ЕлГамал крипто систем - однос ДЛОГ-ДХП

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Ел Гамал крипто-систем

Дифи-Хелманов протокол је започео лавину у асиметричној (public key) криптографији. Један од најзначајнијих асиметричних крипто-система који се појавио користећи ДХ, односно ДЛП као основу је Ел Гамал.

ЕлГамал (1985)

Алиса и Боб дефинишу прости број p и генератор g поља $\mathbb{F}_p$.

А Бира произвољан цио број a, што чува као тајну, а објављује $A \equiv g^a \pmod{p}$.

Б Енкрипцију поруке m врши тако што изабере случајан број k_m по модулу p и врати Алиси пар

$$(g^{k_m}, m \cdot A^{k_m}), \text{ све по модулу } p.$$

ЕлГамал крипто-систем

Јавни подаци у ЕлГамалу су

а. Прост број p, односно одговарајуће поље $\mathbb{F}_p$.

б. Генератор g поља $\mathbb{F}_p$.

в. Алиса објављује свој јавни кључ, $A \equiv g^a \pmod{p}$.

г. Боб објављује $(g^{k_m}, m \cdot A^{k_m})$.

Тајни подаци у ЕлГамалу су

а. Број a који је заправо Алисин тајни кључ.

б. За сваку поруку m, која је заправо неки број између 2 и p, Боб бира тајни број k_m (који је другачији за сваку поруку).

Декрипција у ЕлГамалу

Као што смо видјели, Алиса добија уређени пар

$$(g^{k_m}, m \cdot A^{k_m}), \text{ гдје је } A \equiv g^a \pmod{p}.$$

Алиса, с обзиром да зна a, врши декрипцију на очигледан начин

1. Рачуна $\left(g^{k_m}\right)^a \equiv A^{k_m} \pmod{p}$.
2. У другом кораку рачуна $\left(A^{k_m}\right)^{-1} \equiv B \pmod{p}$.
3. Алиса даље рачуна

$$m \cdot A^{k_m} \cdot B \equiv m \pmod{p},$$

чиме је декрипција завршена.

ЕлГамал оракл

- Примјетимо да у ЕлГамал крипто-систему, порука m је цијели број између 2 и $p-1$, док се енкриптована порука састоји од цијелих бројева (c_1, c_2) који се налази у истом домену. Дакле, енкрипција дуплира број битова основне поруке.
- Пробабилистичка енкрипција. Онемогућена претрага по малом скупу основних порука. Поређење са случајем симетричних крипто система.
- Релација односа сигурности између ДЛП и ЕлГамала. Доказ редукцијом.

Примјер ЕлГамал

Претпоставимо да је Алиса одабрала $p = 107$, $g = 2$, $a = 67$. Потом рачуна

$$A = 2^{67} \equiv 94 \mod 107.$$

Дакле, њени јавни подаци су $(p, g, A) = (107, 2, 94)$. Претоставимо да Боб жели да енкриптује слово "B" (66 ASCII) и да га пошаље Алиси. Он бира $k = 45$ и рачуна

$$(2^{45}, 94^{45} \cdot 66) \equiv (28, 9) \mod 107.$$

Декрипција се обавља на начин што израчунамо $28^{67} \equiv 5 \mod 107$, а потом $5^{-1} \equiv 43 \mod 107$. На крају,

$$9 \cdot 43 \equiv 66 \mod 107,$$

што јесте почетна порука.

ЕлГамал оракл и Дифи-Хелман проблем

- Оракл (deus ex machina) је појам који у криптографији представља неки непознат алгоритам који рјешава одређену врсту тешког, можда нерјешивог проблема.
- Доказујемо да уколико постоји оракл за рјешавање ЕлГамала, онда исто можемо искористити за рјешавање ДХП. И обрнуто.

Теорема

Разбијање ЕлГамал енкрипције је рачунски једнако сложено као и рјешавање ДХП.

ЕлГамал оракл и Дифи-Хелман проблем

Скица доказа:

$\rightarrow$

Нека нам је дат ЕлГамал оракл. Дати су подаци:

- прост број p и генератор g групе $\mathbb{Z}_p$
- јавни кључ g^a

За улаз (c_1, c_2, g^a, g, p) ЕлГамал оракл враћа $c_1^a \dot{(}c_2)^{-1} \pmod p$.
Дакле, ако су

$$(c_1, c_2) = (g^b, 1) \text{ онда је резултат } g^{ab} \pmod p.$$

ЕлГамал оракл и Дифи-Хелман проблем

$\leftarrow$

Нека нам је дат Дифи-Хелман оракл. Дати су подаци:

- прост број p и генератор g групе $\mathbb{Z}_p$

За улаз (g^a, g^b) Дифи-Хелман враћа $g^{ab} \pmod p$. Дакле, како је у ЕлГамалу јавни податак g^a а g^k прва компонента уређеног пара $(g^k, m \cdot g^{ak})$, онда за те улазне податке из ДХ оракла добијамо g^{ak}. Тиме из друге компоненте ЕлГамала добијамо и m.

