IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 19-25
www.iosrjournals.org

Secure Key Generation over Noisy Fingerprints With Intruder Detection

Aparna A[1], Ajish S[2]

[1](Assistant Professor-Adhoc, College of Engineering Perumon , Kollam, Kerala, India) [2](Assistant Engineer, College of Engineering Perumon, Kollam, Kerala, India)

Abstract: *The design of a reliable and secure communication channel for the transfer of confidential data is one of the primary researched topics in the field of security. The most important entity in a secure communication process is the cryptographic key that is used for encryption and decryption purposes. The key used in such a process must be extremely strong so that it is untraceable to attackers. Many methods have been proposed for generating a secure key ranging from biometric techniques to that of the modern quantum cryptography. An innovative approach to generate a shared key between two users is to exploit the contextual information present in the environment the users are in. Many schemes have been proposed to generate a cipher key by processing the contextual audio features. Keys generated from contextual audio tend to possess a greater level of robustness and uniqueness. A common audio fingerprinting approach in connection with error correction codes and fuzzy cryptography provides a predefined noise threshold level. Even though the current techniques are successful in establishing a secure communication process between users in the same context, they are vulnerable to attackers from the same scenario. In this paper, we propose a new key generation scheme to build a secure communication channel between 2 users in the same environment. We also prove that the system is resistant to attacks from malicious users who are present in the same context.*

Keywords: *Audio Fingerprinting, Ambient Audio, Key Generation, Cryptography*

I. Introduction

One of the ever threatening problems in the field of communication is that the establishment of a secure communication channel. Nowadays a large number of people have enough knowledge about the underlying technology; thereby the chance for human impact on security also rises. There exists many possible ways to establish authentication between devices. One of the most widely used primitive approach, password based authentication causes many possible threats on security. Such problems can be eliminated up to certain extend by choosing contextual information as the seed for key generation. The environmental stimuli such as light, audio, RF Channel, proximity and temperature can be used as contextual information. Among that ambient audio is most widely used since it is a spatially centered context and that‘s why it offers more uniqueness among keys generated by each of the devices in a communication scenario.

The need for high security using these ambient audio like contextual information plays a vital role in the instances like highly confidential conference, meeting etc. The secret information sharing regarding all the participants in a communication scenario should be performing in a confidential way. Communication between group members, however should be guarded against access from external devices or individuals. For that each of the devices will records the ambient audio present in that environment.from a third party, it won't assure that the video remains untouched i.e., it won't rescue the video from tampering efforts. Tampering detection techniques can be implemented using data hiding schemes.

Capturing of audio for the purpose of key generation recorded by each of the devices should be synchronized to each other. This means when two participants Alice and Bob are willing to communicate securely with each other, Alice starts protocol by requesting a pairing with Bob. They should synchronize their absolute time by using any sufficiently accurate time protocols.

The major issue regarding this system is that if an intruder who is present in the same environment, he/she is also able to generate the same keys, which are generated by other authenticated participating devices. So choosing ambient audio alone as the criteria for shared key generation causes the situation become more feasible to an intruder or a third party. Incorporation of an attribute based encryption along with the existing scheme prevents such a problem up to certain extend. The technology like Face Recognition [1] consists of the user specific attributes also. Only the previously trained user in a specific communication environment is only considered as an authenticated user by verifying their face attributes.

The standard key generation schemes like AES, DES etc. provides enough security. Even though the proposed scheme demanded by highly confidential communication instances, it requires much more efficient

key generation scheme. Fractal Encryption key generation scheme, a probability based approach generate a set of keys instead of a single key generated by standard encryption schemes. The proposed system verifies the entire set of keys generated on the receiver side.

In the proposed scheme at no point in the protocol the secret itself or information that could be used to derive audio feature values is made public. Definitely there exists a problem like, even though a number of devices which are present in the same environment and records the audio simultaneously, there exists minute or large variation in the recorded sample due to the presence of noise. So we utilize error correction codes to account for noise in the feature vector. Device synchronization has great importance in this system, for that we need an accurately efficient time protocol.

II. Related Work

In the literature, several authors consider authentication among communicating devices based on different environmental stimuli [2], [3], [4], [5]. The entire context based key generation scheme follows a similar frame work [1] which consisting of five modules. Shaking processes from accelerometer data and RF Channel measurements have been utilized as unique context source that contains shared characteristic information.

