Algoritmos de trisección en curvas de género 2 y aplicaciones

Expositor: Edgardo Riquelme (Universidad del Bío-Bío, edriquelme@ubiobio.cl)
Autor/es: Edgardo Riquelme (Universidad del Bío-Bío, edriquelme@ubiobio.cl); Nicolas Thériault (Universidad de Santiago de Chile, nicolas.theriault@usach.cl)

Algoritmos de trisección (división por 3) eficientes para divisores en curvas hiperelípticas en característica impar han sido estudiados por Gaudry y Schost y también por los autores en característica par e impar. El principal interés de estos algoritmos reside en su aplicación a algoritmos tipo Schoof para calcular el orden del grupo para la Jacobiana de curvas de género 2. Calcular el orden del grupo es necesario si nosotros queremos saber si la Jacobiana de la curva de género dos puede ser considerada computacionalmente segura para fines criptográficos.
Nosotros proporcionamos polinomios de trisección simbólicos para Jacobianas de curvas de género 2 sobre cuerpos finitos $\mathbb{F}_q$ de característica impar. Nosotros damos detalles del cálculo simbólico de los polinomios de trisección y como estos pueden ser usados en la práctica.
Como indican nuestros experimentos estos polinomios pueden ser usados para mejorar la eficiencia de algoritmos de trisección los que pueden ser usados para obtener algoritmos de conteo de puntos tipo Schoof más rápidos.

1

2

Referencias

[GS04] P. Gaudry and E. Schost, *Construction of secure random curves of genus 2 over prime fields*, in: Advances in Cryptology – EUROCRYPT 2004,

[GS12] P. Gaudry and E. Schost, *Genus 2 point counting over prime fields*, Journal of Symbolic Computation, **47**, Number 4, 368–400, (2012).

[MPTAMC] J. Miret, J. Pujolàs and N. Thériault, *Trisection for supersingular genus 2 curves in characteristic 2*, Advances in Mathematics of Communications, **8**, Number 4, 375–387, (2014).

[PRT] J. Pujolàs, E. Riquelme, N. Thériault. *Trisection for non-supersingular genus 2 curves in characteristic 2.* Int. J. Comput. Math., **93**, Number 8, 1254–1264, (2016).

[edg] E. Riquelme, *Trisection for genus* 2 *curves in odd characteristic*, Applicable Algebra in Engineering, Communication and Computing, **27**, Number 5, 373–397, (2016).

[RT] Riquelme E., Theriault N., *Symbolic trisection polynomials for genus 2 curves in odd characteristic*, Siam Discrete Mathematic, **32** Number 4, 2421-2440. (2018).

[1]Parcialmente financiado por DIUBB 1738093/I
[2]Parcialmente financiado por FONDECYT grant 1151326