P^2-SAS: Privacy-Preserving Centralized Dynamic Spectrum Access System

Yanzhi Dou, *Student Member, IEEE*, Kexiong Zeng, *Student Member, IEEE*, He Li, Yaling Yang, *Member, IEEE*, Bo Gao, *Member, IEEE*, Kui Ren, *Fellow, IEEE*, and Shaoqian Li, *Fellow, IEEE*

***Abstract*— Centralized spectrum management is one of the key dynamic spectrum access (DSA) mechanisms proposed to govern the spectrum sharing between government incumbent users (IUs) and commercial secondary users (SUs). In the current centralized DSA designs, the operation data of both government IUs and commercial SUs need to be shared with a central server. However, the operation data of government IUs are often classified information and the SU operation data may also be commercial secrets. The current system design dissatisfies the privacy requirement of both IUs and SUs, since the central server is not necessarily trustworthy for holding such sensitive operation data. To address the privacy issue, this paper presents a privacy-preserving centralized DSA system (P^2-SAS), which realizes the complex spectrum allocation process of DSA through efficient secure multi-party computation. In P^2-SAS, none of the IU or SU operation data would be exposed to any snooping party, including the central server itself. We formally prove the correctness and privacy-preserving property of P^2-SAS and evaluate its scalability and practicality using experiments based on real-world data. Experiment results show that P^2-SAS can respond an SU's spectrum request in 6.96 s with communication overhead of less than 4 MB.**

***Index Terms*— Dynamic spectrum access, protection zone, secure multi-party computation, Paillier cryptosystem.**

I. Introduction

DYNAMIC spectrum access (DSA) technique has been widely accepted as a crucial solution to mitigate the potential spectrum scarcity problem. In the U.S., spectrum sharing between the government incumbents (i.e., federal or non-federal agencies) and commercial wireless broadband operators/users is one of the key forms of DSA that are recommended by NTIA [2] and FCC [3]. Recommendations in the President's Council of Advisors on Science and Technology report (PCAST) have identified 1,000 MHz of federal spectrum to create "the first shared-use spectrum superhighways" [4].

The PCAST has also recommended to set up a centralized spectrum access system (SAS) to govern the spectrum sharing between incumbent users (IUs) and secondary users (SUs). This recommendation of SAS-driven design is also reflected in FCC's recent proposal for DSA in 3.5 GHz [5]. In Europe, a similar DSA scheme named licensed shared access (LSA) is also being developed, and 2.3-2.4 GHz band has been identified for an initial deployment of LSA [6]. Without loss of generality, we refer to the central DSA systems as SAS in the remainder of this paper.

One of the critical concerns in light of the increasing prospects of the SAS-driven spectrum sharing is the privacy issue [5]. For national security reasons, operation information of government IUs is often classified data. For example, the IUs in 3.5 GHz DSA band in the U.S. include military and fixed satellite service licensees [5]. In Europe, the IUs of 2.3-2.4 GHz LSA band include military aircraft services and police wireless communications [6]. These IUs' operation data is highly sensitive. Similarly, SUs' operation parameters may also be sensitive commercial secrets for their operators. It is highly likely that SU network operators will be reluctant to share their base stations' deployment and configuration strategies.

Yet, to realize efficient spectrum access, current SAS-driven designs require IUs and SUs to send their operation data to SAS for spectrum allocation. It exposes IUs and SUs to potentially severe privacy violation since SAS is not necessarily trust-worthy for holding such sensitive operation data. For example, according to FCC and PCAST report [4], [7], SAS may be operated by some commercial third parties to enhance its efficiency and scalability. In fact, Google has already developed the third generation of its 3.5GHz SAS prototype [8].

Even if the operator of SAS is trusted, it may be breached by adversaries (e.g., intrusions, malwares, insider attacks). In such cases, adversaries will have access to all IU and SU operation information. In essence, how to protect IU and SU operation privacy from SAS becomes a critical challenge that

Manuscript received May 2, 2016; revised August 12, 2016 and October 13, 2016; accepted November 6, 2016. Date of publication November 24, 2016; date of current version January 12, 2017. This work was supported by the U.S. National Science Foundation under Grant CNS-1228903, Grant CNS-1054697, Grant CNS-1547366, and Grant CNS-1547223. This paper was presented at the ACM MobiHoc, Paderborn, Germany, July 5–8, 2016 [1]. *(Corresponding author: Yaling Yang.)*

Y. Dou, K. Zeng, H. Li, and Y. Yang are with Virginia Tech, Blacksburg, VA 24061 USA (e-mail: yzdou@vt.edu; kexiong6@vt.edu; heli@vt.edu; yyang8@vt.edu).

B. Gao is with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China (e-mail: gaobo@ict.ac.cn).

K. Ren is with The State University of New York at Buffalo, Buffalo, NY 14260 USA (e-mail: kuiren@buffalo.edu).

S. Li is with the University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: lsq@uestc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2016.2633059

can potentially deter the wide adoption of DSA technology. Unfortunately, there is very little existing research on this problem.

The goal of this paper is to fundamentally address the privacy challenge by developing a privacy-preserving SAS (P^2-SAS). Through an efficient multi-party computation (MPC) design, P^2-SAS guarantees that no snooping entities, including SAS itself, can obtain any information about SU and IU operation data during the entire DSA process.

MPC is a well-known technique for secure computation. It allows multiple parties to jointly compute a function over their inputs, while keeping these inputs, the intermediate computation results and the outputs private. However, designing an MPC-based SAS is a nontrivial task. MPC for general function computation is currently not practical due to its huge computation complexity. In the security community, customized MPC solutions for specific applications, such as distributed voting, private bidding and auctions, and private information retrieval [9]–[11], have been explored recently. These customized solutions are much more efficient than general-purpose MPC. Unfortunately, none of them is able to realize MPC for SAS. This is because SAS demands very complex computations that are significantly different from those applications explored in existing literatures. Specifically, designing MPC for SAS encounters the following challenges:

(1) To ensure accurate interference management in DSA, SAS usually adopts complex radio propagation models for interference calculation, e.g., Longley-Rice (L-R) model [12]. These models take multiple parameters, such as IU/SU's geolocation, IU/SU's antenna configuration, terrain data, weather, and soil condition, into some sophisticated math computations. These math computations involve multiple trigonometric, logarithmic, exponential, comparative, multiplicative and additive operations. Realizing such complex computations in MPC incurs huge computation and communication overhead.

(2) SAS needs to ensure that SUs' operation will not disturb any IU. Specifically, to decide whether to approve or deny an SU's spectrum access request, SAS needs to compute whether the accumulated interference from all the SUs will exceed any IU's interference threshold when this SU starts to operate. Achieving the above procedure in MPC needs to compare integers in a secure way. Yet, secure integer comparison is a known complex problem and no existing solution is fast and practical enough for large scale computation [13].

(3) If an SU's spectrum access request is approved, SAS needs to issue a license that permits the SU to access the spectrum in a certain pattern (e.g., location, antenna height, transmit power, etc). To ensure privacy, the above procedures, including the response of permitting the SU or not, and the permissible SU operation parameters in the license, must all remain private in MPC. Yet, the yes/no response and the license's content all need to be digitally signed to prevent forging attempts at the SU side. However, no existing literature has ever provided efficient digital signature generation using MPC.

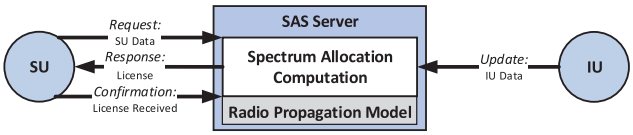


Fig. 1. System model of SAS involves three parties: IUs, SUs, and SAS Server.

At first glance, the above challenges for designing an MPC-based SAS seem daunting. In this paper, we make the following contributions towards completing this difficult mission.

- On a high level, we separate the parameters in a radio propagation model that need privacy protection from those that are public knowledge. Only the part of radio propagation model that involves private parameters needs to be performed by MPC. Then, we disintegrate the computation related to private parameters into a small set of basic operations that can be homomorphically computed using Paillier cryptosystem [14]. In addition, we precompute the non-private part, which transforms this part of computation into simple lookup for further efficiency improvement.
- By investigating the properties of integers involved in SAS's computation, we employ a clever way for integer encoding to circumvent the complex secure integer comparison problem, yet we can still obtain the integer comparison results securely.
- We realize the computation of spectrum license and its digital signature generation in MPC by an innovative combination of radio operation's observable nature with digital signature's integrity property.
- We explore various means to make P^2-SAS practical. We investigate the tradeoff between accuracy and efficiency of P^2-SAS in interference computation, and we formulate it into an optimization problem to search for the optimal P^2-SAS parameter setting. We propose practical acceleration methods to improve P^2-SAS's efficiency, and we demonstrate the scalability and practicality of P^2-SAS using experiments based on real-world data.

The remainder of this paper is organized as follows. Section II describes the system and adversary model, states our design goals, and introduces some preliminaries. Section III describes the basic design of P^2-SAS. Section IV presents several refinement techniques on the basic design for better accuracy and efficiency. Section V evaluates P^2-SAS. Section VI discusses some related work. Section VII concludes this paper.

II. Problem Statement

A. System Model

We consider a SAS involving three parties, as illustrated in Figure 1: IUs, SUs, and SAS Server. SAS Server refers to a central spectrum management infrastructure that allocates spectrum resources while considering incumbent operation protection from interference. A typical scenario of the system is described as follows. Firstly, IUs update SAS Server with their operation data, such as location, interference sensitivity

threshold, and antenna height. Then, any SU that needs the spectrum must send SAS Server a request for spectrum access along with its operation data. Based on some accurate radio propagation model, SAS Server computes whether the accumulated interference from all the SUs will exceed any IU's interference sensitivity threshold when this SU starts to operate. If the answer is yes, a response to the SU denies its request. If the answer is no, a response to the SU permits its spectrum access with a license. Finally, the SU sends a confirmation message to SAS Server to confirm the reception of the response.

The above SAS model belongs to the protection zone approach for interference management, where an SU's operation is permitted as long as the addition of the SU's interference will not exceed any IU's interference sensitivity threshold. We have addressed the privacy issues of SAS for the exclusion zone enforcement approach in [15] and [16]. In exclusion scenario, an SU can only access the spectrum when it is out of the exclusion zones of all IUs. We focus on the protection zone approach in this paper because it can release more frequency opportunities than the exclusion zone approach [17], and thus is considered as the future trend for interference management [18].

B. Adversary Model & Design Goals

We assume SAS Server is semi-honest (a.k.a. honest-but-curious), which means that it acts in an "honest" fashion and exactly follows the protocol design for spectrum allocation, but it is also "curious" and attempts to infer private IU/SU operation data from the information communicated to it. Essentially, a semi-honest SAS Server can only passively monitor the execution of spectrum allocation process to infer IU/SU's operation information, and cannot actively deviate from the process.

The goal of P^2-SAS is to realize the SAS process described in Section II-A correctly, while preserving the IU/SU data privacy from the semi-honest SAS Server. In the following, we formally define correctness and privacy of a SAS scheme in the semi-honest model using the simulation paradigm [19]. Specifically, we denote the computation of the SAS process in Section II-A as a functionality f, and denote any SAS scheme for computing f as π. Since f is deterministic, correctness and privacy can be defined separately as follows.

