A Note on One Privacy-Preserving Centralized Dynamic Spectrum Access System

Lihua Liu[1] and Xinyuan Cao[2]
(Corresponding author: Lihua Liu)
Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai 201306, China
School of Business, East China University of Science and Technology, China[2]
Email: liulh@shmtu.edu.cn
(Received Sept. 24, 2020; Revised and Accepted Apr. 24, 2021; First Online Oct. 19, 2021)

Abstract

Dynamic spectrum access technique is a crucial solution to mitigate the potential spectrum scarcity problem. Recently, Dou *et al.* have presented a privacy-preserving centralized dynamic spectrum access system [IEEE Journal on Selected Areas in Communications, vol. 35, no. 1, pp. 173–187, 2017], based on Paillier public-key encryption and secure multi-party computation. This note shows that the scheme fails to prevent the distributor from determining whether a target secondary user is authorized by the server and recover the user's operation data. The practical running modulus in the suggested public key encryption is 4096 bits, and the encryption should be used to blind all data, not any session key as usual. The shortcoming renders the scheme quite inefficient.

Keywords: Dynamic Spectrum Access; Paillier Encryption; Running Modulus; Secure Multi-party Computation

1 Introduction

Centralized spectrum management is a mechanism to govern the spectrum sharing between government incumbent users (IUs) and commercial secondary users (SUs). With the development of spectrum access system, privacy has become more and more serious. Since operation information of government IUs is often classified, these IUs' operation data are highly sensitive. Similarly, SUs' operation data may also be sensitive commercial secrets for their operators.

In 2013, Gao *et al.* [9] considered the location privacy in database-driven cognitive radio networks. After that, Bahrak *et al.* [1, 20] investigated the problem of location spoofing attack and its countermeasures in database-driven cognitive radio networks. Jin *et al.* [12] presented a scheme for safeguard dynamic spectrum access against fake secondary users. In 2016, Dou *et al.* [7] also presented a scheme for preserving incumbent users' privacy in exclusion-zone-based spectrum access systems.

Thakur *et al.* [17,18] designed several frame structures for hybrid spectrum access strategy in cognitive radio communication systems, and authentication protocols for passive RFID tags. Clark *et al.* [6, 11] proposed a scalable spectrum access system for massive machine type communication. In 2019, Karimi *et al.* [3,5,13] have considered the problem of robust spectrum access for hybrid interweave-underlay cognitive radio systems using probabilistic spectrum access, and that of fair dynamic spectrum management in licensed shared access systems. Very recently, Pan *et al.* [4,10,16] have presented an enhanced secure smart card-based password authentication scheme.

Multi-party computation (MPC) allows multiple parties to jointly compute a function over their inputs, while keeping these inputs, the intermediate computation results and the outputs private. In 2009, Bogetoft *et al.* [2] discussed the practical implementation of MPC. Lindell and Pinkas investigated the possible application of MPC for privacy-preserving data mining. In 2018, Martins *et al.* [14] provided a good survey on fully homomorphic encryption (an engineering perspective). Recently, Yahyaoui and Kettani [19] designed an efficient fully homomorphic encryption scheme.

In 2017, Dou *et al.* [8] have presented a privacy-preserving centralized dynamic spectrum access system based on the Paillier public key encryption [15] and multi-party computation. It claimed that none of the IU (incumbent user) or SU (secondary user) operation data would be exposed to any snooping party. But we find the scheme is flawed, because the new entity, Key Distributor, can decide whether a target SU is authorized by the server. He can also recover the target SU's operation data. Besides, the suggested running modulus in the secure multi-party computation is of 4096 bits which renders the scheme is very inefficient.

2 Preliminaries

The involved secure multi-party computation in the scheme is based on the below variation of Paillier encryption [15].

Key generation. Choose two big primes p and q to compute $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$. Pick $g \in \mathbb{Z}^*_{n^2}$ to compute

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n, \text{where} L(x) = \frac{x-1}{n}$$

Set the public key pk as (n, g) and the secret key sk as (λ, μ).

