Элгамалын хосолмол криптосистем

Б.Магсаржав[1], А.Мекей[2]
[1]МУИС, Математик компьютерийн сургууль, Програм хангамжийн тэнхим
[2]МУИС, Математикийн хүрээлэн
[1]magsarjav@smcs.num.edu.mn, [2]mekei@smcs.num.edu.mn

***Хураангуй*—Криптографийн ил түлхүүртэй нууцлалын системүүдийн нэг болох Элгамалын криптосистем (ElGamal cryptosystem) ба түүний хосолмол криптосистемийн (hybrid cryptosystem) тухай авч үзнэ.**

Түлхүүр үг—Элгамалын криптосистем; хосолмол криптосистем, ил түлхүүртэй криптограф; дискрет логарифмийн бодлого

I. Удиртгал

Ил түлхүүртэй криптосистемүүд нь нийтийн ба хувийн түлхүүрүүдийн хоорондын хамаарлыг нуухын тулд нэг чигт функцын онолд суурилж зохиогдсон байдаг. Орчин цагийн криптографт ашиглагдаж буй ийм хоёр гол функцийн нэг нь анхны тоон үржигдэхүүнд задлах бодлого бөгөөд RSA криптосистем үүнд суурилсан байдаг бол нөгөө нь дискрет логарифмийн бодлого юм. Өнөө үед түгээмэл хэрэглэгдэж буй Диффи-Хелман, Эллиптик муруйн болон өөр цөөнгүй криптосистемүүд дискрет логарифмийн бодлогод суурилсан байдаг.

1984 онд Египетийн криптографч Тахир Элгамал (Taher El Gamal) дискрет логарифмийн бодлогод үндэслэж нэгэн ил түлхүүртэй криптосистемийг зохиосон. Мөн дараа нь уг системд тоон гарын үсэг зурах, шалгах аргыг боловсруулсан нь 1993 онд АНУ-ын Үндэсний стандартчилал, технологийн газраас зарласан уралдаанд шалгарч стандарт болон батлагдаж байсан. Үүнээс эхлэн Элгамалын криптосистем нарийн судлагдаж эхэлсэн ба “chosen ciphertext attack” аргаар довтолж болох нь батлагдсан. Тиймээс уг криптосистемийг сайжруулж, үндсэн алгоритмуудад сунгах механизм (padding) оруулах эсвэл хосолсон (hybrid) хэлбэрээр хэрэглэх гэсэн хоёр хувилбараар ашиглаж байна.

II. Дискрет логарифмийн бодлого

G нь q эрэмбийн цикл бүлэг, g уг бүлгийн үүсгэгч байг. $h \in G$ бүрийн хувьд $g^x = h$ байх $x \in Z_q$цор ганц байдаг. Энд x-ийг h-ийн g суурьтай дискрет логарифм гэж нэрлэдэг ба $x = log_g h$ гэж тэмдэглэнэ. G ба түүний үүсгэгч g өгөгдсөн үед дурын $h \in G$ хувьд $log_g h$-ийг олох бодлогыг дискрет логарифмийн бодлого гэнэ. “Стандарт” логарифм нь утгын төгсгөлгүй олонлогт яригддаг бол энэ логарифм нь утгын төгсгөлөг завсарт яригддаг учраас ялгах үүднээс “Дискрет” гэж тодотгодог [2]. Уламжлалт аргаар g-ийн зэргийг нэг нэгээр ахиулан h-тэй тэнцүү эсэхийг шалгах замаар бодож болох боловч бүлгийн эрэмбэ q том тохиолдолд энэ арга удаан ажиллах ба үүнээс өөр үр ашигтай тооцон бодох алгоритм одоогоор нээгдээгүй байна.

1976 онд Диффи (Whitfield Diffie), Хелман (Martin Hellman) нар дискрет логарифмийн бодлогыг криптографт хэрэглэх санааг анх олж Диффи-Хелманы бодлогыг зохиосон ба түүн дээрээ үндэслэн өөрсдийн нэрээр нэрлэгдсэн түлхүүр солилцох схемийг боловсруулсан байдаг.

III. Элгамалын криптосистем

Дискрет логарифмийн бодлогын үндсэн параметрүүд нь p, q, g болно. p нь том анхны тоо, $\mathbb{Z}_p = \{0,1, \dots, p-1\}$ үлдэгдлийн талбар, $\mathbb{Z}_p^* = \{1,2,..,p-1\}$ нь түүний үржих үйлдлийн бүлэг, q нь $p-1$ тооны хангалттай том анхны тоон хуваагч, $g \in \mathbb{Z}_p^*$ бөгөөд q эрэмбийн элемент буюу $g^q \equiv 1(mod\ p)$ байг. Хувийн түлхүүр x нь $1 < x < p-1$ ба нийтийн түлхүүр нь $y = g^x(mod\ p)$ байна. Мэдээг $c \leftarrow m * y^k\ (mod\ p)$ дүрмээр нууцлах ба буцаан гаргахдаа $m \leftarrow c * (g^k)^{-x}(mod\ p)$ гэж тайлна. Учир нь $m = c * (g^k)^{-x}(mod\ p) = m * y^k * (g^k)^{-x}\ (mod\ p) = m * (g^{kx}) * (g^{kx})^{-1}(mod\ p) = m$ билээ [1].

