# Эллипслэг Муруйн Криптограф ба Түүний Хэрэгжүүлэлт

Б.Магсаржав
МУИС
Хэрэглээний шинжлэх ухаан инженерчлэлийн сургууль
Мэдээлэл компьютерийн ухааны тэнхим
magsarjav@smcs.num.edu.mn

Д.Гармаа
МУИС
Хэрэглээний шинжлэх ухаан инженерчлэлийн сургууль
Мэдээлэл компьютерийн ухааны тэнхим
garmaa@smcs.num.edu.mn

***Хураангуй:*** **Эллипслэг муруйн криптографийн математикийн үндсэн ойлголтууд болох төгсгөлөг талбар, эллипслэг муруй, төгсгөлөг талбарын арифметик үйлдлүүд болон тэдгээрийн хэрэгжүүлэлтийн тухай авч үзсэн болно.**

***Түлхүүр үг—Эллипслэг муруй, төгсгөлөг талбар, эллипслэг муруйн нууцлах алгоритм***

## I. Удиртгал

Өнөө үеийн нууцлалын системүүдэд хамгийн их ашиглаж буй, нууцлал өндөртэй техник нь эллипслэг муруйн криптограф юм. Эллипслэг муруйн криптограф нь Америкийн үндэсний стандартчилал технологийн газраас (NIST) анх баталснаас хойш одоогоор 4 удаа шинэчлэгдээд байна. Мөн ISO-оос баталсан энэ төрлийн хэд хэдэн стандартыг хэрэглээнд мөрдөж байна. Эллипслэг муруйн стандартуудаас хамгийн түгээмэл хэрэглэгдэж байгаа нь 2009 онд баталсан эллипслэг муруйн тоон гарын үсгийн стандарт юм. Эдгээр стандартуудыг банкны системүүдийн онлайн гүйлгээ, картын нууцлал, сүлжээний SSH протокол гэх мэт олон зүйлд ашиглаж байна. Мөн сүүлийн үед ид хөгжиж буй онлайн мөнгө болох Bitcoin нь цаанаа эллипслэг муруйн криптографт суурилсан байдаг [5].

Орчин үеийн онлайн, бодит хугацааны системүүдэд хурдан ажилладаг, нууцлал өндөртэй нууцлалын алгоритмууд илүү чухал болж ирсэн. Эдгээр шаардлагыг эллипслэг муруйн криптографийн алгоритмууд хангаж байна. Бид энэхүү ажилд нууцлалын түвшний хувьд дээр дурьдсан стандартуудтай ижил, хэрэглэхэд хялбар алгоритмийн нэгэн хувилбарыг хэрэгжүүлэх зорилго тавьсан болно.

## II. Эллипслэг муруйн криптограф

1985 онд Вашингтоны ИС-ийн профессор Нил Коблиц (Neal Koblitz) эллипслэг муруйг ил түлхүүртэй криптосистемд ашиглах санааг дэвшүүлсэн билээ. Ингэхдээ төгсгөлөг талбар дээр тодорхойлогдсон эллипслэг муруйн цэгүүдийн олонлогийн алгебрын бүтцийг ашигласан байна. Энэхүү арга нь тухайн үед мэдэгдэж байсан RSA болон Элгамалын алгоритмуудтай харьцуулахад өндөр үр ашигтай арга байв.

Эллипслэг муруйн криптографт дараах үндсэн ойлголтуудыг хэрэглэдэг.

**Тодорхойлолт 1.** $a, b \in \mathbb{F}_p$ талбар дээр тодорхойлогдсон

$$y^2 = x^3 + ax + b \qquad (1)$$

тэгшитгэлийг эллипслэг муруйн тэгшитгэл гэх ба $E(\mathbb{F}_p)$ гэж тэмдэглэнэ.

**Тодорхойлолт 2.** (1) тэгшитгэлийг хангах $x, y \in \mathbb{F}_p$ хосыг уг муруйн цэг гэнэ. Цэгийг $P = (x, y)$, $E(\mathbb{F}_p)$-ийн нийт цэгийн тоог $\#E(\mathbb{F}_p)$ гэж тус тус тэмдэглэнэ.

