ELIAS HASSANI, University of Saskatchewan

A post-quantum, post-AI data encryption method

We discuss a new symmetric-key cipher for digital data encryption. Its implementations are fast, memory efficient, and resilient against classical, AI-assisted, and quantum attacks. Let x, k, and c be elements of a finite abelian group G with operation $+$ and the neutral element 0. Suppose one is given ciphertext $c = x + k$. Retrieving the plaintext $x = c - k$ from the ciphertext c is trivial when one knows the key k. However, not knowing the key, the task is a blind search. To recover x, we would require an efficient criterion for distinguishing x by its characteristic features, if such were known, from all other group elements. Furthermore, even if one were availed of such a tool, the average number of trials is prohibitively difficult when the group is sufficiently large. The challenge to achieve a real-life implementation of the said schema is to find a very large G, and to construct algorithms enabling an immersion of *real digital data* in G and efficient operations $\pm$. In real life, even more security considerations need to be addressed. We outline a solution for this challenge, characterized by additional desirable features. This is joint work with Artur Sowa, Francis Bui, Grant Harris, and Jonathan Norton (all based at USASK).