Сүлжээ чагнагч (eavesdropper) p, q, g, g^x, g^k зэргийг барьж мэдэж чадах хэдий ч энэ бүхнээс хувийн түлхүүр x-ийг тооцож гаргаж чадахгүй (дискрет логарифмийн бодлого).

Энэхүү криптосистем нь дараах 4 дэд алгоритмаас бүрдэнэ.

Алгоритм 1 Дискрет логарифмийн параметр үүсгэх

Оролт: p тооны уртыг заах параметр l

Гаралт: p, q, g

1) l байт урттай анхны тоо p ба $p-1$ тооны хуваагч байх том анхны тоо q тус бүрийг үүсгэнэ
2) $1 < a < p-1$ байх санамсаргүй a тоо сонгоно
3) $g \leftarrow a^{(p-1)/q}(mod\ p)$
4) Хэрэв $g = 1$ бол 2-р алхамд шилжинэ
5) p, q, g -г буцаана

Алгоритм 2 Түлхүүрийн хос үүсгэх

Оролт: p, q, g

Гаралт: Хувийн түлхүүр x, нийтийн түлхүүр y

1) $1 < x < q-1$ байх санамсаргүй x тоо сонгоно
2) $y \leftarrow g^x(mod\ p)$
3) x, y –г буцаана

Алгоритм 3 Мэдээг нууцлах

Оролт: Мэдээ m, (p, q, g), нийтийн түлхүүр y

Гаралт: Нууцлагдсан мэдээ c

1) $1 < k < q - 1$ байх санамсаргүй k тоо сонгоно
2) $c_1 \leftarrow m \cdot y^k (mod\ p)$
3) $c_2 \leftarrow g^k (mod\ p)$
4) $c \leftarrow c_1 || c_2$
5) c –г буцаана

Алгоритм 4 Мэдээг тайлах

Оролт: Нууцлагдсан мэдээ c, (p, q, g), хувийн түлхүүр x

Гаралт: Мэдээ m

1) c –ээс c_1, c_2 тус бүрийг салгаж авна
2) $m \leftarrow c_1 \cdot {c_2}^{-x} (mod\ p)$
3) m –г буцаана

IV. ХОСОЛМОЛ КРИПТОСИСТЕМ

Криптосистем нь ил болон нууц түлхүүртэй нууцлалын аргуудыг давхар (цувуулан) хэрэглэж байвал түүнийг хосолмол (hybrid) криптосистем гэнэ. Нууц түлхүүртэй нууцлах арга нь ил түлхүүртэй нууцлах аргаас харьцангуй хурдан ажилладаг. Тиймээс хосолмол системүүд илүү хурдан ба түгээмэл хэрэглэгддэг. Жишээлбэл ижил өгөгдөл дээр нууц түлхүүртэй алгоритм AES нь RSA-гаас 10000 дахин хурдан ажилладаг [3].

Хосолмол криптосистемийн нууцлах болон тайлах хийсвэр алгоритмийг дараах 5, 6-р алгоритмаар томьёолно. Энд x, y нь хувийн ба нийтийн түлхүүр, ENC_{pub}, DEC_{pub} нь ил түлхүүртэй нууцлах, тайлах алгоритмууд, ENC_{pri}, DEC_{pri} нь нууц түлхүүртэй нууцлах, тайлах алгоритмууд болно.

Алгоритм 5 Мэдээг хосолмол аргаар нууцлах

Оролт: m, y

1) Санамсаргүй s тоо сонгоно
2) $c_1 \leftarrow ENC_{pri}(s, m)$
3) $c_2 \leftarrow ENC_{pub}(y, s)$
4) c_1, c_2 –г нөгөө талдаа илгээнэ

Энд s-ийг завсрын түлхүүр (session key) гэж нэрлэдэг ба илгээгч хүлээн авагч талуудад аль алинд нь мэдэгдэж байдаг тул дундын нууц түлхүүр гэж нэрлэх нь ч бий.

Алгоритм 6 Мэдээг хосолмол аргаар тайлах

Оролт: c_1, c_2, x

1) $s \leftarrow DEC_{pub}(x, c_2)$
2) $m \leftarrow DEC_{pri}(s, c_1)$

V. ЭЛГАМАЛЫН ХОСОЛМОЛ КРИПТОСИСТЕМ

Өмнөх бүлэгт дурдсан 5 болон 6-р алгоритм дэх ENC_{pub}, DEC_{pub} нь Элгамалын криптосистемийн буюу 3, 4-р алгоритмууд байх тохиолдлыг Элгамалын хосолмол криптосистем гэнэ. Тиймээс 5 ба 6-р алгоритмуудад 3 ба 4-р алгоритмуудыг хэрэглэвэл дараах хосолмол нууцлах, тайлах алгоритм гарна.

