**Чацвёрты тэкст**

У цяперашні час шырока распаўсюджаныя крыптасістэмы, стойкасць якіх заснавана на высокай складанасці задач фактарызацыі вялікіх цэлых лікаў і дыскрэтнага лагарыфмавання ў простым канечным полі. Напрыклад, такімі з'яўляюцца крыптасістэмы RSA, схемы Эль-Гамаля, схема Дыфi-Хелмана. На сённяшні дзень асімптатычна і практычна найбольш эфектыўнымі алгарытмамі рашэння задач фактарызацыі і дыскрэтнага лагарыфмавання ў выпадку вялікіх параметраў з'яўляюцца розныя версіі алгарытму рэшата лікавага поля. У той жа час гэты алгарытм з'яўляецца і найбольш складаным для праграмнай рэалізацыі.

Алгарытмы рэшата лікавага поля складаюцца з некалькіх асноўных працаёмкіх стадый (выбар паліномаў, прасейванне па простых ліках з інтэрвалу, рашэнне сістэмы лінейных параўнанняў), кожная з якіх дапускае розныя варыянты рэалізацый з выкарыстаннем тых ці іншых аптымізацый. Адной з асноўных стадый з'яўляецца стадыя выбару двух або некалькіх паліномаў, якія задаюць некаторае алгебраічнае пашырэнне поля Q. Праблема аптымальнага выбару паліномаў важная, так як больш якасныя паліномы могуць значна скараціць час выканання наступнай стадыі прасейвання ў алгарытме рэшата лікавага поля.