УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, Л.В. МАКУТОНІНА

АНАЛІЗ СТІЙКОСТІ ОБЧИСЛЮВАЛЬНИХ ЗАДАЧ, ЩО ЗАСНОВАНІ НА БІЛІНІЙНИХ ВІДОБРАЖЕННЯХ

Вступ

Одним із перспективних напрямів розвитку криптографічних систем на ідентифікаторах є поєднання математичного апарату бінарного відображення (спарювання) точок еліптичних кривих з алгебраїчними решітками [1]. Таке поєднання дозволяє використати переваги спарювання та алгебраїчних решіток, основними з яких є зменшена складність (підвищена швидкодія) обчислень при криптографічних перетвореннях, відмова від використання сертифікатів, порівняно невеликий розмір зашифрованих текстів та ключових даних. Але, як для окремо взятих, так для поєднаного криптографічного перетворення з використанням удосконаленого методу, в першу чергу потрібно порівняти їх за безумовним критерієм криптографічної стійкості та складності (швидкодії) криптографічних перетворень.

Метою цієї статі є аналіз основних обчислювальних задач криптографії з використанням білінійних відображень та, по можливості, визначення основних питань їх використання при поєднанні бінарного відображення точок еліптичних кривих з алгебраїчними решітками.

Основні положення білінійних відображень

Класичні схеми на ідентифікаторах використовують математику білінійних відображень (спарювань). В криптографічних схемах на ідентифікаторах використовується не вироджене, ефективне для обчислювання білінійне відображення:

$$e: G_1 \times G_2 \to G_3, \tag{1}$$

де G_1, G_2, G_3 – циклічні групи однакового порядку p. Найчастіше складовими відображення є елементи еліптичних кривих, таким чином, G_1 і G_2 виступають циклічними підгрупами точок на еліптичній кривій над кінцевим полем, а результатом відображення є підгрупа G_3 мультиплікативної групи над кінцевим полем. Зазвичай груповою операцією для еліптичних кривих є додавання, тому G_1 і G_2 є адитивними підгрупами, в той час, як G_3 є мультиплікативною підгрупою [1]. Основними властивостями білінійного відображення є невиродженість, ефективність обчислення та білінійність.

Невиродженість – це властивість, при якій якщо $e(P,Q)$ тотожно елементу G_3, тоді P тотожно G_1 та/або Q тотожно G_2. Тобто виконуються такі умови:

1) для всіх $P \in G_1$, з $P \neq 0$, існує деяке $Q \in G_2$, таке, що $e(P,Q) \neq 1$;

2) для всіх $Q \in G_2$, з $Q \neq 0$, існує деяке $P \in G_1$, таке, що $e(P,Q) \neq 1$.

Під ефективністю мається на увазі, що існує поліноміальний алгоритм, що дозволяє ефективно обчислювати відображення $e(X,Y)$.

Під білінійністю розуміється лінійність відображення *e* по обом компонентам, що задовольняють таким двом властивостям:

$$\begin{aligned} e(R_1 + R_2, Q) &= e(R_1, Q)e(R_2, Q); \\ e(R, Q_1 + Q_2) &= e(R, Q_1)e(R, Q_2). \end{aligned} \tag{2}$$

Наслідком наведених властивостей є наступне співвідношення, яке і є основною відмінністю всіх схем, що засновані на білінійних відображеннях. Сутність його в тому, що для $a, b \in Z_p$ справедливим є

$$e(aP_1, bP_2) = e(bP_1, aP_2) = e(P_1, P_2)^{ab}. \tag{3}$$

Важливими також є і такі наслідки білінійності.

Нехай $P \in G_1$ і $Q \in G_2$, тоді для білінійного спарювання e виконуються наступні властивості:

1) $e(P,0) = e(0,Q) = 1$, що є наслідком (2), так як $e(P,Q) = e(P+0,Q) = e(P,Q)e(0,Q)$;

2) $e(-P,Q) = e(P,Q)^{-1} = e(P,-Q)$, так як $1 = e(0,Q) = e(P+(-P),Q) = e(P,Q)e(-P,Q)$;

3) $e(jP,Q) = e(P,Q)^j = e(P, jQ)$, для всіх $j \in Z$.

