Medium Galois Fields, their Bases and Arithmetic

Preda Mihăilescu[1]

M_EC

A.5.x Basic Concepts

Let p be a prime, $k > 1$ an integer and $\mathbb{K} = \mathbb{F}_{p^k}$ be the $k-$th degree Galois extension of the prime Galois field $\mathbb{F}_p$.

I **The root power bases of $\mathbb{K}$.**
Let $b \in \mathbb{F}_p$ be such that

$$b^{\frac{p-1}{q}}, \quad \text{for all primes } q|k.$$

Then the polynomial $f_b(x) = x^k - b$ is irreducible over $\mathbb{F}_p$ and it generates $\mathbb{K}$ up to isomorphism. If $\beta \in \mathbb{K}$ is a root of f, thus $\beta^k = b$, then

$$\mathcal{B} = \{\infty, \beta, \beta^{\in}, \ldots, \beta^{\|-\infty}$$

is a **root power base** for $\mathbb{K}$ over $\mathbb{F}_p$. The concept of Kummer extensions over the rational field is related to this.

II **The Frobenius in a root power base** The Forbenius map $\sigma : \mathbb{K} \longrightarrow \mathbb{K}$ defined by

$$\sigma(\alpha) = \alpha^p, \qquad \forall \alpha \in \mathbb{K}$$

is an automorphism and it generates the Galois group of $\mathbb{K}$ over $\mathbb{F}_p$. Suppose that $ip = m_i k + r_i$, with $0 \leq r_i < k$, for $i = 1, 2, \ldots, k-1$. As a consequence, for elements $\alpha \in \mathbb{K}$ developed over the base $\mathcal{B}$,

$$\begin{aligned}\sigma(\alpha) = \sigma\left(\sum_{i=0}^{k-1} a_i\beta^i\right) &= \left(\sum_{i=0}^{k-1} a_i\beta^i\right)^p \\ = \sum_{i=0}^{k-1} a_i \cdot (\beta^{i\cdot p}) &= \sum_{i=0}^{k-1} a_i \cdot b^{m_i} \cdot \beta^{r_i}.\end{aligned}$$

This shows that raising an element in $\mathbb{K}$ to the power p is reduced to

(i) Multiplying its coefficients a_i in the power root base $\mathcal{B}$ by some fixed constants b^{m_i}, which only depend upon the choice of the element $b \in \mathbb{F}_p$ which generates the extension.

(ii) Consequently permuting these products according to the rule $i \mapsto r_i,\ i = 1, 2, \ldots, k-1$.

III **Roots of Unity** Consider the case when p and k are related by

$$p = 2km + 1. \tag{1}$$

In this case, $r_i = i$ and $m_i = 2mi,\ i = 1, 2, \ldots k-1$. Furthermore,

$$b^{m_i} = b^{i \cdot \frac{p-1}{k}} = \zeta^i,$$

where $\zeta = b^{\frac{p-1}{k}} \in \mathbb{F}_p$ is a $p-$th primitive root of unity. In this particular case thus, the action of the Frobenius has the additional properties:

(iii) The permutation in (i) is the identity (since $r_i = i$).

(iv) The multipliers b^{m_i} in (i) are actually roots of unity.

A.5.x+1 Arithmetic

The bases for finite extension fields introduced in A.5.x are practical for high performance arithmetic. The choice of the field characteristic may in this case be made, so as to ease the arithmetic. Practical choices of p will

(v) Be "close" to the machine word length B, so as to take maximal advantage of the base machine arithmetic and make modular reduction simple. Thus $p = B - l$, where l is among the smallest positive integers making p prime, or $p = 2^{31} - 1$, or $p = 2^{64} - 2^{32} + 1$ are some examples of practical choices for the characteristic p.

We shall denote fields with characteristic chosen this way *medium Galois fields*. We also make the implicit assumption that medium Galois fields are presented in a root power base $\mathcal{B}$. The name is given since the characteristic p close to machine word length lays between the most frequent, extreme, cases which are $p = 2$, a small characteristic requiring a large extension degree k and degree $k = 1$, for which the characteristic p has to be large. For medium Galois fields, one may use as a rule of thumb the fact that the amount of information upon which security is based is given by $\Phi_k(p)$, with Φ_k being the $k-$th cyclotomic polynomial. The best security is thus achieved for prime values of k. Note that $\Phi_k(p)$ is the size of the largest multiplicative subgroup of $\mathbb{K}$.

