Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Амгаланбаатарын Мягмарцэрэн

Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь

Бакалаврын төгсөлтийн ажил

Улаанбаатар хот

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Мэдээллийн сүлжээ, аюулгүй байдлын салбар

Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь

Мэргэжлийн индекс: D061940
Мэргэжил: Мэдээллийн системийн аюулгүй байдал

Удирдагч: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч: доктор (Ph.D), Ц.Энхтөр
магистр Ц.Манлайбаатар
Гүйцэтгэгч: А.Мягмарцэрэн

Улаанбаатар хот
2023 он 6 сар

Батлав. Мэдээллийн сүлжээ, аюулгүй байдлын салбарын эрхлэгч:

..... /доктор (Ph.D) Б.Мөнхбаяр/

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

Дипломын төсөл гүйцэтгэх төлөвлөгөө

Дипломын төслийн сэдэв:
Монгол: " Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь"
Англи: " Developing Prototype System of Proxy Re-Encryption Scheme"

Төслийн зорилго: Proxy Re-Encryption схемийн хэрэглээнүүдийг судалж, нэгэн хэрэглээг хэрэгжүүлэх туршилтын систем хөгжүүлэх

Гүйцэтгэх оюутны овог нэр: А.Мягмарцэрэн/B190970106/
Холбоо барих утас: 99899441, 98189441

№	Ажлын бүлэг, хэсгийн нэр	эзлэх хувь	дуусах хугацаа
Бүлэг №1. Proxy Re-Encryption схемийн онолын хэсэг			
1	1.1 Шифрлэлт, түүний ач холбогдол, ангилал, хэрэглээ 1.2 Орчин үеийн ширфлэлтийн схемүүд 1.3 Proxy Re-Encryption схем	20%	
Бүлэг №2. Серверт шифрлэгдсэн файл хуваалцах судалгаа			
2	2.1 Файл шифрлэх аргуудыг судлах 2.2 Сервер талын шифрлэлт болон клиент талын шифрлэлт судлах 2.3 Proxy-encryption ашиглсан системүүд	40%	
Бүлэг №3. Proxy re-encryption систем хөгжүүлэх			
3	3.1 Системийн үйл ажилгааны загвар 3.2 Хөгжүүлэх технологи, хэл сонгох 3.3 Системийн хөгжүүлэх	40%	
Бүлэг №4. Ерөнхий дүгнэлт			

Төлөвлөгөөг боловсруулсан оюутан: ..... /А.Мягмарцэрэн/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 30% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-1		III/01-III/06	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-1 хийсэн багш: ..... /доктор (Ph.D) В.Нямсүрэн/

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 50% -с багагүй байна.	Огноо	доктор (Ph.D), Ц.Энхтөр багшийн гарын үсэг
1	Үзлэг-2			IV/15-IV/19	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-2 хийсэн багш: ..... /доктор (Ph.D), Ц.Энхтөр/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 70% -с багагүй байна.	Огноо	магистр Ц.Манлайбаатар багшийн гарын үсэг
1	Үзлэг-3			VI/29-V/03	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-3 хийсэн багш: ..... /магистр Ц.Манлайбаатар/

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 90% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-4		V/13-V/17	

№	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн үнэлгээ (30 оноо)	Огноо	Удирдагч багшийн гарын үсэг
1		V/17	

Удирдагч багш: ..... /доктор (Ph.D) В.Нямсүрэн/

Жич: Удирдагч багш өөрийн үнэлгээгээ 30 хүртэл оноогоор өгөх ба үнэлгээ тавьсан хуудсыг оюутанд буцааж өгөлгүй төгсөлтийн нарийн бичгийн даргад хураалгана уу.

ТӨГСӨЛТИЙН АЖЛЫН ЯВЦ

№	Хийж гүйцэтгэсэн ажил	Биелсэн хугацаа	Удирдагчийн гарын үсэг
1	Бүлэг №1. Сүлжээний орчин дахь кибер аюулгүй байдлын онолын хэсэг	2022-3-28	
2	Бүлэг №2. Сүлжээний орчин дахь зөрчилд хариу үзүүлэх зааварчилгаа боловсруулах арга зүйг судлах	2022-4-21	
3	Бүлэг №3. Сүлжээний орчин дахь кибер халдлагад хариу үзүүлэх ажлын зааварчилгаа боловсруулах нь	2022-5-18	
4	Бүлэг №4. Ерөнхий дүгнэлт	2022-5-25	

Ажлын товч дүгнэлт

.....