Визначення дивізора

Ключовим поняттям для білінійних відображень є теорія дивізорів (дільників) алгебраїчної кривої, яку запропонував Андре Вейль. Спираючись на [2 – 4] дамо визначення дивізора. Нехай $E: y^2 = x^3 + ax + b$ – еліптична крива над ідеальним полем K, та нехай $E(\overline{K})$ позначає алгебраїчне замикання поля K, тобто, множину точок $P(x,y) \in EC(\overline{K})$, що задовольняють $nP = \infty$, таким чином, поле K – кінцеве, а його замикання нескінчене. Тоді, дивізором над кривою E називають формальну суму

$$D = \sum_{P \in E(\overline{K})} n_P [P], \tag{4}$$

де коефіцієнти $n_P \in Z$ – цілі числа, причому число доданків з ненульовими коефіцієнтами n_P є кінцевим. Множина дивізорів еліптичної кривої утворює адитивну групу відносно операції додавання, а нулем є дивізор, у якого всі коефіцієнти дорівнюють нулю, тобто дивізор з усіма $n_P = 0$ дорівнює нулю. Множина дивізорів на кривій E позначається як $div_{\overline{K}}(E)$, а сума дивізорів визначається природним шляхом. Множина точок P, для яких $n_P \neq 0$ зветься носієм (support) дивізора D і позначається $supp(D)$. Ціле число $k = \sum n_P$, $P \in supp(D)$, зветься ступенем D і позначається $deg(D)$.

Визначимо також поняття групи Галуа. Групою Галуа називають групу ізоморфізмів над певним розширенням поля. Нехай $\overline{K}$ є розширенням поля K. Нехай, визначена множина всіх автоморфізмів поля $\overline{K}/K$, тобто ізоморфізм α з поля $\overline{K}$ сам у себе такий, що $\alpha(x) = x$ для всіх $x \in K$, тоді розширення $\overline{K}/K$ називається розширенням Галуа, і, для нашого випадку, група Галуа позначається як $\sigma \in Gal(\overline{K}/K)$. Визначимо $D^\sigma = \sum_P n_P(\sigma(P))$. Дивізор визначається над K, якщо $D = D^\sigma$ для всіх $\sigma \in Gal(\overline{K}/K)$.

Нехай $f(x,y): E \to K$ – раціональна функція. Якщо f не є константою, тоді існує кінцеве число точок $P \in E$, в яких $f(P) = 0$ або $f(P) = \infty$. Точки виду $f(P) = 0$ називаються нулями функції f, точки виду $f(P) = \infty$ називаються полюсами функції f. З точністю до ненульового множника можна задати функцію f, перераховуючи всі її нулі і полюса, задаючи їх кратність. Якщо f має нуль/полюс кратності k в точці P, тоді функцію f можна представити у вигляді добутку $f = u_P^k \cdot g$, де u_P має нуль/полюс першого порядку в точці P, а $g(P) \neq 0$ і $g(P) \neq \infty$, відповідно. Функція u_P називається уніформізатором функції f в точці P. Якщо f – ненульова функція над кривою E, тоді $ord_P(f)$ містить безліч f для P. Необхідно відмітити, що $ord_P(f)$ є позитивним, коли $f(P) = 0$, і негативним, якщо f має полюс в точці P. Дивізор ненульової функції f, записаної як (f), є дивізор $\sum_{P \in C(\overline{K})} ord_P(f)(P)$. Звідси випливає, що $(fg) = (f) + (g)$ і $(f/g) = (f) - (g)$.

В групі дивізорів найважливішими є, так звані, головні дивізори (principaldivisors). Головний дивізор над кривою E – це дивізор, що дорівнює (f), для деякої функції f, причому $\deg((f)) = 0$ [див. 2,3]. Функція f визначається над K, якщо вона може бути записана

з усіма коефіцієнтами в полі K. Якщо f ненульова функція, визначена над K, тоді дивізор (f) визначено над K. Якщо $f \in \overline{K}^*$ – константа, тоді $(f)=0$, і, навпаки, якщо $(f)=0$, тоді f повинна бути константою. Іншими словами, дивізор (f) визначає функцію f з точністю до ненульового множника.

Два дивізора D і D' є еквівалентними $D \sim D'$, якщо $D' = D + (f)$ для деякої функції f. Якщо $D_1 \sim D'_1$ і $D_2 \sim D'_2$, тоді $(D_1 + D_2) \sim (D'_1 + D'_2)$. Групою класів дивізорів над кривої називають множину всіх дивізорів нульового ступеня, з груповою структурою, що еквівалентна $div_{\overline{K}}(E)$.

