Inclusion of Priority Access in a Privacy-preserving ESC-based DSA System

Chang Lu

Thesis submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Computer Engineering

Yaling Yang, Chair

Allen B. MacKenzie

Walid Saad

July 10, 2018

Blacksburg, Virginia

Keywords: Dynamic Spectrum Access, Homomorphic encryption, Privacy-preserving, Three-Tiered Frame

Inclusion of Priority Access in a Privacy-preserving ESC-based DSA System

Chang Lu

(ABSTRACT)

According to the Federal Communications Commission's rules and recommendations set forth for the 3.5 GHz Citizens Broadband Radio Service, a three-tiered structure shall govern the newly established shared wireless band. The three tiers are comprised of three different levels of spectrum access; Incumbent Access, Priority Access and General Authorized Access. In accordance and fulfillment with this dynamic spectrum access framework, we present the inclusion of Priority Access tier into a two-tiered privacy-preserving ESC-based dynamic spectrum access system.

Inclusion of Priority Access in a Privacy-preserving ESC-based DSA System

Chang Lu

(GENERAL AUDIENCE ABSTRACT)

With the development of wireless communication technologies, the number of wireless communication reliant applications has been increasing. Most of these applications require dedicated spectrum frequencies as communication channels. As such, the radio frequency spectrum, utilized and allocated for these wireless applications, is depleting. This problem can be alleviated by adopting dynamic spectrum access schemes. The current static spectrum allocation scheme assigns designated spectrum frequencies to specific users. This static frequency management approach leads to inefficient frequency utilization as the occupation of frequency channels may vary depending upon time periods. Dynamic spectrum access schemes allow unlicensed users opportunistic access to vacant spectrum spaces. Thus, the adoption of these spectrum sharing schemes will increase the efficiency of spectrum utilization, and slow down the spectrum depletion. However, the design and implementation of these schemes face different challenges. These spectrum sharing systems need to guarantee the privacy of the involved parties while maintaining specific functionalities required and recommended by the Federal Communications Commission. In this thesis, we present the inclusion of a three-tiered frame, approved by the Federal Communications Commission, into a privacy-preserving dynamic spectrum system.

Dedication

This thesis is dedicated to my family and my friends, without them I wouldn't have come this far.

Acknowledgments

First and foremost, I would like to express my most sincere gratitude to Dr. Yaling Yang, my advisor. Her guidance and support have been most valuable and instrumental in my work. Without her help, I couldn't have completed my work. I would also like to express my sincere gratitude to Dr. MacKenzie and Dr. Saad. I much appreciate your advice and guidance.

Secondly, I would like to thank my research lab mates. Their help and support have made my research work and my graduate life much more relaxed and memorable.

Finally, I would like to thank my family and my friends. Their unconditional love and support have kept me going and striving for more significant achievements.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this thesis, we present the inclusion of three-tiered frame structure system into a privacy-preserving Exclusion-Zone based dynamic spectrum access system. The privacy-preserving Exclusion-Zone based dynamic spectrum access system guarantees Incumbent Users' location privacy against untrusted spectrum access system. The three-tiered frame inclusion fulfills the Federal Communications Commission's recommendation set forth for the newly established 3.5 GHz Citizen Radio Broadband Service. Our inclusion of three-tiered frame into the privacy-preserving Exclusion-Zone based dynamic spectrum access system will ensure correct spectrum access rights to corresponding parties while also maintaining Incumbent User's privacy guarantees.

1.1 General Background

Since the introduction of wireless communication technology, our society has fundamentally changed. The introduction of the mobile phone has significantly increased the connectivity between individuals to the rest of the society. The utilization of satellites in the Global Positioning System helps us to accurately position and track our movements. Radio and television have reshaped the way we receive information and spend free time. These are just a few examples of the wireless communication application. With continuous development, more and more wireless communication applications will be introduced and embedded into

our everyday life. Wireless communication will become more prominent and more inseparable from our society. However, these advancements come at a cost. An individual wireless communication application requires a unique wireless frequency as a communication channel. As the number of active applications increases, more and more frequencies are needed. Since the frequency spectrum is fixed and finite, the frequency spectrum is becoming more crowded. Looking at figure 1.1, the U.S. spectrum allocation chart provided by the National Telecommunications and Information Administration, we can observe that most of the frequency spectrum space has already been allocated for existing applications. There is little space left for future applications. As a common belief, many people believe we are running out of frequency spaces. While the number of unallocated frequency space is decreasing, the idea that we are running out of frequency spaces is not entirely accurate.

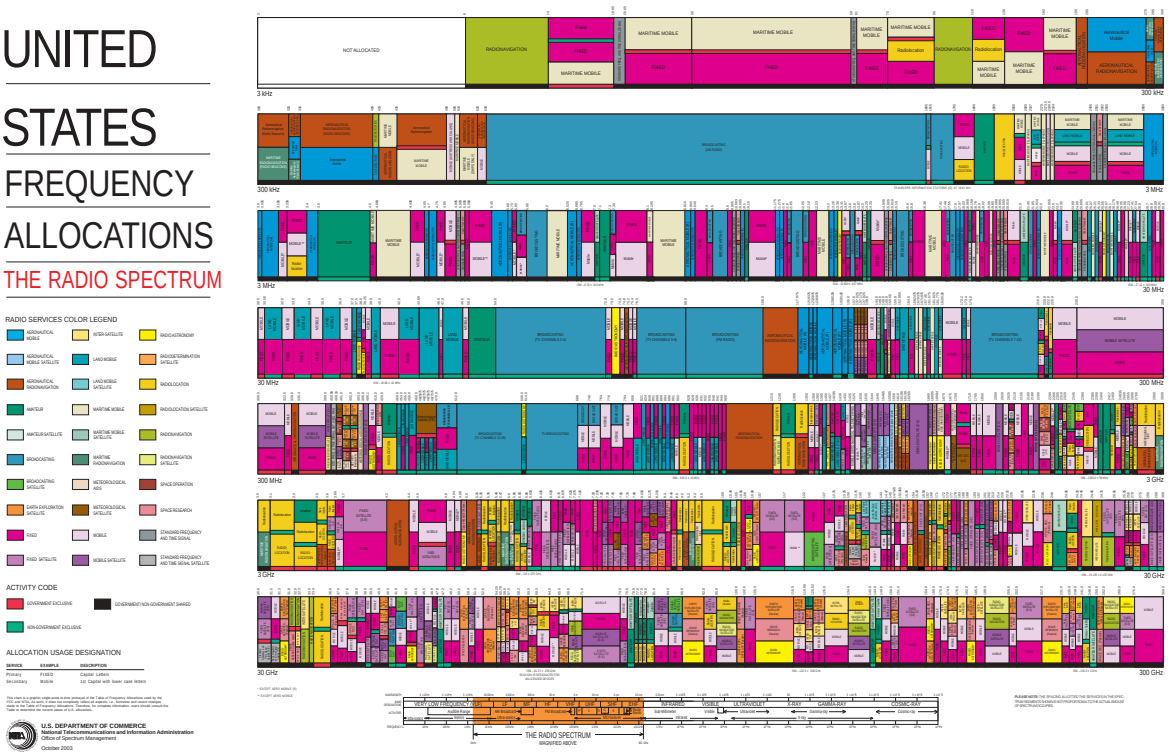

Figure 1.1: U.S. spectrum allocation chart. Source: NTIA

1.2 Static Spectrum Allocation

Currently, all frequency spectrum accesses for wireless communication in the U.S. are governed by the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The FCC administers non-federal spectrum usages, and the NTIA regulates federal spectrum usages. Under these two agencies' regulations, the frequency spectrum is allocated statically. Frequency bands are "designated for use by one or more terrestrial or space radiocommunication services or the radio astronomy service under specified conditions" [1]. This static spectrum allocation scheme is analogous to a parking reservation policy where each parking space in a parking lot is designated to a specific car. Following this static spectrum allocation scheme, frequency bands are dedicated to specific licensed users. As the number of frequency band users increases, the frequency spectrum will eventually deplete. While this static spectrum allocation scheme has been serviceable, it is by no means an efficient one. According to FCC Spectrum Policy Task Force's "Report of the Spectrum Efficiency Working Group" in 2002 and FCC's following "Et docket no 03-222 notice of proposed rulemaking and order" in 2003 [2, 3], the current spectrum utilization of allocated frequency bands varies greatly. The FCC Spectrum Policy Task Force observed that some spectrum frequencies have continuous occupancies, such as frequencies used by television broadcasting and cellular base stations. However, there are other spectrum frequencies with more dynamic occupancy. Dependent upon the nature of the wireless communication application to which a spectrum frequency is allocated, the occupancy of the allocated frequency may vary. Similar to a parking space of an office building, a spectrum frequency may be occupied during the day and become utterly vacant during the night. This variation in the utilization of the spectrum under the current static allocation policy creates inefficient frequency spectrum utilization. While a frequency may be left idle for hours by the authorized user, other users who desire this frequency at the very duration

of its vacancy are barred from accessing the frequency.

1.3 Dynamic Spectrum Access

As the demand for spectrum frequency grows continuously, the issue of inefficient spectrum utilization become more urgent. Dynamic Spectrum Access solves the spectrum utilization inefficiency problem and alleviates the crowding of the spectrum. Dynamic Spectrum Access (DSA) is a scheme "standing for the opposite of the current static spectrum management policy" [4]. Under the DSA scheme, unlicensed secondary users (SUs) are provided opportunistic access to allocated spectrum under the constraint that SUs will not cause any harmful interference to the spectrum license holding incumbent users (IUs). The DSA outlines a flexible spectrum sharing scheme as recommended by the FCC in the "Spectrum Task Force" report [5]. This flexible spectrum sharing scheme dramatically improves the spectrum utilization efficiency and satisfies some spectrum demands.

