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. 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: _____

“*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

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 **P**roxy **R**e-**E**ncryption
BBS **B**laze **B**leumer **S**trauss

Гарчиг

Зургийн жагсаалт

Хүснэгтийн жагсаалт

БҮЛЭГ 1

Proxy Re-Encryption схемийн онолын хэсэг

1.1 Шифрлэлт, түүний ач холбогдол, ангилал, хэрэглээ

Encryption is the process of converting plaintext or readable data into ciphertext or unreadable data using an encryption algorithm. The ciphertext can only be decrypted and read by authorized parties who possess the decryption key. Encryption is a critical tool for protecting sensitive information, ensuring the privacy of individuals and organizations, and securing digital communications. Here are some of the significance, importance, and applications of encryption:

Confidentiality Encryption helps to maintain the confidentiality of sensitive data by making it unreadable to unauthorized parties. It ensures that only authorized parties can access and read the information, protecting it from theft, eavesdropping, or interception.

Privacy Encryption ensures the privacy of individuals and organizations by securing their personal and sensitive information. It allows individuals to control who can access their information and how it can be used, reducing the risk of identity theft, fraud, or other forms of privacy violations.

Authentication Encryption helps to ensure the authenticity of data and messages by verifying the identity of the sender and ensuring that the message has not been tampered with during transmission. This is particularly important in online transactions, where the authenticity of data and messages is crucial to prevent fraud and ensure trust.

Data Integrity Encryption helps to maintain the integrity of data by ensuring that it has not been tampered with or altered during transmission or storage. It allows data to be stored and transmitted securely without the risk of unauthorized modifications, ensuring the accuracy and reliability of information.

Applications Encryption is used in a wide range of applications, including secure online transactions, digital signatures, secure email communication, online banking, e-commerce, and data storage. It is also used to secure sensitive information in industries such as healthcare, finance, and government, where privacy and confidentiality are paramount.

In conclusion, encryption is a critical tool for protecting sensitive information, ensuring privacy, and securing digital communications. Its significance and importance continue to grow as digital technologies become more pervasive and the threats to digital security become more sophisticated. Encryption technology is continually evolving to meet the increasing security needs of individuals and organizations, ensuring that sensitive information remains secure and confidential.

1.2 Орчин үеийн ширфлэлтийн схемүүд

Homomorphic encryption: While homomorphic encryption allows computations to be performed on encrypted data, it does not provide delegation or access control features like PRE.

Secure multi-party computation: SMPC allows multiple parties to jointly compute a function over their private inputs without revealing those inputs to each other, but it does not provide delegation or access control features like PRE.

Attribute-based encryption: ABE allows access to data to be controlled based on certain attributes, but it does not provide delegation or re-encryption features like PRE.

1.3 Proxy Re-Encryption схем

Прокси дахин шифрлэлт нь нийтийн түлхүүрээр шифрлэлтийн нэг хэлбэр бөгөөд хэрэглэгч Алиса-ийн шифрийг Bob-д тайлах боломжийг олгодог.

Үндсэн хоёр төрөлтэй.

Unidirectional PRE: In unidirectional PRE, the proxy can transform ciphertext from the data owner's key to the delegatee's key, but not vice versa. This means that the delegatee can only decrypt data that has been specifically re-encrypted for them, and cannot access the original data or re-encrypt it for someone else.

Bidirectional PRE: In bidirectional PRE, the proxy can transform ciphertext in both directions, allowing for more flexibility in data sharing. This means that the delegatee can both access the original data and re-encrypt it for someone else.

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 dat

БҮЛЭГ 2

Серверт шифрлэгдсэн файл хуваалцах судалгаа

2.1 Файл шифрлэх аргуудыг судлах

2.2 Сервер талын шифрлэлт болон клиент талын шифрлэлт судлах

2.3 Proxy-encryption ашиглсан системүүд

БҮЛЭГ 3

Proxy re-encryption систем хөгжүүлэх

3.1 Системийн үйл ажилгааны загвар

3.2 Хөгжүүлэх технологи, хэл сонгох

3.3 Системийн хөгжүүлэх

Дүгнэлт

Энд дүгнэлтээ бичнэ.