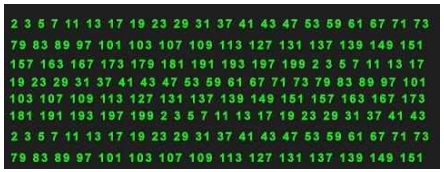
Bajarilishi ikki yilga mo‘ljallangan amaliy loyihalar mavzusi

“Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish fanlari” yo‘nalishi		
№	**Amaliy loyiha mavzusi**	**Loyiha bajarilishidan kutilayotgan natija**
	Katta razryadli tub sonlarni ishlab chiqish algoritmlarini yaratish 	**Tadqiqotning shakli:** Katta razryadli tub sonlarni ishlab chiqish algoritmlarini yaratish bo‘yicha amaliy loyiha bajariladi. **Ilmiy-tadqiqot natijalari:** - zamonaviy kriptografik algoritmlar va protokollarda foydalaniluvchi katta razryadli tub sonlarning o‘ziga xosliklari tahlil qilinadi. - zamonaviy kriptografik algoritmlar va protokollarda foydalaniluvchi turli xususiyatlarga ega bo‘lgan katta razryadli (4096 bitgacha) tub sonlarni qurishning yangi algoritmlari ishlab chiqiladi; - ishlab chiqilgan algoritmlar asosida katta razryadli tub sonlarni hosil qilish dasturiy ta’minotlari yaratiladi; - yaratilgan dasturiy ta’minotlar turli me’zonlar (natijadorlik, tezkorlik, soddalik) asosida sinovdan o‘tkaziladi va ushbu turdagi mavjud dasturiy ta’minotlarga nisbatan samaradorligi baholanadi; - Obyektni autentifikatsiya qilish protokollarini yaratiladi. **Natijalarni sinovdan o‘tkazish:** Tadqiqot natijalari O‘zbekiston Respublikasi Davlat xavfsizlik xizmatida sinovdan o‘tkaziladi.. **Ilmiy natijalarni chop etish:** Tadqiqot natijalariga intellektual mulk obyektlari uchun tegishli hujjatlar olinadi. Nufuzli ilmiy jurnallarda va Web of Science hamda Scopus ma’lumotlar bazasida indeksatsiyalangan jurnallarda ilmiy maqolalar chop etiladi.
Jami yillik: bazaviy hisoblash miqdorining 2300 barobari		

Amaliy loyihaning umumiy moliyalashtirish hajmi bazaviy hisoblash miqdorining 4600 barobaridan oshmasligi va bajarish muddati ikki yilga mo‘ljallangan bo‘lishi shart

Bajarilishi ikki yilga mo‘ljallangan amaliy loyihalar mavzusi

“Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish fanlari” yo‘nalishi		
№	**Amaliy loyiha mavzusi**	**Loyiha bajarilishidan kutilayotgan natija**
	Obyektni autentifikatsiya qilish protokollarini yaratish 	**Tadqiqotning shakli:** Obyektni autentifikatsiya qilish protokollarini yaratish bo‘yicha amaliy loyiha bajariladi. **Ilmiy-tadqiqot natijalari:** - nollik bilim usullari (zero knowledge proofs) asosidagi ob’yektni bir tomonlama va o‘zaro autentifikatsiya qilishning xavfsiz yangi protokollari ishlab chiqiladi; - ishlab chiqilgan protokollar xavfsizligi zamonaviy kriptografik talablar, kriptotahlil usullari va IETF xalqaro tashkilotining G (Goal) xavfsizlik xususiyatlari asosida baholanadi; - ishlab chiqilgan protokollar turli me’zonlar asosida sinovdan o‘tkaziladi va ushbu turdagi mavjud protpkolarga nisbatan samaradorligi baholanadi; - Obyektni autentifikatsiya qilish protokollarini yaratiladi. **Natijalarni sinovdan o‘tkazish:** Tadqiqot natijalari O‘zbekiston Respublikasi Davlat xavfsizlik xizmatida sinovdan o‘tkaziladi. **Ilmiy natijalarni chop etish:** Tadqiqot natijalariga intellektual mulk obyektlari uchun tegishli hujjatlar olinadi. Nufuzli ilmiy jurnallarda va Web of Science hamda Scopus ma’lumotlar bazasida indeksatsiyalangan jurnallarda ilmiy maqolalar chop etiladi.
Jami yillik: bazaviy hisoblash miqdorining 2300 barobari		

Amaliy loyihaning umumiy moliyalashtirish hajmi bazaviy hisoblash miqdorining 4600 barobaridan oshmasligi va bajarish muddati ikki yilga mo‘ljallangan bo‘lishi shart