**Теорем.** Эллипслэг муруйн цэгүүдийн тооны хувьд

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}$$

тэнцэтгэл биш хүчинтэй байна [3].

Дээрх теоремоос талбарын хэмжээ буюу $p$ хүрэлцээтэй их үед эллипслэг муруй нь хангалттай олон цэгтэй байх нь илэрхий юм. Эллипслэг муруйн энэ чанар нь түүнийг нууцлалын системд хэрэглэхийн үндэс болдог.

### *A. Эллипслэг муруйн дискрет логарифмын бодлого*

$P$ нь $n$ эрэмбийн эллипслэг муруйн цэг, $d$ нь $1 < d < n - 1$ байх бүхэл тоо байг.

**Тодорхойлолт 3.** $Q = Pd$ байх $Q$ цэгийг $P$ цэгийн $d$ зэрэг гэнэ.

**Тодорхойлолт 4.** $P$ болон $Q$ цэгүүд мэдэгдэж буй үед $d$ тоог олох бодлогыг эллипслэг муруйн дискрет логарифмын бодлого гэх ба $d = log_P Q$ гэж тэмдэглэнэ. $\#E(\mathbb{F}_p)$ нь их тохиолдолд энэ бодлогыг бодох хурдан алгоритм одоогоор тооцон бодох математикт тодорхойлогдоогүй байна.

### B. *Эллипслэг муруйн параметр*

Эллипслэг муруйг тодорхойлох үндсэн параметрүүд нь $(\mathbb{F}_p, a, b, n, G)$ болно.Энд $\mathbb{F}_p$ нь төгсгөлөг талбар, $a, b$ нь (1) тэгшитгэлийн коэффициентууд, $G$ нь уг муруйн суурь цэг, $n$ нь $Gn = O$ буюу уг цэгийн эрэмбэ болно.

Муруйн суурь цэг $G$-г сонгох ба түүний эрэмбэ $n$-г олох нь тусдаа бие даасан асуудал бөгөөд одоогоор эллипслэг муруйн хэрэгжүүлэлтэд NIST-ийн тооцон олж, шалгаж баталгаажуулсан параметрүүдийг хэрэглэж байна [2]. Хэрэв эдгээр стандарт параметрүүдийг хэрэглэхгүй гэвэл өөрсдийн үүсгэсэн параметрүүдийг шалгах, баталгаажуулах алгоритмууд мөн бий.

### C. *Эллипслэг муруйн түлхүүрийн хос*

Эллипслэг муруйн нийтийн болон хувийн түлхүүрийн хосыг дараах алгоритмаар үүсгэдэг.

**Алгоритм 1** Түлхүүрийн хос үүсгэх

| | |
|---|---|
| Ороолт | $(\mathbb{F}_p, a, b, n, G)$ |
| Гаралт | Хувийн түлхүүр $d$, нийтийн түлхүүр $Q$ |
| 1 | $1 < d < n - 1$ байх санамсаргүй $d$ тоо сонгоно |
| 2 | |
| 3 | $Q = dG$ –г бодно |
| | $(d, Q)$ –хосыг буцаана |

Түлхүүрийн хосыг шалгах, баталгаажуулах алгоритмууд байдаг бөгөөд дээрх алгоритмаар үүссэн хос түлхүүрийг дараа заавал шалгаж байх шаардлагатай.

### D. *Эллипслэг муруйн нууцлах алгоритм*

Одоогоор стандарт болон мөрдөгдөж буй үндсэн хоёр төрлийн нууцлах алгоритм бий. Бид үүнээс PSEC (Provably Secure Encryption Curve scheme) алгоритмийг сонгосон. Ер нь эдгээрийн ерөнхий санааг ашиглан хэрэгжүүлэлтэд ялгаатай алгоритмуудыг янз бүрээр тодорхойлж болно. Ингэх нь нууцлалын түвшний хувьд яг ижил боловч ялгаатай үр дүн бүхий нууцлалын системийг бий болгох ач холбогдолтой юм. PSEC-ийн алгоритмыг дараах хэлбэрээр томъёолж болно.

