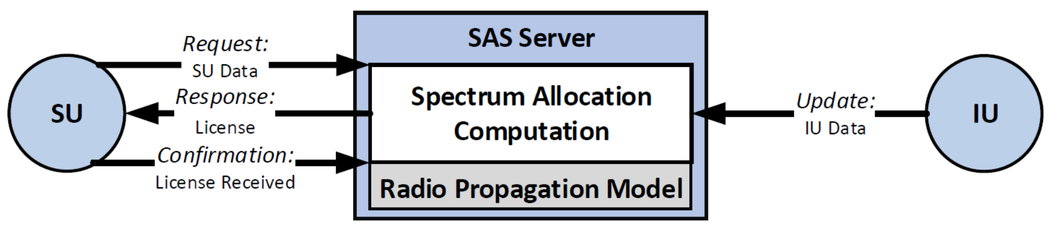
P2-SAS:Preserving Users' Privacy in Dynamic Spectrum Access Systems

Yanzhi Dou
yzdou@vt.edu, yzdou.info

Background:

1. To mitigate the potential spectrum scarcity problem and spur economic growth, PCAST and FCC have proposed spectrum access system (SAS) to realize the full potential of government-hold spectrum by sharing with wireless broadband operators/users.
2. PCAST and FCC allow industry third parties to operate SAS to enhance its efficiency and scalability.
3. Critical Privacy issues.



Goals & Challenges:

Our goal is to fundamentally address the privacy challenge by developing a privacy-preserving SAS (P2-SAS) based on secure multiparty computation (MPC).

However, designing MPC for SAS encounters the following challenges:

1. Radio propagation calculation incurs very high overhead.
2. Determining whether SUs' interference will exceed an IU's sensitivity level involves secure integer comparison.
3. SAS needs to sign a spectrum license to prevent forgery attempts, while efficient signature generation using MPC is unexplored yet.

System Design:

The privacy-related parameters in interference calculation are differentiated from those that are public knowledge. Both IUs and SUs encrypt their privacy-related operation data using the group public key pk_G before sending to SAS.

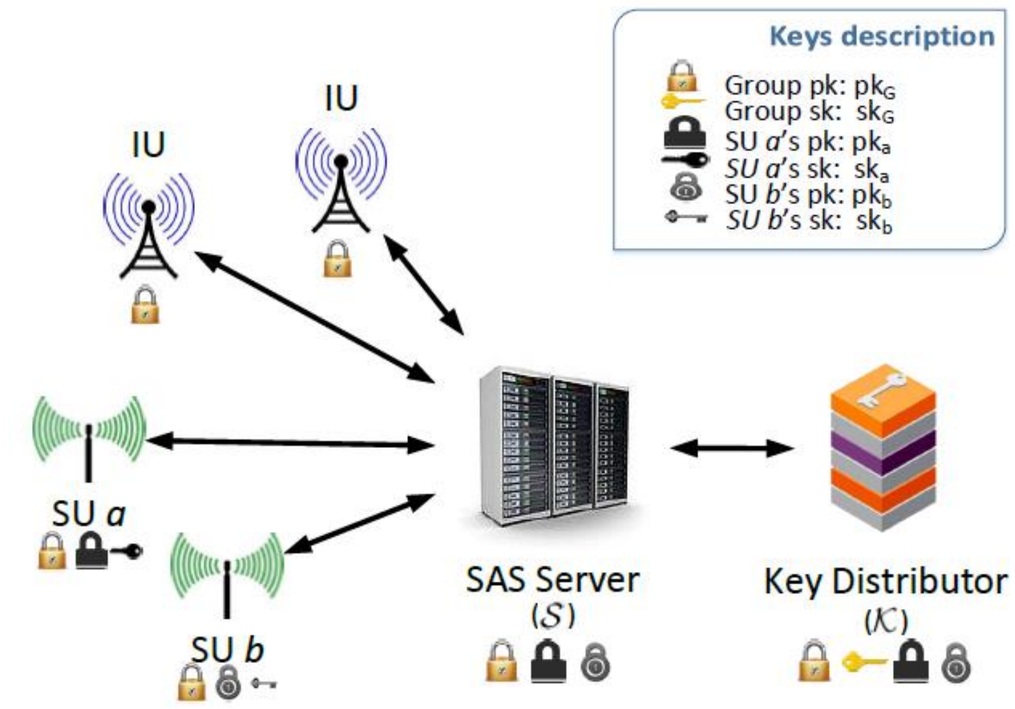
The core operation of spectrum allocation in SAS is firstly to *calculate whether the addition of an SU's interference will exceed any IU's interference threshold,* and then sends the SU a valid/invalid spectrum access license accordingly.