Under the broad definition of DSA, various spectrum management structures and schemes have been proposed. One prominent scheme amongst all the spectrum management schemes is a central server-driven structure. This server-driven spectrum access system employs a central server as a central allocation entity. The central spectrum access system (SAS) would first obtain IUs' operation information such as location and frequency. Basing on the IUs' operation information, SAS then authorizes or deny SUs' access to individual spectrum frequencies following a set of spectrum access policy. The spectrum access policy adopted by a SAS dictates the specific constraints under which SUs may or may not be authorized to a specific spectrum frequency. A spectrum access policy is structured around a principle spectrum sharing method. Two existing principle spectrum sharing methods are exclusion zone and protection zone. In an exclusion zone method, SAS keeps and maintains a rela-

tively static database. This database defines certain spaces within the spectrum frequency space to be exclusion zones where no SUs are allowed to occupy under any circumstances. On the contrary, a SAS server under a protection zone method doesn't produce and rely on a set of rigid exclusion zones. In a protection zone method scheme, SAS keeps tracks of each IU's interference threshold. Alongside the interference thresh holds, SAS also keeps a list of interference aggregates of each frequency space. When an SU requests a certain frequency space, the SU will submit its operation information to the central server. SAS then calculates the SU's interference to the IUs and add this interference to the interference aggregate of the corresponding spectrum space. If the addition result exceeds IUs' interference thresh holds, the SU's request is rejected; otherwise, the SU's request is authorized, and the new interference aggregate replaces the old one [6].

In 2015 the FCC established the 3.5 GHz band as the Citizens Broadband Radio Service for shared wireless broadband use following the adoption of the "Report and Order and Second Further Notice of Proposed Rulemaking" [7]. This new Citizens Broadband Radio Service defines a development and testing ground for DSA server-driven schemes. The FCC defines the 3.5GHz band "is governed by a three-tiered spectrum authorization framework to accommodate a variety of commercial uses on a shared basis with incumbent federal and non-federal users of the band. Access and operations will be managed by a dynamic spectrum access system, conceptually similar to the databases used to manage Television White Spaces devices. The three tiers are Incumbent Access, Priority Access, and General Authorized Access" [8]. In the "Report and Order and Second Further Notice of Proposed Rulemaking" under section G, Incumbent Protection, FCC stated that the list of Federal incumbent applications operating in the 3.5 GHz band includes high confidential applications such as defense applications from the Department of Defense (DoD). Due to the confidential, sensitive nature of such incumbent application, FCC proposed and recommended the central SAS maintains a database of Exclusion Zones (EZones) [7].

1.4 Challenges

While DSA schemes are very promising in their capabilities to increase spectrum utilization efficiency and alleviate the current spectrum crowding problem, there exist some challenges associated with developing and implementing these DSA schemes.

1.4.1 Information Security

For a SAS server to operate accurately and efficiently as recommended by FCC, the SAS server would require specific operation parameters from both the IUs and the SUs. This disclosure may lead to certain security violations for both IUs and SUs. According to FCC's "Shared Commercial Operations in the 3550–3650 MHz Band" document, SAS servers may be operated by commercial third parties for scalability [9]. Since IUs may include military and defense applications, allowing a commercially operated SAS server to obtain operation information from IUs may lead to the leakage of classified information. Even if SAS servers are operated by federal agencies or by total trustworthy entities, SAS servers may still be targeted and attacked by malicious adversaries.

1.4.2 Three-tiered Frame

According to FCC Citizens Broadband Radio Service rules, the SAS server should implement and employ an innovative three-tiered spectrum management frame [7, 8]. The three tiers include Incumbent Access from IUs, Priority Access from authorized SUs and General Authorized Access from general SUs. Incumbent Access is the top tier access channel that is protected from any SU interferences. Priority Access is the second middle tier which is granted to Priority Access Licenses (PAL) holders. PAL is assigned to individual SUs

through competitive bidding. Priority Access is exclusive access that is protected from non-PAL users' interference given that the channel access doesn't interfere with any Incumbent Access. The third and last tier is the Generalized Authorized Access (GAA). GAA has no protective benefits; all GAA channel are subject to spectrum sharing with other GAA SUs.

1.4.3 Priority Access Registration

When a PAL user requests and receives a Priority Access spectrum channel from SAS, this channel should be protected from access requests from any GAA users and any other PAL users. Once a registered channel is no longer in use, corresponding PAL user must inform the SAS. If a PAL user fails to make contact with SAS within seven days, the registered channel will be relieved of its Priority Access protections. As such, PAL users may extend their current registrations within seven day periods of registration confirmation [10]. Under these FCC regulations, SAS server should develop and implement a set of protocol to facilitate the aforementioned functionalities.

1.5 Contributions

In previous research and development, we were able to design and implement a privacy-preserving Exclusion-zone based DSA system called PriDSA. In this PriDSA system, we can achieve standard semantic privacy as well as individual privacy for IUs with untrusted SAS that may collude with SUs. To guarantee IUs' privacy in an untrusted environment, we implemented and introduced multiple different security measures. This collection of security measures is complex in design and implementation, but it is also relatively efficient in its maintenance and service in comparison to some of the other proposed systems.

While PriDSA provides sound and efficient security guarantees for IUs in an untrusted environment, it also has certain aspects that need improvements. First, PriDSA is a two-tiered system; it only facilitates IUs access and GAA. Second, in the absence of PAL tier, PriDSA doesn't include any structure that facilitates the registration and renewal of Priority Access channels for PAL users. Basing on PriDSA, this thesis propose the following contributions:

1. We propose a three-tiered structure to incorporate and facilitate Priority Access for PAL users. Priority Access channels established for PAL user will be exclusive and protect against other spectrum requests made by PAL holding SUs and general SUs. Priority Access request will be authorized if and only if the requested frequency doesn't reside in any IU Exclusion Zone and is not protected by any active Priority Access registration made by other PAL holders. Within the proposed three-tiered structure, we also implement security measures to validate each Priority Access registration.

2. We introduce a registration and renewal system that allows PAL users to register and renew their Priority Access registration for a spectrum frequency. The system includes security protocols to prevent impostures and collisions. In designing and implementing this renewal system and the aforementioned three-tiered structure, we ensure IU's privacy guarantees will not be compromised. We will maintain IUs's operation data to be isolated from any contamination. Encryptions and blindings will consistently protect IUs's operation data.

Chapter 2

Related Work

With increasing exploration and development of SAS driven DSA systems, privacy issues become more and more prominent. Due to DSA's nature of spectrum sharing, IUs are required to share their operation information with SAS for the SAS to service querying SUs accurately and efficiently. However, IUs may include privacy sensitive government applications such as military service and defense applications. For instance, in the US, the FCC defines the IUs to include military satellites services applications [7]. In Europe, 2.3-2.4 GHz frequency band under Licensed Shared Access regime (LSA) facilitates frequency sharing between mobile broadband and IUs. The list of IUs subject to frequency sharing within the 2.3-2.4 GHz frequency band includes government applications such as military airborne telemetry applications [11]. Due to the privacy sensitivity of these aforementioned government IUs, the operation information of these applications is often labeled as classified information that can't be compromised. Under the assumption that SAS servers may be commercially operated, SAS servers can't be fully trusted with IUs' operations information. SAS servers would need to operate without true knowledge of IUs' operation information to ensure the integrity of IUs' operation information while also guaranteeing the efficiency and accuracy of the system.

2.1 Obfuscation

One way of preserving IUs' privacy, namely their geographical operation location, is by introducing obfuscation to the true information. "Obfuscation is a technique to protect user privacy by altering the location of the users while preserving the capability of the server to compute few mathematical functions which are useful for the user over the obfuscated location information" [12]. There are many different techniques for applying obfuscation; for example, there are Spatial Discretization, K-Anonymity, and Decimal Rounding [13]. In application to DSA schemes, obfuscations are often introduced on to SAS's database of IUs' operation information as explored in [14, 15, 16]. When applying obfuscation to the location information of IUs, false positives, fake IU locations, are added into SAS's IUs' operation information database. These false positives distort and mask the true IUs' locations such that SAS has no knowledge of IU(s) true location information. Another advantage of applying obfuscations in DSA systems is that obfuscations can help to counter inference attacks. Inference attack is an attack on SAS's database [14]. The attacker assumes the identity of an SU and repeatedly queries SAS for spectrum access at different locations. From the series of SAS's query responses, the attacker can log and map protected locations. With large enough number of queries at various locations, the attacker and infer SAS's IU location database. From this inferred location database, the attacker can then map and deduce high probabilistic areas where IU(s) may be located. By applying obfuscations to SAS's database, an attacker can only obtain the obfuscated location information from SAS. Since the obfuscated location information contains false positives, the attacker is prevented from correctly inferring the true location(s) of IU(s).

However, the benefits of applying obfuscations come at a price. Obfuscation techniques introduce false positives locations to the true IU location database. By doing so, the introduced false positive locations are also protected from non-malicious general SUs. This

decreases the number of available spectrum spaces for the SUs to access and utilize, and thus reducing the system's overall frequency sharing efficiency. As such, the beneficial privacy protection provided by obfuscations exists as a trade-off against the systems frequency sharing efficiency. Increasing number of introduced false positives leads to higher privacy protection and lower spectrum sharing efficiency [17].

2.2 Homomorphic Encryption

Another method that can ensure IUs' privacy is encryption. Encryption techniques ensure the integrity of IUs operation information by encrypting the operation information into ciphertext. When the communication link between SAS and IUs is compromised, the attacker would only be able to obtain the encrypted ciphertext. However, traditional encryption schemes require the ciphertext to be decrypted before a service party can correctly carry out any operation on the information. Implementation of such traditional encryption scheme in a SAS driven DSA system would mean that the SAS server will have access to the unencrypted plain-text IUs' operation information.

Fortunately, not all encryption schemes suffer such downfall. Homomorphic encryption is first introduced in 1978; in [18] the term homomorphism is introduced to describe "possible solution to the computing without decrypting problem" [19]. Homomorphic encryption schemes allow third party service providers to correctly carry out a set of defined operations on encrypted message without decrypting the message.

