TP 7: applications of polynomial arithmetic

Jean-Sébastien Coron

Université du Luxembourg

1 Secret-sharing

Implement the secret-sharing protocol described in the course.

2 Finite field

2.1 Finite-field implementation

Implement addition, multiplication and inversion operations in the finite field $GF(2)/(f)$ where $f = x^8 + x^4 + x^3 + x + 1$ is irreducible over $GF(2)$.

2.2 AES

The finite field $GF(2)/(f)$ is used in the definition of the AES algorithm [1].

Using the previous implementation of $GF(2)/(f)$, implement the substitution table (S-Box) over $GF(2^8)$ described in [1]. Check you results with Figure 7 in [1].

References

1. FIPS 197, *The Advanced Encryption Standard (AES)*, available at `csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.