

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/В190970106/

**Холбоо барих утас:**

99899441, 98189441

№	Ажлын бүлэг, хэсгийн нэр	эзлэх хувь	дуусах хугацаа
Бүлэг №1. Прокси дахин шифрлэлт схемийн онолын хэсэг			
1	1.1 Шифрлэлт, түүний ач холбогдол, ангилал, хэрэглээ 1.2 Өгөгдөл аюулгүй хуваалцах схемүүд 1.3 Proxy Re-Encryption схем	20%	
Бүлэг №2. Прокси дахин шифрлэлт серверт шифрлэгдсэн файл хуваалцах судалгаа			
2	2.1 Файл хуваалцах үйлчилгээнүүд 2.1 Файл шифрлэх аргууд 2.2 Клоуд орчинд өгөгдөл файл хадаглах	40%	
Бүлэг №3. Прокси дахин шифрлэлт 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		IV/03-IV/07	

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/17-IV/21	

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			V/08-V/12	

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/15-V/19	

№	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. Proxy Re-Encryption схемийн онолын хэсэг	2023-4-28	
2	Бүлэг №2. Серверт шифрлэгдсэн файл хуваалцах судалгаа	2023-4-21	
3	Бүлэг №3. Proxy re-encryption систем хөгжүүлэх	2023-5-18	
4	Бүлэг №4. Ерөнхий дүгнэлт	2023-5-25	

### 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: \_\_\_\_\_

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*

# 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

**PRE** Proxy Re-Encryption  
**BBS** Blaze Bleumer Strauss

# Гарчиг

# Зургийн жагсаалт

# Хүснэгтийн жагсаалт

---

БҮЛЭГ 1

---

Proxy Re-Encryption схемийн онолын  
хэсэг

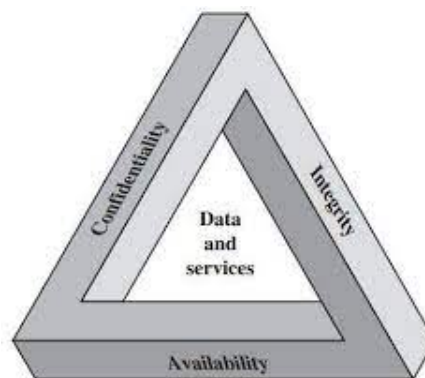


## 1.1 Шифрлэлт, түүний ач холбогдол, ангилал, хэрэглээ

Мэдээллийн аюулгүй байдал үндсэн гурван зарчмыг тэнцвэртэй хангахыг зоридог.

- **Нууцлаг байдал (Confidentiality):** Мэдээлэлийг нууц хэвээр нь хамгаалж үлдэх. Санаатай болон санамсаргүй мэдээллийг зөвшөөрөлгүй хуваалцах таараахаас сэргийлэх.
  - Өгөгдлийн нууцлал (Data confidentiality)
  - хувийн нууц (Privacy)
- **Бүрэн бүтэн байдал (Integrity):** Өгөгдөлд үнэн зөв найдвартай гадны нөлөө ороогүйг шалгах, бүрэн бүтэн хадаглах.
  - Өгөгдлийн бүрэн бүтэн байдал (Data integrity)
  - Системийн бүрэн бүтэн байдал (System integrity)
- **Хүртээмжтэй байдал (Availability):** Тухайн системийн хэрэглэгчид хүртээмжтэй байх.

Мэдээлэл болон өгөгдлийг шифрлэлт хийсэнээр нууцлаг байдлыг хангах хамгийн том давуу тал мөн бүрэн бүтэн байдал хүртээмжтэй байдал дээр ашиглах боломжтой.



Зураг 1.1: CIA гурвалжин

Шифрлэлт ерөнхийд нь гурав ангилна.

- **Тэгш хэмт шифрлэлт (symmetric):**
- **Тэгш бус шифрлэлт (asymmetric):**
- **Хаш (Hash)**

Нууцлаг байдлыг хангахад

- Тэгш хэмт шифрлэлт (symmetric)
- Тэгш бус шифрлэлт (asymmetric)
- Хаш (Hash)

Бүрэн бүтэн байдлыг хангахад ашиглана.

- Хаш (Hash)
- Мессежийн баталгаажуулалтын код (MACs)
- Тоон гарын үсэг (Digital Signatures)

## 1.2 Орчин үеийн шифрлэлтийн схемүүд

Identity-based encryption (IBE): This is a type of public key encryption that allows users to encrypt and decrypt data using their identities instead of public keys. IBE can be used for secure data sharing in scenarios where users are known by their identities.

Attribute-based encryption (ABE): This is a type of encryption that allows access to data based on predefined attributes, such as age, job title, or organizational role. ABE can be used for fine-grained access control to data, and can be used in scenarios where access is granted based on certain attributes.

Homomorphic encryption (HE): This is a type of encryption that allows computations to be performed on encrypted data without first decrypting it. HE can be used for secure data processing in scenarios where data needs to be kept confidential while still allowing for computation.

Secure multiparty computation (MPC): This is a cryptographic technique that allows multiple parties to jointly compute a function over their private inputs without revealing their inputs to each other. MPC can be used for secure data processing in scenarios where data needs to be kept confidential and multiple parties need to collaborate.

## 1.3 Proxy Re-Encryption схем

Прокси дахин шифрлэлт нь нийтийн түлхүүрээр шифрлсэн өгөгдөлийг дахин шифрлэж өөр хувийн түлхүүрээр тайлах боломжийг олгодог.

Давуу талууд: Гурав дахь сервер гэх мэт өгөгдлийг байршуулах боломжтой.

Сул талууд:

Үндсэн хоёр төрөлтэй.

Unidirectional PRE: Зөвхөн нэг талдаа дахин шифрлэх боломжтой.

Bidirectional PRE: 2 талдаа дахин шифрлэх боломжтой.

Some features of PRE schemes include:

Delegation: PRE allows data owners to delegate access to their data to third-party entities, without giving them complete access to the data.

Access control: PRE allows data owners to control who can access their data and under what circumstances, even after the data has been shared.

Efficiency: PRE can be more efficient than traditional re-encryption techniques, as it does not require the data to be decrypted and re-encrypted.

Security: PRE provides a high level of security, as the proxy does not have access to the data itself and can only transform the encrypted data.

## 1.4 Бүлгийн Дүгнэлт