.....

.....

.....

.....

.....

.....

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

ЗӨВШӨӨРӨЛ

Оюутан А.Мягмарцэрэн–н бичсэн төгсөлтийн ажлыг УШК-д хамгаалуулахаар тодорхойлов.

Салбарын эрхлэгч: ..... /доктор (Ph.D) Б.Мөнхбаяр/

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

ШҮҮМЖИЙН ХУУДАС

Мэдээллийн сүлжээ, аюулгүй байдлын салбар–н салбарын төгсөх курсийн оюутан А.Мягмарцэрэн-н "Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь" сэдэвт төгсөлтийн ажлын шүүмж.

1. Төслөөр дэвшүүлсэн асуудал, үүнтэй холбоотой онолын материал уншиж судалсан байдал. Энэ талаар хүмүүсийн хийсэн судалгаа, түүний үр дүнг уншиж тусгасан эсэх.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

2. Төслийн ерөнхий агуулга. Шийдсэн зүйлүүд, хүрсэн үр дүн. Өөрийн санааг гарган, харьцуулалт хийн, дүгнэж байгаа чадвар.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

3. Эмх цэгцтэй, стандарт хангасан өөрөөр хэлбэл диплом бичих шаардлагуудыг биелүүлсэн эсэх. Төсөлд анзаарагдсан алдаанууд, зөв бичгийн болон өгүүлбэр зүйн гэх мэт /Хуудас дугаарлагдаагүй, зураг хүснэгтийн дугаар болон тайлбар байхгүй, шрифт хольсон, хувилсан зүйл ихээр оруулсан/.

   .....
   .....
   .....
   .....
   .....

4. Төслөөр орхигдуулсан болон дутуу болсон зүйлүүд. Цаашид анхаарах хэрэгтэй зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

5. Төслийн талаар онцолж тэмдэглэх зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

6. Ерөнхий оноо. (30 оноо)

   .....

Шүүмж бичсэн: ..... /магистр Г.Баяр/

Ажлын газар: .....

Хаяг (Утас) .....

Зохиогчийн эрх хамгаалал

Миний бие А.Мягмарцэрэн, "Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь" сэдэвт энэ ажил нь минийх бөгөөд дараахыг нотолж байна. Үүнд:

- Горилогч энэ ажлыг тус сургуулиас боловсролын зэрэг авахаар бүхэлд нь буюу голлон хийсэн болно.
- Энэ ажлын аль нэг хэсгийг тус сургуульд эсвэл өөр байгууллагад боловсролын зэрэг, мэргэшил авахаар өмнө нь илгээсэн бол түүнийгээ тодорхой заасан болно.
- Бусад хүмүүсийн хэвлүүлсэн ажлаас зөвлөгөө авсан бол түүнийгээ үндэслэсэн болно.
- Бусад хүмүүсийн ажлаас ишлэл хийхдээ эх үүсвэрийг нь заасан болно.
- Миний ажилд тусалсан голлох бүх эх үүсвэрт талархаж байна.
- Ажлыг бусадтай хамтарсан бол алийг нь бусад хүмүүс хийсэн болохыг тодорхой заасан болно.

Гарын үсэг: _____

Огноо: _____

“*Амжилт нь эцсийн зогсоол биш,*
алдаа нь хөнөөлтэй зүйл биш.
Энэ хоёр зүйлтэй дэс дараалан тулгарах зоригтой байх хэрэгтэй.”

Winston Churchill

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Хураангуй

Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь

А.Мягмарцэрэн
b190970106@must.edu.com

Түлхүүр үгс: мэдээллийн аюулгүй байдал, тоон гарын үсэг

Энэхүү төслийн хүрээнд шинжлэх ухааны баримт бичиг, ном гаргахад дэлхий нийтээр түгээмэл хэрэглэдэг LaTeX системийг ШУТИС –ийн төгсөгч оюутны төгсөлтийн ажил, диссертацид хэрхэн ашиглаж болохыг судалж, шаардлагад нийцсэн загвар гаргахыг зорьсон билээ.