Definition 1 (Correctness): We say that π correctly computes f if

$$\{\mathsf{output}_{SUs}(x, y, z, n)\} \stackrel{\mathrm{c}}{\equiv} \{f(x, y, z)\}, \tag{1}$$

where x, y, z are the input data from IUs, SUs, and SAS Server respectively, n is the security parameter, and output_{SUs} is the output of SUs during an execution of π. In our scenario, it is the approval/deny information SUs finally obtain. $\stackrel{\mathrm{c}}{\equiv}$ denotes computationally indistinguishability. Intuitively, in this definition, we say a privacy-preserving SAS scheme π is correct if the output of π, which is defined as the approval/deny response sent to an SU, is the same as the original SAS process defined in Section II-A. Basically, this means that π will not alter the spectrum allocation results.

TABLE I
PAILLIER CRYPTOSYSTEM

Key generation: $(\mathsf{pk}, \mathsf{sk}) = \mathsf{KeyGen}(n)$
1. Choose two large random prime numbers p and q, ensuring that $\gcd(pq, (p-1)(q-1)) = 1$.
2. Compute $n = pq$, $\lambda = \mathrm{lcm}(p-1, q-1)$.
3. Choose random integer g where $g \in \mathbb{Z}^*_{n^2}$. Compute $\mu = \left(L\left(g^{\lambda} \mod n^2\right)\right)^{-1} \mod n$ if exists, where $L(x) = \frac{x-1}{n}$.
4. The public key pk is (n, g), and the secret key sk is (λ, μ). n is security parameter.
Encryption: $[\![m]\!] = \mathsf{Enc}_{\mathsf{pk}}(m, r) = g^{(m+nr)} \mod n^2$
$[\![m]\!]$ is an encryption of m with a one-time random number r.
Decryption: $m = \mathsf{Dec}_{\mathsf{sk}}([\![m]\!]) = L\left([\![m]\!]^{\lambda} \mod n^2\right) \cdot \mu \mod n$

Homomorphic properties:

Addition($\oplus$):	$\mathsf{Dec}_{\mathsf{sk}}([\![m_1]\!] \oplus [\![m_2]\!]) = m_1 + m_2$.
Scalar multiplication($\otimes$):	$\mathsf{Dec}_{\mathsf{sk}}(c \otimes [\![m]\!]) = c \cdot m$.
Subtraction($\ominus$):	$\mathsf{Dec}_{\mathsf{sk}}([\![m_1]\!] \ominus [\![m_2]\!]) = m_1 - m_2$.

Definition 2 (Privacy): We say that π securely computes f in the presence of semi-honest SAS Server if there exist probablistic polynomial-time algorithms, denoted as S, such that

$$\{S(z, \mathsf{output}_{SAS}(x, y, z, n), n)\} \stackrel{\mathrm{c}}{\equiv} \{\mathsf{view}^{\pi}(x, y, z, n)\}, \tag{2}$$

where view is the view of SAS Server during an execution of π, i.e., the transcript of messages that it receives and its internal states. $\mathsf{output}_{SAS}(x, y, z, n)$ is the output of SAS Server during an execution of π, i.e., the data it finally sends to SUs. The definition essentially says that an SAS scheme is secure in the presence of semi-honest SAS Server if SAS Server cannot obtain any information about IU/SU's operation from the encrypted IU/SU input data and the encrypted spectrum allocation results.

C. Preliminaries on Paillier Cryptosystem

The design of P^2-SAS heavily leverages the homomorphic properties of Paillier cryptosystem [14]. Paillier cryptosystem efficiently supports homomorphic addition, subtraction and scalar multiplication operations on the ciphertexts, and the generated results, when decrypted, match the results of the operations on the plaintexts. The details are shown in Table I. Note that Enc is a probabilistic algorithm due to the introduction of the random number r while Dec is deterministic, so one plaintext can be encrypted to different ciphertexts while one ciphertext can only be decrypted to one plaintext.

III. BASIC P^2-SAS DESIGN

In this section, we present the basic design of P^2-SAS. In Section IV, we will introduce several refinement techniques on the basic design to accelerate its execution speed.

A. P^2-SAS Design Overview

As shown in Figure 2, our P^2-SAS design involves four parties: (1) a SAS Server $\mathcal{S}$ for computing spectrum allocation, (2) IUs, (3) SUs, and (4) a Key Distributor $\mathcal{K}$. $\mathcal{K}$ creates a group Paillier public/private key pair $(\mathsf{pk}_G, \mathsf{sk}_G)$. pk_G is distributed to $\mathcal{S}$ and all the users, while sk_G is kept as a secret only known to $\mathcal{K}$. In addition, each SU b has his own

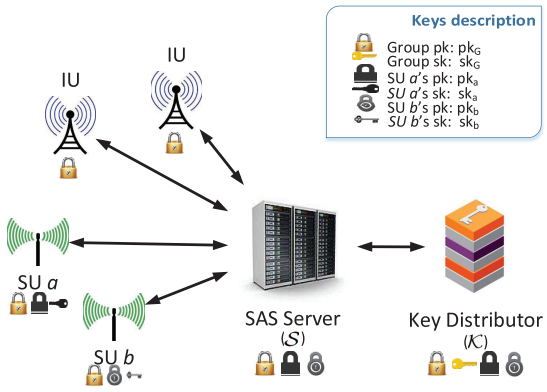


Fig. 2. P^2-SAS overview.

TABLE II
NOTATIONS

Notation	Description
$\mathcal{S}$	SAS Server
$\mathcal{K}$	Key Distributor
$(\mathsf{pk}_G, \mathsf{sk}_G)$	Group key pair
$(\mathsf{pk}_b, \mathsf{sk}_b)$	SU b's individual key pair
$[\![\cdot]\!]$	Encryption by pk_G
$[\![\cdot]\!]_{\mathsf{pk}_b}$	Encryption by pk_b

pair of Paillier public/private keys $(\mathsf{pk}_b, \mathsf{sk}_b)$, and pk_b is sent to $\mathcal{K}$. Using sk_G and pk_b, $\mathcal{K}$ can provide key conversion service, where it converts a ciphertext encrypted by pk_G to a ciphertext encrypted by pk_b for SU b to decrypt. We assume $\mathcal{K}$ is trusted in keeping sk_G secret only to itself, and $\mathcal{K}$ will not collude with $\mathcal{S}$ to compromise IU/SU operation data. In the real world, $\mathcal{S}$ can be operated by some commercial third party (e.g., Google) for enhanced efficiency and scalability; $\mathcal{K}$ is operated by IUs.

P^2-SAS works as follows. Both IUs and SUs encrypt their operation data using the group public key pk_G before sending to $\mathcal{S}$. Upon receiving SU b's spectrum access request, $\mathcal{S}$ performs secure computation on the encrypted operation data to calculate whether the addition of SU b's interference will exceed any IU's interference threshold. Based on the private spectrum computation results, $\mathcal{S}$ is able to generate a response to SU b. The response includes a ciphertext message encrypted by SU b's individual public key pk_b, which is created by leveraging $\mathcal{K}$'s key conversion service. Upon decrypting the ciphertext message, SU b finds out whether its spectrum request is approved or not. If the request gets approved, SU b also obtains a spectrum access license. The license contains SU b's operation parameter specification and is properly signed by $\mathcal{S}$ to prevent any potential forging or tampering attempt. Finally, SU b sends a confirmation message to $\mathcal{S}$ to confirm its reception of the response. In the entire process, all the IU/SU operation data, and the intermediate and final computation results stay private and are never exposed to any of the SAS components, including $\mathcal{S}$ and $\mathcal{K}$. Table II gives the description of notation to be used in our scheme.

It is worth mentioning that in some cases, for example 3.5 GHz band, IUs will not provide operation information directly to $\mathcal{S}$ due to policy reasons. Instead, FCC allows one or more environmental sensing capabilities (ESCs) to sense federal IU activity and provide the sensing data to $\mathcal{S}$ for spectrum allocation computation [20]. FCC requires that ESCs should be managed and maintained by a non-governmental entity. And to protect the privacy of federal operations, FCC also requires that ESC does not store, transmit, or disclose any IU operation information. If the requirement can be relaxed, such that the encrypted IU operation information can be transmitted as long as it is impossible for unauthorized parties to decrypt it, then P^2-SAS can support such ESC-based system. Specifically, under P^2-SAS, ESC service can derive the IU operation data from its sensing result, encrypt the operation data and send the ciphertext to $\mathcal{S}$. All these computations can be done in memory and then all sensing data and intermediate results can be deleted from memory immediately after the ciphertext is transmitted. In this way, location data of IUs is never stored and retained in ESC. The transmitted ciphertext is encrypted by the group public key pk_G and hence will never be exposed to any entities, satisfying the non-disclosure requirement of FCC as well. From $\mathcal{S}$'s point of view, the same secure computation will be performed regardless of whether the source of encrypted IU operation data is from IU itself or from the ESC services. Thus, P^2-SAS can work well in an ESC-based system. Without loss of generality, we will discuss the design of P^2-SAS assuming the source of IU operation data is IU itself in the remainder of this paper.

The remainder of this section presents the details of the above P^2-SAS design. First, we describe the content and format of the input data to $\mathcal{S}$. Then, we show how we realize the secure spectrum computation over the input data. Specifically, we firstly introduce the spectrum computation in the plaintext domain, and then we illustrate how each plaintext computation step can be carried out securely in the ciphertext domain.

B. Private Input Data to SAS

To reduce secure computation overhead, we need to separate the privacy-related parameters in interference calculation from those that are public knowledge. For interference calculation, we adopt the highly-sophisticated L-R model, which takes 13 parameters as input [12]. Among these input parameters, only frequency, distance, antenna height, transmit power, polarization, and terrain data need to be specifically considered. The other parameters are environmental parameters, such as earth dielectric constant, earth conductivity, atmospheric bending constant, climate, etc., which describe the statistics of the environment in which the L-R system is to operate. These environmental parameters are independent of individual users' operation settings and hence need no privacy protection. In addition, polarization only affects the reflectivity of the ground, which is also a known constant when frequency is above 100MHz [12]. Since DSA systems usually consider spectrum sharing in GHz band [4], polarization is also considered to be non-private. Finally, terrain information is public knowledge, which can be easily found in government terrain

TABLE III
PRIVACY-RELATED PARAMETERS

Parameter	Notation	Quantization level
IU, SU location	l, j	L
IU, SU antenna height	h_I, h_S	H_I, H_S
IU, SU operating frequency	f_I, f_S	F
IU interference threshold	ζ	–
SU maximum transmit power	η	–

database, such as USGS [21] and STRM3 [22]. With the above elimination of non-private parameters, all the privacy-related parameters for interference calculation can then be summarized in Table III.

To reduce MPC's computation overhead in the later stages, we next need to represent these private IU/SU operation data of Table III in proper form. Specifically, we quantize the service area of $\mathcal{S}$ into L equal-sized grids, and express users' location using the grid number. In addition, we quantize IU antenna height into H_I levels and SU antenna height into H_S levels, and we assume there are F frequency bands for spectrum sharing. Based on the above quantization, an IU i's operation data can be represented by a three-dimensional matrix $\mathbf{T}_i := \{T_i(l, h_I, f_I)\}_{L\times H_I\times F}$. If IU i is located in grid l with antenna height of h_I and operating frequency of f_I (a.k.a. operation position of (l, h_I, f_I) in the spatial and spectrum domains), $T_i(l, h_I, f_I)$ is set to IU i's interference threshold ζ. The rest entries of $\mathbf{T}_i$ are set to 0. Similarly, a three-dimensional matrix $\mathbf{R}_b := \{R_b(j, h_S, f_S)\}_{L\times H_S\times F}$ is used to represent an SU b's operation data. If SU b's operation position is (j, h_S, f_S), $R_b(j, h_S, f_S)$ is set to SU b's maximum transmit power η. The rest entries of $\mathbf{R}_b$ are set to 0, indicating that no active transmission exists in these operation positions.

