On a (Flawed) Proposal to Build More Pairing-Friendly Curves

Michael Scott[1] and Paulo S. L. M. Barreto[2]

[1] School of Computer Applications, Dublin City University.
mike@computing.dcu.ie
[2] Escola Politécnica, Universidade de São Paulo.
pbarreto@larc.usp.br

Abstract. In a recent letter, Cui, Duan and Chan propose a generalisation of the Scott-Barreto method to build a larger family of MNT curves, and they claim that their proposal is also applicable to other curve construction methods. Here we show that the Cui-Duan-Chan technique is irrecoverably flawed.

1 Introduction

Pairing-friendly curves are important to instantiate the ever-growing family of pairing-based cryptosystems, but much fewer such curves are known compared to the number of general elliptic curves. It may be the case that no prime order curve is available for some application, motivating constructions with a small cofactor like the methods of Scott and Barreto [6] and Galbraith, McKee, and Valença [4].

Recently, Cui, Duan and Chan [2] announced the discovery of a trick to extend the Scott-Barreto construction, so as to nearly double the number of available curves. Besides, the authors claimed that their technique can be applicable to other construction methods like [3] and [1].

Unfortunately, the method proposed by Cui, Duan and Chan is flawed beyond repair, as we show next.

2 The flaw in the Cui-Duan-Chan construction

The Cui-Duan-Chan method relies on their Lemma 2, which we copy here verbatim for reference:

Lemma 1. *Any suitable prime l satisfies that l divides $\Phi_k(t-1)$ and l doesn't divide $\Phi_i(t-1)$ for all $0 < i < k$. In particular, when k is even, any suitable prime l satisfies that l divides $\Phi_k(1-t)$ and l doesn't divide $\Phi_i(1-t)$ for all $0 < i < k$.*

The problem is that the "particular" clause of Lemma 2 does *not* hold in general.

Let $a = (t-1)$ be a primitive k-th root of unity modulo r where $k = 2m$ and m is odd. Then $a^k \equiv 1 \pmod{r}$ but $a^m \equiv -1 \pmod{r}$. The authors consider $-a = (1-t)$ and claim that $-a$ is a primitive k-th root of unity. But $(-a)^m \equiv 1 \pmod{r}$ when m is odd. Hence $(1-t)$ is only an m-th root of unity. Therefore, all the later constructions in the Cui-Duan-Chan paper have embedding degree $k/2$ instead of k.

A special case relevant to the present discussion is the form of Φ_p and Φ_{2p} where p is an odd prime [5]:

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$
$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \ldots - x + 1$$

Thus it is clear that $\Phi_{2p}(-x) = \Phi_p(x)$. The Cui-Duan-Chan paper deals with $p = 3$ and $x = t - 1$, hence $\Phi_6(1 - t) = \Phi_3(t - 1)$.

To substantiate this observation empirically, A contains a Magma program to compute the embedding degree of the examples in the Cui-Duan-Chan paper. Needless to say, the result is that both examples are reported to have embedding degree $k = 3$ rather than $k = 6$.

We point out that for $k = 4p$ with odd p the embedding degree is not halved by the use of $1 - t$, but since in this case all terms of the cyclotomic polynomial have even degree, it follows that $\Phi_k(1 - t) = \Phi_k(t - 1)$ and hence no new solution can be found, as the authors acknowledge for $k = 4$.

Interestingly, the authors claim in the conclusion that, "compared with the examples in [6], the new examples [obtained with their method] are strong enough to resist the index-calculus attack." This assertion is quite odd because, on the one hand, no example in [6] is susceptible to index calculus, and on the other hand, the halved embedding degree attainable with their method most probably succumbs to that attack, since the elliptic discrete logarithm is mapped to the conventional discrete logarithm in a 516-bit or 519-bit finite field in the given examples.

3 Conclusion

We have seen that the Cui-Duan-Chan technique relies entirely on a false assumption, and hence cannot produce any new elliptic curves with the same embedding degree as existing curve construction methods. We can see no way to fix this problem. Obtaining more pairing-friendly curves remains a research topic.

4 Acknowledgments

We are grateful to Steven Galbraith for his valuable comments on this work, in particular on the formal refutation of Lemma 2.

References

1. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Cryptology ePrint Archive, Report 2003/143, 2003. Available from `http://eprint.iacr.org/2003/143`.
2. S. Cui, P. Duan, and C. W. Chan. A method for building more non-supersingular elliptic curves suitable for pairing-based cryptosystems. *IEICE Transactions on Fundamentals*, E88-A(9):2468–2470, 2005.

3. R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. Cryptology ePrint Archive, Report 2002/094, 2002. http://eprint.iacr.org/2002/094.
4. S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004. Available from http://eprint.iacr.org/2004/365.
5. H. Riesel. *Prime Numbers and Computer Methods for Factorization*. Birkhaeuser, Boston, MA, 1994.
6. M. Scott and P. S. L. M. Barreto. Compressed pairings. In *Advances in Cryptology – Crypto'2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 140–156, Santa Barbara, USA, 2004. Springer-Verlag.

A Magma program to check the Cui-Duan-Chan examples

```
"1st Cui-Duan-Chan example:";
r := 189289937412957245115365840918073 65\
41988272177240807;
p := 37857987482591449023073167748540096\
53783645424845931;
for k in [1..6] do
   if p^k mod r eq 1 then
       "p =", p;
       "r =", r;
       "k =", k;
       break;
   end if;
end for;
"2nd Cui-Duan-Chan example:";
r := 41649787595643595146574771666378513\
86588983459113201;
p := 83299575191287190293149542687390561\
32959980498708977;
for k in [1..6] do
   if p^k mod r eq 1 then
       "p =", p;
       "r =", r;
       "k =", k;
       break;
   end if;
end for;
```