Definition 2.1. An encryption scheme is called homomorphic over an operation $*$ if it supports the following equation:

$$E(m_1) * E(m_2) = E(m_1 * m_2), \forall m_1, m_2 \in M, \tag{2.1}$$

where E is the encryption algorithm and M is the set of all possible messages [19].

The application of homomorphic encryption schemes in SAS driven DSA systems has been explored in numerous proposals [20, 21]. In these proposals, IU location information is encrypted using a homomorphic cryptosystem. SAS perform spectrum allocation computation by applying defined homomorphic operations on encrypted IU location information ciphertext. Since SAS has no access to IUs' location information in plaintext, IUs' privacy is preserved regardless of SAS's trustworthiness.

2.3 Proxy Re-encryption

With homomorphic encryption schemes, SAS can safely perform defined operations upon IUs' encrypted location data. Once the operations are carried out by the SAS, SAS maintains a database of IUs' Exclusion-zones. Now, a question arises; how can SAS send a frequency allocation reply to an SU in the form such that SU can decrypt the reply all the while SAS itself cannot do so. One simple way of doing so is to give SUs the ability to decrypt IU encrypted ciphertext. However, such an approach would lead to the possibility of the leakage of classified information as SUs can obtain individual IUs' location information by listening to IUs' communication to SAS. Another more secure approach is to give SAS the ability to re-encrypt the allocation reply from IUs' encryption ciphertext to another encryption ciphertext such that SUs can decrypt this re-encrypted ciphertext with their decryption keys. This process is called proxy re-encryption.

Proxy re-encryption allow a semi-trusted proxy service party to re-encrypt a ciphertext encrypted under the public key of an entity, A, into another ciphertext under the public key of a different object, B, without revealing the plaintext message of the encrypted messages or private keys of A and B to the proxy service provider [22]. The inclusion of proxy re-

encryption in a SAS driven DSA system ensures both IUs' and SUs' privacy. An IU encrypts their location information and sends it to SAS for database process and maintenance. SAS will only have IU's public key which only allows SAS to encrypt information without the ability to decrypt them. When an SU requests access to particular frequency space, this SU will also send its public key to SAS. SAS processes the request base on the encrypted IUs location database and obtains a reply. SAS re-encrypts the reply using both IU's public key and SU's public key and sends the re-encrypted reply to the SU.

Chapter 3

System Design

This section we first present the basic design of PriDSA. Then we will also introduce the designs for the three-tiered service structure and PAL user frequency registration and registration renewal systems.

3.1 Attack Model

As mentions in 1.4.1, SAS server may be operated by commercial third parties while some IUs may be privacy sensitive government applications. Thus, in this thesis, we assume that SAS is not trustworthy and our goal is to protect IU location privacy from untrustworthy SAS. We define an attack model against untrustworthy SAS with powerful attack capabilities.

1. We define an untrustworthy SAS as curious. SAS will attempt to derive sensitive IU location data from information that it receives.

2. We define an untrustworthy SAS as malicious. SAS may deviate from the spectrum allocation computation process to corrupt the spectrum allocation decisions.

3. We define an untrustworthy SAS as cooperative. SAS may collude with a small number of SUs in order to break the location privacy of IUs.

3.2 PriDSA

In PriDSA we consider a database driven spectrum sharing system consisting of a SAS, IUs, and SUs. Each IU operating at frequency f has an Exclusion-zone (Ezone) that is a circle with a specific radius. Inside this radius, an SU operating on frequency f should not be permitted to proceed. IUs send their EZones to SAS for SAS to build and maintain an overall Ezone database. An SU sends SAS its present location and its desired frequency channel to request spectrum access. Base on the Ezone database, SAS approves the request if the SU doesn't reside in any Ezone or SAS denies the request if otherwise. In PriDSA we assume that SAS is not involved and shares no responsibility in the specific co-channel spectrum sharing between SUs. SUs that have obtains access to a common spectrum band can use common medium access control means to share the band.

3.2.1 Overview of Cryptosystem

PriDSA employs AFGH scheme; AFGH is a widely used proxy re-encryption scheme with homomorphic properties proposed by G. Ateniese et al [23]. To setup the system, a Type 1 bilinear pairing system is required. The Following this the definition of bilinear groups.

Definition 3.1. (Bilinear Groups): $(\mathbb{G}_1, \mathbb{G}_1)$ is called a type 1 bilinear group pair, if there exists a group $\mathbb{G}_T$ and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ with the following properties:

1. $\mathbb{G}_1$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p; g is a generator of $\mathbb{G}_1$.
2. e is an efficiently computable bilinear map with the following properties:
   - Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$, $\forall u, v \in \mathbb{G}_1$, $a, b \in \mathbb{Z}_p^*$;
   - Non-degenerate: $e(g, g) \neq 1$.

We define g as the generator of $\mathbb{G}_1$, and set $Z = e(g, g)$. Define p as the order of group $\mathbb{G}_1$ and let $\mathbb{Z}_p^* = \{1, \cdots p-1\}$. The following describes the construction of the AFGH scheme, which is "Third Attempt" in [23].

Key Generation(KG): a user A generates a pair of secret and public key by taking two inputs $a_1, a_2 \in \mathbb{Z}_p^*$. A sets its secret key as $\mathtt{sk} = (a_1, a_2)$ and compute the public key as $\mathtt{pk} := (Z^{a_1}, g^{a_2})$.

Re-Encryption Key Generation ($\mathsf{RG}(\mathtt{sk}_a, \mathtt{pk}_b)$): taking private key $\mathtt{sk}_a = (a_1, a_2)$ of user A and public key $\mathtt{pk}_b = (Z^{b_1}, g^{b_2})$ of user B, the re-encryption key is computed by $\mathtt{rk}_{A \to B} := (g^{b_2})^{a_1} = g^{a_1 b_2}$.

First-Level Encryption ($\mathsf{E}_I(M, \mathtt{pk}_a)$): for a message $M \in \mathbb{G}_T$ and public key $\mathtt{pk}_a = (Z^{a_1}, g^{a_2})$, select a random nonce $r \leftarrow_\$ \mathbb{Z}_p^*$, and compute $c_1 = Z^r \cdot M$, $c_2 = Z^{ra_2}$. The ciphertext is $C := (c_1, c_2)$.

First-Level Decryption ($\mathsf{D}_I(C_r, \mathtt{sk}_b)$): for a first-level ciphertext $C_r = (c_1, c_2)$ and its corresponding private key $\mathtt{sk}_b = (b_1, b_2)$, the plaintext is obtained by computing $M^* := \frac{c_1}{c_2^{1/b_2}}$.

Second-Level Encryption ($\mathsf{E}_{II}(M, \mathtt{pk}_a)$): for a message $M \in \mathbb{G}_T$ and public key $\mathtt{pk}_a = (Z^{a_1}, g^{a_2})$, select $r \leftarrow_\$ \mathbb{Z}_p^*$, and compute $c_1 = Z^{ra_1} \cdot M$, $c_2 = g^r$. The ciphertext is $C := (c_1, c_2)$.

Second-Level Decryption ($\mathsf{D}_{II}(C_r, \mathtt{sk}_a)$): for a second-level ciphertext $C_r = (c_1, c_2)$ and its corresponding private key $\mathtt{sk}_a = (a_1, a_2)$, the plaintext is obtained by computing $M^* := \frac{c_1}{e(g^{a_1}, c_2)}$.

Re-Encryption ($\mathsf{R}(C, \mathtt{rk}_{A \to B})$): for a message M encrypted by public key (Z^{a_1}, g^{a_2}), its second-level ciphertext $C = (c_1, c_2)$ can be re-encrypted to be a first-level ciphertext encrypted by public key $\mathtt{pk}_b = (Z^{b_1}, g^{b_2})$ by computing $c_2^* := e(c_2, \mathtt{rk}_{A \to B}) = Z^{(ra_1)b_2}$. The re-encrypted first level ciphertext is $C_r := (c_1, c_2^*)$.

While the AFGH is a proxy re-encryption cryptosystem, it also inherits some homomorphic properties which we will leverage in PriDSA. These homomorphic properties are defined as the following.

Definition 3.2. Homomorphic multiplication: Given an AFGH public and private key pair $(\mathtt{pk}, \mathtt{sk})$, consider two AFGH second-level encrypted ciphertexts $C = \mathsf{E}_{II}(M, \mathtt{pk}) = (c_1, c_2)$ and $C' = \mathsf{E}_{II}(M', \mathtt{pk}) = (c'_1, c'_2)$. The homomorphic multiplication operation $C \otimes C' := (c_1 c'_1, c_2 c'_2)$ produces a ciphertext of MM'. In another word, $\mathsf{D}_{II}(C \otimes C') = MM'$.

Homomorphic inverse: Given an AFGH public and private key pair $(\mathtt{pk}, \mathtt{sk})$, consider an AFGH second-level encrypted ciphertext $C = \mathsf{E}_{II}(M, \mathtt{pk}) = (c_1, c_2)$. The homomorphic inverse operation $\mathsf{inv}(C) := (c_1^{-1}, c_2^{-1})$ produces a ciphertext of M^{-1}. In another word, $\mathsf{D}_{II}(\mathsf{inv}(C)) = M^{-1}$.

The proof of these AFGH homomorphic properties are discussed and presented in [24].