It is worth to note that if an IU worries that malicious SUs may infer its operation data by analyzing multiple SAS's spectrum responses, the IU can add obfuscation noises to its operation data $\mathbf{T}_i$ as follows:

$$T_i(l, h_I, f_I) \leftarrow T_i(l, h_I, f_I) + \phi, \tag{3}$$

where ϕ is the noise. Some preliminary noise generation techniques, such as introducing fake IU locations and fake interference thresholds, are proposed in [23] for traditional SAS. Moreover, we can use differential privacy [24] to generate Laplace noise for more rigorous privacy guarantee. Note that these obfuscation techniques for traditional SAS are fully compatible with our P^2-SAS design since they only affect $\mathbf{T}_i$ by noise addition, and the following process of P^2-SAS stays the same. As pointed out by the existing work [23], the potential downside of such obfuscation techniques is the lowered spectrum utilization efficiency due to the added noise. We leave the work of finding the right balance between obfuscation effectiveness and spectrum efficiency for a more comprehensive privacy-preserving solution in the future.

C. Spectrum Computation in Plaintext

In this subsection, we outline the spectrum computation steps in the plaintext domain to ease the understanding of the secure spectrum computation steps in the ciphertext domain in Section III-D, III-E and III-F.

1) Initialization: $\mathcal{S}$ precomputes an attenuation map $\mathbf{I} := \{I(l, j, h_I, h_S, f_I, f_S)\}_{L^2\times H_I\times H_S\times F^2}$ based on the public terrain data and L-R model. Entry $I(l, j, h_I, h_S, f_I, f_S)$ is set to the path attenuation from an SU with operation position (j, h_S, f_S) to an IU with operation position (l, h_I, f_I).

2) IUs Update SAS With Their Operation Data $\mathbf{T}_i$: To reduce the amount of transmitted information, if multiple IUs have the same operation position in both the spatial and spectrum domains, we assume they will locally coordinate with one another so that only the IU with the smallest interference threshold sends its $\mathbf{T}_i$ to $\mathcal{S}$. Note that the need for coordination does not occur frequently in the real world since the grid size is usually very small (e.g., a couple hundreds of meters in length). Even if IU co-location happens, the IUs that are so densely packed in the same small grid and frequency band likely belong to the same organization. Thus, the coordination is fairly easy.

3) $\mathcal{S}$ Initializes the Interference Budget Matrix $\mathbf{N}$: Upon receiving all the IUs' input $\mathbf{T}_i$, $\mathcal{S}$ aggregates $\mathbf{T}_i$ to create $\mathbf{T}'$ by:

$$\mathbf{T}' := \sum_{i\in\text{all IUs}} \mathbf{T}_i, \tag{4}$$

such that $T'(l, h_I, f_I) := \sum_{i\in\text{all IUs}} T_i(l, h_I, f_I)$, $\forall(l, h_I, f_I)$. Note that if there exists an IU with operation position (l, h_I, f_I), $T'(l, h_I, f_I)$ equals the interference threshold of the IU. If no such IU exists, $T'(l, h_I, f_I)$ equals 0.

$\mathcal{S}$ then initializes an interference budget matrix $\mathbf{N} := \{N(l, h_I, f_I)\}_{L\times H_I\times F}$ as follows:

$$N(l, h_I, f_I) := \begin{cases} T'(l, h_I, f_I), & \text{if } T'(l, h_I, f_I) \neq 0 \\ \infty, & \text{if } T'(l, h_I, f_I) = 0 \end{cases}. \tag{5}$$

4) $\mathcal{S}$ Makes Spectrum Allocation Decision Based on SU Operation Data $\mathbf{R}_b$ and $\mathbf{N}$: SU b transmits a spectrum access request along with its operation data $\mathbf{R}_b$ to $\mathcal{S}$. Upon receiving the request, $\mathcal{S}$ computes SU b's interference to each IU operation position (l, h_I, f_I) by:

$$F_b(l, h_I, f_I) := \sum_{j, h_S, f_S} I(l, j, h_I, h_S, f_I, f_S) \times R_b(j, h_S, f_S). \tag{6}$$

$\mathcal{S}$ subtracts SU b's interference from $\mathbf{N}$ to create an interference indicator matrix $\mathbf{G}_b$ by:

$$G_b(l, h_I, f_I) := N(l, h_I, f_I) - F_b(l, h_I, f_I), \forall(l, h_I, f_I). \tag{7}$$

Based on $\mathbf{G}_b$, S will take one of the following two sets of actions.

a) If $\exists(l^\star, h_I^\star, f_I^\star)$ such that $G_b(l^\star, h_I^\star, f_I^\star) \leq 0$: In this case, the interference budget of the IU with operation position $(l^\star, h_I^\star, f_I^\star)$ is exceeded if SU b is allowed to operate. Thus, $\mathcal{S}$ denies SU b's spectrum access request.

b) Otherwise (i.e., $G_b(l, h_I, f_I) > 0, \forall(l, h_I, f_I)$): In this case, all the IUs are still safe even if SU b is allowed to operate. Thus, $\mathcal{S}$ permits SU b's spectrum access request and provides it with a valid license. $\mathcal{S}$ then lowers the interference budget matrix $\mathbf{N}$ by deducting SU b's interference from it:

$$N(l, h_I, f_I) \leftarrow N(l, h_I, f_I) - F_b(l, h_I, f_I), \forall(l, h_I, f_I). \quad (8)$$

From Step IV.A. and IV.B, we can see that, when SU b obtains the spectrum license, the interference budgets are reduced by SU b's interference. Otherwise, the budgets stay the same. In such manner, $\mathbf{N}$ is gradually reduced as more SUs obtain spectrum licenses.

Note that Step I does not require any private input data. Hence, it can be carried out in the plaintext domain. In contrast, Step II to IV involves the private IU/SU input data. Therefore, as shown in the next three subsections, they will be carefully realized in the ciphertext domain.

D. Secure Computation of Step II

To preserve the privacy of IU operation data, IU i encrypts each entry of $\mathbf{T}_i$ by pk_G, and sends the encrypted operation data $[\![\mathbf{T}_i]\!]$ to $\mathcal{S}$.

E. Secure Computation of Step III

Secure computation of Step III is tricky since formula (5) needs to determine the equality of $T'(l, h_I, f_I)$ and 0 in the ciphertext domain. This is a secure integer comparison problem, which is known as a hard problem. Even though the existing literatures have provided methods to do secure integer comparison [25], [26], they require that the integers involved in the secure computation are bit-wise encrypted. $T'(l, h_I, f_I)$, unfortunately, cannot be encrypted in this way since bit-wise encryption would make the rest of interference computation extremely complex and time-consuming. Secure integer comparison also needs multiple rounds of communications, which is also undesirable. We completely avoid the overhead of secure integer comparison by the following novel integer encoding scheme.

Our method leverages the fact that to perform homomorphic computation on both positive and negative integers in the spectrum computation, integers should be encoded in two's-complement scheme. Under this encoding scheme, representing practical radio signal strength requires only a small number of bits. For example, representing 1000W in the extremely small unit fW (i.e., 10^{-15} watt) requires only 60 bits. On the other hand, to ensure the recommended 112-bit security strength by NIST [27], the security parameter n of Paillier cryptosystem needs to be 2048 bits long. This means that the Paillier plaintext space is also 2048 bits long. Thus, we can easily identify a number k that is much smaller than 2048 but large enough so that (i) all the integer values involved in Section III-C's spectrum computation can be safely encoded in k-bit two's-complement form without the risk of overflow; (ii) $Z = 2^{k-1} - 1$, which is the largest positive value for k-bit two's-complement integers, can be used to represent ∞ in formula (5) without affecting the computation results.

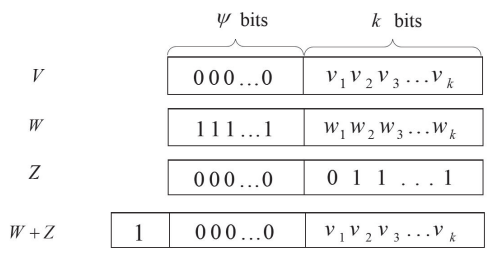


Fig. 3. Integer encoding.

With k fixed, the extra unused bits in the plaintext domain can then be leveraged to realize Step III in the ciphertext domain. Assume ψ is a small positive number. Using two's-complement encoding scheme, the representation of a k-bit positive integer V in $(k + \psi)$ bits is shown in Figure 3. Also in the context of $(k+\psi)$-bit two's-complement representation, we create two integers $W = V + 1 - 2^{k-1}$ and $Z = 2^{k-1} - 1$. We calculate $W + Z$ and the result is shown in Figure 3. Constrained by $(k + \psi)$-bit representation, the leftmost bit of $(W + Z)$ is ignored. Thus $(W + Z)$ equals V. Essentially, the above property of two's-complement encoding means that: For an $(k + \psi)$-bit integer T',

$$T' + Z = \begin{cases} V, & \text{if } T' = W = V + 1 - 2^{k-1} \\ Z = \infty, & \text{if } T' = 0 \end{cases}.$$

Based on the above property, we realize Step III in the ciphertext domain as follows. We slightly adjust an IU i's way of computing $\mathbf{T}_i$. Assume IU i's interference threshold is a k-bit positive integer V. IU i creates a $(k + \psi)$-bit integer $W = V + 1 - 2^{k-1}$ in two's-complement form. If IU i's operation position is (l, h_I, f_I), $T_i(l, h_I, f_I)$ holds W. The rest entries of $\mathbf{T}_i$ are set to 0. IU i encrypts $\mathbf{T}_i$ and submits $[\![\mathbf{T}_i]\!]$ to $\mathcal{S}$. When $\mathcal{S}$ receives all the IUs' input $[\![\mathbf{T}_i]\!]$, it executes

$$[\![\mathbf{T}']\!] := \oplus_{i \in \text{all IUs}} [\![\mathbf{T}_i]\!], \quad (9)$$

where $\oplus_{i \in \text{all IUs}}$ is the homomorphic version of $\sum_{i \in \text{all IUs}}$. Then, $[\![\mathbf{N}]\!]$ is computed by

$$[\![\mathbf{N}]\!] := [\![\mathbf{T}']\!] \oplus [\![\mathbf{Z}]\!], \quad (10)$$

where $\mathbf{Z}$ is a $(L \times H_I \times F)$-sized matrix whose entries are all set to $2^{k-1} - 1$, and we enforce a policy that the bits higher than the $(k + \psi)$th position in decrypted plaintexts should be ignored.

F. Secure Computation of Step IV

Formula (6) and (7) in Step IV can be computed securely by straightforwardly applying homomorphic operations:

$$[\![F_b(l, h_I, f_I)]\!] := \oplus_{j, h_S, f_S} I(l, j, h_I, h_S, f_I, f_S) \otimes [\![R_b(j, h_S, f_S)]\!], \quad (11)$$

$$[\![G_b(l, h_I, f_I)]\!] := [\![N(l, h_I, f_I)]\!] \ominus [\![F_b(l, h_I, f_I)]\!]. \quad (12)$$

Securely computing Step IV.A and IV.B is nontrivial. First, to decide which step to take, $\mathcal{S}$ has to determine the sign of $G_b(l, h_I, f_I)$ given only its ciphertext $[\![G_b(l, h_I, f_I)]\!]$. This is again a secure integer comparison problem.