Encryption. Given $m \in \mathbb{Z}_n$, pick a one-time random number r to compute

$$[[m]] = \text{Enc}_{pk}(m, r) = g^{(m+nr)} \bmod n^2.$$

Decryption. Given the ciphertext $[[m]]$, recover the plaintext by computing

$$m = \text{Dec}_{sk}([[m]]) = L([[m]]^\lambda \bmod n^2) \cdot \mu \bmod n.$$

3 Review of the Scheme

In the scheme, there are four entities: incumbent users (IUs), secondary users (SUs), a SAS Server $\mathcal{S}$, and a Key Distributor $\mathcal{K}$. The Server is semi-honest who can only passively monitor the executions to infer IU/SU's operation information, and cannot actively deviate from the process. The server $\mathcal{S}$ is responsible for computing spectrum allocation. The distributor $\mathcal{K}$ will not collude with the server $\mathcal{S}$ to compromise IU/SU's operation data.

The challenges for a SAS system include:

1) To ensure accurate interference management, it usually adopts complex radio propagation models, which could incur huge computation and communication overhead;
2) It should ensure that SUs' operation will not disturb any IU;
3) If an SU's spectrum access request is approved, it needs to issue a license that permits the SU to access the spectrum in a certain pattern.

The goal of the system is to realize the SAS process correctly, while preserving the IU/SU's data privacy from the semi-honest SAS server. The privacy-related parameters are summarized as follows (Table 1).

The plain scenario of spectrum access system and its secure multi-party computation scenario can be described below (Table 2). The involved operations are defined as follows, where the integers $m_1, m_2 \in \mathbb{Z}_n$ are encoded in the two's complement forms without the risk of overflow.

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

Table 1: The related parameters

parameter parameter	notation 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	—

4 Analysis

Let $\text{sign}(x) = 1$ if $x > 0$, or -1 if $x \leq 0$. The essential relations in the scheme are that

$$\begin{aligned}
\text{sign}(X_b(l, h_I, f_I)) &= \text{sign}(G_b(l, h_I, f_I)) \cdot \text{sign}(\epsilon(l, h_I, f_I)), \\
\text{sign}(Y_b(l, h_I, f_I)) &= \text{sign}(X_b(l, h_I, f_I)), \\
Q_b(l, h_I, f_I) &= \text{sign}(\epsilon(l, h_I, f_I)) \cdot \text{sign}(Y_b(l, h_I, f_I)) - 1 \\
&= \text{sign}(G_b(l, h_I, f_I)) - 1 \\
&= 0 \text{ or } -2, \\
\mathbf{D}_b &= \mathbf{C}_b + \sigma \sum_{l, h_I, f_I} Q_b(l, h_I, f_I).
\end{aligned}$$

If and only if $\sum_{l, h_I, f_I} Q_b(l, h_I, f_I) = 0$, *i.e.*,

$$\sum_{l, h_I, f_I} (\text{sign}(G_b(l, h_I, f_I)) - 1) = 0$$

. The signature $\mathbf{C}_b$ is valid, and the user SU_b is securely authorized. The corresponding requirement in the plain scenario is that $G_b(l, h_I, f_I) > 0, \forall (l, h_I, f_I)$.

◇ *The new scenario should introduce a special entity to play the role of Distributor $\mathcal{K}$.* In the secure multi-party computation scenario, the server $\mathcal{S}$ only obtains $[[\mathbf{R}_b]], [[\mathbf{T}_i]], [[\mathbf{Y}_b]]_{pk_b}, [[\mathbf{U}_b]]$, but fails to recover the plaintexts $\mathbf{R}_b, \mathbf{T}_i$. How about the new entity $\mathcal{K}$ (the key distributor)? It suggests that [8]: "In the real world, S can be operated by some commercial third party (*e.g.*, Google) for enhanced efficiency and scalability; $\mathcal{K}$ is operated by IUs." It also specifies that: "$\mathcal{K}$ creates a group Paillier public/private key pair (pk_G, sk_G)." We want to stress that the suggestion is hard to implement practically because there are generally many incumbent users, and it is a big challenge to share the secret key sk_G among them. Moreover, it is not easy for them to answer $\mathcal{S}$'s requests dynamically and collaboratively. So, it is better to introduce a special entity to play the role.