3.2.2 System Overview

As shown in figure 3.1, PriDSA is consist of four major entities: IUs, SAS, SUs and an IU-tracker. IUs are responsible for encrypting and blinding their Ezone information and sending the encrypted Ezone map, denoted as $[\![\mathbf{X}]\!]$, to SAS. IUs will also provide Ezone tracking commitments to the IU-tracker. IU-Tracker is responsible for storing and aggregating all the Ezone commitments from all IUs. SAS receives $[\![\mathbf{X}]\!]$ from all IUs and homomorphically aggregated all them into a single EZone map, denoted as $[\![\mathbf{D}]\!]$. After that, SAS request the aggregated commitments from IU-tracker and use it to remove the blinding on $[\![\mathbf{D}]\!]$. Blinding can only be removed from aggregated Ezones. SUs request spectrum access by sending a request to SAS containing the specific location of the requested spectrum space. SAS generate a potential encrypted spectrum licenses for SUs, denoted as *cred*, based on

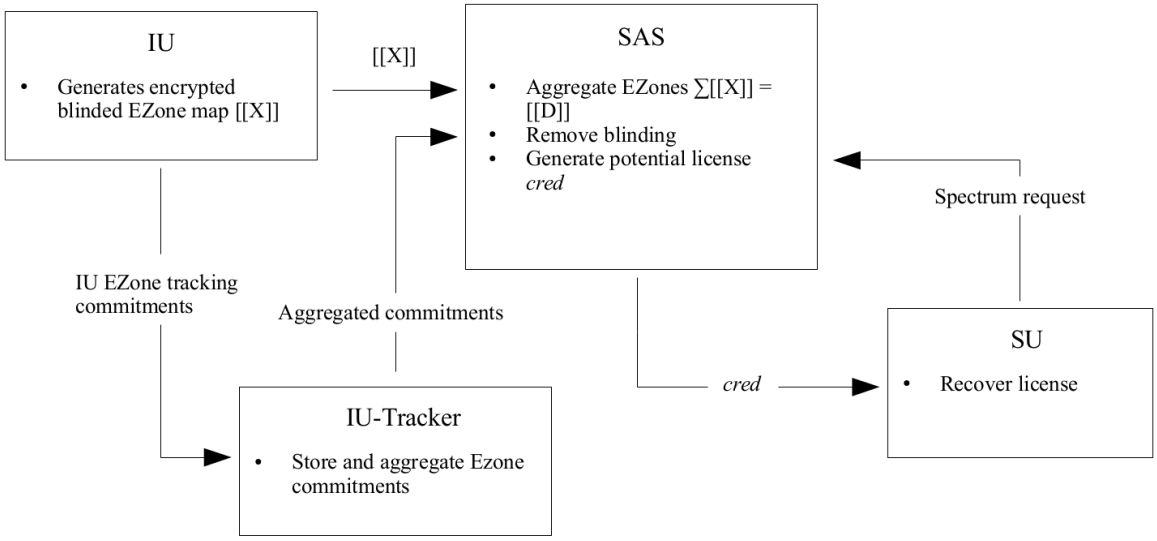

Figure 3.1: PriDSA system overview

$[\![\mathbf{D}]\!]$ and sends *cred* to SUs. Only if the request spectrum space is not inside an IU EZone, will SUs be able to decrypt *cred* to recover the proper license. In the following, we will present the operation of PriDSA in detailed steps.

3.2.3 System Initialization

The system is initialized first by setting up the AFGH cryptosystem. The setup for AFGH cryptosystem and encryption key generations is outlined in 3.2.1. After the cryptosystem has been initialized, we also establish system parameters as $\texttt{params} = (\mathbb{G}_1, \mathbb{G}_T, p, e, g, Z, f_1, h, Y)$ where $f_1, h \leftarrow_{\$} \mathbb{G}_1$, $H \leftarrow_{\$} \mathbb{G}_T$ and compute $Y := e(f_1, h)$. These parameters are shared with all the entities within PriDSA to ensure the correctness of their operations.

3.2.4 IU EZone Encryption and Blinding

The IUs' EZone data are discretized, which divides PriDSA system's service area into a total of L same size grids and the spectrum into F channels. In this way, the Ezone information is represented as a matrix $\mathbf{T}$ of dimension $L \times F$. If IUs define channel f at grid l as EZone, then $\mathbf{T}$'s entry $\mathbf{T}_{l,f}$ is a random non-zero element picked from $\mathbb{Z}_p$; if not, we set $\mathbf{T}_{l,f}$ to be 0. To blind the EZone data at each location l and channel f, IUs picks a random nonce $\mathbf{A}_{l,f}$ in $\mathbb{Z}_p$ as a blinding mask. To prepare the EZone data for encryption and to incorporate the blinding mask into the EZone data, IUs converts the sum of $\mathbf{A}_{l,f}$ and $\mathbf{T}_{l,f}$ to group $\mathbb{G}_T$ by an exponentiation operation:

$$\mathbf{X}_{l,f} \leftarrow Y^{\mathbf{T}_{l,f}+\mathbf{A}_{l,f}}. \tag{3.1}$$

Then, IUs encrypt every entry of $\mathbf{X}$ using AFGH's level 2 encryption and IUs' public key `ipk`. We denote the encrypted results as $[\![\mathbf{X}]\!]$. Note that the blinding factor ensures that even if malicious SUs obtains $\mathbf{X}$ from an individual IU by colluding with SAS, the malicious SUs still can't see the true EZone information.

IUs also computes the Pedersen commitment on $\mathbf{T}_{l,f} + \mathbf{A}_{l,f}$. That is:

$$\mathbf{r}_{l,f} \leftarrow_{\$} \mathbb{Z}_p, \mathbf{C}_{l,f} \leftarrow Y^{\mathbf{T}_{l,f}+\mathbf{A}_{l,f}} H^{\mathbf{r}_{l,f}} \tag{3.2}$$

The blinding remove helper value $\mathbf{B}$ is computed by:

$$\mathbf{B}_{l,f} \leftarrow Y^{\mathbf{A}_{l,f}} \mathbf{C}_{l,f} \tag{3.3}$$

Finally, IUs send the encrypted Ezone report $[\![\mathbf{X}]\!]$ and the encrypted blinding remove helper

value $[\![\mathbf{B}]\!]$ to SAS. SAS can't decrypt these encrypted reports since it does not have the decryption key. $[\![\mathbf{B}]\!]$ is obtained by IUs following the same encryption step as $[\![\mathbf{X}]\!]$.

3.2.5 SAS EZone Database Maintenance

Upon receiving the encrypted EZone report from IUs $\left\{[\![\mathbf{X}(i)]\!], [\![\mathbf{B}^(i)]\!]\right\}_{i=1}^{N}$ from all N IUs, where (i) indicates the input of the ith IU, SAS integrates them together to form aggregated maps by computing element-wise homomorphic product of all input maps:

$$\begin{aligned} [\![\mathbf{D^b}_{l,f}]\!] &\leftarrow \otimes_{i=1}^{N} [\![\mathbf{X}(i)_{l,f}]\!] \\ [\![\mathbf{B'}_{l,f}]\!] &\leftarrow \otimes_{i=1}^{N} [\![\mathbf{B}(i)_{l,f}]\!] \end{aligned} \tag{3.4}$$

After SAS is finish aggregating all N EZone reports, SAS queries the cumulative commitment values, $\mathbf{C'}$, from the IU-tracker. The IU tracker maintains the cumulative commitment values $\mathbf{C'}$ by aggregating commitment values, $\mathbf{C}$, from IUs:

$$\mathbf{C'}_{l,f} := \prod_{i=1}^{N} \mathbf{C}_{l,f}(i) \tag{3.5}$$

When SAS receives $\mathbf{C'}$, SAS removes the blinding on $[\![\mathbf{D^b}_{l,f}]\!]$:

$$[\![\mathbf{D}_{l,f}]\!] \leftarrow [\![\mathbf{D}^b_{l,f}]\!] \otimes \mathsf{inv}\left([\![\mathbf{B'}_{l,f}]\!]\right) \otimes [\![\mathbf{C'}_{l,f}]\!] \tag{3.6}$$

3.2.6 Spectrum Computation and License Generation

First, SAS generates a valid license `cred` for an SU spectrum request at location l and frequency f. Then, SAS picks a random element α in $\mathbb{G}_T$ and hashes it to a random bit string

$\mathtt{k}$. SAS encrypts the valid license $\mathtt{cred}$ by any symmetric key cryptosystem, such as AES, with $\mathtt{k}$ as the secret key. The result of the encryption is denoted as $[\![\mathtt{cred}]\!]_{\mathtt{k}}$. Meanwhile, SAS encrypts α to level 2 ciphertext using IUs' public key $\mathtt{ipk}$ and homomorphically multiplies it with the $[\![\mathbf{D}_{l,f}]\!]$. That is, set $\hat{K} \leftarrow \mathsf{E}(\alpha, \mathtt{ipk}) \otimes [\![\mathbf{D}_{l,f}]\!]$. Note that if the SU is not located in any EZone, $\mathbf{D}_{l,f} = 1_{\mathbb{G}_T}$ and hence $\hat{K}$ can be decrypted to α. Otherwise, $[\![\mathbf{D}_{l,f}]\!]$ is the ciphertext of some random number and decryption of $\hat{K}$ just result in a random number. Finally, SAS sends $\hat{K}$ and encrypted license $[\![\mathtt{cred}]\!]_{\mathtt{k}}$ to the SU as response to the SU's spectrum access request.

3.2.7 Spectrum License Recovery

When SU receives the response to its spectrum access request, the SU decodes the response as first by using the re-encryption key $\mathtt{rk}_b$ obtained during its registration process to re-encrypt and the decrypt $\hat{K}$. This would yield an AES key. As explained in 3.2.6, if the requested spectrum space doesn't reside in any EZone, then $\hat{K}$ can be decrypted to α. Otherwise, SU will only obtain a random number. With decrypted α, SU can recover $\mathtt{k}$, the secret for $[\![\mathtt{cred}]\!]_{\mathtt{k}}$. Thus if SU successfully decrypts $[\![\mathtt{cred}]\!]_{\mathtt{k}}$ and obtains $\mathtt{cred}$, SU is permitted to access the requested spectrum space with license $\mathtt{cred}$. If SU fails to decrypts $[\![\mathtt{cred}]\!]_{\mathtt{k}}$, SU's request is denied and SU has no valid decrypted license.

