CLASSIFYING TRACE ZERO VARIETIES SUSCEPTIBLE TO GENUS 3 COVER ATTACKS

SYED LAVASANI AND COLIN WEIR
UNIVERSITY OF CALGARY

Poster Abstract

Let $\mathcal{C}$ be a Hyperelliptic curve of genus 2. The trace zero (sub)variety (TZV) $\mathcal{G}$ of $\mathrm{Jac}_{\mathbb{F}_{q^3}}\mathcal{C}$, is defined as $\mathcal{G} := \left\{D \in \mathrm{Jac}_{\mathbb{F}_{q^3}}\mathcal{C} \mid \sigma^2(D) + \sigma(D) + D = 0\right\}$ where σ is the Frobenius automorphism of $\mathbb{F}_{q^3}/\mathbb{F}_q$. In [Lan03], it was shown that $\mathcal{G}$ is a suitable candidate for discrete logarithm (DLP) based cryptography. It was also shown theoretically in [Lan03] and practically in [Ava09] that TZV arithmetic in cryptographically interesting cases can be performed faster than other popular primitives, such as the Jacobians of elliptic and hyperelliptic curves.

In [DSnt], it was shown that one can transfer the DLP in $\mathcal{G}$ to the DLP in $\mathrm{Jac}_{\mathbb{F}_q}\mathcal{X}$, where $\mathcal{X}$ is a cover of $\mathcal{C}$ with an automorphism of order 3. A construction of $\mathcal{X}$, based on Galois theory, was also introduced in [DSnt]. They showed that the method almost always constructs a cover of genus 6. This would reduce the security of TZV DLP based systems by a factor of 6, which can be easily compensated for in practice. However, as the reduction in size of the base field is always of degree 3, a cover with a lower genus imposes an even higher reduction factor to the TZV DLP,as the size of $\mathrm{Jac}_{\mathbb{F}_q}\mathcal{X}$ is exponential in term of genus of $\mathcal{X}$. Hence, it is essential to classify all TZV that can be covered by lower genus curves to avoid them in cryptographic application.

In this research, we used the results of [Bra88], [Bre00] and [MSSV02], to classify all curves of genus 3 that admit an automorphism of degree 3. Furthermore, considering the ramification locus of each class along with the automorphism group structure, we identified and eliminated all classes of curves of genus 3 whose ramification structure does not allow them to cover a genus 2 curve. With extensive SAGE [S$^+$12] programming, we then computed the fixed field of each conjugacy class of order 2 of the automorphism group of each potential cover. Finally, by listing the resulting fixed fields of genus 2, we have symbolically computed the equations of all families of genus 2 curves whose TZV is susceptible to genus 3 cover attack. In this way, we have classified all genus 2 curves with an unramified cover of degree 2 that has an automorphism of degree 3.

Based on the result of this research, TZV based cryptosystems should check and avoid using hyperelliptic curves isomorphic to an instance of one of the listed families.

References

[Ava09] Roberto Avanzi. Trace zero varieties. Slides from SPEED-CC – Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers, 2009.

[Bra88] Rolf Brandt. *Über die Automorphismengruppen von algebraischen Funktionenkörpern*. PhD thesis, Universität-Gesamthochschule Essen, 1988.

[Bre00] Thomas Breuer. *Characters and automorphism groups of compact Riemann surfaces*, volume 280 of *London Math. Soc. Lect. Notes*. Cambridge Univ. Press, 2000.

[DSnt] Claus Diem and Jasper Scholten. An attack on a trace-zero cryptosystem. `www.math.uni-leipzig.de/ diem/preprints/trace-zero.ps`, preprint.

[Lan03] Tanja Lange. Trace zero subvariety for cryptosystems, 2003. Cryptology ePrint Archive, Report 2003/094, `http://eprint.iacr.org/2003/094`.

[MSSV02] Kay Magaard, Tanush Shaska, Sergey Shpectorov, and Helmut Volklein. The locus of curves with prescribed automorphism group. In *Communications in Arithmetic Fundamental Groups*, volume 1267 of *RIMS Kokyuroku*, pages 112–141. Kyoto University, Research Institute for Mathematical Sciences, 2002.

[S+12] William Stein et al. *Sage Mathematics Software (Version 5.0)*, 2012. `http://www.sagemath.org`.