TABLE IV
KEY CONVERSION

$\mathcal{S}$:
(i) Generate $[\![\mathbf{X}_b]\!]$ by letting

$$[\![X_b(l,h_I,f_I)]\!] := \Big(\alpha(l,h_I,f_I) \otimes [\![G_b(l,h_I,f_I)]\!] \oplus [\![\tau(l,h_I,f_I)]\!] \ominus [\![\beta(l,h_I,f_I)]\!]\Big) \otimes \epsilon(l,h_I,f_I), \quad (14)$$

where $\alpha(l,h_I,f_I)$, $\beta(l,h_I,f_I)$ are ψ-bit random numbers, and $\alpha(l,h_I,f_I) > \beta(l,h_I,f_I) > 0$. They are used to blind the true value of $G_b(l,h_I,f_I)$ without affecting its sign. $\epsilon(l,h_I,f_I)$ is chosen in $\{-1,1\}$ uniformly at random to obfuscate the sign of $G_b(l,h_I,f_I)$. $\tau(l,h_I,f_I)$ is used to avoid the undesirable reveal of $\alpha(l,h_I,f_I)$ value in the product of $\alpha(l,h_I,f_I)$ and $G_b(l,h_I,f_I)$.
(ii) Send $[\![\mathbf{X}_b]\!]$ to $\mathcal{K}$.

$\mathcal{K}$:
(iii) Decrypt $[\![\mathbf{X}_b]\!]$.
(iv) Generate $[\![\mathbf{Y}_b]\!]$ by letting

$$Y_b(l,h_I,f_I) := \begin{cases} 1, & \text{when } X_b(l,h_I,f_I) > 0 \\ -1, & \text{when } X_b(l,h_I,f_I) \le 0 \end{cases}. \quad (15)$$

(v) Encrypt $\mathbf{Y}_b$ by pk_b and send $[\![\mathbf{X}_b]\!]_{\mathsf{pk}_b}$ to $\mathcal{S}$.

$\mathcal{S}$:
(vi) Generate $[\![\mathbf{Q}_b]\!]_{\mathsf{pk}_b}$ by letting

$$[\![Q_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b} := \Big(\epsilon(l,h_I,f_I) \otimes [\![Y_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}\Big) \ominus [\![1]\!]_{\mathsf{pk}_b}, \quad (16)$$

where $\epsilon(l,h_I,f_I)$ is the same as the one in formula (14).

Second, in Step IV.B, a spectrum license specifying the operation parameters needs to be generated if an SU is allowed to operate. To preserve the privacy of the SU, these parameter specifications need to remain in the ciphertext domain and should only be revealed to the SU. In addition, to prevent the SU from forging the operation parameters, these parameter specifications also need be digitally signed. Yet, creating a digital signature in the ciphertext domain is still an open problem.

We solve the above challenges by a two-step approach as follows.

Step (1): Using the key conversion algorithm in Table IV, $\mathcal{S}$ creates $[\![Q_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$, whose plaintext satisfies:

$$Q_b(l,h_I,f_I) = \begin{cases} 0, & \text{when } G_b(l,h_I,f_I) > 0 \\ -2, & \text{when } G_b(l,h_I,f_I) \le 0 \end{cases}. \quad (13)$$

Here, $[\![Q_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$ denotes the encryption of $Q_b(l,h_I,f_I)$ by SU b's individual public key pk_b. Based on the description in Section III-C, we know that the sign of $G_b(l,h_I,f_I)$ holds the information that whether the IU with operation position (l,h_I,f_I) will be disturbed if SU b is allowed to operate. Now this information is also reflected in $Q_b(l,h_I,f_I)$. It will later be used to generate a pk_b-encrypted license in Step (2) that can be eventually decrypted by SU b.

In the algorithm of Table IV, $\mathcal{S}$ uses the blinding factors $\alpha(l,h_I,f_I)$, $\beta(l,h_I,f_I)$ and $\epsilon(l,h_I,f_I)$ in formula (14) to obfuscate the true value and sign of $G_b(l,h_I,f_I)$ respectively before sending $[\![G_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$ to $\mathcal{K}$ for key conversion. By doing this, the intermediate computation results $G_b(l,h_I,f_I)$ will not be leaked to $\mathcal{K}$. Specifically, given $X_b(l,h_I,f_I)$ by decrypting $[\![X_b(l,h_I,f_I)]\!]$ with sk_G, $\mathcal{K}$ cannot infer the true value or sign of $G_b(l,h_I,f_I)$.

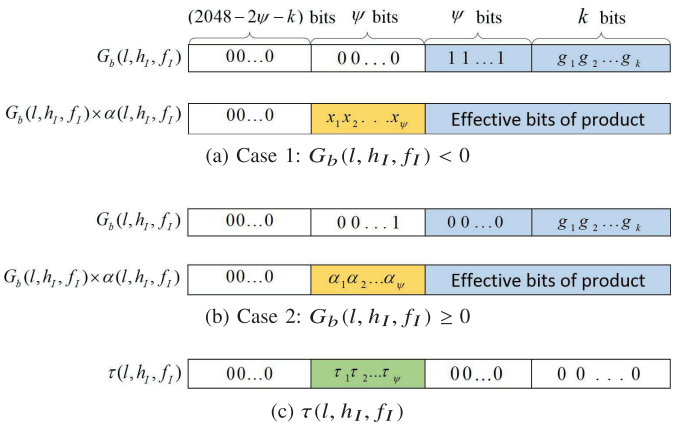


Fig. 4. Adding $\tau(l,h_I,f_I)$ for masking (a) Case 1: $G_b(l,h_I,f_I) < 0$ and (b) Case 2: $G_b(l,h_I,f_I) \ge 0$. (c) $\tau(l,h_I,f_I)$.

$\mathcal{K}$ generates $Y_b(l,h_I,f_I)$ based on the sign of $X_b(l,h_I,f_I)$ in formula (15), and encrypts it using pk_b before sending it back to $\mathcal{S}$. Finally, using the recorded sign blinding factor $\epsilon(l,h_I,f_I)$, $\mathcal{S}$ creates $[\![Q_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$ by firstly recovering the sign information of $G_b(l,h_I,f_I)$ through multiplying $[\![Y_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$ by $\epsilon(l,h_I,f_I)$, and then subtracting $[\![1]\!]_{\mathsf{pk}_b}$ in formula (16). It is easy to verify that the plaintext of $[\![Q_b(l,h_I,f_I)]\!]_{\mathsf{pk}_b}$ generated in this way conforms formula (13). Formal analysis of the relation between the value selection of the blinding factors and the effectiveness of the obfuscation can be found in Appendix 1.

Careful readers may have noticed $\tau(l,h_I,f_I)$ in formula (14). To understand the purpose of $\tau(l,h_I,f_I)$, consider the plaintext message format of $G_b(l,h_I,f_I)$ as shown in Figure 4. The upper rows of subfigure 4 and 4 illustrate how the plaintext looks like when $G_b(l,h_I,f_I)$ is negative and positive, respectively. The lower rows show the plaintext of $\alpha(l,h_I,f_I) \times G_b(l,h_i,f_I)$. As described in Section III-E, our secure computation steps assume the lower $(\psi+k)$ bits in the plaintext hold the effective data in two's-complement form, which are marked by blue color in Figure 4. Note that $\alpha(l,h_I,f_I)$ is a ψ-bit integer, so the product of $G_b(l,h_I,f_I)$ and $\alpha(l,h_I,f_I)$ takes $(k+2\psi)$-bit space. While the lower $(\psi+k)$ bits still hold the effective computation results under two's-complement encoding, the yellow part that holds the overflowed bits from the product can potentially leak information of the blinding factor $\alpha(l,h_I,f_I)$. The overflowed bits are denoted as $x_1x_2...x_\psi$ and $\alpha_1\alpha_2...\alpha_\psi$ for case 1 and case 2 in Figure 4, respectively, and $\alpha_1\alpha_2...\alpha_\psi$ is the binary representation of $\alpha(l,h_I,f_I)$. Therefore, this threat is especially acute for case 2, where the yellow part holds an exact copy of $\alpha(l,h_I,f_I)$. Therefore, to avoid the undesirable leakage of $\alpha(l,h_I,f_I)$, we add a mask $\tau(l,h_I,f_I)$ shown in subfigure 4 to the product, where $\tau_1, \tau_2, \tau_3, ..., \tau_\psi$ are random bits.

Step (2): In this step, we show how to approve/deny SU b's spectrum request by generating valid/invalid signature for spectrum license. Specifically, $\mathcal{S}$ first creates a spectrum license for SU b. The license includes the identity of SU b, the identity of license issuer $\mathcal{S}$, and $[\![\mathbf{R}_b]\!]$, which is the encrypted operation parameters of SU b that are submitted in the spectrum request.

Then, $\mathcal{S}$ uses some digital signature system (e.g., Digital Signature Algorithm) to generate a signature C_b of the license. SAS encrypts C_b by SU b's public key pk_b and obtains $[\![C_b]\!]_{\mathsf{pk}_b}$. It then computes

$$[\![D_b]\!]_{\mathsf{pk}_b} := [\![C_b]\!]_{\mathsf{pk}_b} \oplus \left(\sigma \otimes \left(\oplus_{l,h_I,f_I} [\![Q_b\,(l, h_I, f_I)]\!]_{\mathsf{pk}_b}\right)\right), \tag{17}$$

where σ is a random integer. In essence, D_b holds the valid license signature C_b if $Q_b\,(l, h_I, f_I) = 0, \forall (l, h_I, f_I)$. If for some (l^*, h_I^*, f_I^*), $Q_b(l^*, h_I^*, f_I^*) = -2$, D_b is equal to C_b+*some random number*, which is an invalid signature. This process guarantees that only the SU whose spectrum request is approved by $\mathcal{S}$ can get valid license signature.

Finally, $\mathcal{S}$ sends the spectrum license along with $[\![D_b]\!]_{\mathsf{pk}_b}$ and $[\![\mathbf{F}_b]\!]$ back to SU b. Upon decrypting $[\![D_b]\!]_{\mathsf{pk}_b}$, SU b finds out whether it is allowed to access the spectrum by examining the validity of D_b using the verification algorithm of the digital signature system. If its request is approved, SU b generates $[\![U_b(l, h_I, f_I)]\!] := [\![F_b(l, h_I, f_I)]\!] \oplus [\![0]\!]$. Otherwise, SU b generates $[\![U_b(l, h_I, f_I)]\!] := [\![0]\!]$. $[\![\mathbf{U}_b]\!]$ is then sent back to $\mathcal{S}$ along with SU b's confirmation message. $\mathcal{S}$ executes formula (8) securely by

$$[\![N(l, h_I, f_I)]\!] \leftarrow [\![N(l, h_I, f_I)]\!] - [\![U_b(l, h_I, f_I)]\!]. \tag{18}$$

Proving Forging Attempts: The above two-step approach ensures that SU b can obtain a properly signed spectrum license if and only if its operation does not disturb any IU. Note that the license only holds $[\![\mathbf{R}_b]\!]$, which can only be decrypted with sk_G. In the following, we show that a verifier $\mathcal{V}$, even without sk_G, can still easily prove an SU b' forging attempt to deviate its operation parameters from the licensed $\mathbf{R}_b$ to some other values (denoted as $\mathbf{R}'_b$).