Визначимо також поняття групового гомоморфізму з адитивної групи дивізорів до мультиплікативної групи поля K. Нехай $P_1(x_1, y_1)$ і $P_2(x_2, y_2)$ – дві точки на кривій $E(K)$. Припустимо, що пряма, проведена повз точки P_1 і P_2 має вигляд $l(x, y)=0$. Якщо l не є дотичною в точках P_1 і P_2, тоді існує деяка третя точка $S(x_s, y_s)$, в який вона перетинає E. Лінійний многочлен $l(x, y)$ можна інтерпретувати, як функцію відображення точки еліптичної кривої в K. Функція $l = ax + by + c$ має дивізор $div(l_{P_1,P_2}) = 1[P_1] + 1[P_2] + 1[S] - 3[O]$. Вертикальна пряма $v(x) = (x - x_s)$, що проходить через точки S і $P_3 = P_1 + P_2$, і є функцією на кривій E, має дивізор $div(v_{S,P_3}) = 1[S] + 1[P_3] - 2[O]$. Таким чином, рівняння $P_3 = P_1 + P_2$ є еквівалентним рівнянню дивізора $[P_3] - [O] = [P_1] - [O] + [P_2] - [O] - div(l/v)$ і, тоді, відображення P до дивізору класу $[P] - [O]$ є груповим гомоморфізмом.

Визначимо поняття дивізора нульового ступеню. Нехай E – еліптична крива над полем K. Тоді, дивізор нульового ступеню на кривій E є дивізор, виду $D = \sum_P n_P(P)$. Далі, дивізор D з нульовим ступенем є дивізором деякої функції f тоді і тільки тоді, коли $\sum_P [n_P]P = O$, тобто тоді, коли сума дивізорів для цієї функції дорівнює нескінченності.

Нехай f – деяка функція, і нехай $D = \sum_P n_P(P)$ – дивізор нульового ступеню, такий, що $supp(D)$ не перетинається з $supp(f)$. Визначимо

$$f(D) = \prod_P f(P)^{n_P}. \qquad (5)$$

Якщо $g = cf$, для деякої константи $c \in \overline{K}^*$, тоді, якщо D нульового ступеню, $g(D) = f(D)$. Отже, в цьому випадку величина $f(D)$ залежить тільки від дивізорів (f) і D. Якщо f і D визначені над полем K, тоді $f(D) \in K$.

З урахуванням наведеного вище можна дати визначення закону взаємності Вейля (Weilreciprocity). *Нехай f і g будуть ненульовими функціями кривої C над полем K. Якщо $div(f)$ і $div(g)$ не мають спільних точок, тобто $supp(f)$ і $supp(g)$ не перетинаються, тоді $f(div(g)) = g(div(f))$.*

Спарювання Тейта та його основні властивості

В якості основних в криптографії використовується два типи спарювань – спарювання Тейта і спарювання Вейля [5]. Спочатку дамо визначення спарюванню Тейта. Існує декілька варіантів спарювання Тейта. Так, Тейт запропонував досить узагальнене визначення спарювання на абелевих різноманіттях над локальними полями. Пізніше, було запропоновано спарювання на кривій Якобіана над локальними полями, яке можна явно обчислити [6]. Фрей і Рак у роботах [7, 8] ввели визначення спарювання Тейта над кінцевим полем, яке зараз використовується в криптографії.

Нехай $E: y^2 = x^3 + ax + b$ – еліптична крива над полем K_0 та нехай n буде позитивним цілим, яке є взаємно простим з характеристикою поля K_0. Нехай також множина коренів n-го ступеня буде визначена як $\mu_n = \{u \in \overline{K}_0^* : u^n = 1\}$. Визначимо поле $K = K_0(\mu_n)$, розширення K_0 породжених n коренів з одиниці. Визначимо також:

$$\begin{aligned} E(K)[n] &= \{P \in E(K) : [n]P = O\}, \\ nE(K) &= \{[n]P : P \in E(K)\}. \end{aligned} \tag{6}$$

де $E(K)[n]$ – група показників ступеню n; $nE(K)$ – підгрупа $E(K)$, множина точок $\{nQ \mid Q \in E\}$;

Тоді, $E(K)/nE(K)$ – фактор-група ступенів n, множина класів еквівалентності кривої $E(K)$ по множині $nE(K)$, над відношенням $P_1 \equiv P_2$ еквівалентності, в тому випадку, якщо $(P_1 - P_2) \in nE(K)$. Також визначимо:

$$(K^*)^n = \{u^n : u \in K^*\}. \tag{7}$$

де $(K^*)^n$ – підгрупа групи K^* і фактор-група $K^*/(K^*)^n$ – група ступенів n. Групи $K^*/(K^*)^n$ і μ_n є ізоморфними.