Homomorphic properties:

Addition($\oplus$): $\mathsf{Dec}_{\mathsf{sk}}\left(\widehat{m_1} \oplus \widehat{m_2}\right) = m_1 + m_2.$

Scalar multiplication($\otimes$): $\mathsf{Dec}_{\mathsf{sk}}\left(c \otimes \widehat{m}\right) = c \cdot m.$

Subtraction($\ominus$): $\mathsf{Dec}_{\mathsf{sk}}\left(\widehat{m_1} \ominus \widehat{m_2}\right) = m_1 - m_2.$



SAS:

$$\widehat{F_b}(l,h_I,f_I) := \oplus_{j,h_S,f_S}\left[I(l,j,h_I,h_S,f_I,f_S)\otimes\widehat{R_b}(j,h_S,f_S)\right]$$

$$\widehat{G_b}(l,h_I,f_I) := \widehat{N}(l,h_I,f_I)\ominus\widehat{F_b}(l,h_I,f_I)$$

$$\widehat{X_b}(l,h_I,f_I) := \left[[\alpha(l,h_I,f_I)\otimes\widehat{G_b}(l,h_I,f_I)]\oplus\widehat{\tau}(l,h_I,f_I)\ominus\widehat{\beta}(l,h_I,f_I)\right]\otimes\epsilon(l,h_I,f_I)$$

Key Distributor:

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

SAS:

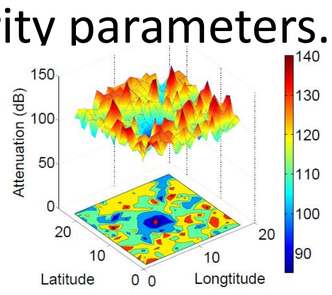
$$\widehat{Q_b}^{\mathsf{pk}_b}(l,h_I,f_I) := \left[\epsilon(l,h_I,f_I)\otimes\widehat{Y_b}^{\mathsf{pk}_b}(l,h_I,f_I)\right]\ominus\widehat{1}^{\mathsf{pk}_b}(l,h_I,f_I)$$

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

$$\widehat{N}(l,h_I,f_I)\leftarrow\widehat{N}(l,h_I,f_I)-\widehat{U_b}(l,h_I,f_I)$$

System Refinement

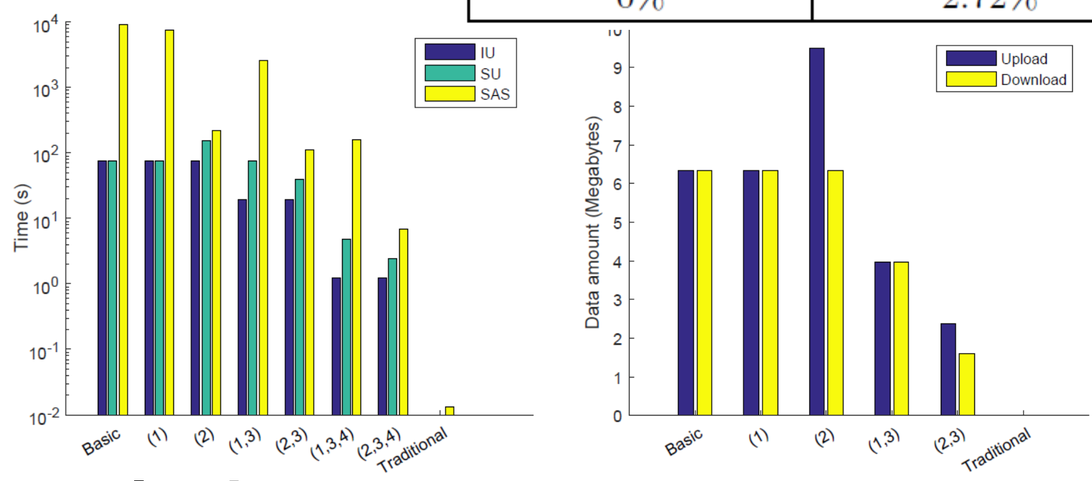
- Optimize the quantization granularity parameters.
- Factoring
- Precomputing
- Ciphertext Packing
- Parallelization



Implementation & Evaluation

- 3 laptops @3.4GHz, 24 threads.
- 2048-bit Paillier, 112-bit security level
- Washington D.C.

False positive rate	False negative rate
0%	2.72%



Conclusion

In this paper, we build P2-SAS for privacy-preserving SAS 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 P2-SAS.

This work got accepted to *ACM* MobiHoc 2016.