First, $\mathcal{V}$ can observe SU b's operation near its physical location. Note that when we say $\mathcal{V}$ observes an SU's operation, we mean it is close enough to measure the radio signal of the SU so that the SU's antenna height, transmit power, transmit frequency, and location can be estimated. Techniques such as radio localization and signal spectrum analyzing can be used to derive such operation data from the emitted radio signal of the SU. It is worth mentioning that observing SUs' operation requires additional monitoring equipment, which causes additional cost. Then, $\mathcal{V}$ requests SU b to provide its operation parameters. SU b can only submit $\mathbf{R}'_b$ since if SU b lies, the operation parameters provided will not match $\mathcal{V}$'s observation. Next, $\mathcal{V}$ requests SU b to provide a copy of the signed spectrum license. Note that the license includes $[\![\mathbf{R}_b]\!]$. Then, $\mathcal{V}$ requests SU b to provide the the random number r used to create $[\![R_b(j, h_S, f_S)]\!]$ from $R_b(j, h_S, f_S)$ in the encryption process of Paillier cryptosystem. Using the Enc algorithm in Table I, $\mathcal{V}$ attempts to re-encrypt $R_b(j, h_S, f_S)$ using pk_G and r. Since pk_G and r are the same used to create $[\![R_b(j, h_S, f_S)]\!]$ from $R_b(j, h_S, f_S)$, $[\![R'_b(j, h_S, f_S)]\!]$ should be the same as $[\![R_b(j, h_S, f_S)]\!]$ if $R_b(j, h_S, f_S)$ equals $R'_b(j, h_S, f_S)$. If $[\![R_b(j, h_S, f_S)]\!] \neq [\![R'_b(j, h_S, f_S)]\!]$, $\mathcal{V}$ proves that SU b has forged its operation parameter specification. The above verification process is performed for all the operation positions. Note that SU b cannot find another random number r' that can be used to re-encrypt $R'_b(j, h_S, f_S)$ to get $[\![R_b(j, h_S, f_S)]\!]$. This is because one ciphertext can only be decrypted to one plaintext.

G. Security Analysis

1) Correctness: It is straightforward to see that, if the underlying Paillier cryptosystem is correct, P^2-SAS correctly performs the SAS process described in Section II-A. Detailed correctness proof of Paillier cryptosystem can be found in [14].

2) Privacy:

Theorem 1: P^2-SAS securely performs the SAS process in the presence of semi-honest $\mathcal{S}$ and $\mathcal{K}$ as long as Paillier cryptosystem is semantically secure, blinding factors are properly generated, and $\mathcal{S}$ and $\mathcal{K}$ are non-colluding.

Proof: This theorem can be proved using the composition theorem [19] under the semi-honest model by analyzing the security of each step in P^2-SAS. Specifically, the computation steps in $\mathcal{S}$ are all performed in the ciphertext domain, so if $\mathcal{K}$ is not colluding with $\mathcal{S}$, $\mathcal{S}$ cannot infer any private IU/SU operation information from these computation steps due to the semantic security of Paillier cryptosystem [14].

In the key conversion service, $\mathcal{K}$ can obtain the plaintext of $X_b(l, h_I, f_I)$. The privacy is still preserved if knowing $X_b(l, h_I, f_I)$ gives $\mathcal{K}$ negligible advantage in distinguishing $G_b(l, h_I, f_I)$ compared with random guesses [28]. This requirement can be fulfilled by properly generating blinding factors $\alpha(l, h_I, f_I)$, $\beta(l, h_I, f_I)$, and $\epsilon(l, h_I, f_I)$ to obfuscate the true value and sign of $G_b(l, h_I, f_I)$. The guidelines for proper generation of blinding factors and the formal security proof can be found in Appendix 1. □

IV. Tuning & Acceleration

In this section, we investigate the tradeoff between accuracy and computation overhead in interference calculation by tuning the quantization granularity parameters. We also propose effective acceleration methods to improve P^2-SAS's efficiency.

A. Tuning of Quantization Granularity

As mentioned in Section III-B, to reduce computation overhead, we quantize location and antenna height values. Quantization introduces error in attenuation estimation, which may lead to either interference underestimation or interference overestimation.

Interference underestimation happens when the estimated attenuation value is larger than the true value. It should be strictly forbidden since it may cause the accumulative interference to IUs exceeds the interference threshold. The key to eliminate interference underestimation is to always choose the quantized values that make the estimated attenuation smaller. For example, the antenna height should always be rounded up since the higher antenna makes the estimated attenuation value smaller.

Interference overestimation happens when the estimated attenuation value is smaller than the true value, which causes more consumption of interference budget in $\mathcal{S}$'s computation than necessary. Interference overestimation leads to underutilization of spectrum, which is undesirable yet tolerable.

TABLE V
BENCHMARK OF PAILLIER CRYPTOSYSTEM

Encryption	11.73 ms
Decryption	6.69 ms
Homomorphic addition	0.008 ms
Homomorphic scale (20 bits constant)	0.200 ms
Homomorphic scale (112 bits constant)	0.685 ms
Homomorphic subtraction	0.058 ms
Public key size	4096 bits
Secret key size	4096 bits
Plaintext message size	2048 bits
Ciphertext size	4096 bits

More fine-grained quantization yields more precise attenuation map, which reduces interference overestimation error at the cost of larger computation overhead. We quantitatively study the impact of quantization granularity on the tradeoff between interference overestimation error and computation overhead. Specifically, we use 4 integer metrics A, B_s, B_i, B_a to denote the quantization granularity. A is the side length of grid. SU height, IU height, and attenuation are quantized into 2^{B_s}, 2^{B_i} , 2^{B_a} levels, respectively. We formulate the following optimization problem to seek for the optimal quantization granularity setting that minimizes the interference overestimation error under constrained computation overhead.

$$\begin{aligned} \underset{A,B_s,B_i,B_a}{\text{minimize}} \quad & err(A, B_s, B_i, B_a) \\ \text{subject to} \quad & cost(A, B_s, B_i, B_a) \le C, \\ & A \in \{100, 200, ..., 500\}, \\ & B_s \in \{1, 2, 3\}, \\ & B_i \in \{1, 2, 3, 4\}, \\ & B_a \in \{1, 2, ..., 30\} \end{aligned} \tag{19}$$

Function $err(A, B_s, B_i, B_a)$ is defined as the root-mean-square error (RMSE) between the estimated attenuation values under the granularity setting (A, B_s, B_i, B_a) and the true attenuation values. Function $cost(A, B_s, B_i, B_a)$ is measured as the estimated response time to an SU's spectrum request under the granularity setting (A, B_s, B_i, B_a). Specifically, given the values of A, B_s, B_i, B_a, we can count the number of different Paillier operations executed in $\mathcal{S}$ by analyzing the formulas in Section III. For example, formula (12) needs $L*2^{B_i}*F$ homomorphic subtraction operations. The estimation of response time is obtained by multiplying the number of different Paillier operations with the average execution time per operation. A benchmark of Paillier cryptosystem is given in Table V. The cost budget C is selected according to the response time required in specific application scenarios. Note that in (19), we assume $B_s \le 3, B_i \le 4$ since 3 and 4 have been shown to be usually larger than our optimal solution of B_s and B_i and hence are safe boundary values. We set $B_a \le 30$ since 30-bit space is more than enough to accommodate all the practical attenuation values.

To solve the optimization problem of (19), we observe that it is a monotonic integer optimization problem. This type of optimization problem can be efficiently solved by the branch-and-bound method [29]. Notably, the optimization problem only needs to be solved once at the initialization stage of P^2-SAS and is not recomputed for runtime decision making.

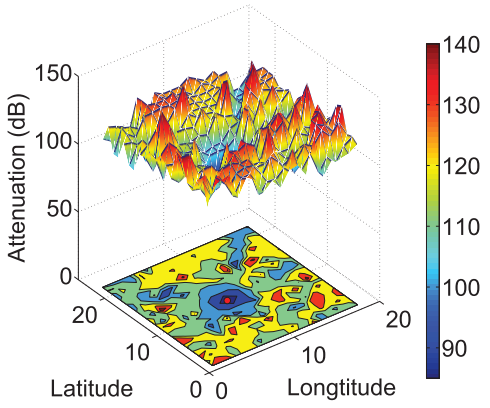


Fig. 5. Sample of attenuation map in Washington D.C. The attenuation value is measured from each coordinate point to the center.

B. Improving Efficiency

Since P^2-SAS potentially needs to serve a large number of IUs and SUs, its efficiency is critical for the scalability and practicality in the real-world deployment. In this subsection, we present some acceleration methods to improve P^2-SAS's efficiency.

1) Factoring: Through estimating the response time of $\mathcal{S}$ in Section IV-A, we observe that computing $[\![\mathbf{F}_b]\!]$ in formula (11) dominates the computation overhead of the whole system. It needs $L^2 * 2^{B_i} * 2^{B_s} * F^2$ number of $\otimes$ operations and the same number of $\oplus$ operations. By reducing the computation complexity of formula (11), we can greatly improve P^2-SAS's efficiency.

Our method is based on factoring, i.e., $\oplus_{i=1}^{K} ([\![a_i]\!] \otimes b) = \left(\oplus_{i=1}^{K} [\![a_i]\!]\right) \otimes b$. Note that the transformation from the left side of the equation to the right side can reduce the number of $\otimes$ operation from K to 1, while keeping the number of $\oplus$ operation the same. We also observe that in the real world, large areas often share the same attenuation values, as demonstrated by the sample attenuation map in Figure 5. Thus, given (l, h_I, f_I), we group the $I(l, j, h_I, h_S, f_I, f_S)$ entries that have the same value. Assume there are totally K groups and all the entries in group a equal I_a, $a = \{1, 2, ..., K\}$. Then, formula (11) can be converted to the following more efficient form:

$$[\![F_b(l, h_I, f_I)]\!] := \oplus_{a=1}^{K} \Big(I_a \otimes \Big(\oplus_{I(l,j,h_I,h_S,f_I,f_S)\in a} [\![R_b(j, h_S, f_S)]\!] \Big) \Big). \tag{20}$$

2) Precomputing if $\mathbf{I}$ Is Published: In the case where $\mathcal{S}$ does not consider the interference map $\mathbf{I}$ as proprietary data, we can further reduce $\mathcal{S}$'s computation overhead by letting $\mathcal{S}$ publish $\mathbf{I}$. Leveraging the published interference map $\mathbf{I}$, SU b can directly compute $F_b(l, h_I, f_I)$ of formula (11) in the plaintext domain, encrypt the result and send $[\![\mathbf{F}_b]\!]$ to $\mathcal{S}$ as part of the spectrum request. In this way, $\mathcal{S}$ does not need to execute formula (11) (or (20)), so that the most computationally intensive part in P^2-SAS is avoided.

This acceleration method is based on the assumption that SUs can faithfully perform the interference calculation. The assumption might not necessarily be true because there are incentives of SUs to cheat in the interference calculation process to gain illegal access to spectrum. We propose a verification mechanism to prove such cheating behavior of a suspicious SU. Specifically, a verifier can firstly get the SU's real operation parameters $\mathbf{R}_b$ by monitoring near the SU, adopting the similar technique in Section III-F. Then, the verifier requires $\mathcal{K}$ to provide the decryption of $[\![\mathbf{F}_b]\!]$. If the verifier finds that equation (6) does not hold, it proves that the suspicious SU cheats in the interference calculation.

3) Ciphertext Packing: Ciphertext packing technique [30] allows P^2-SAS to pack multiple integers into one ciphertext to reduce computation and communication overhead. Specifically, the ciphertext packing technique is applied to the formulas (9), (10), (20), (12), (14) as follows.