We now give some rules for the arithmetic in medium Galois fields. In the complexity discussion of these operations, one must consider that multiplication in $\mathbb{F}_p$ is machine integer multiplication, since by the choice of p, elements of $\mathbb{F}_p$ require one machine word.

A.5.x+1.1 Multiplication in the medium Galois fields

Let first $x, y \in \mathbb{F}_p$; multiplication in $\mathbb{F}_p$, thus computing $z = x \cdot y \in \mathbb{F}_p$ consists of one integer multiplication and a subsequent reduction mod p, where use of the special choice (v) of p may be made.

Let $\alpha, \alpha' \in \mathbb{K}$. Then

$$\alpha \cdot \alpha' = \Big(\sum_i a_i \beta^i\Big) \cdot \Big(\sum_i a_i{}' \beta^i\Big) = \sum_{j=0}^{2k-1} c_j \beta^j = \sum_{j=0}^{k-1} (c_j + b c_{k+j}) \beta^j, \qquad \text{where :}$$

$$c_j = \sum_{i=0}^{j} a_i \cdot a'_{j-i}, \quad j = 1, 2, \ldots 2k-1,$$

and the coefficients with index $i \geq k$ are supposed to be 0. The advantage of the root power consists in the fact that the reduction modulo $f(x)$ of the product of the polynomial representations for α and α' is trivial essentially amounting to k multiplications and k additions in $\mathbb{F}_p$. to $c_j, j < k$. The action of the Frobenius automorphism on β is:

A.5.x+1.2 Exponentiation in the medium Galois fields

If $1 < n < p^k - 1$ is an exponent, a quick way for computing α^n uses the p - adic representation of $n : n = \sum_i n_i p^i$. With this,

$$\alpha^n = \alpha^{\sum_i n_i p^i} = \prod_i \sigma^i\big(\alpha^{n_i}\big);$$

one has thus to compute the powers α^{n_i}, apply the Frobenius map – resp. powers thereof – and multiply. Compared to the naive binary method, one reduces thus the number of squarings by a factor of $1/k$, from $k \log(p)$ to $\log(p)$.

A.5.x+1.3 Fast Convolutions

The multiplication of two elements $\alpha, \alpha' \in \mathbb{K}$, represented as polynomials in β can be done by using fast convolutions. We recommend in particular two types of fast convolutions:

(vi) The Fourier transform, which becomes with the special choice of p given by (1) a Number Field Transform (NFT, [2]). This is particularly efficient when k is close to a power of 2 – e.g. $k = 31$. Products of powers of small primes $(2, 3, 5)$ are the next best guess: e.g. $k = 11 = 2^2 \cdot 3 - 1, k = 17 = 2 \cdot 3^2 - 1, k = 23 = 2^3 \cdot 3 - 1, etc.$.

(vii) The Karatsuba method or the more general Toom - Cook transforms [5], resp. "small Winograd transforms" [2] are a possible alternative to NFT and may be appealing, for instance by the ease of implementation.

Note that the use of fast convolutions is responsible for the major performance improvements for arithmetic in medium Galois fields as compared to prime fields. This is due to the fact that the operations required by these convolutions take place in the prime field of the extensions itself and we thus have no explosion of the size of intermediate values, which a typical problem specially for Toom – Cook. In practice the advantages due to convolutions are superior to the ones resulting from the ease of modular reduction and use of Frobenius.

A.5.x+1.4 Parallelization

The use of automorphisms for exponentiation has a further advantage: the algorithm for exponentiation in Galois extensions is highly parallel. In fact the exponentiations α^{n_i} can all be performed in parallel; they share the computation of the squares $s_i = \alpha^{2^i}, i = 1, 2, \ldots, \log(p)$. With k processors, the run-time may thus be reduced by a further factor $k/2$ – the half stems from the fact that on the average only $1/2$ of the processors will be active for each value of s_i.