3.3 Priority Access Tier

As mentioned in section 1.4.2, the 3.5 GHz band Citizens Broadband Radio Service (CBRS) established by the FCC is governed by a three-tiered spectrum authorization framework. The three tiers are Incumbent Access, Priority Access, and General Authorized Access (GAA).

PriDSA, as presented in the previous section, is a two-tiered system. PriDSA only supports Incumbent Access or IUs and General Authorized Access for all SUs; PriDSA doesn't support Priority Access for SUs with Priority Access Licenses. In this section, we will present the design and implementation of the incorporation of the Priority Access tier into PriDSA.

3.3.1 Priority Access System Design

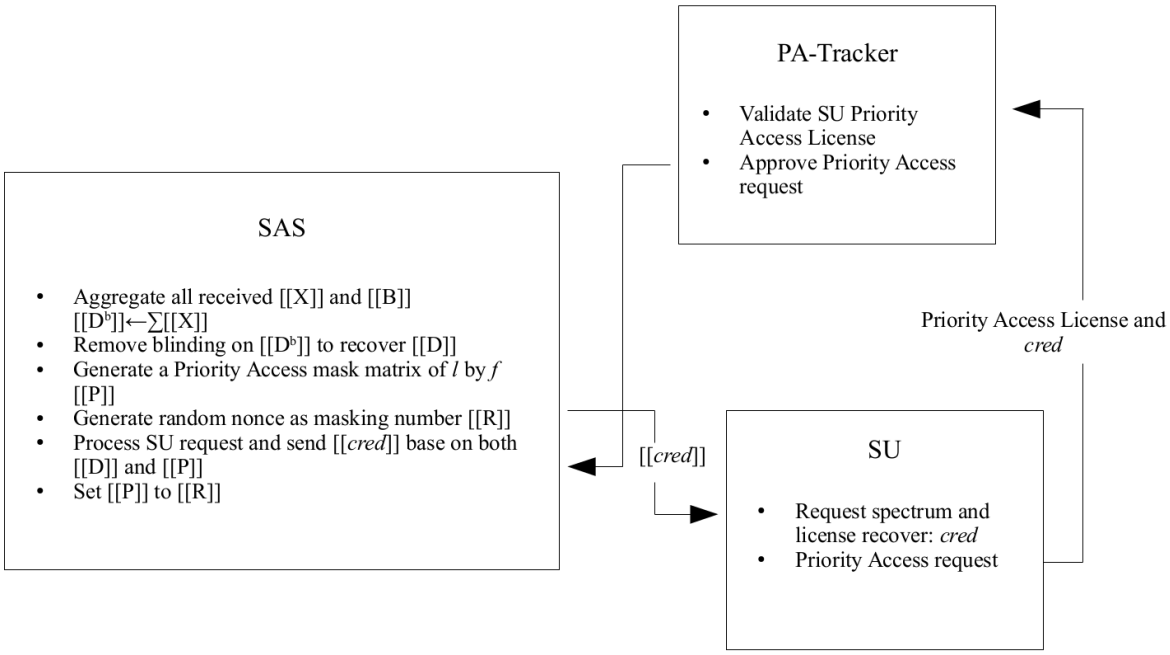

Figure 3.2: Priority Access system overview

Figure 3.2 presents an overview of our Priority Access design. Note that IUs and IU-tracker are omitted from figure 3.2 as we don't impose any changes upon them and their interactions with SAS. The inclusion of a Priority Access tier into PriDSA imposes some changes on SAS and SUs as well as introduces a new entity, PA-tracker.

SAS establishes an encrypted EZone database, $[\![\mathbf{D}]\!]$, by receiving and aggregating EZone information reports from all IUs. Thereafter, SAS creates a Priority Access masking matrix, $[\![\mathbf{P}]\!]$, with the same size as $[\![\mathbf{D}]\!]$. When an SU send a spectrum request, SAS process the request by generating a potential license `cred` basing on both the values of $[\![\mathbf{D}_{\mathbf{l},\mathbf{f}}]\!]$ and $[\![\mathbf{P}_{\mathbf{l},\mathbf{f}}]\!]$. Then SAS sends the encrypted $[\![\texttt{cred}]\!]$ to SU for license recovery. If SU fails to recover the license, SU is denied for any access to the requested spectrum. If SU successfully recovers the license, SU is only granted the common shared GAA. To request a Priority Access channel, SU would need to send its Priority Access License (PAL) identification and the recovered `cred` to a PA-tracker. The PA-tracker maintains a complete database of active PAL holders within the SAS service area. Any PAL holder who migrates into a new SAS service area will need first to register its PAL with the local PA-tracker. When an PA-tracker receives a Priority Access request for a specified spectrum space, containing the SU's PAL identification and its `cred`, the PA-tracker checks the validity of both the PAL identification and the `cred`. If the validations are successful, the PA-tracker then submits a Priority Access approval message to SAS; PA-tracker will also keep a record of all active Priority Access registrations. Upon receiving a Priority Access approval message from PA-tracker, SAS generates a random nonce as a masking number, $[\![\mathbf{M}]\!]$, and apply this masking number onto $[\![\mathbf{P}_{\mathbf{l},\mathbf{f}}]\!]$. We will present these operations in detailed steps in the following subsections.

3.3.2 SAS Priority Mask Map Generation

To allocate Priority Access spectrum spaces to a PAL holders, SAS generates and maintains Priority Mask Map, $[\![\mathbf{P}]\!]$, along with the EZone database, $[\![\mathbf{D}]\!]$. $[\![\mathbf{P}]\!]$ is a matrix of the same size as $[\![\mathbf{D}]\!]$. The functionality of $[\![\mathbf{P}]\!]$ is similar to $[\![\mathbf{D}]\!]$.

To create a Priority Mask Map, SAS first generates a non-Priority Access constant, $\mathbf{N}$, and

set $\mathbf{N}$ to be 0. Then we prepare $\mathbf{N}$ for encryption:

$$\mathbf{P}_{l,f} \leftarrow Y^{\mathbf{N}}. \tag{3.7}$$

Then SAS encrypts every $\mathbf{P}$ using AFGH's level 2 encryption and IUs' public key $\texttt{ipk}$, and thus SAS creates a Priority Mask Map, $[\![\mathbf{P}]\!]$. Note that when SAS first initializes $[\![\mathbf{P}]\!]$ during system initialization, every $\mathbf{P}$ is initialized with $\mathbf{N}$ which indicates the absence of Priority Access.

3.3.3 SAS License Generation with Priority Access

First, SAS generates and encrypts a valid license $\texttt{cred}$ for an SU spectrum request at location l and frequency f; the procedures is the same as described in section 3.2.6. However the processing of $\hat{K}$ has some changes. After SAS has generated $[\![\texttt{cred}]\!]_{\texttt{k}}$, then SAS encrypts $\texttt{k}$ using a AFGH's second level encryption:

$$\begin{aligned} \mathbf{K} &\leftarrow Y^{\mathbf{k}} \\ [\![\mathbf{K}]\!] &\leftarrow \mathsf{E}(\mathbf{K}, \texttt{ipk}) \end{aligned} \tag{3.8}$$

Then, $[\![\mathbf{K}]\!]$ is homomorphically multiplied with both $[\![\mathbf{D}_{l,f}]\!]$ and $[\![\mathbf{P}_{l,f}]\!]$:

$$\hat{K} \leftarrow [\![\mathbf{K}]\!] \otimes [\![\mathbf{D}_{l,f}]\!] \otimes [\![\mathbf{P}_{l,f}]\!] \tag{3.9}$$

Finally, SAS sends $\hat{K}$ and encrypted license $[\![\texttt{cred}]\!]_{\texttt{k}}$ to SU as response to the SU's spectrum access request. Note that only if the requested spectrum space is not inside an IU Ezone and is also not register for Priority Access, $\mathbf{D}_{l,f} = 1_{\mathbb{G}_T}$ and $\mathbf{P}_{l,f} = 1_{\mathbb{G}_T}$, then $\hat{K}$ is equal to

$[\![\mathbf{K}]\!]$ and thus can be decrypted to α by an SU.

3.3.4 SAS Priority Access Registration

Following a successful license recovery, presented in section 3.2.7, if the SU also holds a PAL, this SU can register its licensed spectrum space to be a Priority Access channel. To do so, SU sends its PAL identification and `cred` to the local PA-tracker for verification. If PA-tracker successfully verifies a Priority Access registration, it sends a Priority Access registration request to SAS. Upon receiving such Priority Access registration request, SAS picks a random nonce $\mathbf{R}$ and encrypts using AFGH's second level encryption and IUs' public key `ipk`. Then this encrypted $[\![\mathbf{R}]\!]$ is homomorphically multiplied to $[\![\mathbf{P}_{l,f}]\!]$:

$$\mathbf{R}_{l,f} \leftarrow_{\$} \mathbb{Z}_p, [\![\mathbf{P}_{l,f}]\!] \leftarrow \mathsf{E}(Y^{\mathbf{R}_{l,f}}, \mathtt{ipk}) \otimes [\![\mathbf{P}_{l,f}]\!] \tag{3.10}$$

The Priority Access registration expires when the SU's `cred` expires. When this happens, SAS resets $[\![\mathbf{P}_{l,f}]\!]$ to a non-Priority Access spectrum space:

$$[\![\mathbf{P}_{l,f}]\!] \leftarrow \mathsf{E}(Y^{\mathbf{N}}, \mathtt{ipk}) \tag{3.11}$$

3.3.5 Design Discussion

Following the logic of the above-presented procedures, a PAL holder can only request and register a Priority Access channel if and only if the SU has already obtained a corresponding `cred` from SAS. This ensures that no Priority Access channel can be allocated within IU Ezone locations. A successful Priority Access allocation blocks all other Priority Access allocations and GAA spectrum access on the same spectrum space as described in 3.3.3.