Recall the integer encoding policy specified in Section III-F. All the integers involved in $\mathcal{S}$'s computation can be represented in $p := (k + 2\psi)$-bit space and the lower $(k + \psi)$ bits are effective. Therefore, we can divide the 2048-bit plaintext space into $q := \lfloor 2048/p \rfloor$ segments, and each segment holds one p-bit integer. This means that q p-bit integers can be packed into one 2048-bit plaintext message. After encryption, the integers packed in one ciphertext can be homomorphically operated simultaneously.

Leveraging the ciphertext packing technique, an IU i packs q $\mathbf{T}_i$ entries together before encryption. For an SU b, if the interference map $\mathbf{I}$ is shared among SUs (Section IV-B.2's scheme is used), it packs q $\mathbf{F}_b$ entries together before encryption. If $\mathbf{I}$ is kept secret in $\mathcal{S}$ (Section IV-B.1's scheme is used), SU b can only submits the unpacked $[\![\mathbf{R}_b]\!]$ in the spectrum request to $\mathcal{S}$. The packing of $\mathbf{R}_b$ happens on $\mathcal{S}$ side. Specifically, $\mathcal{S}$ packs $[\![\mathbf{R}_b]\!]$ entries directly in the ciphertext domain by first shifting each entry using homomorphic scalar multiplication to the right bit position, and then combining these entries using homomorphic addition. With the packed $[\![\mathbf{T}_i]\!]$ and $[\![\mathbf{R}_b]\!]$, the computation overhead in formulas (9), (10), (20), (12), (14) is reduced by a factor of q.

It is worth mentioning that when applying the packing technique to formula (14), the sign-bit blinding factor ϵ cannot be packed and one ϵ will be used to scale all the $\mathbf{G}_b$ entries that are packed together, which can potentially weaken the protection on $\mathbf{G}_b$' sign. To address this problem, note that for a $(k + \psi)$-bit integer, adding $\Delta = (1\underbrace{00...0}_{k+\psi-1})_2$ only changes the sign bit. Thus, we can modify formula (14) as:

$$[\![X_b(l, h_I, f_I)]\!] := \Big(\alpha(l, h_I, f_I) \otimes [\![G_b(l, h_I, f_I)]\!] \oplus [\![\tau(l, h_I, f_I)]\!] \ominus [\![\beta(l, h_I, f_I)]\!]\Big) \oplus [\![\delta(l, h_I, f_I)]\!], \quad (21)$$

where $\delta(l, h_I, f_I)$ is uniformly chosen in $\{0, \Delta\}$. With formula (21), the packing technique can be applied to $\delta(l, h_I, f_I)$ so that the signs of the $\mathbf{G}_b$ entries packed in the same plaintext can be individually perturbed.

Careful readers may also have noticed that in formula (21), the $\mathbf{G}_b$ entries that are packed in the same plaintext are scaled by the same blinding factor α since α cannot be packed. This can cause certain loss of α's blinding effectiveness. However, it can be shown that the loss of blinding effectiveness is slight and the blinding technique is still secure. The formal proof can be found in Appendix 2.

4) Parallelization: The computation tasks of P^2-SAS are readily to be parallelized. Specifically. the entries of a matrix can be divided into subsets and the computation tasks of different subsets can be distributed to different threads and servers.

TABLE VI
EXPERIMENT PARAMETER SETTINGS

Side length of grid (A)	500 m
Bit length for SU height (B_s)	1
Bit length for IU height (B_i)	1
Bit length for attenuation (B_a)	20
Number of IUs	350
Number of SUs	20000
Number of grids (L)	650
Number of frequency channel (F)	5
Bit length of integer encoding (k)	60
Bit length of blinding factors (ψ)	220
Packing block size (p)	502
Number of packing blocks in one plaintext (q)	4

V. EVALUATION

A. Implementation

We construct the Paillier cryptosystem based on GMP library [31]. Security parameter n is set to be 2048 bits long. Table V shows a benchmark of the Paillier implementation. For parallelization implementation, we divide the computation into 24 threads and evenly distribute them to three desktops with Intel i7-3770 CPU @ 3.40GHz and 12GB RAM.

B. Evaluation Settings

To evaluate P^2-SAS, we set the service area to be a 154.82 km^2 area in Washington D.C. We employ L-R model provided by SPLAT! [32] to calculate the attenuation map $\mathbf{I}$ in this area. Real terrain data from USGS [21] and SRTM3 [22] is used in L-R model. Important experiment parameter settings are presented in Table VI. The first four parameter values are obtained by solving the optimization problem (19) in Section IV-A. There are 20000 SUs in the experiment, and we assume that each SU is scheduled to send an SU request to $\mathcal{S}$ to renew its SU license in a dedicated time slot, which is determined through some central scheduler in $\mathcal{S}$. The interference thresholds of IUs are randomly assigned between -80 dBm and -130 dBm to simulate the interference thresholds of typical radar receivers.

C. Accuracy

In this subsection, we evaluate the accuracy of P^2-SAS in spectrum allocation. Specifically, we measure the error rates of the spectrum allocation decisions made by P^2-SAS compared with the traditional SAS implementation as ground truth. In the

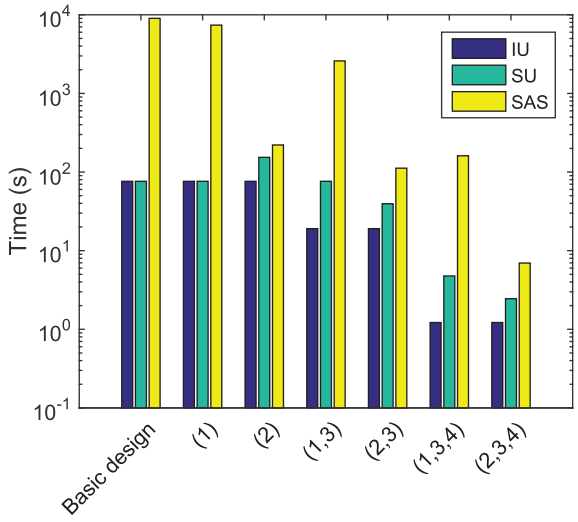


Fig. 6. Computation overhead.

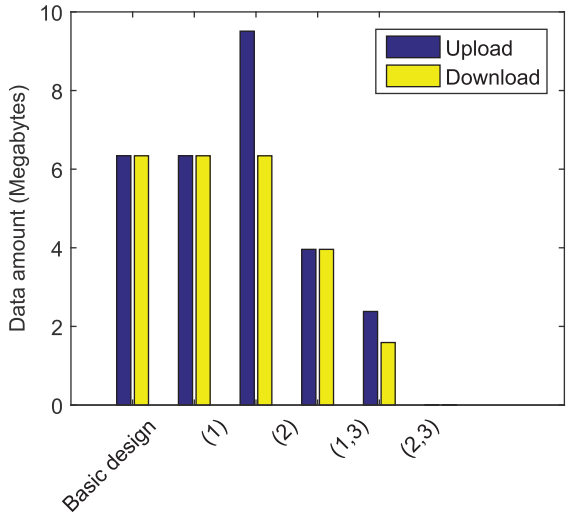


Fig. 7. Communication overhead.

traditional SAS implemented, no privacy-preserving feature is adopted, and no quantization process in the interference computation is employed. The errors we focus on include false positive error and false negative error. False positive error refers to the situation that an SU's request that should be denied in traditional SAS gets approved in P^2-SAS. This error is usually caused by interference underestimation. In contrast, false negative error refers to the situation that an SU's request that should be approved in traditional SAS gets denied in P^2-SAS. This is usually caused by interference overestimation. We run P^2-SAS for 1000 times. In each run, the operation parameters of IUs and SUs are all randomly generated. We measure the average false positive rate and false negative rate in the experiment, and the results show that the false positive rate and false negative rate are 0 and 2.72%, respectively. Therefore, P^2-SAS incurs no false positive error and very small false negative error due to the optimal tuning of quantization in Section IV-A.

D. Effectiveness of Acceleration Methods

In this subsection, we evaluate the performance improvement of different acceleration methods introduced in Section IV-B. In terms of the performance metrics, we focus on the computation overhead of each party and the communication overhead of SU in one spectrum access process. These metrics are critical to assess P^2-SAS's scalability for mobile SUs in highly dynamic environment.

The evaluation results of computation overhead and communication overhead are shown in Figure 6 and Figure 7, respectively. For simplicity, we denote the acceleration method of Section IV-B.x as (x). As can be seen in the figures, the combination of acceleration methods (2,3,4) produces the largest performance improvement with respect to both computation overhead and communication overhead. Note that the acceleration method (4) is parallelization, which will not affect the communication overhead. We will use $(2, 3, 4)$ as the default acceleration setting, and compare the accelerated P^2-SAS with the traditional SAS in Section V-E.

E. Comparison With Traditional SAS

In this subsection, we compare the performance of the accelerated P^2-SAS with the traditional SAS that has no privacy protection. For computation overhead, P^2-SAS's average processing time per SU spectrum request is 6.96 seconds as seen from Figure 6, while the average processing time of traditional SAS implementation is 0.13 seconds. For the communication overhead of SU, the uplink and downlink data amounts are 2.38 MB and 1.59 MB respectively as seen from Figure 7. For traditional SAS, the uplink and downlink data amounts are 3.51 KB and 2.53 KB, respectively. Based on the experiment result, we can compute that all the 20000 SUs' licenses can be renewed in 38.7 hours. This means that a license issued for each SU must be valid for at least 38.7 hours. We can also see that while P^2-SAS's performance is still not as good as the traditional SAS service due to the overhead of privacy protection, its performance is already very encouraging as a proof-of-concept implementation. In the real-world deployment, P^2-SAS can be hosted on advanced computing clusters to further improve its performance.

VI. Related Work

A. Privacy and Security in SAS-Driven Systems

The most relevant related work are [23] and [33]. In [33], private information retrieval (PIR) techniques are employed to protect SU's location privacy against untrusted SAS. However, in [33], only SU's privacy protection is considered, while in many DSA cases involving government-commercial sharing, IU's privacy is a more critical concern that needs to be preferentially addressed. In [23], an inference attack is identified where a malicious SU can derive IUs' operation information by examining the returned spectrum access permissions from SAS. To counter this attack, obfuscation techniques are adopted to introduce noises in the response to the SU's spectrum query, so that IUs' operation information can be somewhat protected from the malicious SU. Although the malicious SUs' threat to IUs' privacy is mitigated in [23],

it does not address the privacy threat from untrusted SAS. Other related work about security of SAS-driven DSA systems aim at mitigating attacks include malware infection [34], location spoofing [35], and secondary user faking [36].

B. Multi-Party Computation (MPC)

The secure MPC problem was introduced by Yao [37]. In general, secure MPC allows a set of n parties, each with a private input, to securely and jointly compute the output of an n-party function f over their inputs. Theoretically, the general secure multi-party computation problem is solvable using circuit evaluation protocol [38]. While this approach seems appealing in its generality, the communication complexity of the protocol depends on the size of the circuit that describes the function f, and in addition, involves large constant factors in their complexity. In recent years, fully homomorphic encryption (FHE), which can homomorphically perform both additive and multiplicative operations, are also being proposed for general MPC. The first FHE scheme was proposed in 2009 in [39]. Although research in FHE has made tremendous progress in improving efficiency [40], it is still far from practical for most of the real-world applications. Therefore, as Goldreich pointed out in [38], since these general solutions can be impractical for many MPC problems, special solutions should be developed for special cases for efficiency reasons. DSA problem, due to its complex nature, belongs to the type that cannot be efficiently solved by the general method. The purpose of this work is to find a customized solution that is much more efficient than the general theoretical solutions.