**Алгоритм 2** PSEC нууцлах алгоритм

| | |
|---|---|
| Ороолт | $(\mathbb{F}_p, a, b, G, n)$, $Q$, нууцлах өгөгдөл $m$ |
| Гаралт | Нууцлагдсан өгөгдөл $(R, C, s, t)$ |
| 1 | $l$ бит урттай санамсаргүй $r$ тоо сонгоно |
| 2 | $(k', k_1, k_2) \leftarrow KDF(r)$ |
| 3 | $k \leftarrow k' mod\ n$ |
| 4 | $R \leftarrow kP$ |
| 5 | $Z \leftarrow kQ$ |
| 6 | $s \leftarrow r \oplus KDF(R, Z)$ |
| 7 | $C \leftarrow ENC(k_1, m)$ |
| 8 | $t \leftarrow MAC(k_2, C)$ |
| 9 | $R \| C \| s \| t$ –г буцаана |

Энд $l$ нь $n$-ийн бит урт, $KDF$ нь хэш функцэд суурилсан түлхүүр байгуулагч функц, $ENC$ нь тэгш хэмт өгөгдөл нууцлах функц, $MAC$ нь өгөгдлийн баталгаажуулах код үүсгэгч функц юм. Эдгээр функцуудын сонголт ерөнхийдөө дурын байж болно. Үндсэн түлхүүрүүд болох $k'$ нь $l + 128$ бит урттай, $k_1$ нь сонгосон $ENC$ функцийн түлхүүрийн урттай ижил, $k_2$ нь сонгосон $MAC$ функцийн түлхүүрийн урттай тус тус ижил байх ёстой. 2-р алгоритмийн урвуу буюу PSEC нууцалсан өгөгдлийг тайлах алгоритмийг [2] ажлаас үзэж болно. PSEC нь нууцлагдсан өгөгдөл болох $(R, C, s, t)$-д өгөгдөл дамжих явцад дундаас ямар нэгэн өөрчлөлт орсон эсэхийг шалгаж тогтоох боломжтойгоороо давуу талтай.

## III. Төгсгөлөг талбарын арифметик

Эллипслэг муруйн криптосистемийн хэрэгжүүлэлтэд анхны тоон (prime field) болон хоёртын (binary field) гэсэн үндсэн хоёр талбарыг авч үздэг. Талбарын арифметик үйлдлүүдийн оновчтой хэрэгжүүлэлт нь нууцлах алгоритмийн хурданд чухал нөлөө үзүүлдэг. Бид судалгаандаа 2 характеристиктай буюу $p = 2^m$ байх $\mathbb{F}_{2^m}$ талбар дээр тодорхойлогдсон эллипслэг муруйг ашигласан бөгөөд уг талбар нь нийтдээ $2^m$ ширхэг элементтэй.

### A. *Талбарын дүрслэл*

**Хоёртын** талбарын элементийг 0 ба 1 коэффициенттэй олон гишүүнт хэлбэрээр дүрсэлдэг. Уг талбарын бүх элементүүд нь $m$ зэргийн үл задрах олон гишүүнтээр факторлож үүссэн байдаг.

$f(z) = z^m + r(z)$ нь $m$ зэргийн үл задрах олон гишүүнт байг. Тэгвэл $\mathbb{F}_{2^m}$ талбарын элементүүд $m - 1$ зэргийн бүх олон гишүүнтүүд байна. Уг олон гишүүнтийг 0 ба 1-ээс тогтох вектор хэлбэрээр илэрхийлж болно. Энэ нь талбарын элементийг хоёртын тоо хэлбэрээр сэтгэн үйлдэл хийх боломжийг олгохын зэрэгцээ талбарыг компьютерийн системд дүрслэх, тэдгээрийн арифметикийг битийн операторууд ашиглан хурдтай гүйцэтгэхэд дөхөм болно. Иймээс хэрэгжүүлэлтэд $\mathbb{F}_{2^m}$ талбарыг $m$ зэргийн $f(z)$ үл задрах олон гишүүнтээр илэрхийлж явдаг.

### B. *Нэмэх ба үржих үйлдэл*

Талбарын хоёр элементийн нэмэх үйлдэл нь тэдгээрт харгалзах хоёр векторын харгалзах координатуудын хооронд битийн $\oplus$ (XOR) үйлдэл хийсэнтэй ижил байна. Харин үржих үйлдэл нь хоёр олон гишүүнтийг үржихтэй ижил ба гарсан үр дүнг $f(z)$-ээр факторлаж $\mathbb{F}_{2^m}$ талбарын элемент рүүбуцааж шилжүүлнэ.