The authors propose to utilize the accelerometer of the Smart-It [6] device to extract characteristic features from simultaneous shaking processes of two devices. Later, Mayrhofer and Gellerson presented an authentication mechanism based on this principle. According to the similar protocol [8] used by all of the participating devices to establish a common secret key, the authentication is possible only if all the devices are shaking simultaneously. The simultaneous shaking based authentication is unlikely for a third person trying to mimic the correct movement pattern remotely. The approach in which noisy acceleration readings are utilized to establish a secure communication channel among devices, they utilize a hash function that maps similar acceleration patterns to identical key sequences. The patterns generated by all participating devices should be similar and analyzed in a same way. When patterns are located at boarder of neighborhood regions, the tolerance for noise in the input is based on the direction of the center of this region. For the key generation, exponentially quantized Fast Fourier Transformation (FFT) coefficients of a sequence of accelerometer samples are utilized. It is also possible to utilize the noisy acceleration readings for establishing a secure communication channel among devices [9][3], a hash function is utilized for mapping to the identical key.

An error correction scheme is used to account for noise in the input data. By using error correction schemes it is possible to map any sequence within a predefined threshold of a hamming distance to a unique sequence for establishing a sufficient synchronization among nodes the Network Time Protocol (NTP) is used. RF Channel is another sensor class utilized for context based device authentication [5]. In the absence of interference and nonlinear components transmitter and receiver experience identical channel response [11], the information is utilized to generate a secret key among node pair. The channel characteristics are spatially sharply concentrated and not predictable [12] at remote locations there by the probability for prediction of behavior of the channel by an eavesdropper is comparatively lesser.

In secure mobile phone communication based on ambient audio, the microphone equipped with each of the mobile devices willing to establish a common key conditioned on ambient audio will capture synchronized audio samples. Each device then extracts the perceptual features of ambient audio and then computes a binary characteristic sequence for recorded audio. This sequence is unique for each of the captured audio samples with the surrounding noise and thereby the name audio fingerprint. These unique binary codes designed to fall on to a code-space of an error correcting code. In general, a fingerprint will not be exactly match with any other fingerprint generated from the same environment due to the presence of noise. Also the considered context, audio is spatially centered at particular instants. Fingerprints generated from similar ambient audio resemble but due to noise and inaccuracy in the audio sampling process, it is unlikely that two fingerprints are identical. Devices were utilizing their error codes for mapping fingerprints to corresponding code words. For the fingerprints which have the hamming distance within a certain predefined threshold, pointing to identical code words and then utilized as secure keys. The hamming distance between the fingerprints rises as the distance between devices increases.

Instead we utilize purely ambient audio to establish a shared cryptographic key among a set of devices participating in a specific communication context. We record NTP synchronized audio samples to generate characteristic audio fingerprint and map this to a unique secret key with the help of error correcting codes. With fuzzy-cryptographic schemes it is also possible to generate an identical key based on noisy input data [15]. The authors utilize a secure sketch [17] to produce public information about an input audio sequence without revealing it. The authors also established a fuzzy vault [19], [20] based key distribution, using data measured by devices worn on the human body.

III. Ambient Audio Based Encryption

Key aspect of audio based encryption is the audio fingerprinting. There exist mainly two aspects of audio fingerprinting. Most of the researchers think about audio fingerprinting in such a way that, in the applications like finding duplicates or tracks in a large database. In the concerned applications we are considering the music specific properties of audio like pitch, contour etc. As per the contextual view it is not enough to consider the structured audio only, due to the presence of noise. An error scheme in combination with Fuzzy Cryptography tolerates a specific amount of noise. The seed for shared key generation among devices are the ambient audio, an audio sequence that does not have any formal structures. For establishing a secure communication channel all devices should capture the contextual ambient audio and from that a fingerprint will be generated, which is a compact representation of the large audio stream recorded from the communication environment. For fingerprints with a hamming distance within the error correction threshold of the error correcting code the resulting code word are identical and then utilized as secure keys. Devices exploit the error correction capabilities of the error correcting code utilized to map fingerprints to code words.

The following sections provide an overview over audio acquisition and device synchronization, audio fingerprinting, Encryption using Fractal Keys, Error correction over cryptographic keys, implementation, problems and possible solutions.