◇ *The Distributor $\mathcal{K}$ can decide whether the secondary user SU_b is authorized by the server. Besides, he can recover the SU_b's operation data.* It specifies that [8]: "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." That means $\mathcal{K}$ is not fully honest. Otherwise, the server $\mathcal{S}$ can simply send $[[\mathbf{G}_b]]$ to $\mathcal{K}$, instead of its camouflage $[[\mathbf{X}_b]]$. So, the new entity $\mathcal{K}$ is assumed to have the intention to snoop IU/SU operation data. But

Table 2: Two different scenarios of SAS

The plain scenario		
SU_b (secondary user)	$\mathcal{S}$ (centralized spectrum access system server)	IUs (incumbent users)
Generate $\mathbf{R}_b$. $\xrightarrow{\mathbf{R}_b}$	Compute the attenuation map $\mathbf{I} = \{I(l, j, h_I, h_S, f_I, f_S)\}$, $\mathbf{T}' = \sum_i \mathbf{T}_i$, and the interference budget matrix $\mathbf{N} = \{N(l, h_I, f_I)\}$, where $N(l, h_I, f_I) = T'(l, h_I, f_I)$ if $T'(l, h_I, f_I) \neq 0$, otherwise set $N(l, h_I, f_I) = \infty$. Compute the interference indicator matrix $\mathbf{G}_b$ by $F_b(l, h_I, f_I) = \sum_{j,h_S,f_S} R_b(j, h_S, f_S) \times I(l, j, h_I, h_S, f_I, f_S)$, $G_b(l, h_I, f_I) = N(l, h_I, f_I) - F_b(l, h_I, f_I)$. If $\exists\ (l^*, h_I^*, f_I^*)$ s.t., $G_b(l^*, h_I^*, f_I^*) \leq 0$, deny SU_b's request. Otherwise, return a valid license to SU_b. Update $\mathbf{N}$ by $N(l, h_I, f_I) \leftarrow N(l, h_I, f_I) - F_b(l, h_I, f_I)$.	Update $\mathbf{T}_i$. $\xleftarrow{\mathbf{T}_i}$
The secure multi-party computation based scenario		
SU_b	$\mathcal{S}$	IUs
Generate $\mathbf{R}_b$ and encrypt it as $[[\mathbf{R}_b]]$ by pk_G. $\xrightarrow{[[\mathbf{R}_b]]}$	Compute $\mathbf{I} = \{I(l, j, h_I, h_S, f_I, f_S)\}$, $[[\mathbf{T}']] = \sum_i [[\mathbf{T}_i]]$, $[[\mathbf{N}]] = [[\mathbf{T}']] \oplus [[\mathbf{Z}]]$, where $\mathbf{Z}$'s entries are all set to $2^{k-1} - 1$. Compute $[[F_b(l, h_I, f_I)]] = \oplus_{j,h_S,f_S} [[R_b(j, h_S, f_S)]] \otimes I(l, j, h_I, h_S, f_I, f_S)$, $[[G_b(l, h_I, f_I)]] = [[N(l, h_I, f_I)]] \ominus [[F_b(l, h_I, f_I)]]$. Choose $\alpha(l, h_I, f_I) > \beta(l, h_I, f_I) > 0, \tau(l, h_I, f_I)$, and pick $\epsilon(l, h_I, f_I) \in \{-1, 1\}$ to compute $[[X_b(l, h_I, f_I)]] = (\alpha(l, h_I, f_I) \otimes [[G_b(l, h_I, f_I)]] \oplus [[\tau(l, h_I, f_I)]] \ominus [[\beta(l, h_I, f_I)]]) \otimes \epsilon(l, h_I, f_I)$. $\xrightarrow{[[\mathbf{X}_b]]}$	Update $\mathbf{T}_i$ and encrypt it as $[[\mathbf{T}_i]]$ by pk_G. $\xleftarrow{[[\mathbf{T}_i]]}$ $\mathcal{K}$ who is practically operated by IUs, uses sk_G to decrypt $[[\mathbf{X}_b]]$. Generate $[[\mathbf{Y}_b]]$ by letting $Y_b(l, h_I, f_I) = 1$ if $X_b(l, h_I, f_I) > 0$, or $Y_b(l, h_I, f_I) = -1$ if $X_b(l, h_I, f_I) \leq 0$. Encrypt it as $[[\mathbf{Y}_b]]_{pk_b}$ by pk_b. $\xleftarrow{[[\mathbf{Y}_b]]_{pk_b}}$
	Generate $[[\mathbf{Q}_b]]_{pk_b}$ by letting $[[Q_b(l, h_I, f_I)]]_{pk_b} = \left(\epsilon(l, h_I, f_I) \otimes [[Y_b(l, h_I, f_I)]]_{pk_b}\right) \ominus [[1]]_{pk_b}$. Create a spectrum license $\mathfrak{L}$ for SU_b. Generate a signature $\mathbf{C}_b$ of the license $\mathfrak{L}$. Pick a random integer σ to compute $[[\mathbf{D}_b]]_{pk_b} = [[\mathbf{C}_b]]_{pk_b} \oplus (\sigma \otimes\ (\oplus_{l,h_I,f_I} [[Q_b(l, h_I, f_I)]]_{pk_b}))$. $\xleftarrow{\mathfrak{L},[[\mathbf{D}_b]]_{pk_b},[[\mathbf{F}_b]]}$	
Decrypt $[[\mathbf{D}_b]]_{pk_b}$. For $\forall\ (l, h_I, f_I)$, check whether $\mathbf{D}_b$ is a valid signature. If true, compute $[[\mathbf{U}_b]]$ by setting $[[U_b(l, h_I, f_I)]] = [[F_b(l, h_I, f_I)]] \oplus [[0]]$. Otherwise, set it be $[[0]]$. $\xrightarrow{[[\mathbf{U}_b]]}$	Update $[[\mathbf{N}]]$ by $[[N(l, h_I, f_I)]] \leftarrow [[N(l, h_I, f_I)]] \ominus [[U_b(l, h_I, f_I)]]$.	

