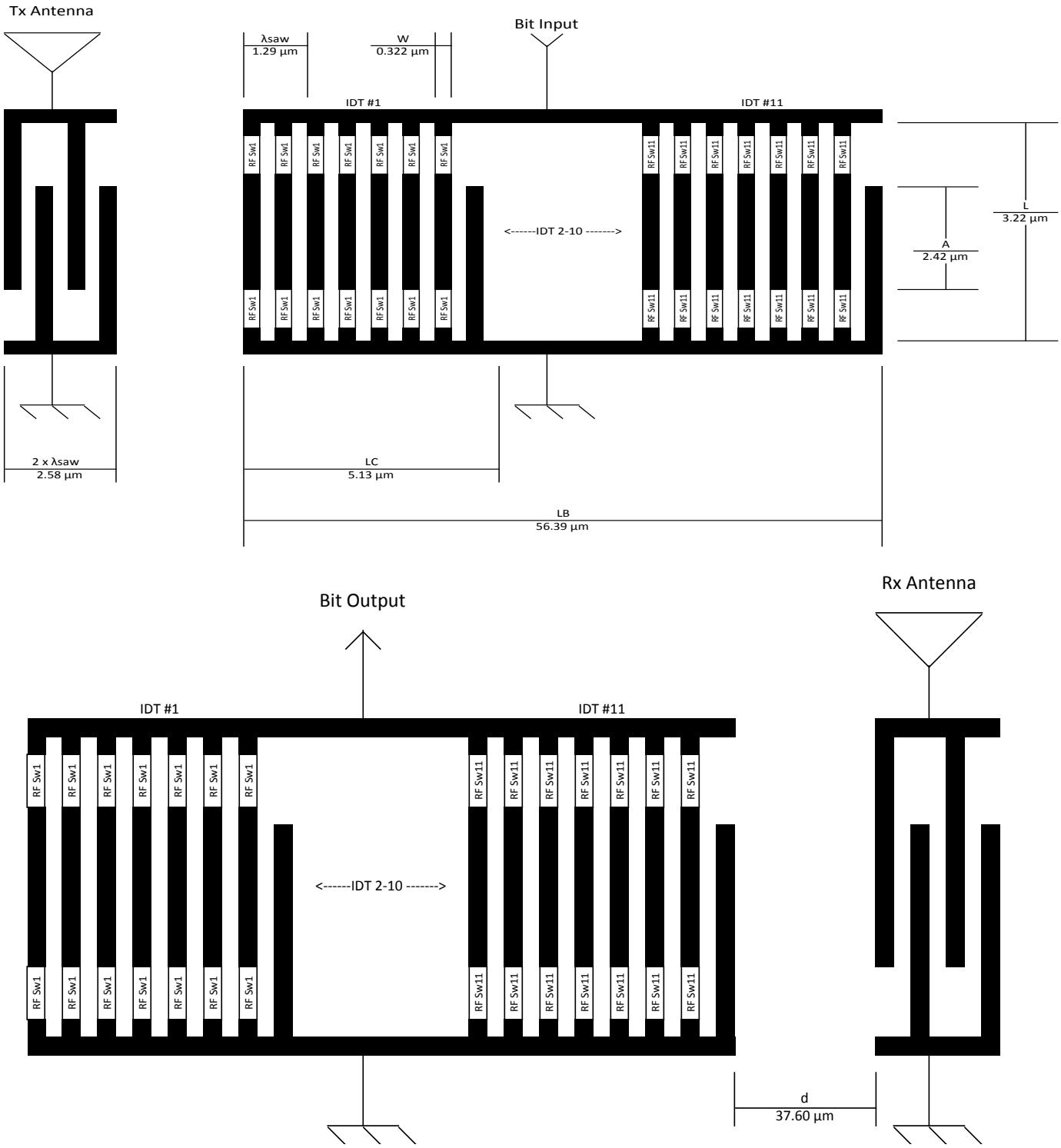
US Department of Energy. (2013). *DSIRE*. Retrieved July 6, 2013, from DSIRE Web site: http://www.dsireusa.org

US Department of Energy. (2013, April 23). *Home: LEDP*. Retrieved July 6, 2013, from Laboratory Equipment Donation Program Web site: http://www.osti.gov/ledp/index.jsp

US Government. (2013). *Find. Apply. Succeed.* Retrieved July 6, 2013, from Grants.gov Web site: http://www.grants.gov

Yildiz, F., & Coogler, K. L. (2012). Design And Development Of A Multiple Concept Educational Renewable Energy Mobile Mini-Lab For Experimental Studies. *International Journal Of Engineering Research And Innovation , 4* (2), 27-33.

Appendix A: PSAW Correlator Design



Appendix B: PSAW Correlator Design Calculations

Terms	Value	Units
Frequency (f)	2.45E+09	Hz
SAW Velocity ST Quartz (v)	3.16E+03	m/s
Speed of Light (c)	300.00E+06	m/s
No. Barker chips (j)	11.00	-
Bit Rate (bps)	56.00E+06	bps

Calculations

Bit Period (τB)	#bits	bps	τB	Units
τB = #bits/bps	1.00	56.00E+06	**17.86E-09**	**s**

Wavelength SAW	v	f	λsaw	Units
λsaw = v/f	3.16E+03	2.45E+09	**1.29E-06**	**m**

IDT Finger Width	λsaw	-	W	Units
W = λsaw/4	1.29E-06	-	**322.24E-09**	**m**

Total Length of Coded IDT	τB	v	LT	Units
LT = v*τB	17.86E-09	3.16E+03	**56.39E-06**	**m**

Distance Between IDT	Δϕ	λsaw	d	Units
d = ([1+(Δϕ/π)]λsaw)/2)	180.00	1.29E-06	**37.59E-06**	**m**

Chip Period	τB	j	τC	Units
τC = τB/j	17.86E-09	11.00	**1.62E-09**	**s**

Chip Length	τC	v	LC	Units
LC = v*τC	1.62E-09	3.16E+03	**5.13E-06**	**m**

Number IDT Fingers per chip	LC	W	Fchip	Units
Fchip = (LC/W)*0.5	5.13E-06	322.24E-09	**8.00**	**-**

Finger Length	W	-	L	Units
L = W*10	322.24E-09	-	**3.22E-06**	**m**

Apodization Length	L	-	A	Units
A = 0.75*L	322.24E-09	-	**241.68E-09**	**m**