Групи $E(K)[n]$ і $E(K)/nE(K)$ мають однакове число елементів, але точки групи $E(K)[n]$ можуть і не бути представниками класів групи $E(K)/nE(K)$. Так, наприклад, нехай p і r – прості числа, такі, що r^4 ділить $(p-1)$. Існує еліптична крива E над F_p з $p-1$ точками, що має r^4 точок порядку r^2 визначених над F_p. В даному випадку $E[r] \subseteq rE(F_p)$.

Нехай $P \in E(K)[n]$, $Q \in E(K)$. Вважаємо, що Q представляє клас еквівалентності в $E(K)/nE(K)$. Доки $[n]P = O$, існує функція f така, що $(f) = n(P) - n(O)$. Нехай D буде будь-яким дільником нульового ступеню еквівалентним $(Q) - (O)$, таким, що D визначено над K і основа D не перетинається з основою (f). У більшості випадків такий дільник може бути легко побудований шляхом вибору довільної точки $S \in E(K)$ і визначається $D = (Q + S) - (S)$. Оскільки f і D визначені над K, значення $f(D)$ є елементом K. Доки основи (f) і D не перетинаються, маємо $f(D) \neq 0$, і тоді $f(D) \in K^*$.

Спарювання Тейта над P і Q визначається як

$$\langle P, Q \rangle_n = f(D), \tag{8}$$

та інтерпретується як елемент $K^*/(K^*)^n$. Значення спарювання Тейта є класом еквівалентності, тобто символ «=» використовується для позначення еквівалентності над цим відношенням, доказ цього твердження наведено в [5].

Тобто, спарювання Тейта – це білінійне відображення виду

$$\tau_n : E[n] \times E / E[n] \to F_{q^k}^* \times F_{q^k}^* \setminus \mu_n, \tag{9}$$

де μ_n – мультиплікативна підгрупа коренів n-го ступеню з одиниці поля F_{q^k}, визначена як:

$$\tau_n(T, S) = \frac{f_T(S + R)}{f_T(R)}, \text{ де } R \notin \{T, -S, T - S, \infty\}. \tag{10}$$

Визначимо основні властивості спарювання Тейта. Нехай E – еліптична крива над K_0 і n – взаємно просте з характеристикою K_0. Нехай $K = K_0(\mu_n)$. Тоді спарювання Тейта задовольняє наступним властивостям:

1) Білінійність. Для всіх $P, P_1, P_2 \in E(K)[n]$ і $Q, Q_1, Q_2 \in E(K)/nE(K)$ справедливо:

$$\langle P_1 + P_2, Q\rangle_n = \langle P_1, Q\rangle_n \langle P_2, Q\rangle_n,$$
$$\langle P, Q_1 + Q_2\rangle_n = \langle P, Q_1\rangle_n \langle P, Q_2\rangle_n.$$

2) Невиродженість. Нехай K – кінцеве поле. Для всіх $P \in E(K)[n]$, $P \neq O$, існує деяке $Q \in E(K)/nE(K)$, таке, що $\langle P, Q\rangle_n \neq 1.3$ іншого боку, для всіх $Q \in E(K)/nE(K)$ з $Q \notin nE(K)$ існує деяке $P \in E(K)[n]$, таке, що $\langle P, Q\rangle_n \neq 1$.

3) Інваріантність Галуа. Якщо $\sigma \in Gal(\overline{K}/K_0)$, тоді $\langle \sigma(P), \sigma(Q)\rangle_n = \sigma(\langle P, Q\rangle_n)$.

Доказ наведених властивостей наведено у джерелах [5, 7, 9]. Найважливішою є властивість невиродженості, на відміну від спарювання Вейля, відображення Тейта не дорівнює одиниці, при $P = Q$, ця властивість дозволяє обчислити деяке m, таке, що $Q = mP$ за одне обчислення. Відмітимо також, що значення перетворення Тейта $\tau(P, Q)$ визначається точками P і Q не однозначно, а з точністю до множника, що належить до групи μ_n. Для того щоб отримати конкретне унікальне значення, елемент $\tau(P, Q)$ підносять до ступеня $(q^k - 1)/n)$, тобто, $\tau_{un}(P, Q) = \tau(P, Q)^{(q^k-1)/n}$.