Алгоритм 7 Мэдээг Элгамалын хосолмол аргаар нууцлах

Оролт: (p, q, g), y, m

1) $1 < k < q - 1$ байх санамсаргүй k тоо сонгоно
2) $1 < s < p - 1$ байх санамсаргүй s тоо сонгоно
3) $c_1 \leftarrow g^k (mod\ p)$
4) $c_2 \leftarrow s \cdot y^k (mod\ p)$
5) $c_3 \leftarrow ENC_{pri}(s, m)$
6) $c \leftarrow c_1 || c_2 || c_3$
7) c –г нөгөө талдаа илгээнэ

Алгоритм 8 Мэдээг Элгамалын хосолмол аргаар тайлах

Оролт: (p, q, g), x, c

1) c –ээс c_1, c_2, c_3 тус бүрийг салгаж авна
2) $s \leftarrow c_2 \cdot {c_1}^{-x} (mod\ p)$
3) $m \leftarrow DEC_{pri}(s, c_3)$

Хэрэгжүүлэлтэд ENC_{pri}, DEC_{pri} –ийн оронд AES, Triple DES гэх мэт дурын нууц түлхүүртэй алгоритм сонгож болно.

VI. ХЭРЭГЖҮҮЛЭЛТ

Элгамалын хосолмол криптосистемд 1, 2, 7, 8–р алгоритмууд хамаарна. Алгоритмуудад дурдагдсан хувьсагчууд бүгд 100-аас дээш оронтой тоонууд тул програмд бүхэлдээ том тооны тооцоолол хийгдэнэ. Мөн $\mathbb{Z}_p$ талбарын элементийн үйлдлүүдтэй холбоотой цөөнгүй алгоритмууд хэрэглэгдэнэ. Хэрэгжүүлэлтэд тулгардаг гол хоёр асуудлыг авч үзье.

A. Мэдээг талбарын элемент хэлбэрээр дүрслэх

Алгоритмуудад мэдээ болох m –ийг талбарын элемент хэлбэрээр тооцож хийсэн байгаа. Гэвч хэрэгжүүлэлтэд m нь компьютерийн систем дэх өгөгдөл буюу байтуудын дараалал байна. Тиймээс байт дарааллыг талбарын элемент рүү, талбарын элементийг байтуудын дараалал руу хөрвүүлэх нэмэлт алгоритмууд ашиглагдана.

B. Дискрет логарифмийн параметр байгуулах

Дискрет логарифмийн параметр болох p, q том анхны тоонууд нь ихэвчлэн 100-аас дээш оронтой байдаг тул $q|p - 1$ нөхцөл биелдэг байхаар байгуулах нь хялбар биш.

Криптографт хэрэглэгддэг том анхны тоо байгуулах магадлалт алгоритмууд байдаг хэдий ч тэдгээр нь ийм нөхцөлийг хангах хос тоог үүсгэж чадахгүй.

Тиймээс ийм анхны тоонуудыг байгуулах тусгай програмыг боловсруулсан ба уг програмын жишээ үр дүнг дараах хүснэгтэд харуулав.

ХҮСНЭГТ I. АНХНЫ ТООНУУД

Алхам	Утга	Орон (10т)	Бит урт
p_0	60773	5	16
p_1	3140384003	10	32
p_2	13212247890274551227	20	64
p_3	134230900369637019125287723298186137919	39	127
p_4	315762403145345506929752661488690653454628568823659204559274448247983886725 1	77	255
p_5	294329809849821439621892705436691262649439207880391406243720134695564507344783327426009236456837919585310855708141276203691471356359413800938839039315399	154	510
p_6	326785557080863111658019572259858399188865585781153509606724012909018352402990523329502463446328865526346465424453658193489851522535453690861762237958098440942290912368337894031872119668779816439672456550902278092333261550584569448993894585372231129012495677447991424393728154172482994458822165716987487699 69	308	1022

Хүснэгт дэх p_0 нь анхны утга бөгөөд програм 6 алхам ажиллаж дээрх анхны тоонуудыг үүсгэсэн. Эдгээр нь $p_{i-1}|(p_i - 1)$ чанартай анхны тоонууд ба $p \leftarrow p_i$ -ийг сонгосон бол $q \leftarrow p_{i-1}$ –ийг сонгоно.

НОМ ЗҮЙ

[1] А. Мекей, “Дискрет логарифмийн бодлогод үндэслэсэн Элгамалын криптосистем, түүний тоон гарын үсгийн тухай”, гар бичмэл

[2] J. Katz, Y. Lindell, “Introduction to modern cryptography”, 2008

[3] Bryce Allen, ”Implementing several attacks on plain ElGamal encryption”, Master thesis, Iowa State University, 2008