Summary

Теория эллиптических кривых в первую очередь является доминирующим инструментом при решении ряда фундаментальных проблем математики, связанных с прикладными областями, как например современная криптография с отрытым ключом.

Естественным обобщением теории эллиптических кривых является теория абелевых многообразий. В настоящее время существенному расширению теории абелевых многообразий над конечными полями способствует решение задач, возникающих в современной облачной криптографии. Данные задачи открывают новые связи между смежными областями математики.

Наиболее перспективным направлением исследования, требующим глубоких знаний арифметики якобианов над конечными полями и теории спариваний в криптографии, является теория гиперэллиптических кривых p-ранга 1. Проблема дискретного логарифма достаточно хорошо изучена как для эллиптических кривых (как обычных, так и суперсингулярных), так и для якобианов обычных гиперэллиптических кривых (то есть гиперэллиптических с максимальным p-рангом).

Цель данной работы заключается в нахождении связи между инвариантами Хассе-Витта и различными видами спариваний на якобианах кривых над конечными полями. Ценность полученного исследования в первую очередь будет связана с исследованием уязвимости криптосистем на якобианах гиперэллиптических кривых.

Данное исследование требует поэтапного решения.

Первый этап предусматривает построение базы данных гипреэллиптических кривых рода 2 p-ранга 1 и нахождение матриц Хассе-Витта для кривых из созданной базы. Завершающим моментом является сравнение скорости различных спариваний на полученных кривых со скоростью спариваний на обычных и суперсингулярных кривых рода 2 над одним и тем же конечным полем.

Второй этап исследования предполагает, помимо нахождения соотношений на тэта-нулях, налагаемых матрицей Хассе-Витта, также адаптацию теории канонического подъема для кривых рода 2 p-ранга 1 через устранение сингулярностей, возникающих при поэтапной реализации канонического подъема.