VII. Conclusion & Future Work

In this paper, we build P^2-SAS for privacy-preserving centralized DSA by converting complex spectrum allocation computation and certification procedures into the limited homomorphic computation types. Combining the unique characteristics of spectrum allocation computation with the nature of Paillier cryptosystem, we are able to significantly reduce the computation overhead of P^2-SAS. We evaluate its scalability and practicality using experiments based on real-world data. Experiment results show that P^2-SAS can respond an SU's spectrum request in 6.96 seconds with communication overhead of less than 4 MB.

The current design of P^2-SAS only manages the spectrum sharing between IUs and SUs. The spectrum sharing among SUs is not yet considered. Some recent DSA proposals by FCC and the research community [5] also explore the possibility of using SAS to manage spectrum sharing among SUs. We plan to incorporate this new feature of SAS design into the future version of P^2-SAS. We also plan to extend the current design to handle some specific DSA scenarios, such as 3-tier model in 3.5 GHz. Finally, we seek to relax the semi-honest requirement of P^2-SAS and consider malicious adversary scenarios in the future. The discussion of countering malicious SUs in Section III-B is the first step towards this direction.

Appendix

A. Security Analysis on the Blinding Factor in Formula (14)

We use blinding factors $\alpha(l, h_I, f_I)$, $\beta(l, h_I, f_I)$, and $\epsilon(l, h_I, f_I)$ in formula (14) to obfuscate the sensitive intermediate results $G_b(l, h_I, f_I)$ to Key Distributor. By carefully choosing these blinding factors, the security can be guaranteed by making the probability of distinguishing $G_b(l, h_I, f_I)$ given $X_b(l, h_I, f_I)$ at Key Distributor negligible compared with random guesses. Formally, it means that we need to carefully determine the distribution of the random integers α and β so that, given that one knows X and the fact that $X = \epsilon(\alpha G - \beta), \epsilon \xleftarrow{\$} \{1, -1\}$ ($\xleftarrow{\$}$ denotes that ϵ is drawn uniformly at random from $\{1, -1\}$) for some integer G, the value of G can have ρ different uniformly distributed choices and the probability of distinguishing the right G value is only $1/\rho$. When ρ is large enough, we can say the obfuscating technique is secure enough. Let us first consider the case where $\epsilon = 1$ and $G > 0$, that is to say: $X + \beta = \alpha \times G$ and $G > 0$. Since $\alpha > \beta \geq 0$, we also have $X > 0$ in this case. Under this case, we have the following definition and theorem.

Definition 3: Given that one knows X, $X > 0$, we define the set $S_G(X)$

$$S_G(X) = \{G_1, G_2, ..., G_n\} \tag{22}$$

be the set of possible G values, where (1) $\exists \alpha_i > \beta_i \geq 0$, $s.t. X + \beta_i = \alpha_i \times G_i$. (2) $G_i \neq G_j, \forall i \neq j$. (3) $G_i > 0, \forall i$.

Theorem 2: If $X = a^2$ or $X = a^2 \pm a$, for some $a \geq 2$, $a \in \mathbb{Z}$, $|S_G(X)| + 1 = |S_G(X + 1)|$. Otherwise, $|S_G(X)| = |S_G(X + 1)|$.

Proof of Theorem 2: Assuming that $G_i \in S_G(X)$, by Definition 3, there exists $\alpha_i > \beta_i \geq 0$ that makes $X + \beta_i = \alpha_i \times G_i$.

Case 1.1: $\beta_i \neq 0$ In this case, rearranging $X + \beta_i = \alpha_i \times G_i$, we get $(X + 1) + (\beta_i - 1) = \alpha_i \times G_i, \alpha_i > \beta_i - 1 \geq 0$, which means that $G_i \in S_G(X + 1)$. In essence, it means that in this case, an element $G_i \in S_G(X)$ is mapped to the same element $G_i \in S_G(X + 1)$.

Case 1.2: $\beta_i = 0$ and $G_i - \alpha_i < -1$

In this case, $X = \alpha_i \times G_i$. So we also have $X = G_i \times \alpha_i$ and $G_i > 0$, which means $\alpha_i \in S_G(X)$. Rearrange $X = \alpha_i \times G_i$ as $(X + 1) + (G_i - 1) = (\alpha_i + 1) \times G_i$. Since $\alpha_i + 1 > G_i - 1$, so $G_i \in S_G(X + 1)$. Since $G_i > G_i - 1$, so $(\alpha_i + 1) \in S_G(X + 1)$.

Next, we prove $\alpha_i + 1 \notin S_G(X)$. The proof is based on considering the contradiction. Assume there exists Δ satisfying $X + (G_i + \Delta + \Delta \times \alpha_i) = (G_i + \Delta)(\alpha_i + 1)$. To make $\alpha_i + 1 \in S_G(X)$, we should have $G_i + \Delta > G_i + \Delta + \Delta \times \alpha_i \geq 0$. Equivalently, $G_i + \Delta > G_i + \Delta + \Delta \times \alpha_i \Leftrightarrow \Delta \times \alpha_i < 0 \Leftrightarrow \Delta < 0$. $G_i + \Delta + \Delta \times \alpha_i \geq 0$ & $\Delta < 0 \Leftrightarrow G_i \geq -(1 + \alpha_i)\Delta \geq 1 + \alpha_i$, which contradicts with $G_i - \alpha_i < -1$. So $\alpha_i + 1 \notin S_G(X)$.

We also can prove that $\alpha_i \notin S_G(X + 1)$. The proof is also based on contradiction.

In summary, in case 1.2, element $G_i \in S_G(X)$ and its companion element $\alpha_i \in S_G(X)$ uniquely maps to two entries $G_i \in S_G(X + 1)$ and $(\alpha_i + 1) \in S_G(x + 1)$.

Case 1.3: $\beta_i = 0$ and $G_i - \alpha_i > 1$

In this case, we have $X = \alpha_i \times G_i$ and $\alpha_i - G_i < -1$. This case is the same as case 1.2 except that G_i and

α_i is exchanged. Thus, using the same proof of case 1.2, we can get $G_i \in S_G(X), \alpha_i \in S_G(X), \alpha_i \in S_G(X+1), G_i+1 \in S_G(x+1), G_i \notin S_G(X+1)$ and $G_i+1 \notin S_G(X)$.

In summary, in case 1.3, element $G_i \in S_G(X)$ and its companion element $\alpha_i \in S_G(X)$ uniquely maps to two entries $G_i+1 \in S_G(X+1)$ and $\alpha_i \in S_G(x+1)$.

With the above case studies, we can draw the following conclusions. In case 1.1, one element in $S_G(X)$ uniquely maps to one element in $S_G(X+1)$. In case 1.2 and 1.3, two companion entries in $S_G(X)$ uniquely map to two entries in $S_G(X+1)$. Similarly, we can also prove that the map holds from the opposite direction, i.e. $S_G(X+1)$ to $S_G(X)$. Specifically, given $\forall G_j \in S_G(X+1)$, there exists $(X+1)+\beta_j = \alpha_j * G_j$. $\alpha_j > \beta_j \geq 0$. When $\alpha_j > \beta_j + 1$, we can prove one element in $S_G(X+1)$ uniquely maps to one element in $S_G(X)$. This condition corresponds to case 1.1. When $\alpha_j = \beta_j + 1$ & $G_j - \beta_j < 1$, or $\alpha_j = \beta_j + 1$ & $G_j - \beta_j > 3$, we can also find two companion entries in $S_G(X+1)$ uniquely map to two entries in $S_G(X)$. These conditions corresponds to case 1.2 and 1.3.

Case 2: $\beta_i = 0$ and $|G_i - \alpha_i| \leq 1$, equivalently $X = G_i^2$ or $X = G_i * (G_i - 1)$

Similar to Case 1.2, from $X = \alpha_i \times G_i$, we have $\alpha_i \in S_G(x)$. Rearrange $X = \alpha_i \times G_i$ as follows:

$(X+1)+(G_i-1) = (\alpha_i+1) \times G_i$. Since $|G_i - \alpha_i| \leq 1 \Leftrightarrow (\alpha_i+1) > (G_i-1)$, so $G_i \in S_G(X+1)$. Since $G_i > (G_i-1)$, $\alpha_i + 1 \in S_G(X+1)$.

$(X+1)+(\alpha_i-1) = (G_i+1) \times \alpha_i$. Since $|G_i - \alpha_i| \leq 1 \Leftrightarrow (G_i+1) > (\alpha_i-1)$, $\alpha_i \in S_G(X+1)$. Since $\alpha_i > (\alpha_i-1)$, $G_i + 1 \in S_G(X+1)$.

When $G_i - \alpha_i = 0$, $X = G_i^2$. We have $G_i \in S_G(X+1)$ and $G_i + 1 \in S_G(X+1)$. Using proof by contradiction (similar with the proof in case 2), we can show that $G_i + 1 = \alpha_i + 1 \notin S_G(X+1)$. In this case, we have $G_i = \alpha_i \in S_G(X), G_i = \alpha_i \in S_G(X+1), G_i + 1 = \alpha_i + 1 \in S_G(X+1)$ and $G_i + 1 = \alpha_i + 1 \notin S_G(X)$.

When $G_i - \alpha_i = -1$, $X = G_i \times (G_i - 1)$, we have $G_i \in S_G(X), G_i + 1 \in S_G(x), G_i \in S_G(X+1), G_i + 1 \in S_G(X+1), G_i + 2 \in S_G(X+1)$. In addition, using contradiction, we can also show that $G_i + 2 \notin S_G(X)$.

In Case 2, two companion entries in $S_G(X)$ map to three entries in $S_G(X+1)$. Since Case 2 only happens for one G_i value in $S_G(X)$ when $X = a^2$ or $X = a^2 - a$, we know that $|S_G(X)| + 1 = |S_G(X+1)|$ in this case. For other X values, only case 1.1, 1.2 and 1.3 can happen, which makes $|S_G(X)| = |S_G(X+1)|$. □

From Theorem 2, it is not hard to see that $|S_G(X)|$ can be expressed by the following fomula:

$$|S_G(X)| = \begin{cases} 2a-1 & \text{if } a(a-1)+1 \leq X \leq a^2 \\ 2a & \text{if } a^2+1 \leq X \leq a(a+1), \end{cases} \quad (23)$$

where $a \geq 2, a \in \mathbb{Z}$. Formula (23) also completely matches the numerical analysis results shown in Figure 8.

When ϵ is randomly picked in $\{-1, 1\}$ and G can be both positive and negative integers, it is easy to see that the possible number of choices of G values to a given X will be $2|S_G(X)|$. Then, we can use $2|S_G(X)|$ to determine the parameter settings of $\alpha(l, h_I, f_I)$ and $\beta(l, h_I, f_I)$ in formula (14). Specifically, if we want the time/advantage ratio to be 2^w, we can tune the blinding factors $\alpha(l, h_I, f_I)$ and $\beta(l, h_I, f_I)$ so that in the distribution of $X_b(l, h_I, f_I)$, the probability of $X(l, h_I, f_I) < 2^{2*w-4}$ is negligible. In this way, each $X_b(l, h_I, f_I)$ is mapped to at least 2^w choices of $G_b(l, h_I, f_I)$, so the time/advantage ratio to guess the real one is at least 2^w. In this paper, we set $\alpha(l, h_I, f_I)$ and $\beta(l, h_I, f_I)$ as 220 bits random positive integers so that the blinding factor scheme has security strength of at least 112 bits, which is consistent with the 2048 bit Paillier cryptosystem that we have implemented.