Тезисийн загвар гаргахдаа ШУТИС –д одоо мөрдөгдөж байгаа төгсөлтийн ажил бичих гарын авлага болон гадаадын их сургуулиудад LaTeX ашиглаж тезис бичих туршлагыг судалсан болно.

Энэ ажил нь манай сургуулийн практикт өмнө хийгдэж байгаа тул гарсан загвар хэрэгцээ, шаардлагыг бүрэн тусгаагүй байж болох талтай. Гэхдээ ажлыг цааш үргэлжлүүлэн судалснаар ШУТИС –ийн хэмжээнд бүрэн нутагших загвар гаргаж болно гэж үзэж байна.

Талархал

Энэхүү дипломын ажлыг бичихэд туслалцаа үзүүлсэн удирдагч багш Н.Чулуунбаатар болон ШУТИС-ийн Мэдээлэл холбоо технологийн сургуулийн Электроникийн салбарын багш нарт талархсанаа илэрхийлье.

Товчилсон үгс

CPU	**C**entral **P**processing **U**nit
UML	**U**nified **M**odelling **L**anguage
GPU	**G**raphic **P**rocessing **U**nit
ННТ	**Н**исэгчгүй **Н**исэх **Т**өхөөрөмж
ЦДҮС	**Ц**ахилгаан **Д**амжуулах **Ү**ндэсний **С**үлжээ
ЦДАШ	**Ц**ахилгаан **Д**амжуулах **А**гаарын **Ш**угам
NLP	**N**atural **L**anguage **P**rocessing
CNN	**C**onvolutional **N**eural **N**etworks
ReLU	**R**ectified **L**inear **U**nit

Гарчиг

Зургийн жагсаалт

Хүснэгтийн жагсаалт

БҮЛЭГ 1

Proxy Re-Encryption схемийн онолын хэсэг

1.1

БҮЛЭГ 2

А.Эрдэнэбаатарын зөвлөмж

БҮЛЭГ 3

Бүлгийн нэр

3.1 Сэдвийн нэр

Шинэ бүлэг эндээс эхэлнэ.

БҮЛЭГ 4

Томъёо хэрхэн бичих вэ?

4.1 Математик горим

Доорх **??** дүгээр томъёонд харуулсан тэгшитгэлээр .....[**zorigt1**]

$$\int_s rotE \quad dS = -\int_s \frac{\partial B}{\partial t} dS \qquad \textit{Бодлого1} \tag{4.1}$$

$$\begin{bmatrix} V_{e1} \\ V_{e2} \\ V_{e3} \end{bmatrix} = \begin{bmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

$$V(x,y) = \sum_{i=1}^{3} \alpha_i(x,y) V_{ei}$$

Дохионы давтамж $\omega = 4000 rad/sec$, чадал нь $p = 30\mu W$ байсан бол.... [**uguulel**]

4.2 Хүснэгт

Хүснэгт 4.1: Жишээ хүснэгт

нэр	1.00	3.5	“Электроникийн үндэс” хичээлийг судалж буй оюутнуудыг заавар, аргачлалын дагуу туршилт, хэмжилтийн ажил гүйцэтгэх, тэмдэглэл хийхэд зориулсан сургалтын материал болно [**online1**].
	2.00	4.5	“Электроникийн үндэс” хичээлийг судалж буй оюутнуудыг заавар, аргачлалын дагуу туршилт, хэмжилтийн ажил гүйцэтгэх, тэмдэглэл хийхэд зориулсан сургалтын материал болно [**vhdl**].

Дүгнэлт

Энд дүгнэлтээ бичнэ.

ХАВСРАЛТ А

Хавсралтын нэр

Хавсралтыг эндээс эхэлж бичнэ.

ХАВСРАЛТ В

LED контроллер AT89C51ED2

ХАВСРАЛТ С

Хавсралтын нэр

Хавсралтыг эндээс эхэлж бичнэ.