3.1 Audio Acquisition and Device Synchronization

Framework introduced for context based key generation approach is similar for all contextual information like light, audio, temperature, RF Channel etc. One of the module which demands more importance in that framework is that the device synchronization. All devices in a considered communication environment should be synchronizing their clocks using similar time protocol. It requires a tight synchronization among devices, since audio is time dependent. Due to the frequent fluctuation of context, feature values taken from ambient audio at distinct time will likely not be sufficiently similar to establish a common secret among devices [pintext]. For synchronization any sufficiently accurate protocols like NTP [15] [16], the Precision Time Protocol(PTP) [17] or a similar protocol can be utilized on the existing system, we require much more exact time synchronization would reduce the computational complexity of the approach.

In the proposed scheme the first step involves the extraction of feature from a piece of audio. Yang presented a method to identify energy peaks in signal spectrum to extract a unique pattern [13], this scheme supported by a general framework presented by Yang [14].

To create fingerprints split up the entire sequence ‘S‘ into ‘n‘ frames each of equal length. Then on each frame a DFT weighted by a Hanning window is applied. After that each frames divided into ‘m‘ non overlapping frequency bands and computes sum of energy values on each band and stored in an energy matrix. Using this matrix a fingerprint ‘f‘ is generated from the energy matrix ‘E‘, where each bit describes the difference between two consecutive frames.

$$f(i,j) = \begin{cases} 1, & \big(E(i,j) - E(i,j+1)\big) - E(i-1,j) - E(i-1,j+1)) > 0 \\ 0, & otherwise \end{cases}$$

The Accoustid Chromaprint, a tool which used to extract the informal parameters of audio stream to generate a unique fingerprint, chroma features are extensively used in a number of music retrieval applications. Acoustic fingerprinting is a technique for identifying songs from the way they sound rather from their existing previously collected metadata. This plugin uses an open-source fingerprinting technology called Chromaprint and its associated Web service, called Acoustid. First, it can be trickier to set up the native fingerprinting library, whereas the entire beets core is written in pure Python. Also, fingerprinting takes significantly more CPU and memory than ordinary tagging which means that imports will go substantially slower.

Chroma features are used as indexes for a collection of classical music recordings. These recordings are stored in a database system, and are used to create statistical models aimed at identification of input sequences. The basic idea is that information retrieval techniques can be generally employed outside the textual domain, because the underlying models are likely to be shared by different media [13]. Chroma features are considered as pointers to the recordings they belong to, playing the same role of words in textual documents. The information on the time position of chroma features is used to directly access to relevant audio excerpts that we are inputs. The major advantage is that this index terms accessing only requires logarithmic or even constant time. Once the chroma vector is computed for a window of the signal,we proposed to compute its rank-based quantization q(i) through the following rule,

$$q(i) = \begin{cases} rank[c(i)], & rank[c(i)] \leq k \\ 0, & elsewhere \end{cases}$$

where k is the number of quantization levels that are taken into account and rank[c(i)] is a function that outputs the rank of the value of the energy in pitch class i over the values of the whole array, that is rank[c(j)] = 1 if pitch class j has the highest energy and so on. These computations are followed by the steps like feature extraction from audio query, locality sensitive hashing, HMM based identification etc.

3.2 Unique Codeword Mapping using Reed Solomon Error Correction Scheme

A perfect match in fingerprints is unlikely since devices are spatially separated, not exactly synchronized with each other. Even though a number of devices which presented in a similar environment and records the contextual audio simultaneously, definitely there will be minute or large variations in fingerprints generated by each of the devices due to the presence of noise. The system should satisfy the requirement of a unique code word sequence for particular environments. The Reed-Solomon error correction scheme is most suitable for such a requirement. In coding theory, the Reed–Solomon code belongs to the class of non-binary cyclic error-correcting codes. The Reed–Solomon code is based on univariate polynomials over finite fields. It is able to detect and correct multiple symbol errors. By adding ‘t‘ check symbols to the data, a Reed–Solomon code can detect any combination of up to ‘t‘ erroneous symbols, or correct up to ‘t/2’ symbols. As an erasure code, it can correct up to ‘t‘ known erasures, or it can detect and correct combinations of errors and erasures. Furthermore, Reed–Solomon codes are suitable as multiple-burst bit-error correcting codes, since a sequence of b + 1 consecutive bit errors can affect at most two symbols of size ‘b‘. The choice of ‘t‘ is up to the designer of the code, and may be selected within wide limits. A Reed-Solomon code is specified as RS(n, k) with s-bit symbols. This means that the encoder takes k data symbols of s bits each and adds parity symbols to make an n symbol codeword. There are n-k parity symbols of s bits each. A Reed-Solomon decoder can correct up to t symbols that contain errors in a codeword, where 2t = n-k.