### C. *Модулаар жиших үйлдэл*

Модулаар жишихдээ олон гишүүнтийг үлдэгдэлтэй хуваах алгоритмийг ашиглана. Ихэнх тохиолдолд $f(z)$-р факторлох тул түүний утгаас хамаарсан үлдэгдэлтэй хуваах хурдан алгоритмийг урьдчилан бэлдэж ашигладаг.

### D. *Урвуу олох ба хуваах үйлдэл*

**Тодорхойлолт 5.** Талбарын $a(z)$ элементийн хувьд $a(z) \cdot b(z) = 1$ байх $b(z)$ элементийг түүний урвуу элемент гэнэ.

Энд $b(z) = a^{-1} \bmod f(z)$ байх ба урвуу элементийг олох хэд хэдэн алгоритм байдгаас хамгийн түгээмэл нь Эвклидийн өргөтгөсөн алгоритм юм. Энд хуваах үйлдлийг $a(z)/b(z) = a(z) \cdot c(z)^{-1}$ гэж урвууг олох болон үржих үйлдэл хоёроор илэрхийлнэ.

### E. *Квадрат язгуур гаргах үйлдэл*

**Тодорхойлолт 6.** $a(z)^2$ мэдэгдэж буй үед $a(z)$ олон гишүүнтийг олох үйлдлийг квадрат язгуур гаргах гэнэ. Энэ үйлдэл нь (1) тэгшитгэлийг хангах цэгийн $x$ координат мэдэгдэж буй үед $y$ координатыг олох гэх мэт хэд хэдэн алгоритмд ашиглана.

## IV. Эллипслэг муруйн арифметик

Эллипслэг муруйн криптосистемийг хоёртын талбарт хэрэгжүүлэхэд дараах хэлбэрийн муруйг авч үздэг.

$$y^2 + xy = x^3 + ax + b \qquad (2)$$

### A. *Цэгийн дүрслэл*

Муруйн цэгийг түүний координат болох $(x, y) \in \mathbb{F}_{2^m}$ хосоор илэрхийлнэ. $x$ координат мэдэгдэж буй үед $y$-г олохдоо (2) тэгшитгэлд $x$-г орлуулж бодож олж болдог. Иймээс цэгийг аль болох бага хэмжээтэй хадгалах үүднээс зөвхөн $x$ координатыг хэрэглэдэг ба ийм хэлбэрийг цэгийн шахалттай формат гэнэ. Цэгийн шахалттай хэд хэдэн формат байдаг ба үүнийг [3] ажлаас үзэж болно. Шахалттай формат хэрэглэх нь өгөгдлийн хэмжээ багасах давуу талтай ч тооцоолол хийхэд цэгээ буцаан задалж гарган авах нэмэлт алхам шаарддаг.

Мөн цэгийг дүрслэх хэд хэдэн проекцон координат байдаг. Цэгийн дүрслэлээс хамаарч тэдгээрийн арифметик үйлдлийн алгоритмууд нь ялгаатай байна.

### B. *Цэгийн нийлбэр ба үржвэр*

Эллипслэг муруйн дурын хоёр цэгийн нийлбэр буцаад уг муруйн цэг байдаг. $E(\mathbb{F}_p)$-ийн энэ бүтэц нь эллипслэг муруйг криптографт хэрэглэх гол үндэс болсон [1]. Муруй бүрт хязгааргүйн цэг гэж байдаг ба түүнийг $O$ гэж тэмдэглэнэ. Муруйн дурын хоёр цэгийн нийлбэрийг олох нь RSA, Элгамалын криптосистемүүдэд хэрэглэдэг анхны тоон талбарын элементийн нийлбэр олохоос хэд дахин хүнд. Эдгээрийн тооцооллыг талбарын хэмжээгээр нь харьцуулсан харьцуулалтыг [2] ажлын 19-р хуудаснаас харж болно. Энэ нь алгоритмуудыг нууцлалын түвшний хувьд хооронд нь харьцуулдаг гол үзүүлэлт юм. Цэгийн хасах үйлдлийг нэмэх үйлдэл дээр үндэслэн тодорхойлж болох бөгөөд $P = (x, y)$ цэгийн сөрөг цэг $-P$ нь

$-P = (x, x + y)$ байдаг. Эндээс хасах үйлдэл нь

$$P - Q = P + (-Q)$$

гэсэн нэмэх үйлдлээр илэрхийлэгдэнэ.