The introduction of an independent PA-tracker is non-essential. PA-tracker's functionalities and responsibilities can be carried out by the IU-tracker. PA-trackers (or IU-tracker) will also keep a record of all active Priority Access registrations. This record helps a validation party to check all current Priority Access registrations to check for SAS's malfunctions.

3.4 Priority Access Renewal

According to FCC's rules for the 3.5 GHz CRBS, once a registered channel is no longer in use, corresponding PAL user must inform the SAS. If a PAL user fails to make contact with SAS within seven days, the registered channel will be relieved of its Priority Access protections until contact is re-established. As such, PAL users may extend their current registrations within seven day periods of registration confirmation [10]. As such, a proposed three-tiered system DSA should also implement a Priority Access renewal system. In the previous section 3.3 we have described the design of a three-tiered framework for PriDSA. However, this system doesn't fulfill the registration renewal functionality; when an SU obtains a Priority Access registration, the SU has no way of extending its registration. With the goal of perfecting PriDSA to fulfill FCC recommendations and rules, we present aPriority Access renewal system for PriDSA in this section.

3.4.1 System Overview

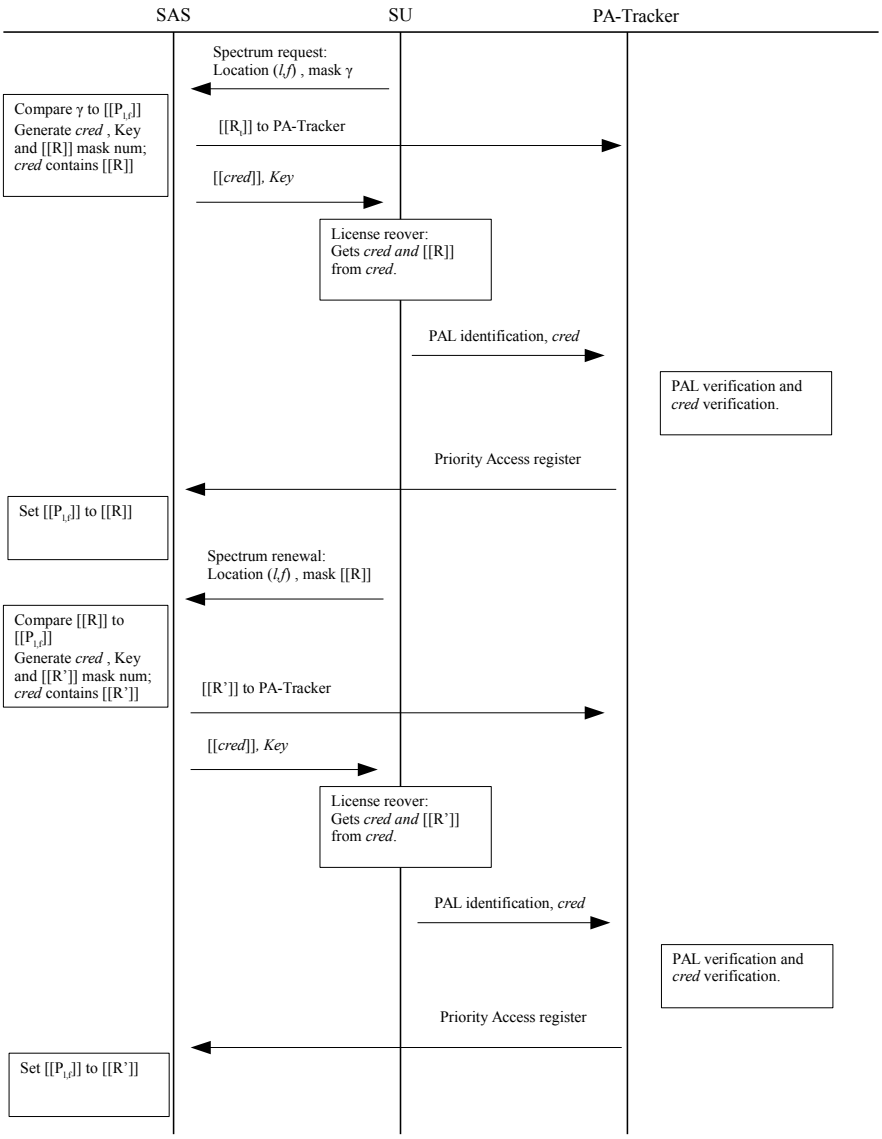

Figure 3.3: Priority Access Registration and Renewal

The Priority Access registration renewal is a protocol modification upon the three-tiered framework presented in the previous section 3.3. Thus, to be presented here in this section,

the registration renewal system imposes no structural changes to the three-tiered frame structure. The changes take place in the interactions between SAS, SU, and PA-tracker.

Figure 3.3 presents an overview of the new communication protocol between SAS, SU, and PA-tracker with the inclusion of Priority Access registration renewal. When an SU first requests a spectrum space from SAS, SU sends the specific spectrum space identifier, (l, f), as well as a Priority Access mask number, γ, to SAS. The γ is an essential parameter for Priority Access renewal but a purposeless one during spectrum request. However, since SAS doesn't keep a record of SUs' Priority Access registrations, for efficient maintenance and simple structure, SAS is designed to process new spectrum access requests and Priority Access renewals indifferently. When an SU sends spectrum access, SU should set γ to a non-impacting number, 0. Afterwards, SAS generates a random potential masking number, $[\![\mathbf{R}]\!]$ and includes $[\![\mathbf{R}]\!]$ into the license `cred`. Then SAS follows the procedure as presented in 3.3.3 to generate $[\![\texttt{cred}]\!]_k$. During the calculation of $\hat{K}$, 3.9, SAS will apply γ to $\hat{K}$ as well as $[\![\mathbf{P}_{l,f}]\!]$ and $[\![\mathbf{D}_{l,f}]\!]$. SAS sends $[\![\texttt{cred}]\!]_k$ and $\hat{K}$ to SU for license recover while so sending $[\![\mathbf{R}]\!]$ to the PA-tracker. After SU has successfully recover the spectrum license `cred`, SU extract $[\![\mathbf{R}]\!]$ from it. SU sends its PAL identification and $[\![\mathbf{R}]\!]$, as identification of its spectrum license, to PA-tracker to request Priority Access. PA-tracker compares the $[\![\mathbf{R}_t]\!]$ it obtained from SAS and $[\![\mathbf{R}]\!]$ from SU as a license verification method. After the successful verifications of SU's PAL and `cred`, PA-tracker signals SAS for a Priority Access registration at spectrum space (l, f). Upon receiving such signal, SAS sets $[\![\mathbf{P}_{l,f}]\!]$ to be $[\![\mathbf{R}]\!]$.

When an SU wishes to extend its Priority Access registration, SU sends a spectrum request with the specific spectrum space identifier, (l, f), and the Priority Access masking number, $[\![\mathbf{R}]\!]$, it has obtained from SAS during the previous successful spectrum request. Given that SU has a Priority Access masking number, this would indicate the spectrum space at (l, f) is not inside an Ezone and $[\![\mathbf{R}]\!]$ is equal to $[\![\mathbf{P}_{l,f}]\!]$. This ensures a successful spectrum license allocation and recovery for SU. Following the same steps described in above, SU would

obtain a new spectrum license and $[\![\mathbf{R}]\!]$, a renewal of its spectrum license and Priority Access registration. We present these operations in detailed steps in the following subsections.

3.4.2 SU Spectrum Request

When an SU request access to a specific spectrum space, this SU sends spectrum request containing the spectrum space identifier, (l, f), and a Priority Access renewal masking number γ. If SU is requesting a new spectrum license, γ should be set to a non-impacting number. If SU is seeking a Priority Access renewal on its Priority Access registration at (l, f), SU will set γ to equal to $[\![\mathbf{R}]\!]$ from the current active `cred` it had recovered.

$$\begin{aligned} \texttt{Request} : \gamma &\leftarrow \mathsf{E}(Y^{\mathbf{0}}, \texttt{ipk}), \\ \texttt{Renewal} : \gamma &\leftarrow [\![\mathbf{R}]\!] \end{aligned} \tag{3.12}$$

3.4.3 SAS License Generation

Once SAS receives an SU's request, no matter of if it's spectrum request or Priority Access renewal, SAS generates a potential Priority Access masking number $[\![\mathbf{R}]\!]$. Generation of $[\![\mathbf{R}]\!]$ is the same as presented in section 3.3.4 equation 3.11. Then SAS creates a potential spectrum license `cred` which contains $[\![\mathbf{R}]\!]$. Then SAS proceeds to encrypt `cred` and create a corresponding key $[\![\mathbf{K}]\!]$ as present in section 3.3.3. Then SAS applies the Ezone data, Priority Access mask and γ onto $[\![\mathbf{K}]\!]$.

$$\hat{K} \leftarrow [\![\mathbf{K}]\!] \otimes [\![\mathbf{D}_{l,f}]\!] \otimes [\![\mathbf{P}_{l,f}]\!] \otimes \mathsf{inv}\,(\gamma) \tag{3.13}$$

Afterwards, SAS sends $[\![\mathbf{R}]\!]$ to PA-tracker and sends $\hat{K}$ and $[\![\texttt{cred}]\!]_k$ to SU.

3.4.4 SAS Priority Access Registration

After SU recovers the `cred`, PAL holders can request a Priority Access registration by sending its PAL identifier and $[\![\mathbf{R}]\!]$, contained `cred`, to the PA-tracker. The PA-tracker verifies the PAL verifies the SU's spectrum license. The PA-tracker verifies the SU's spectrum license by comparing the two $[\![\mathbf{R}]\!]$ it receives from SAS and SU. Once both the PAL and spectrum license has been verified, PA-tracker sends a Priority Access registration request to SAS, containing (l, f) and $[\![\mathbf{R}]\!]$. Upon receiving such request from PA-tracker SAS sets the correspond $[\![\mathbf{P}_{l,f}]\!]$ to $[\![\mathbf{R}]\!]$.