3.3 Encryption using Fractal Encryption Key Generation Scheme

Security is the major concern in the set of communication scenarios. In the proposed system we are considering the contextual information for the purpose of key generation among the participating devices. Due to the spatially centeredbehavior of contextual audio, it offers more uniqueness regarding the generated keys. It is convenient to utilize the standard encryption schemes like DES, AES etc. The system demanding higher security requires much more complicated and efficient encryption scheme. A probability based key generation scheme, Fractal Encryption Key Generation associated with a set of keys instead of a single key generated by the standard encryption schemes. The major motivation of using fractal encryption is to reduce the computation cost and increase the security for the public-key systems, and this leads us to propose new public-key cryptosystem based on Fractal.

Fractal Encryption Key Generation is most widely used in cryptography for the image security, the algorithm is quantum safe (can't be broken with a quantum computer, unlike many commonly-used algorithms) . The fractal research field, explored image encryptions also. The common method is using the fractal keys generated from the corresponding field directly. There is a proposed method of encrypting a Mandelbrot set with the RSA method and Elliptical curve [5]. Liu studied a novel fractal cryptographic algorithm based on a fractal model and fractal dimension [6]. Rozouvan encrypted an image with the transformed Mandelbrot set [7]. In case of image encryption the original picture for matrix multiplication with the fractal image [8] will be compressed. There is a Mandelbrot set and the Hilbert transformation to generate the random key [9]. Encrypted the image by assembling the fractal image additional method and the binary encoding method [10].

Many conventional fractal-based encryption methods are combined with fractal coding compression or treat the fractal image as a host image to hide some information, e.g., keys. For the former, fractal coding operation itself may bring the time consumption. This will result in reducing efficiency of the algorithm. For the latter, usually the key length is invariant, which is not flexible and may have some restrictions in the encryption. To meet these challenges, we propose a novel image encryption algorithm. The algorithm uses several parameters to generate the keys with the same size as the plain images and has a good efficiency in the encryption. Firstly, we generate a Julia set and scramble it with the Hilbert curve in bit-level, and then make the scrambled Julia set modulo with the plain image. Finally, the cipher image is obtained by diffusion process. The Julia set is a classical set in fractal theory and can be calculated by several parameters iteratively. For this property, the key is much easier to store and transmit. What‘s more, the Julia set has the infiniteness and the chaotic features, so tiny changes of the parameters will lead to dramatic changes of the cipher image. In addition, the diffusion process guarantees that if one pixel value changes, then all the pixels will change, which makes the algorithm resist the chosen plaintext attack effectively.