Спарювання Вейля

Нехай $E: y^2 = x^3 + ax + b$ – еліптична крива, визначена над алгебраїчно замкнутим полем точок кривої K_0 та нехай n буде позитивним цілим яке є взаємно простим з характеристикою поля K_0, і $E[n]$ – підгрупа точок кривої E порядку n: $E[n] = \{P \in E \mid n \cdot P = \infty\}$. Також нехай $K = K_0(E[n])$ буде розширенням поля K_0, що генероване координатами усіх точок поля $E(\overline{K})$, порядку, що ділиться на n. Спарювання Вейля – це відображення:

$$e_n : E[n] \times E[n] \to \mu_n \subseteq K^*. \tag{11}$$

Нехай $P, Q \in E[n]$ і $D_P = [P] - [O]$ і $D_Q = [Q] - [O]$ – два дивізори нульового ступеню, такі, що їх носії не перетинаються. Також нехай $f(P) = nD_P$ і $f(Q) = nD_Q$ будуть двома функціями, тоді спарювання Вейля можна визначити наступним чином:

$$e_n(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}. \tag{12}$$

Спарювання Вейля приймає значення в $\mu_n \subseteq K^*$, де μ_n – це мультиплікативна підгрупа коренів ступеню n з одиниці поля K. Тоді спарювання Вейля задовольняє наступним властивостям:

1) Білінійність. Для всіх $P, P_1, Q, Q_1 \in E[n]$ справедливо:

$$\begin{aligned} e_n(P + P_1, Q) &= e_n(P, Q) e_n(P_1, Q), \\ e_n(P, Q + Q_1) &= e_n(P, Q) e_n(P, Q_1). \end{aligned} \tag{13}$$

2) Змінність. $e_n(P, P) = 1$, тоді $e_n(P, Q) = e_n(Q, P)^{-1}$.

3) Невиродженість. Якщо $e_n(P, Q) = 1$, для всіх $Q \in E[n]$, тоді $P = Q$.

4) Інваріантність Галуа. Для всіх $\sigma \in Gal(\overline{K}/K)$, справедливо

$$e_n(\sigma(P),\sigma(Q)) = = \sigma(e_n(P,Q)).$$

5) Сумісність. Якщо $P \in E[nm]$ і $Q \in E[n]$, тоді $e_{nm}(P,Q) = e_n([m]P,Q)$.

6) Якщо $\phi : E \to E'$ – ізоендоморфізм з подвійним $\hat{\phi}$, тоді $e_n(\phi(P),Q) = e_n(P,\hat{\phi}(Q))$.

Усі наведені властивості, окрім невиродженості, можна довести, використовуючи закон взаємності Вейля [див. 2].

Найважливішим наслідком наведених властивостей є наступне твердження. *Нехай E – еліптична крива над полем k, і, нехай, r – просте число. Нехай $P,Q \in E(k)[r]$, такі, що $P \neq Q$. Тоді Q лежить в підгрупі, що породжена P, тоді і тільки тоді, коли $e_r(P,Q) = 1$.*

Порівняльний аналіз спарювання Тейта і Вейла

Спочатку звернемо увагу на деяку схожість між визначеннями спарювання Тейта і спарювання Вейля. Для спарювання Вейля функція $f(D')$ еквівалентна по модулю n – го ступеню до $\langle P,Q\rangle_n$, тоді, як $g(D)$ є еквівалентним по модулю n – го ступеню до $\langle Q,P\rangle_n$. За цих умов можна записати:

$$e_n(P,Q) = \frac{\langle P,Q\rangle_n}{\langle Q,P\rangle_n}, \tag{14}$$

з точністю до n – го ступеня, якщо $\mu_n \not\subseteq (K^*)^n$.

Однією із відмінностей між спаровуваннями Вейля і Тейта, є той факт, що для спарювання Тейта використовується поле $K_0(\mu_n)$, а для спарювання Вейля потенційно набагато більше за розміром поле $K_0(E[n])$. У роботі [10] Кобліц та ін. показали, що у більшості випадках ці два поля співпадають. Дійсно, нехай E – еліптична крива над полем F_q, r – просте число, що ділить $\#E(F_q)$. Припустимо також, що r не ділить $(q-1)$ і НОД$(r,q) = 1$, тоді $E[r] \subset E(F_{q^k})$, тоді і тільки тоді, коли r ділить $(q^k - 1)$.

Спарювання Вейля може бути узагальнено з $E[n] = \ker([n])$ до $\ker(\phi)$, де ϕ – ізоендоморфізм. Так, у роботі [11] було показано, що для деяких випадків узагальнене спарювання Вейля по суті є еквівалентним спарюванню Тейта.

