A note on MNT4 and MNT6 curves: estimation of STNFS cost

Aurore Guillevic[1]

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
aurore.guillevic@inria.fr

In [2], Guillevic, Massson and Thomé estimated the cost of the Special-Tower Number Field Sieve algorithm (STNFS) and its variants for MNT6 curves (MNT curves of embedding degree 6) for curve parameters obtained from PBC library developed by Ben Lynn [4,5]. In [3], Guillevic and Singh refined the cost model. In this short note we are interested more precisely in MNT curves designed for proof compositions. In particular, we focus on four curves: MNT4-298, MNT6-298, MNT4-753 and MNT6-753 [1] and `https://coinlist.co/build/coda/pages/MNT4753` whose parameters are given below. MNT curves have parameters p, r, t of polynomial form with the following properties.

Table 1. MNT-4 and MNT-6 parameters

MNT6	MNT4
$p(x) = 4x^2 + 1$	$p(x) = x^2 + x + 1$
$r(x) = 4x^2 - 2x + 1$	$r(x) = x^2 + 1$
$t(x) = 2x + 1$	$t(x) = x + 1$

Note that for MNT-4 parameters, we need x to be even to ensure p and r to be odd, and x can be positive or negative. If we re-write with $-2x$ for MNT4 parameters, we obtain $p_{\mathrm{MNT4}}(-2x) = 4x^2 - 2x + 1 = r_{\mathrm{MNT6}}(x)$, $r_{\mathrm{MNT4}}(-2x) = 4x^2 + 1 = p_{\mathrm{MNT6}}(x)$.

– $E_{\mathrm{MNT4-298}}\colon y^2 = x^3 + ax + b$

$$
\begin{aligned}
k =& 4 \\
u =& \texttt{0x1eef5546609756bec2a33f0dc9a1b671660000} \\
D =& 614144978799019 \\
a =& 2 \\
b =& \texttt{0x3545a27639415585ea4d523234fc3edd2a2070a085c7b9} \\
& \texttt{80f4e9cd21a515d4b0ef528ec0fd5}
\end{aligned}
$$

- $E_{\mathrm{MNT6-298}}\colon y^2 = x^3 + ax + b$

$$\begin{aligned}
k =& 6 \\
u =& -\texttt{0xf77aaa3304bab5f61519f86e4d0db38b30000} \\
D =& 614144978799019 \\
a =& 11 \\
b =& \texttt{0xd68c7b1dc5dd042e957b71c44d3d6c24e683fc09b420b1} \\
& \texttt{a2d263fde47ddba59463d0c65282}
\end{aligned}$$

- $E_{\mathrm{MNT4-753}}\colon y^2 = x^3 + ax + b$

$$\begin{aligned}
k =& 4 \\
u =& -\texttt{0x15474b1d641a3fd86dcbcee5dcda7fe51852c8cbe26e600} \\
& \texttt{733b714aa43c31a66b0344c4e2c428b07a7713041ba18000} \\
D =& 241873351932854907 \\
a =& 2 \\
b =& \texttt{0x01373684a8c9dcae7a016ac5d7748d3313cd8e39051c59} \\
& \texttt{6560835df0c9e50a5b59b882a92c78dc537e51a16703ec98} \\
& \texttt{55c77fc3d8bb21c8d68bb8cfb9db4b8c8fba773111c36c8b} \\
& \texttt{1b4e8f1ece940ef9eaad265458e06372009c9a0491678ef4}
\end{aligned}$$