it is hard for $\mathcal{K}$ to practically eavesdrop all communications between all secondary users and the server, or that between all incumbent users and the server.

In the new scheme, $\mathcal{K}$ needs to generate $[[\mathbf{Y}_b]]_{pk_b}$ for the target user SU_b. So, he only needs to eavesdrop the communications between the target user and the server to obtain $[[\mathbf{F}_b]]$, $[[\mathbf{U}_b]]$. He then recovers $\mathbf{F}_b$, $\mathbf{U}_b$, and checks that

$$U_b(l, h_I, f_I) = F_b(l, h_I, f_I), \forall\ (l, h_I, f_I).$$

If true, $\mathcal{K}$ can decide that the user SU_b is authorized. Clearly, he can also recover the operation data $\mathbf{R}_b$ from the tapped data $[[\mathbf{R}_b]]$. Thus, the scheme cannot truly prevent the Distributor $\mathcal{K}$ from knowing the data.

$\diamond$ *The new scheme is too inefficient to implement practically.* As we see, the computations in the plain scheme can be restricted to an upper bound w, say $w = 2^{40}$, because only the usual multiplications are involved. The new scheme needs to perform lots of modular exponentiations with the modulus n^2, where n is of 2048 bits. The working parameter is of 4096 bits. It is very time-consuming because one modular exponentiation almost takes 0.0156 second (on PC, Intel(R) Core(TM) i7-479 CPU 3.60GHz, RAM 4.00GB). Note that the working parameter for RSA cryptosystem is of 2048 bits. Moreover, RSA is only used for encrypting session keys (invoked by the subsequent symmetric key encryption, such as AES), instead of any practical message.