3.4.5 Design Discussion

The spectrum request and Priority Access renewal are designed to be indifferentiable to SAS; SAS process them through a same set of procedures. The primary reason for doing so is that SAS is oblivious to the outcome of individual spectrum request. As such, SAS has no record of active spectrum licenses to refer to when an SU requests a Priority Access registration. During a new spectrum request, if SU chooses to not to set γ to the non-impacting number 0 as discussed in 3.4.2, the SAS would apply γ regardless of its actual value. However, this would in term alter the correctness of $\hat{K}$ and causes SU to be unable to recover the spectrum license. Potentially an SU may guess a correct γ value and obtain spectrum access to a Priority Access protected spectrum space. However, this is highly improbable given an SU has no way of telling if a spectrum space has been masked for Priority Access and the probability of it guessing the correct $[\![\mathbf{R}]\!]$ value is very low due to the security of the cryptosystem.

Chapter 4

Implementation and Results

In this section, we present our implementation of PriDSA with extended three-tiered structure and Priority Access renewal system. We will also show and discuss the results of our implementation.

4.1 Implementation Details

The security level of our evaluation is set to be symmetric 160 bits, which provides approximately the same level of security as an RSA signature with a modulus size of 2048 bits. By using the pairing-based cryptography (PBC) library available at [25], we instantiate a secure Type 1 pairing with "A-internal" and implement all SAS protocols and algorithms on a laptop with 8x Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz.

As presented in table 4.1, we define a 40 km^2 geographical area to our SAS's service area.

Table 4.1: Implementation Parameters

Geograpich Arae	40 km^2
Frequency Channels	10
Grid Side Length	100 m
Total Matrix Size	4000
Number of IUs	5
EZone Percentage	0.2

Within this 40 km^2 service area there are 10 frequency channels that can be queried by SUs for spectrum access. We discretized this 40 km^2 service area into 100 m by 100 m area grids; this produces a 4000 square grids.

In this 4000 grid service area map, we define that there are a total of 5 different IUs. When an IU submit its EZone information, it first generates a 4000 grid matrix depicting the entire service area. Then, for each matrix grid, we define a random 0.2 percentage chance for that grid to be considered an EZone. All 4000 grids area encrypted using the AFGH second level encryption method before sending them to SAS.

4.2 Simulation Results

Table 4.2: System initialization

Task	Execution Time (ms)
IU Key Generation	1.400
SU Key Generation	1.322
Re-encryption conversion Key	1.309
SAS Priority Access Mask Generation	5734.359

Table 4.2 presents the system initialization executions times required to set up the AFGF cryptosystem as presented in 3.2.1. Note that most of the system parameter initialization require less than 2 ms. SAS Priority Access mask generation requires more than 5000 ms of execution time is expected. During SAS Priority Access mask generation, SAS allocate 4000 matrix grids and initializes them to be non-impacting encrypted values as $\mathsf{E}(Y^{\mathbf{0}}, \mathtt{ipk})$. As such, 5000 ms of execution time is reasonable and expected execution time.

Table 4.3 presents the IUs's generation of Ezone and SAS's Ezone database maintenance.

Table 4.3: EZone database generation and maintenance

	IU 1	IU 2	IU 3	IU 4	IU 5
EZone Data Generation (ms)	2764.896	2761.826	2758.309	2772.841	2763.850
EZone Data Encryption (ms)	11434.973	11504.760	12293.553	11457.141	11395.519
Comm. Overhead to SAS (B)	64000	64000	64000	64000	64000
Comm. Overhead to IU-Tracker (B)	64004	64004	64004	64004	64004
SAS EZone Aggreagtion (ms)	0.827	54.154	54.675	55.734	54.704

From this table, we can observe that it take an IU an average of less than 3000 ms to create a 4000 grid Ezone matrix map filled with Ezones and non-Ezones. Then, it takes an IU less than 15000 ms to encrypt the entire Ezone matrix map. Thus we can assume that, on average, it takes less than 20 seconds for an IU to prepare an encrypted Ezone matrix map that ready to be sent to the SAS. 20 seconds may be considered too long with respect to scalability. However, given the assumption that IU Ezones are relatively static, IUs will not perform these operations regularly. This assumption is reasonable concerning FCC's definition of Exclusion-zone. Furthermore, IUs preparation of encrypted Ezone matrix map is carried out individually during system's initialization. As such, these processes are done concurrently, and their computation time will not affect SAS's service speed.

The communication overheads are relatively small. Given the 64000 byte communication overhead from IU to SAS, since 64000 byte is 512000 bits, it would take less than one second for the Ezone matrix map to be transferred to SAS with an upload speed of 1 Mbps. Once SAS receives an encrypted EZone matrix map, it only take less than 60 ms for the SAS to aggregate the map into its EZone database. Considering the communication overhead and EZone aggregation time, the EZone database maintenance time is relatively small.

Table 4.4 presents the SAS spectrum request service time. Notice that the table doesn't

Table 4.4: SAS Spectrum Request Processing

SAS Remove Blinding (ms)	67.591
SU γ Generation (ms)	1.465
SU γ Comm. Over Head to SAS (B)	16
SAS Priority Access Mask Number Generation (ms)	1.658
SAS Credential Key Encryption (ms)	2.052
SAS Comm. Over Head to SU (B)	2856

include spectrum license `cred` generation time and its encryption time. The generation of an encryption of `cred`, as presented in 3.2.6, required the utilization of cryptosystems other than AFGH. The generation and encryption time of `cred` depends on the choice of cryptosystem chosen and thus may vary greatly. In our implementation, we chose to use SHA-1 and AES to generation and encrypt `cred`. The combined computation overhead of these two processes is less 10 ms. The communication overhead of transferring the spectrum space identifier, (l, f), from SU to SAS is dependent upon the format and size of (l, f). In our implementation, given that l is less than 400 and f is less than 10, the communication overhead of (l, f) is the size of two regular *int* integers in C, 8 bytes.

Table 4.5: SU license recovery and Priority Access Registration

SU Re-encryption (ms)	0.943
Credential Key Decryption (ms)	0.202
Comm. Over Head SU to PA-Tracker (B)	76
Comm. Over Head PA-Tracker to SAS (B)	24
SAS Priority Access Mask Update (ms)	<0.001

Table 4.5 presents the SU spectrum license recover time as well as Priority Access registration process times. Note that depending upon the chosen `cred` generation and encryption schemes, the decryption time of `cred` may vary. SU-tracker `cred` verification method is implemented as a comparison between SAS sent and SU sent $[\![\mathbf{R}]\!]$ values. The computation overhead of this method is less than 1 ms. However, different verification methods may yield

different computation times.

4.3 Implementation Efficiency

From the previously presented results of our implementation and simulation, we can observe that the combined computation overhead of SAS spectrum request processing and SU spectrum license recovery is relatively insignificant. The combined computation time is less than 1 second. With that said, the other major potential bottleneck of SAS request service speed is the communication overhead. However, in our implementation, we were able to keep the required communication messages to be relatively small. This would help to relieve and reduce communication overheads and possible communication delays.

The majority of computations are carried out by IUs and SAS. IUs are required to perform laborious encryptions. However, the majority of these computations can be done off-line and concurrently such that these computations will have no real effect on the efficiency of the system. Computations performed by SAS are relatively simple and less time-consuming. Each aggregation and update to the Ezone database and Priority Access mask takes less than 60 ms to complete.

Considering a different servicing area with a different size and a different number of IU, the SAS spectrum request servicing time would be mostly unchanged. First, with a different number IU the SAS Ezone map aggregation time will differ as caused by the change in the communication overhead. However, this change will not affect the SAS spectrum request service time as the Ezone aggregation operations are carried out during system initialization. To verify this property, we have changed the number IUs from 5 to 10. From Table 4.6 we can observe that the new computation times of the spectrum servicing operations are similar

to the corresponding computation times from the previously presented first simulation.

Table 4.6: 10 IU Test SAS Spectrum Request Servicing Time Results

SU γ Number Generation (ms)	1.498
SAS Priority Access Mask Number Generation (ms)	1.627
SAS Credential Key Encryption (ms)	1.448
SU Re-encryption (ms)	0.894

Then we extended our test; we changed the number of IU from 10 to 50, as presented in Table 4.7. Again, the new test results are similar to the results from the previous two simulations. By comparing the three different sets of results, we can observe that the spectrum servicing time is independent of the number of IU.

Table 4.7: 50 IU Test SAS Spectrum Request Servicing Time Results

SU γ Number Generation (ms)	1.487
SAS Priority Access Mask Number Generation (ms)	1.641
SAS Credential Key Encryption (ms)	1.456
SU Re-encryption (ms)	0.879

We repeated our tests for different service area grids. The results are presented in table 4.8 and 4.9. Similar to the varying IU number tests, the spectrum servicing times are mostly the same. Thus, we can observe that the spectrum servicing time is independent of the size of the servicing area.

Table 4.8: 400 Grids Test SAS Spectrum Request Servicing Time Results

SU γ Number Generation (ms)	1.447
SAS Priority Access Mask Number Generation (ms)	1.608
SAS Credential Key Encryption (ms)	1.578
SU Re-encryption (ms)	0.899

Table 4.9: 2000 Grids Test SAS Spectrum Request Servicing Time Results

SU γ Number Generation (ms)	1.518
SAS Priority Access Mask Number Generation (ms)	1.600
SAS Credential Key Encryption (ms)	1.505
SU Re-encryption (ms)	0.863

Since spectrum servicing time is independent of the service area and number IU, the only possible variable that may affect the spectrum servicing time is the number of SU (number of SU requests). With a close examination of the spectrum servicing operations, we can observe that each spectrum request is processed independently and individually. SAS is oblivious to the outcome of each request and SAS processes each request indifferently; this causes the processing procedures for all request to be the same, regardless of the volume of the request. Given that the input sizes are structured to be constant, the computation time of each spectrum request is the same. Thus, with varying number of SU and varying number of SU requests, the individual SU request servicing time is constant. When inspecting the servicing time of SU multiple requests as whole, the servicing time will be linearly related to the number of SU requests.