- $E_{\mathrm{MNT6-298}}\colon y^2 = x^3 + ax + b$

$$\begin{aligned}
k =& 6 \\
u =& \texttt{0xaa3a58eb20d1fec36e5e772ee6d3ff28c296465f137300} \\
& \texttt{399db8a5521e18d33581a262716214583d3b89820dd0c000} \\
D =& 241873351932854907 \\
a =& 11 \\
b =& \texttt{0x7da285e70863c79d56446237ce2e1468d14ae9bb64b2bb} \\
& \texttt{01b10e60a5d5dfe0a25714b7985993f62f03b22a9a3c737a} \\
& \texttt{1a1e0fcf2c43d7bf847957c34cca1e3585f9a80a95f40186} \\
& \texttt{7c4e80f4747fde5aba7505ba6fcf2485540b13dfc8468a}
\end{aligned}$$

In MIRACL one finds other MNT parameters, under `MIRACL/source/curve/pairing/`, files `mnt.ecs` and `k4mnt.ecs`. But the curves do not have prime order.

We now are interested in the expected cost of computing discrete logarithms in $\mathrm{GF}(r^4)$ and $\mathrm{GF}(p^6)$ with the NFS os TNFS algorithms. Following [3], we estimate the cost of NFS with Conjugation variant, and TNFS with Conjugation variant, as they are the most competitive for fields of characteristic up to 1500 bits. We obtain the following Figure 1.

Since the security of $\mathrm{GF}(p^6)$ and $\mathrm{GF}(r^4)$ are related, we draw in Figure 2 the estimated DL cost as in Figure 1 but with respect to the size of the characteristic, that is, r and p.

