KENZA GUENDA, UVIC/ USTHB

Code-based cryptography

In the realm of post-quantum cryptography, code-based cryptography has garnered significant attention. The ongoing NIST standardization process for post-quantum cryptographic primitives has further heightened interest and accelerated research in this field. Code-based cryptographic primitives, which rely on the difficulty of decoding seemingly random error-correcting codes, have proven particularly robust against quantum computer-based attacks. Unlike traditional cryptographic methods that rely on the hardness of number-theoretic problems (such as the factorization problem or the discrete logarithm problem), code-based cryptography exploits the complexity of general decoding issues, like the syndrome decoding problem. The purpose of this talk is to discuss the codes based cryptography. We will discuss some systemes preset their weakess, discuss some attacks. We also present our new variants .