Considering the properties of our system and implementation mentioned above, we believe that our PriDSA with complete three-tiered structure and Priority Access renewal is an efficient and scalable system.

Chapter 5

Discussion

5.1 Design and Implementation

In section 3.4.4 we presented the process for SAS to update the Priority Access mask as by receiving the mask number and spectrum space identifier from the PA-tracker. This mask number, $[\![\mathbf{R}]\!]$, is originally generated and sent to PA-tracker by SAS, as presented in section 3.4.3. This redundancy in communication can be eliminated to reduce communication overhead. However, this redundancy in communication is intentionally left in place.

In our design and implementation, the SAS is oblivious to the outcome of each spectrum request. Each time SAS receives a spectrum request, it generates a potential $[\![\mathbf{R}]\!]$ of the requested spectrum space. Due to the fact that this $[\![\mathbf{R}]\!]$ may or may not be utilized by the SU, SAS is designed to send the $[\![\mathbf{R}]\!]$ to PA-tracker instead of storing itself. If we choose to have SAS store every $[\![\mathbf{R}]\!]$, as the number of spectrum request increases due either continuous service and scaling service area, the memory space needed to store these potential $[\![\mathbf{R}]\!]$ value increases exponentially. Thus, our design trades communication overhead for memory storage efficiency. However, if a situation arises where the communication link between different entities are considered constraining, such redundancy in communication can be eliminated without imposing large system overhaul.

5.2 Security Guarantees

By inspecting the interaction protocols amongst different entities within this system, we can ensure the following:

1. SAS will not be able to obtain IUs' Ezone information in plaintext. Given a correct system initialization, SAS will only have access to IUs' shared public key `ipk`. This only allows SAS to encrypt messages instead of decrypting IUs' messages. As such, given a malicious and compromised SAS, IUs' EZone information are still encryption protected.

2. SAS will not be able to obstruct specific SUs from correctly obtaining spectrum licenses. Given that SAS is oblivious to the outcome of each spectrum request, thus all spectrum licenses generated by SAS, regardless of approval or denial, are the same. Since SAS has no way of identifying SUs, SAS can't obstruct specific SUs from correctly obtaining spectrum licenses.

3. Due to the inclusion of the blinding method, individual IU's Ezone map is protected until blinding removal. Before blinding removal, even if SAS collude with SUs, individual IU's Ezone maps are protected by the blinding method.

4. The correctness of SAS's operations can be verified by the IU-tracker's commitment records and PA-tracker Priority Access registrations. A third party investigator can detect any alteration to the Ezone map and Priority Access mask by referring to IU commitments and SU Priority Access registrations.

5. Malicious PA-tracker can only prevent certain SUs' from registering Priority Access and avoid certain spectrum space to be accessed. Such SU-tracker can cause no harm to IUs.

6. The previous mentioned malicious PA-trackers can be detected. PA-tracker's operation can be verified by referring to the Ezone database and spectrum request results.

5.3 Future Works

While our PriDSA system proposed in this thesis has sound security guarantees and promising system efficiency and scalability, there are many other problems and weaknesses that we are currently unable to address. Such issues and weaknesses require future explorations and works. The following sections introduce two possible future works.

5.3.1 Protection Zone Inclusion

According to FCC, an Exclusion-zone maybe considered to be Protection-zone by the incorporation of ESC sensors into a DSA system [9]. As such, ESC sensors scan and determines IUs' interference thresh holds at each spectrum space. By inspecting these threshold values, SAS may then allow SUs' to operate in protected zones if their wireless operations don't produce interferences that exceed the IUs' thresh hold values.
Our current PriDSA design doesn't support such functions as mentioned earlier. Given that under the contemporary design SAS can only perform an insufficient number of homomorphic operations, the inclusion of these functions may require a complete overhaul of the entire system.

5.3.2 Protection Against Inference Attack

In situation case where IUs are not sparse and with continuous service, individual IU Ezone information is protected from inference attacks [14] by the blinding method and the Priority

Access mask. However, in the case where IUs are sparsely located, individual IU Ezones are vulnerable to an inference attack once the blinding has been remove by SAS during its service. While continuous Priority Access registration may help to mask the true IU Ezone locations from such attack, such method is not reliable and is not intended for such propose in the first place.

To prevent any successful inference attacks on IU Ezons, PriDSA can include a system of limiting the number of spectrum requests from each SU. However, this inclusion may require SAS to perform more laborious and unsupported operations. Moreover, this may lead to a decrease in system efficiency and a possible system rework.

Chapter 6

Conclusions

In this thesis, we first presented a security sound DSA system proposed for the 3.5 GHz CRBS. This DSA system, PriDSA, utilizes an array of different cryptosystems and security measures to ensure the privacy of IU Ezone information while also providing an efficient SAS. While PriDSA is more focused on IU privacy protections; it lacks some of the critical requirement set forth by the FCC. In light of these requirements, we extended the PriDSA system to incorporate PAL Priority Access functionalities into PriDSA's two-tiered frame to fulfill FCC's three-tiered frame recommendation. Afterward, we have also included a new Priority Access renewal system into PriDSA to support all PAL Priority Access operations fully.

Upon finishing our new extended PriDSA system, we present our implementation of the system. By utilization a set of published libraries, we were able to implement all introduced system functions and operations, and then, we carried out simulations to inspect the efficiency of our design. Through close inspection of the simulation results, we were able to conclude that our design is efficient and scalable. The SU spectrum request service time from request to license recovery can be completed under seconds. With an increasing number of SU requests and IUs Ezone, the SAS Ezone database maintenance time and request service time will not experience an exponential increase.

To conclude our exploration, we have also identified two issues that need future attention and work to further perfect our system.

Chapter 7

Summary

With growing demands for spectrum access and the depletion of the frequency spectrum, spectrum sharing is becoming a prominent issue for exploration. In light of the 3.5 GHz CRBS adopted by FCC, we propose a DSA system. Our system, PriDSA, provides sound privacy guarantees for IUs through the deployment of an array of security measure. PriDSA is designed to fully support the FCC's propose three-tiered framed spectrum sharing structure. PAL users may register and renew their Priority Access under our proposed system with ease, while the integrity of IUs' Ezones are upheld and ensured at all times. With detailed simulation results presented, we evaluate our system to be a robust and efficient system.

Bibliography

[1] FCC. Radio spectrum allocation. https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation.

[2] FCC Spectrum Policy Task Force. Report of the spectrum efficiency working group. 2002.

[3] FCC. Et docket no 03-222 notice of proposed rule making and order. 2003.

[4] Q. Zhao and B. M. Sadler. A survey of dynamic spectrum access. *IEEE Signal Processing Magazine*, 24(3):79–89, May 2007.

[5] P. Kolodzy and I. Avoidance. Spectrum policy task force. *Federal Commun. Comm., Washington, DC, Rep. ET Docket*, (02-135), 2002.

[6] M. Altamimi, M. B. Weiss, and M. McHenry. Enforcement and spectrum sharing: Case studies of federal-commercial sharing. 2013.

[7] FCC. Amendment of the commission's rules with regard to commercial operations in the 3550- 3650 mhz band. *Report and Order and Second Further Notice of Proposed Rulemaking in GN Docket 12-354*, 2015.

[8] FCC. 3.5 ghz band / citizens broadband radio service. https://www.fcc.gov/wireless/bureau-divisions/broadband-division/35-ghz-band/35-ghz-band-citizens-broadband-radio.

[9] FCC. Shared commercial operations in the 3550–3650 mhz band. *Federal Register*, 80(120), 2015.

[10] FCC. 47 cfr c - priority access.

[11] Mobile broadband services in the 2300 mhz - 2400 mhz frequency band under licensed shared access regime. *ETSI TR 103 113*, 1.1.1, 2013.

[12] V. A. Kachore, J. Lakshmi, and S. K. Nandy. Location obfuscation for location data privacy. In *2015 IEEE World Congress on Services*, pages 213–220, June 2015.

[13] K. Maharaj and P. Hosein. Location obfuscation using smart meter readings. In *2016 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, pages 449–453, Nov 2016.

[14] B. Bahrak, S. Bhattarai, A. Ullah, J. M. J. Park, J. Reed, and D. Gurney. Protecting the primary users' operational privacy in spectrum sharing. In *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pages 236–247, April 2014.

[15] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong. Optimal strategies for defending location inference attack in database-driven crns. In *2015 IEEE International Conference on Communications (ICC)*, pages 7640–7645, June 2015.

[16] Z. Zhang, H. Zhang, S. He, and P. Cheng. Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks. In *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*, pages 181–189, Oct 2015.

[17] Sudeep Bhattarai. *Spectrum Efficiency and Security in Dynamic Spectrum Sharing*. PhD dissertation, Virginia Polytechnic Institute and State University, 2 2018.

[18] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. 1978.

[19] Abbas Acar, Hidayet Aksu, and A. Selcuk Uluagac. A survey on homomorphic encryption schemes: Theory and implementation. 1978.

[20] Y. Dou, H. Li, K. C. Zeng, J. Liu, Y. Yang, B. Gao, and K. Ren. Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2486–2493, June 2017.

[21] Y. Dou, K. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li. p^2 -sas: Privacy-preserving centralized dynamic spectrum access system. *IEEE Journal on Selected Areas in Communications*, 35(1):173–187, Jan 2017.

[22] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza. A survey of proxy re-encryption for secure data sharing in cloud computing. *IEEE Transactions on Services Computing*, pages 1–1, 2017.

[23] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30, February 2006.

[24] Hossein Shafagh, Anwar Hithnawi, Lukas Burkhalter, Pascal Fischli, and Simon Duquennoy. Secure sharing of partially homomorphic encrypted iot data. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, SenSys '17, pages 29:1–29:14, New York, NY, USA, 2017. ACM.

[25] PBC: Pairing-based cryptography. https://crypto.stanford.edu/pbc/.