Stream cipher over Finite Fields: A Difference Algebra Approach

Roberto La Scala
Università degli Studi di Bari, Italy

30th Applications of Computer Algebra - ACA 2025

Many stream ciphers of real practical interest, such as Trivium and Bluetooth's E0, can be modeled as systems of difference equations with coefficients and solutions in a finite field. Alongside this system of equations, one also needs a polynomial that enables the calculation of the keystream elements from the cipher register. This register can indeed be considered the state whose evolution is governed by the system of explicit ordinary difference equations. Such a system ensures that each state is uniquely determined by the initial state, which effectively serves as the cipher's key. We will refer to this class of stream ciphers as "difference ciphers".

Using the formalism of Difference Algebra, it is possible to define some relevant properties of stream ciphers, in particular their invertibility and periodicity. These properties are introduced in terms of fundamental functions associated with the difference system, such as the "state transition endomorphism" and its corresponding "state transition map". Additionally, it is possible to precisely define an algebraic attack on the cipher based on the knowledge of a certain number of keystream elements. The property of a cipher being invertible also allows for the optimization of such an attack, which can drastically reduce the security of the cryptosystem. Indeed, assuming invertibility, it is sufficient to calculate any internal state, such as the one from which the keystream begins, to know the initial state that contains the key. To determine if a difference cipher is invertible, one can use the calculation of a Gröbner basis of an ideal associated with the state transition endomorphism. This computation also yields the inverse difference system, enabling the reversal of the cipher's clock progression.

Another critical property for the security of such stream ciphers is the non-linearity of the difference equations and/or the keystream polynomial. Indeed, it is well known that a system of LFSRs, which corresponds to the fully linear case, can be attacked in polynomial time. In the presence of non-linear equations in the system, however, an algebraic attack corresponds to solving a system of non-linear polynomial equations over a finite field, the resolution of which is generally an NP-complete problem. Using the notion of difference cipher, we can analyze the various systems of polynomial equations corresponding to different types of algebraic attacks and understand why they are complex to solve.

Finally, to illustrate these concepts and the corresponding cryptanalytic techniques, we consider the stream ciphers Trivium and E0. These ciphers have been the subject of recent attacks in [1], [2], [3].

References

[1] La Scala, Roberto; Pintore, Federico; Tiwari, Sharwan K.; Visconti, Andrea. A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium. *Finite Fields Appl.*, 98 (2024), Paper No. 102452, 1–33.

[2] La Scala, Roberto; Polese, Sergio; Tiwari, Sharwan K.; Visconti, Andrea. An algebraic attack to the Bluetooth stream cipher E0. *Finite Fields Appl.*, 84 (2022), Paper No. 102102, 1–29.

[3] La Scala, Roberto; Tiwari, Sharwan K. Stream/block ciphers, difference equations and algebraic attacks. *J. Symbolic Comput.*, 109 (2022), 177–198.