عنوان مقاله:

Reducing The Computational Complexity of Fuzzy Identity-Based Encryption from Lattice

محل انتشار:

مجله بین المللی ارتباطات و فناوری اطلاعات, دوره 16, شماره 1 (سال: 1402)

تعداد صفحات اصل مقاله: 8

نویسندگان:

Sedigheh Khajouei-Nejad - North Tehran Branch, Islamic Azad University Tehran, Iran

Hamid Haj Seyyed Javadi - Shahed University Tehran, Iran

Sam Jabbehdari - North Tehran Branch, Islamic Azad University Tehran, Iran

Seyed Mohammad Hossein Moattar - Mashhad Branch, Islamic Azad University Mashhad, Iran

خلاصه مقاله:

In order to provide access control on encrypted data, Attribute-based encryption (ABE) defines each user using a set of attributes. Fuzzy identity-based— encryption (FIBE) is a variant of ABE that allows for a threshold access structure for users. To address the potential threat posed by future quantum computers, this paper presents a postquantum fuzzy IBE scheme based on lattices. However, current lattice-based ABE schemes face challenges related to computational complexity and the length of ciphertext and keys. This paper aims to improve the performance of an existing fuzzy IBE scheme by reducing key length and computational complexity during the encryption phase. While negative attributes are not utilized in our scheme, we prove its security under the learning with error (LWE) hard problem assumption in the selective security model. These improvements have significant implications for the field of .ABE

کلمات کلیدی:

(Attribute-Based Encryption (ABE), Fuzzy Identity-Based Encryption (FIBE), policy, access structure, lattice, Learning with Errors (LWE

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1957575