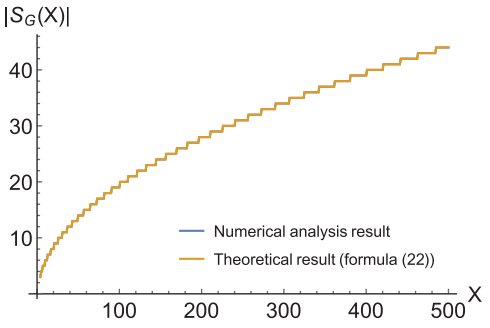


Fig. 8. Theoretical result in formula (23) and numerical analysis result.

B. Security Analysis of the Packing Technique in Formula (14)

As discussed in Section IV-B.3, while using the packing technique, the same α will be used to scale the $G_b(l, h_I, f_I)$ entries packed in the same 2048-bit plaintext. We have the following theorem to address the security issue.

Theorem 3: In formula (14), using the same α to scale the $G_b(l, h_I, f_I)$ entries packed in the one plaintext message will reduced the security level by $2q$-2 bits, where q is the number of $G_b(l, h_I, f_I)$ entries packed together in one plaintext.

Proof of Theorem 3: Consider the whole plaintext denoted as G. Given X which is calculated by G following (14), the number of different G satisfying $X = \epsilon(\alpha G - \beta)$ is $2*2\sqrt{2^{2048}} = 2^2 * 2^{1024}$. Now we consider each $G_b(l, h_I, f_I)$ entry packed in the plaintext G. Assume we are using different α for each entry, so the total number of $G_b(l, h_I, f_I)$ combinations to get X is $(2 * 2\sqrt{2^{2048/q}})^q = 2^{2q} * 2^{1024}$. So the time/advantage ratio is reduce from $2^{2q} * 2^{1024}$ to $2^2 * 2^{1024}$ and the security level is reduced by $2q - 2$ bit. □

Since we only pack $q = 4$ segments in one 2048-bit plaintext, we only lose 6-bit security level.

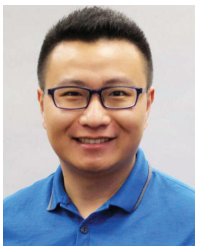
ACKNOWLEDGMENT

The authors would like to thank the reviewers for their helpful comments and feedback.

REFERENCES

[1] Y. Dou *et al.*, "P^2-SAS: Preserving users' privacy in centralized dynamic spectrum access systems," in *Proc. ACM MobiHoc*, 2016, pp. 321–330.

[2] G. Locke and L. Strickling, "Plan and timetable to make available 500 megahertz of spectrum for wireless broadband," U.S. Dept. Commerce, Washington, DC, USA, 2010.
[3] P. Kolodzy and I. Avoidance, "Spectrum policy task force," Federal Commun. Commission, Washington, DC, USA, Tech. Rep. 02-135, 2002.
[4] *Report to the President Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth*, PCAST, Washington, DC, USA, 2012.
[5] "Amendment of the commission rules with regard to commercial operations in the 3550-3650 MHz band," Notice Proposed Rulemaking Order, Federal Commun. Commission, Washington, DC, USA, Tech. Rep. DA-15-955., 2012, pp. 112–148.
[6] *Mobile Broadband Services in the 2300 MHz—2400 MHz Frequency Band Under Licensed Shared Access regime*, document ETSI TR 103113 V1.1.1, 2013.
[7] FCC, "Shared commercial operations in the 3550–3650 MHz band," *Federal Register*, vol. 80, no. 120, pp. 73674–73675, Jun. 2015.
[8] *Google's Spectrum Access System Allows Spectrum Sharing*, accessed on July 2016. [Online]. Available: http://www.androidheadlines.com/2015/05/googles-spectrum-access-system-allows-spectrum-sharing.html
[9] P. Bogetoft *et al.*, "Secure multiparty computation goes live," in *Financial Cryptography Data Security*. Berlin, Germany: Springer, 2009, pp. 325–343.
[10] Y. Lindell and B. Pinkas, "Secure multiparty computation for privacy-preserving data mining," *J. Privacy Confidentiality*, vol. 1, no. 1, p. 5, 2009.
[11] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical," in *Proc. 3rd ACM Workshop Cloud Comput. Secur. Workshop*, 2011, pp. 113–124.
[12] *Longley-Rice Methodology for Evaluating TV Coverage and Interference*, document FCC 69, Office of Eng. and Technol. (OET) Bulletin, 2004.
[13] M. Schneider and T. Schneider, "Notes on non-interactive secure comparison in 'image feature extraction in the encrypted domain with privacy-preserving SIFT,"' in *Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur.*, 2014, pp. 135–140.
[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, 1999, pp. 223–238.
[15] Y. Dou *et al.*, "Preserving incumbent users' privacy in server-driven dynamic spectrum access systems," in *Proc. IEEE ICDCS*, Jun. 2016, pp. 729–730.
[16] Y. Dou, K. C. Zeng, Y. Yang, and K. Ren, "Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems: Poster," in *Proc. ACM MobiCom*, 2016, pp. 473–474.
[17] C. Bazelon, *The Economic Basis of Spectrum Value: Pairing AWS-3 With the 1755 MHz Band is More Valuable Than Pairing it With Frequencies From the 1690 MHz Band*. Washington, DC, USA: The Brattle Group, 2011.
[18] Commerce Spectrum Management Advisory Committee, "Final report of working group 1—1695–1710 MHz meteorological-satellite," Nat. Telecommun. Inf. Agency, Washington, DC, USA, Tech. Rep. 22, 2013.
[19] O. Goldreich, *Foundations of Cryptography: Basic Applications*, vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[20] *Small Entity Compliance Guide: Amendment of the Commission's Rules With Regard to Commercial Operations in the 3550–3650 MHz Band*, document FCC Gaussian Noise Docket 12-354, FCC, 2015.
[21] *USGS Terrain Datasets*, accessed on Jul. 2016. [Online]. Available: http://dds.cr.usgs.gov/pub/data/DEM/250/
[22] *SRTM3 Terrain Datasets*, accessed on Jul. 2016. [Online]. Available: http://dds.cr.usgs.gov/srtm/version2_1/SRTM3/
[23] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Proc. IEEE DYSPAN*, Apr. 2014, pp. 236–247.
[24] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*. Berlin, Germany: Springer, 2006, pp. 1–12.
[25] O. Catrina and S. de Hoogh, "Improved primitives for secure multiparty integer computation," in *Security and Cryptography for Networks*. Amalfi, Italy: Springer, 2010, pp. 182–199.
[26] I. Damgård, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft, "Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation," in *Theory of Cryptography*. Berlin, Germany: Springer, 2006, pp. 285–304.
[27] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, "Recommendation for key management—Part 1: General (revision 3)," *NIST Special Pub.*, vol. 800, no. 57, pp. 1–147, 2012.
[28] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC, 2014.
[29] M. Minoux, H. Tuy, and N. T. Hoai-Phuong, "Discrete monotonic optimization with application to a discrete location problem," *SIAM J. Optim.*, vol. 17, no. 1, pp. 78–97, 2006.
[30] T. Ge and S. Zdonik, "Answering aggregation queries in a secure system model," in *Proc. VLDB*, 2007, pp. 519–530.
[31] T. Granlund and The GMP Development Team, *GNU MP: The GNU Multiple Precision Arithmetic Library*, 6th ed. 2014. [Online]. Available: http://gmplib.org/
[32] *SPLAT!*, accessed on Jul. 2016. [Online]. Available: http://www.qsl.net/kd2bd/splat.html
[33] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2751–2759.
[34] Y. Dou, K. C. Zeng, Y. Yang, and D. D. Yao, "MadeCR: Correlation-based malware detection for cognitive radio," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 639–647.
[35] K. Zeng, S. K. Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2014, pp. 202–210.
[36] X. Jin, J. Sun, R. Zhang, and Y. Zhang, "SafeDSA: Safeguard dynamic spectrum access against fake secondary users," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 304–315.
[37] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. FOCS*, Oct. 1986, pp. 162–167.
[38] O. Goldreich, "Secure multi-party computation," in *Proc. Manuscript Preliminary Version*, 1998, pp. 86–97.
[39] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.
[40] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical GapSVP," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2012, pp. 868–886.



Yanzhi Dou (S'15) received the B.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2013. He is currently pursuing the Ph.D. degree in computer engineering at Virginia Tech, Blacksburg, VA, USA. His research interests include wireless networking, mobile systems, network security, and privacy. He has authored papers in the ACM MobiHoc, the IEEE INFOCOM, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is a student member of the IEEE and ACM.

Kexiong (Curtis) Zeng (S'14) received the B.S. degree in communications engineering from UESTC, China, in 2013. He is currently pursuing the Ph.D. degree in computer engineering at Virginia Tech, Blacksburg, VA, USA. His research is mainly focused on building/securing computer networks and systems, especially for wireless and mobile ones.

He Li received the B.Sc. and M.S. degrees in electrical and computer engineering from Shanghai Jiao Tong University, Shanghai, China, in 2010 and 2013, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical And Computer Engineering, Virginia Tech, Blacksburg, VA, USA. His research interests include security and privacy issues in wireless networks, spectrum enforcement, and applied cryptography.

Yaling Yang (M'06) received the Ph.D. degree in computer science from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 2006. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, USA. Her current research interests include network security and privacy, wireless network modeling and design, and networks powered by energy harvesting. She was a recipient of U.S. NSF Faculty Early Career Award. She has been the Principle Investigator of eight NSF funded projects.

Bo Gao (M'15) received the B.S. degree in electrical engineering from Beijing Jiaotong University, Beijing, China, in 2006, the M.S. degree in electrical engineering from Shanghai Jiaotong University, Shanghai, China, in 2009, and the Ph.D. degree in computer engineering from Virginia Tech, Blacksburg, VA, USA, in 2014. He is currently an Assistant Professor with the Institute of Computing Technology, Chinese Academy of Sciences. His research interests include next-generation wireless communications and networking, dynamic spectrum sharing, and mobile computing.

Kui Ren (M'07–SM'11–F'16) received the Ph.D. degree from the Worcester Polytechnic Institute, Worcester, MA, USA. He is currently a Professor of Computer Science and Engineering and the Director of the UbiSeC Lab, State University of New York at Buffalo, Buffalo, NY, USA. His current research interest spans cloud and outsourcing security, wireless and wearable systems security, and mobile sensing and crowdsourcing. His research has been supported by the NSF, the DoE, the AFRL, the MSR, and the Amazon. He was a recipient of SEAS Senior Researcher of the Year in 2015, Sigma Xi/IIT Research Excellence Award in 2012, and NSF CAREER Award in 2011. Kui has authored 150 peerreview journal and conference papers and received several Best Paper Awards including IEEE ICNP 2011. He currently serves as an Associate Editor of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE WIRELESS COMMUNICATIONS, the IEEE INTERNET OF THINGS JOURNAL, and the IEEE TRANSACTIONS ON SMART GRID. He is also a Distinguished Lecturer of the IEEE, a member of the ACM, and a past Board Member of the Internet Privacy Task Force, State of Illinois.

Shaoqian Li (F'16) received the B.S.E. degree in communication technology from the Northwest Institute of Telecommunication, Xidian University, Xi'an, China, in 1982, and the M.S.E. degree in communication system from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1984. He is currently a Professor, a Ph.D. Supervisor, and the Director of the National Key Laboratory of Communication, UESTC, and a member of the National High Technology Research and Development Program (863 Program) Communications Group. His research interests include wireless communication theory, anti-interference technology for wireless communications, spread-spectrum and frequency-hopping technology, and mobile and personal communications.