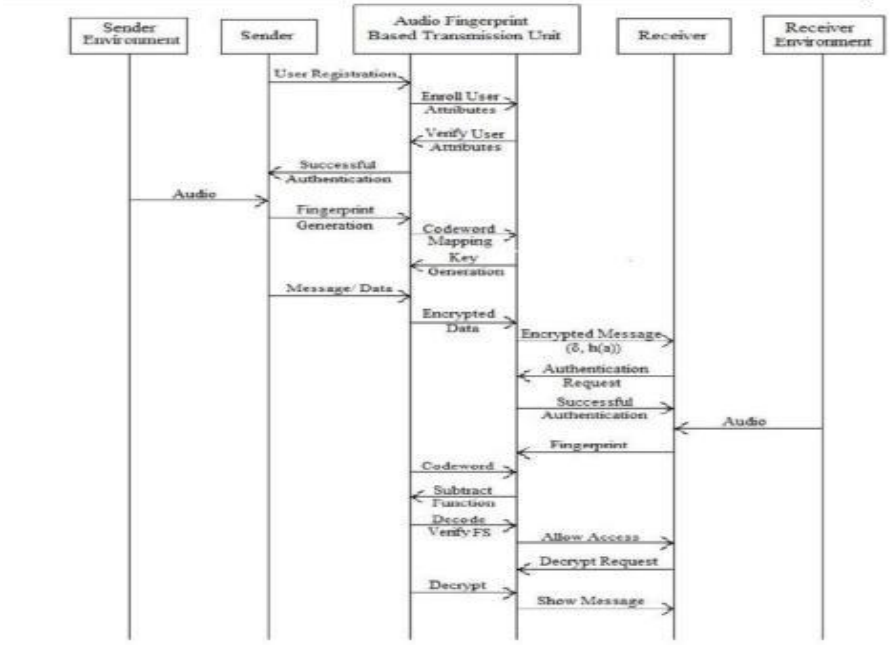

Figure – 1: Workflow of the proposed system

All fractal mappings that I know are not strictly 1 to 1. This is a good reason to believe that for this encryption scheme there is no efficient way to break the code. The fractal is used as a "master key" to enable simultaneous generation of "local" or "sequential" keys that are then used to encrypt and decrypt the actual messages. When we want to encrypt a message the message will be continuously encrypting the resultant message iteratively.

3.4 Fractal Decryption

Fractal encryption allows encryption of any kind of information like audio files, video files, word documents, simple text files, images etc. The encryption performs in some complicated manner like at each time particularly selects the keys from key set generated from the contextual information. The information what to be send will be continuously encrypted until the key set completely utilizes. Decryption of encrypted message is possible only for an authenticated receiver. A participating device results in a successful authentication if and only if they are present in the same environment in which the sender is present.

Table 1. Authorization and un-authorization scenarios of the system

Environment	Ambience	IP Range	Authorized/ Unauthorized
Yes	Yes	No	Unauthorized
Yes	No	No	Unauthorized
No	Yes	No	Unauthorized
Yes	Yes	Yes	Authorized

IV. Factors Incorporated For Intruder Detection

Face Recognition: Major problem regarding the system is that finding out the intruder who present in the same ambience in which the communication takes place. In the present system the only attributes which are under consideration are the user id and password only. The system becomes much more efficient if we are considering the attribute face also. The administrator will be train the faces of all possible participants in a certain scenario previous to the communication starts. During the time of login along with the basic attributes face also verified against the trained faces stored in the database.

Predefined IP Address Range: Only the codewords of Levels within P-frames are modified for data hiding. Simulation results have demonstrated that we can embed the additional data with a large capacity into P-frames while preserving high visual quality. PSNR (Peak Signal to Noise Ratio) have been adopted to evaluate

the perceptual quality of the video. The observations are tabulated below. The observations are tabulated based on the foreman standard video sequence.

V. Experimental Results and Evaluation

The standard encryption scheme utilized in present system is the AES. In proposed scheme we are incorporating the probability based fractal encryption scheme. Comparing to other encryption scheme passes through 1000 iterations. Instead of a single key used for encryption in AES, fractal encryption associates with a set of keys.

The security regarding fractal encryption is very high in comparison with the other schemes since the secure message or information passes through multiple encryptions by using all keys present in the set. For evaluating the time is taken as factor for these two schemes for both encryption and decryption. The results are shown as under using the graphical data obtained from the experiments.

