Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

Stellingen

Behorende bij het proefschrift

Algorithmic Techniques in Algebraic Cryptanalysis and their Applications

1. In contrast to traditional approaches in Gröbner bases algorithms, it is preferable to optimize and describe the algorithm design alongside its data structures (taking into account the density or sparsity of the polynomials). (*Chapter 5 of this thesis*)

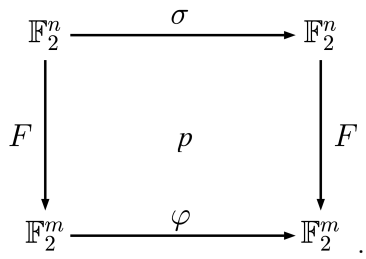
2. The hybrid approach with a Gröbner bases algorithm is the most effective strategy in practice to find a solution for underdefined quadratic system of equations over $\mathbb{F}_{256}$ and $\mathbb{F}_{31}$. However, the same strategy does not apply as effectively to systems of equations over $\mathbb{F}_2$.
(*Chapter 6 of this thesis*)

3. A common technique in transforming a system of polynomial equations in the variables $x_1, x_2, \ldots, x_n$ into an equivalent one with lower degree is to substitute quadratic terms using auxiliary variables, say $x_i x_j = y_{i,j}$, and add the corresponding equations $x_i x_j - y_{i,j}$ to the system. However, when modelling logical constraints as a system of polynomial equations, a different choice of ring of coefficients (than the ring of definition) may produce polynomials of lesser degree without the need for extra variables or additional polynomials.
(*Chapter 7 of this thesis*)

4. In differential (resp. linear) cryptanalysis of a cryptographic function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, to understand the algebraic implications of a chosen differential (resp. linear approximation) one should study the corresponding polynomial ideal. As a system of equations, the polynomials in a Gröbner basis of the ideal represent the necessary and sufficient conditions for such differential (resp. linear approximation) over F to hold.
(*Chapter 8 of this thesis*)

---

5. A unifying view that generalizes the cryptanalysis of a symmetric-key primitive $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ operating on a pair of inputs (resp. outputs), such as differential cryptanalysis, is to express one input (resp. output) as a function of the other. This leads to a probabilistic equality of the form $F(\sigma(x)) = \varphi(F(x))$ which holds with probability p when x is sampled uniformly at random. This relationship can be illustrated by the following probabilistic commutative diagram:



For instance, a differential $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ over F is represented by a pair of translations (σ, φ) where $\sigma(x) = x + \alpha$ and $\varphi(y) = y + \beta$. This point of view offers a greater degree of freedom than those techniques that require a chosen binary operation, such as differential or rotational-XOR cryptanalysis.

6. To analyze the security of symmetric-key primitives, an integrated use of different automated tools, such as SMT (Satisfiability Modulo Theories) and MILP (Mixed-Integer Linear Programming), can yield better results than those obtained by using each tool independently. [MR22]

7. Global competition for new cryptographic standards serve as a catalyst for gathering the complexity estimates of all known attacks on the proposed schemes, implemented as open-source software (like [BMSV22]). This promotes transparency, guarantees the verifiability of results, improves understanding of the trade-offs between the attacks, and helps in deciding new parameters for the schemes.

8. The development and standardization effort of post-quantum cryptographic schemes are worthwhile irrespective of the existence of quantum computers.

---

9. Individuals have a right to privacy and it is the duty of democratic nation-states to safeguard this right regardless of whether a person can or wishes to pay for its protection.

References

[BMSV22] Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. In Lejla Batina and Joan Daemen, editors, *Progress in Cryptology - AFRICACRYPT 2022: 13th International Conference on Cryptology in Africa, Fes, Morocco, July 18-20, 2022, Proceedings*, volume 13503 of *Lecture Notes in Computer Science*, pages 323–347. Springer Nature Switzerland, 2022.

[MR22] Rusydi H. Makarim and Raghvendra Rohit. Towards Tight Differential Bounds of Ascon: A Hybrid Usage of SMT and MILP. *IACR Transactions on Symmetric Cryptology*, 2022(3):303–340, Sep. 2022.

Rusydi H. Makarim
Leiden, 27 May 2026