5 Conclusion

We show that the Dou *et al.*'s scheme fails to prevent the Key Distributor from knowing users' operation data,

although it can prevent the Server from knowing the data. It is still a challenge to efficiently and systematically combine homomorphic encryption into secure multi-party computation. We would like to stress that the Paillier cryptosystem is a public key encryption which seems unsuited to directly blinding any information data because of its huge working modulus.

Acknowledgements

We thank the National Natural Science Foundation of China (project 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] B. Bahrak and *et al.*, "Protecting the primary users' operational privacy in spectrum sharing," in *Proceedings of IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN'14)*, pp. 236–247, Apr. 2014.

[2] P. Bogetoft and *et al.*, "Secure multiparty computation goes live," in *International Conference on Financial Cryptography and Data Security*, pp. 325–343, Feb. 2009.

[3] M. M. Butt and *et al.*, "Fair dynamic spectrum management in licensed shared access systems," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2363–2374, 2019.

[4] Y. H. Chen and *et al.*, "Research on the secure financial surveillance blockchain systems," *International Journal of Network Security*, vol. 22, no. 4, pp. 708–716, 2020.

[5] S.F. Chiou and *et al.*, "Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications," *International Journal of Network Security*, vol. 21, no. 1, pp. 100–104, 2019.

[6] M. A. Clark and K. Psounis, "Trading utility for privacy in shared spectrum access systems," *IEEE/ACM Transactions on Networking*, vol. 26, no. 1, pp. 259–273, 2018.

[7] Y. Z. Dou and *et al.*, "Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems: Poster," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom'16)*, pp. 473–474, Oct. 2016.

[8] Y. Z. Dou and *et al.*, "P^2-SAS: Privacy-preserving centralized dynamic spectrum access system," *IEEE Journal of Selected Areas in Communications*, vol. 35, no. 1, pp. 173–187, 2017.

[9] Z. Y. Gao and *et al.*, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proceedings IEEE INFOCOM*, pp. 2751–2759, Apr. 2013.

[10] L. C. Huang, C. H. Chang, and M. S. Hwang, "Research on malware detection and classification based on artificial intelligence," *International Journal of Network Security*, vol. 22, no. 5, pp. 717–727, 2020.

[11] B. A. Jayawickrama and *et al.*, "Scalable spectrum access system for massive machine type communication," *IEEE Network*, vol. 32, no. 3, pp. 154–160, 2018.

[12] X. C. Jin and *et al.*, "Safedsa: Safeguard dynamic spectrum access against fake secondary users," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 304–315, Oct. 2015.

[13] M. Karimi, S. Sadough, and M. Torabi, "Robust spectrum access for hybrid interweave-underlay cognitive radio systems using probabilistic spectrum access," *IET Signal Processing*, vol. 13, no. 9, pp. 806–813, 2019.

[14] P. Martins, L. Sousa, and A. Mariano, "A survey on fully homomorphic encryption: An engineering perspective," *ACM Computing Surveys*, vol. 50, no. 6, pp. 83:1–83:33, 2018.

[15] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, May 1999.

[16] H. T. Pan, H. W. Yang, and M. S. Hwang, "An enhanced secure smart card-based password authentication scheme," *International Journal of Network Security*, vol. 22, no. 2, pp. 358–363, 2020.

[17] P. Thakur and *et al.*, "Advanced frame structures for hybrid spectrum access strategy in cognitive radio communication systems," *IEEE Communications Letters*, vol. 21, no. 1, pp. 410–413, 2017.

[18] C. H. Wei, M. S. Hwang, and A. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[19] A. Yahyaoui and M. Kettani, "An efficient fully homomorphic encryption scheme," *International Journal of Network Security*, vol. 21, no. 1, pp. 91–99, 2019.

[20] K. C. Zeng, S. K. Ramesh, and Y. L. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in *Proceedings of IEEE Conference on Communications and Network Security (CNS'14)*, pp. 202–210, Oct. 2014.

Lihua Liu, associate professor, with Department of Mathematics at Shanghai Maritime University, received her PhD degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics and cryptography.

Xinyuan Cao is currently pursuing her bachelor degree from School of Business, East China University of Science and Technology. Her research interests include E-business and marketing management.