With the above notation, an exponentiation in $\mathbb{K}$ can use parallel processor capacity according to the following scheme:

A Input $\alpha \in \mathbb{K}$ and n, such that the power $\gamma = \alpha^n$ needs to be computed.
B Write the p-adic representation of $n : n = \sum_j \; n_j p^j$.
C For $j = 0, 1, \ldots, k-1$ set $\gamma_j = 1$.
D For $i = 0, 1, \ldots, \log_2(p)$ do following:
  a) compute $\alpha_i = \alpha^{2^i}$ (serial step).
  b) **for** $j = 0, 1, \ldots, k-1$, **if** $n_j \;\&\; 2^i$ **then** $\gamma_j = \gamma_j \cdot \alpha_i$ (parallel step).
E Compute $\gamma = \prod_j \; \gamma_j$

For special values of p as for example $p = 2^{64} - 2^{32} + 1$, a parallel chip architecture for the single multiplications and squarings may be considered. Using fast Fourier transform and k parallel gates, multiplication may be reduced to $\log(k)$ steps. Using k such special purpose processors, exponentiation is reduced from $O\big(k^3 \cdot \log(p)\big)$ to $O\big(\log(k)\log(p)\big)$ steps.

1 Claimed Advantages

This particular presentation of finite extension fields was first suggested to the cryptographic community in a paper presented in 1997 at the Workshop for Fast Software Encryption in Haifa [6]. In 1998, [3] coined the name of OEF (optimal extension fields) for finite extension fields presented over a root power base. The name thus implicitly refers both to the fields (which are unique up to isomorphism) and to the special base in which their elements are presented. Special choices of prime characteristics close to machine word length are made as above. The use of properties of the Frobenius was suggested in the 1999 paper [4] for applications to elliptic curves cryptosystems. The choice (1) of p such as that $\mathbb{F}_p$ contains a $2k-$th root of unity together with the use of fast convolutions for multiplication and Frobenius for exponentiation was first (only ?) suggested in [6]. This improvements apply clearly to the cases treated in [3] and [4] too. Medium galois fields may by used not only for elliptic curve but also for discrete logarithm based curve systems. This holds without restriction for the Diffie - Hellman algorithm, why other algorithms require some adaptions. The use of medium galois fields may turn Diffie Hellman into a very performant public key algorithm, improvement factors of over 10 being current.

2 Security Assesment Considerations

The security of discrete logarithm based public key cryptosystems over medium galois fields is given by the security of the corresponding discrete logarithm problem, which is according to [1] comparable to the one in prime fields and superior to characteristic 2 fields. Considering the possibility of subfield attacks, the proper measure of information for an extension field $\mathbb{F}_q = \mathbb{F}_{p^k}$ is $\Phi_k(p)$ rather then $q-1$; the two figures are equal when k is a prime and differ the most when k is even. The known complexity bounds for a given attack should thus be applied to $\Phi_k(p)$ rather then $q-1$. E.g., for a discrete logarithm attack with complexity $L_n(1/3)$, the security evaluation is $L_{\Phi_k(p)}(1/3)$.

3 Known Limiatations and Disadvantages

The adaption of algorithms which, like DSA, require a prime factor of fixed length, $r|p-1$ is more difficult, when relpacing p by a prime power p^k for the case of medium galois fields.

4 Intellectual Property Issues

The intellectual property of the described techniques is protected by FingerPIN AG, Zurich, together with the author. A letter of intention has been provided.

References

1. Leonard M. Adleman, Johnathan DeMarrais "A subexponential algorithm for discrete logarithms over all finite fields ". Advances in Cryptology: CRYPTO '93, Douglas R. Stinson, editor. Lecture Notes in Computer Science, volume 773, Springer-Verlag, New York, 1994. Pages 147–158.
2. Blahut,R.: Fast Algorithm for Digital Signal Processing, Addison Wesley, 1987.
3. [BP] Bailey,D; Paar,C.:"Optimal Extension Fields for Fast Arithmetic Public-Key Algorithms", Advances in Cryptogology - CRYPTO98, Lecture Notes in Computer Science 1462, pp. 472-485, Springer 1998.
4. [HKKM] Hoshino,F; Kobayashi,K; Kobayashi,T; Morita,H:"Fast Elliptic Curve Algorithm Combining Frobenious Map and Table Reference to Adapt to Higher Characteristic", Proceedings Eurocrpyt'99, LNCS **1582**, (1999) pp. 176-189.
5. D.E.Knuth: The art of computer programming, Vol.2, Seminumerical algorithms, Addison-Wesley, Reading, Mass. second edition, 1981.
6. Mihailescu,P:"Optimal Galois Field Bases which are not Normal", presented at the 1997 Workshop on Fast Software Encryption in Haifa.

This article was processed using the LaTeX macro package with LLNCS style