Сигурност ЕлГамала

ЕлГамал се може разбити ако се не води рачуна о неким основним сигурносним претпоставкама. Наводимо најпознатији начин за разбијање.

Напад заснован на једнаком експоненту енкрипције

Ако за двије различите поруке m и m^* користимо исти степен енкрипције k, онда ЕлГамал енкрипција даје парове (g^k, mg^{ak}) и (g^k, m^*g^{ak}). Уколико нападач има поруку, рецимо m, очигледно је како долази и до m^*.

Претходни напад се у литератури назива **напад са изабраном енкрипцијом** (chosen plaintext attack).

Сигурност ЕлГамала

Постоји још један напад на ЕлГамал протокол у ком нападач не декриптује текст, али је у стању да у одређеној мјери утиче на оно што ће се декриптовати.

Напад мултипликацијом

Претпоставимо да је Боб послао ЕлГамал енкриптовану поруку (g^k, mg^{ak}). Оскар бира број s и мијења одаслату поруку тако што шаље (g^k, smg^{ak}). Након декрипције, Алиса на крају добија sm.

Дакле, уколико Оскар претпоставља из ког домена се размјењују поруке, онда овом мултипликацијом може смислено и битно утицати на оно што ће Алиса прихватити као поруку.

Основни појмови комплексности

- Математички апарат за мјерење комплексности.

Дефиниција

Нека су $f(x)$ и $g(x)$ функције чије су вриједности позитивне. Ознака $f(x) = O(g(x))$ значи да постоје позитивне константе c и C тако да

$$f(x) \leq cg(x) \text{ за све } x \geq C.$$

Лема

Ако постоји коначан лимес

$$\lim_{x \to \infty} \frac{f(x)}{g(x)},$$

онда је $f(x) = O(g(x))$.

Основни појмови комплексности

У односу на величину улазног податка, рецимо број битова k, вријеме извршавања алгоритма, којим се рјешава одређени проблем, можемо подијелити на

- **Полиномно вријеме**, ако је број корака $O(k^A)$, за неку константу A.
  - За $A = 1$, кажемо да је вријеме **линеарно**.
  - За $A = 2$ кажемо да је вријеме **квадратно**.
- У случају да постоји константа $c > 0$, тако да је број корака једнак $O(e^{ck})$, онда кажемо да је вријеме **експоненцијално**.
- Ако је за произвољно $\epsilon > 0$ могуће наћи алгоритам који ради у $O(e^{\epsilon k})$ корака, онда кажемо да је вријеме **субекспоненцијално**.

Комплексност ДЛП

- Рјешавамо оригинални ДЛП, $g^x = h$ у $\mathbb{F}_p$.

Trial-and-error метод

Ако је прост број p изабран између 2^k и 2^{k+1}, тада су g, h, и p највише k битова дужине, тако да је величина улазних података $O(k)$ битова. (Примјетимо да је $O(k)$ исто што и $O(\log_2(p))$. Ако покушавамо ријешити ДЛП примјењујући trial-and-error метод, то захтјева $O(p)$ корака за његово рјешавање. Пошто је $O(p) = O(2^k)$, ово је алгоритам са експоненцијално временом извршења.

Шанксов Baby step-Giant step алгоритам

Шанксов алгоритам је заснован на идеји формирања двије листе и тражењу елемента који се налази у обје.

- Нека G група и нека је $g \in G$ елемент реда $N \geq 2$. Следећи алгоритам рјешава $g^x = h$ дискретни логаритам у $O(\sqrt{N}\log(N))$ корака.
  (1) Нека је $n = 1 + \lfloor \sqrt{N} \rfloor$, што посебно значи $n > \sqrt{N}$.
  (2) Формирамо двије листе,

  Листа 1. $e, g, g^2, \ldots, g^n$,
  Листа 2. $h, hg^{-n}, hg^{-2n}, \ldots, hg^{-n^2}$.

  (3) Наћи заједнички елемент у двије листе, рецимо $g^i = hg^{-jn}$.
  (4) Тада је $x = i + jn$ рјешење једначине (ДЛП) $g^x = h$.