`Surf2113`: A key-exchange cryptosystem based on a Kummer surface in characteristic 2

P. Gaudry and E. Thomé

Version 2. June 2007

The `Surf2113` cryptosystem is a key-exchange cryptosystem based on the Kummer surface of a genus 2 hyperelliptic curve over the finite field $\mathbb{F}_{2^{113}}$. The implementation follows the formulae described in [1].

1 Parameters of the Kummer surface

The Kummer surface that is used has the following parameters (with the notations of [1]):

$$\begin{aligned} \alpha^{-1} &= 1 \\ \beta^{-1} &= u^9 + u^3 + u + 1 \\ \gamma^{-1} &= u^3 + u \\ \delta^{-1} &= u^2 \,, \end{aligned}$$

where u is such that $u^{113} + u^9 + 1 = 0$. It was chosen so that the group orders of the Jacobians of the curve and of its twist are 4 times a prime:

$$\begin{aligned} N &= 4 \times 2695994666715063982985526249408423759746859005043661814141024205081 1 \\ \tilde{N} &= 4 \times 2695994666715063975947876767995501816228800080582600589731299628657 9 \,. \end{aligned}$$

The point counting has been done using the Magma computer algebra system.

The following point P on the Kummer surface has order $N/4$ and can therefore be used as a base point in a Diffie-Hellman key exchange.

$$P = (1, 1, 4, 908681679267597915035722095941517),$$

where the polynomials in u have been written as integers by setting $u = 2$.

Security. We consider here the elementary security of this cryptosystem, without taking into account the potential weaknesses of the implementation (there are some in this version) or in the inclusion in a larger protocol (authentication is not done, for instance). Let us then consider the best known algorithm for solving one discrete logarithm in the N-order Jacobian corresponding to this Kummer surface, namely Pollard's Rho algorithm or distributed variants of it. This takes about the square root of the largest prime factor of the group order: $\sqrt{N/4} \approx 2^{112}$. This is well beyond any feasible computation.

2 Some implementation details

2.1 Finite field arithmetic

Elements of the finite field are represented as a table of `unsigned long` of fixed length (2 or 4 words, depending on 32- or 64- architecture). A polynomial basis representation is used, with a sparse reduction polynomial. A good speed-up is obtained by using SSE-2 registers and the corresponding 128-bit instructions.

2.2 Encoding of keys

A secret key is an integer between 0 and $2^{224} - 1$. We impose it to be a multiple of 2 in order to avoid subgroups attacks. This secret key is stored in big-endian form in 28 bytes.

The public key and the shared secret are points of the Kummer surface. Since these are projective coordinates, we can (or we must in the case of the share secret) make them affine by, for instance, putting the first coordinate to 1. There are 3 elements left to store, that all fill in 128 bits (actually 113), therefore it takes 48 bytes to store a public key or a shared secret.

One byte could be gained for each element.

3 Future work

Here is our "to do" list for the next version.

- Key validation.

  It is necessary to check that the public key of the other party is valid. Since the curve and its twist are secure, this should be simplified.

- Study and avoid degenerate cases.

  The current version does not take into account the potential exceptional cases that would create a non-point with all-zero coordinates. There is some theory to do here before fixing the implementation.

- Study the point compression.

  There is some redundency in the 48 bytes used for representing a Kummer point. We can put all the information in 32 bytes, but then it is required to compute the roots of a polynomial of degree 2. We might implement that in the next version.

- Implement Montgomery's PRAC algorithm.

  The Lucas chain we use is the classical double and add which is not optimal. If we assume that resistance to side-channel attack is not an issue, we can use the PRAC algorithm to save some work.

References

[1] P. Gaudry. Variants of the Montgomery form based on Theta functions. Talk given at the workshop "Computational Challenges Arising in Algorithmic Number Theory and Cryptography", Toronto, Novembre 2006.