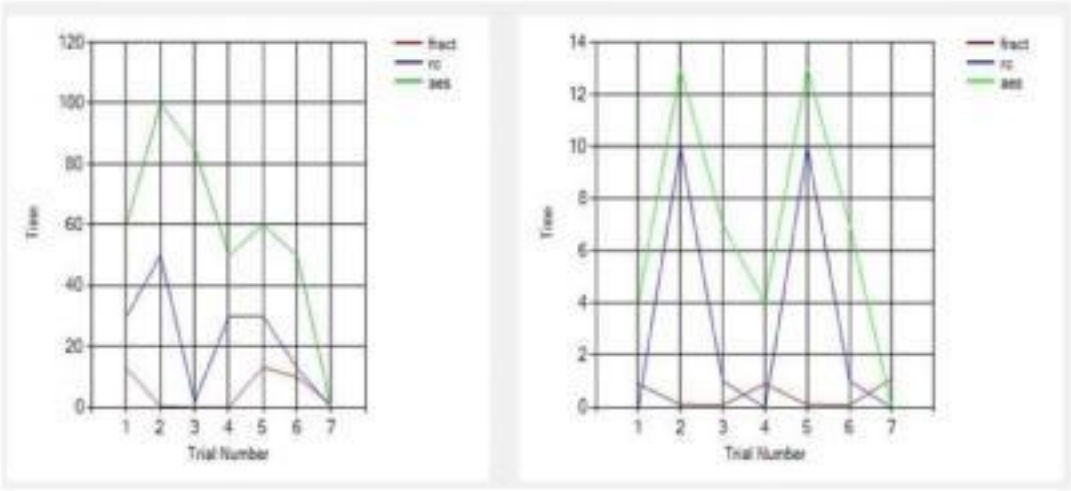

Figure 2: Experimental Analysis

References

[1] DominikSchurmann and Stephan Sigg, Member, IEEE Computer Society, ―Secure Communication on Based on Ambient Audio‖, IEEE Transactions On Mobile Computing, Vol. 12, No. 2, February 2013.

[2] R. Mayrhofer and H. Gellersen, ―Spontaneous Mobile Device Authentication Based on Sensor Data,‖ Information Security Technical Report, vol. 13, no. 3, pp. 136-150, 2008.

[3] D. Bichler, G. Stromberg, M. Huemer, and M. Loew, ―Key Generation Based on Acceleration Data of Shaking Processes,‖Proc. Ninth Int'l Conf. Ubiquitous Computing, J. Krumm, ed., 2007.

[4] L.E. Holmquist, F. Mattern, B. Schiele, P. Schiele, P. Alahuhta, M. Beigl, and H.W. Gellersen, - Smart-Its Friends: A Technique for Users to Easily Establish Connections Between Smart Artefacts,‖Proc. Third Int'l Conf. Ubiquitous Computing, 2001.

[5] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, ―Amigo: Proximity-Based Authentication of Mobile Devices,‖ Int'l J. Security and Networks, vol. 4, pp. 4-16, 2009.

[6] H.-W. Gellersen, G. Kortuem, A. Schmidt, and M. Beigl, ―Physical Prototyping with Smart-Its,‖IEEE Pervasive Computing, vol. 4,pp. 10-18, 2004.

[7] Kumar S (2006) Public key cryptographic system using Mandelbrot sets. Military Communications Conference in Washington DC, 1–5.

[8] WT, Sun WS (2008) Application of Fractal theory in cryptographic algorithm. Journal of China Acadamy of Electronics and Information Technology 3: 580–585 (In Chinese).

[9] Rozouvan V (2009) Modulo image encryption with fractal keys. Optics and Lasers in Engineering 47: 1–6

[10] Lock AJJ, Loh CH, Juhari SH, Samsudin A (2010) Compression-encryption based on fractal geometric. Second International Conference on Computer Research and Development. 213–217.

[11] Sun YY, Kong RQ, Wang XY, Bi LC (2010) An Image Encryption Algorithm Utilizing Mandelbrot Set. International Workshop on Chaos-Fractal Theories and Applications. 170–173.

[12] Lin KT, Yeh SL (2012) Encrypting image by assembling the fractal-image addition method and the binary encoding method. Optics Communications 285: 2335–2342

[13] C. Yang, ―MACS: Music Audio Characteristic Sequence Indexing for Similarity Retrieval,‖ Proc.IEEE Workshop Applications of Signal Processing to Audio and Acoustics, pp. 123-126, 2001.

[14] C. Yang, ―Efficient Acoustic Index for Music Retrieval with Various Degrees of Similarity,‖ Proc. 10th ACM Int'l Conf. Multimedia (MULTIMEDIA '02), pp. 584-591, http://doi.acm.org/10.1145/641007.641125, 2002.

[15] D. Mills, J. Martin, J. Burbank, and W. Kasch, ―Network Time Protocol Version 4: Protocol and Algorithms Specification,‖ IETF RFC 5905, http://www.ietf.org/rfc/rfc5905.txt, June 2010.

[16]. D.L. Mills, ―Improved Algorithms for Synchronising Computer Network Clocks,‖ IEEE/ACM Trans. etworking, vol. 3, no. 3, pp. 245-254, June 1995.

[17] S. Meier, H. Weibel, and K. Weber, ―IEEE 1588 Syntonization and Synchronization Functions Completely Realized in Hardware,‖Proc. IEEE Symp. Int'l Precision Clock Synchronization for Measurement, Control and Comm. (ISPCS '08), 2008.