Муруйн цэгийн хувьд өөр дээр нь өөрийг нь нэмэхийг $P + P = 2P$ буюу хоёроор үржих үйлдэл гэнэ. Үүн дээр үндэслэж эллипслэг муруйн цэгийн үржих үйлдлийг тодорхойлдог бөгөөд цэгийн $k$ удаагийн нийлбэрийг $\underbrace{P + P + .. + P}_{k} = kP$ гэж тэмдэглэн цэгийг тоогоор үржих үйлдэл гэнэ. Мөн өөрөөр үүнийг $P$-ийн $k$ зэрэг гэдэг. Хоёртын талбарт зориулсан цэгийг үржих тусгайлсан, хурдан хэд хэдэн алгоритм байдаг. Мөн $2P$ мэдэгдэж үед $P$-г олох бодлого тавигддаг ба үүнийг таллан хуваах үйлдэл (point halving) гэх бөгөөд цэгийн үржих үйлдлийг ашиглаж хийдэг.

## V. Хэрэгжүүлэлт

Эллипслэг муруйн нууцлах, тайлах алгоритмууд нь нэлээд олон дэд алгоритм, функцуудаас тогтох нарийн бүтэцтэй ажил юм. Үүнийг хэрэглэгч ахин ашиглах боломж бүхий сан хэлбэрээр програмчлалын Жава хэл дээр хөгжүүлэв. Төгсгөлөг талбар болон муруйн арифметикийн алгоритмууд дээр нэг үгийн урт (word size) 64 бит байх хувилбараар програмчлав.

### A. *Эллипслэг муруйн параметрийн сонголт*

NIST-ээс 2010 онд гаргасан эллипслэг муруйн стандартад дэвшүүлсэн хэд хэдэн параметр бий [4]. Тэдгээрээс бид $\mathbb{F}_{2^{239}}$ талбарт тодорхойлогдсон муруйг сонгож ашиглав.

TABLE I. ЭЛЛИПСЛЭГ МУРУЙН ПАРАМЕТРУУД

| Параметр | Утга |
|---|---|
| $f(z)$ | $z^{239} + z^{158} + 1$ |
| $a$ | 0000000000000000000000000000000000000000000000000000000000000000 |
| $b$ | 0000000000000000000000000000000000000000000000000000000000000001 |
| $G$ | 0329A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC |
| $n$ | 2000000000000000000000000000005A79FEC67CB6E91F1C1DA800E478A5 |

### B. *Нууцлах алгоритм дэх функцуудын сонголт*

Нууцлах алгоритм дэх $KDF$ функцэд ANS X9.63 стандартад заасан түлхүүр байгуулах алгоритмийг,

$MAC$ функцэд $HMAC-SHA-1-160$ алгоритмийг, $ENC$ функцэд $AES-256$ нууцлах алгоритмийг тус тус ашигласан.

## VI. Дүгнэлт

Хэрэглэх салбарын онцлог болон нууцлах мэдээллийн хэмжээ, бүтэц зэрэгтэй уялдуулан эллипслэг муруйн криптографийг нууцлалын янз бүрийн зэрэг бүхий олон хувилбараар практикт хэрэгжүүлж болно.

### *Ном зүй*


[1] А.Мекей, ” Эллипслэг муруйн криптограф”, гар бичмэл, 2012

[2] Hankerson, Menezes, Vanstone, “Guide to Elliptic Curve Cryptography”, Springer, 2004

[3] National Institute of Standards and Technology, “Standards for Efficient Cryptography: Elliptic Curve Cryptography”, 2009

[4] National Institute of Standards and Technology, “Standards for Efficient Cryptography, Recommended Elliptic Curve Domain Parameters”, 2010

[5] Joppe W. Bos, J. Alex Halderman, “Elliptic Curve Cryptography in Practice”, Asiacrypt 2013