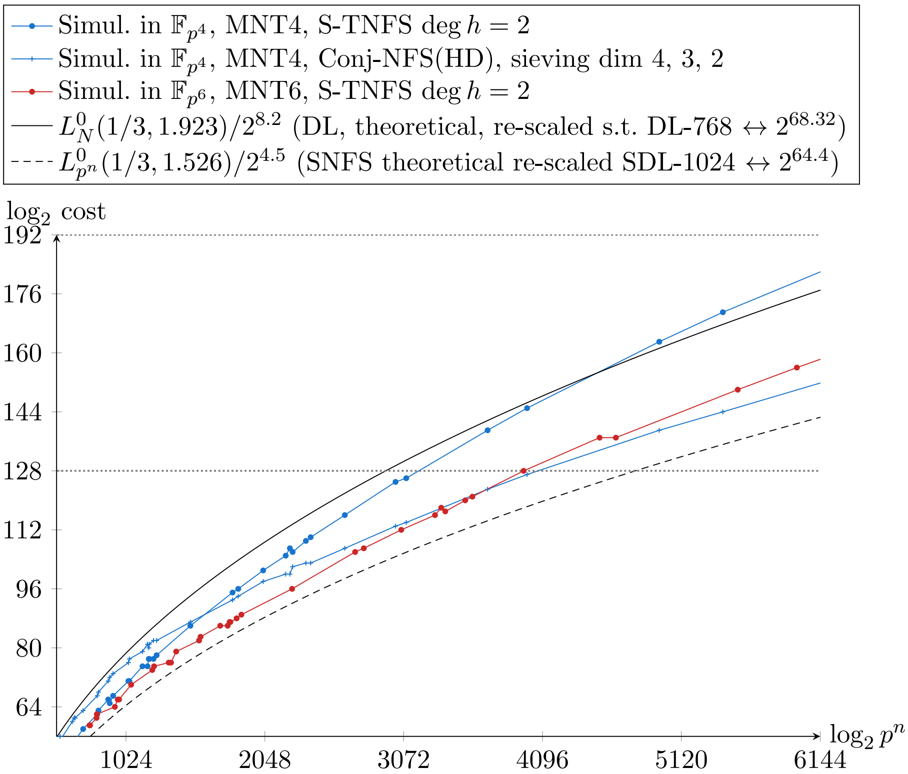

Fig. 1. Estimated cost of DL computation with NFS and TNFS

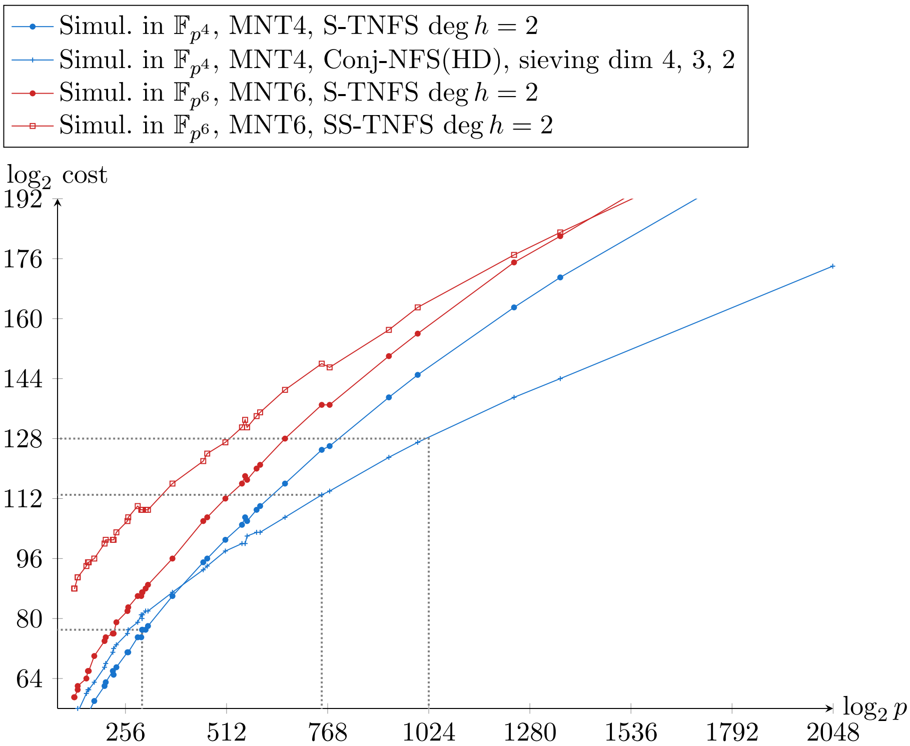

Fig. 2. Estimated cost of DL computation with NFS and TNFS

1 Conclusion

The MNT-4 curves of order p defined over a prime field $\mathrm{GF}(r)$ need r of about 1024 bits to ensure an estimated DL computation cost of about 2^{128} (in $\mathrm{GF}(r^4)$) following the model of [3]. The MNT-4 curve defined over a 753-bit prime field has estimated DL cost in in $\mathrm{GF}(r^4)$ of about 2^{112} (a simulation gave 2^{113}). The MNT-4 curve defined over a 298-bit prime field has estimated DL cost in in $\mathrm{GF}(r^4)$ of a bit less than 2^{80} (a simulation gave 2^{77}). The data is available in `https://gitlab.inria.fr/tnfs-alpha/alpha/-/blob/master/sage/tnfs/param/TestVectorMNT_k.py` It is very difficult to generate MNT parameters of large size. We found parameters with prime p, r of 773, 923, 996, 1240, 1357, and 2047 bits in PBC. The curve parameters are reported in the above file.

References

1. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Scalable zero knowledge via cycles of elliptic curves. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 276–294. Springer, Heidelberg (Aug 2014). https://doi.org/10.1007/978-3-662-44381-1_16
2. Guillevic, A., Masson, S., Thomé, E.: Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation. Des. Codes Cryptogr. pp. 1–35 (March 2020). https://doi.org/10.1007/s10623-020-00727-w
3. Guillevic, A., Singh, S.: On the alpha value of polynomials in the tower number field sieve algorithm. ePrint 2019/885 (2019)
4. Lynn, B.: Pairing-based cryptography (PBC) library. `https://crypto.stanford.edu/pbc/` (2013)
5. Lynn, B.: On the implementation of pairing-based cryptosystems. Phd thesis, Stanford University, department of computer science (2007), `https://crypto.stanford.edu/pbc/thesis.html`