Аналіз стійкості основних обчислювальних задач, що засновані на білінійних відображеннях

Розглянемо основні задачі, наведені в літературі, що засновані на білінійних відображеннях, і є важко розв'язувальними. Стійкість наступних задач базується на твердженні, що на даний момент не існує ні єдиного алгоритму, який міг би вирішити дану задачу за поліноміальний час. Базовою задачею для криптосистем на ідентифікаторах, що використовують спарювання, є задача дискретного логарифмування [1, 5]. Для циклічної групи, що найчастіше використовується в криптографічних додатках, задача дискретного логарифмування у групі є складно обчислювальною, тобто не існує жодного алгоритму, який би вирішував цю задачу за поліноміальний час. Обчислювальна складність інших задач залежить від складності розв'язку задачі дискретного логарифму. Тому, спочатку дамо визначення задачі розв'язання дискретного логарифму над циклічною групою $\langle g\rangle$, але перед цим визначимо типи спарювань, що будуть необхідні в подальшому.

Нехай $e : G_1 \times G_2 \to G_T$ – білінійне відображення, що визначено над групами еліптичних кривих. Нехай G_1 і G_2 – циклічні групи однакового простого порядку, які є ізоморфними.

В залежності від структури групи G_2 білінійні спарювання можна класифікувати наступним чином [12]:

Тип 1. Спарювання належить до першого типу, якщо $G_1 = G_2$.

Тип 2. Спарювання належить до першого типу, якщо можна ефективно обчислити ізоморфізм ψ із G_2 до G_1.

Тип 3. Спарювання належить до першого типу, якщо не можна ефективно обчислити ізоморфізм із G_2 до G_1.

Для Типу 2 ізоморфізм є легко обчислювальним, тоді, як для Типу 3 на даний момент не існує даного ізоморфізму, але для двох даних типів припускається, що не існує ефективно обчислювального ізоморфізму з G_1 до G_2. Під Типом 1 розуміється використання симетричного спарювання, тобто $e(P,Q) = e(Q,P)$. Тип 2 і Тип 3 належать до асиметричного спарювання. Так як на практиці спарювання третього типу зазвичай не використовується, тому такі задачі не розглядатимуться в цій статті.

1) DLP-задача (Discrete Logarithm Problem).

Вхідні дані: Циклічна група $\langle g \rangle$, порядку p і елемент $h \in \langle g \rangle$.

Завдання: Обчислити $a \in Z_p$, що $h = g^a$.

Тобто, a зветься дискретним логарифмом від h, щодо основи g, і записується, як $\log_g h = a$. Для циклічної групи, що найчастіше використовується в криптографічних додатках, задача дискретного логарифмування у групі є складно обчислювальною, тобто не існує жодного алгоритму, який би вирішував цю задачу за поліноміальний час. Нехай також, основа логарифму над $\langle g \rangle$ має розмір n. Очевидно, можна знайти a шляхом повного перебору всіх елементів $\langle g \rangle$ за час $O(2^n)$, тобто за експоненціальний час. Звичайно, існують загальні алгоритми, такі, як, наприклад, метод Полларда, що дозволяють знизити складність до $O(2^{n/2})$, але вона все-таки залишається експоненціальною.Тобто, можна сказати, що на даний момент, задача дискретного логарифмування для деяких груп кінцевого поля та на еліптичних кривих є обчислювально складною і широко використовується у криптографії.

2) CDH-задача (Computational Diffie-Hellman).

Вхідні дані: Циклічна група $\langle g \rangle$, порядку p і елементи, де $a,b \in Z_p$ – рівномірні і випадкові елементи.

Завдання: Обчислити g^{ab}.

Іншими словами, якщо криптоаналітик (далі – КРА) A має мету вирішити CDH-задачу, за вхідні дані він має (g, g^a, g^b), а на виході повинен отримати g^{ab}. Тобто, A повинен вирішити наступне рівняння:

$$Adv^{CDH}(A) = \Pr[(g, g^a, g^b) \to g^{ab}]\,(g, g^a, g^b) \qquad (15)$$

Говорять, що CDH-задача є (ε, t)-складною, якщо для будь-якого A щонайбільше за час t, $Adv^{CDH}(A) \le \varepsilon$.

3) DDH-задача (Decisional Diffie-Hellman)

Вхідні дані: Циклічна група $\langle g \rangle$, порядку p і елементи (g, g^a, g^b, g^c), де $a,b \in Z_p$ – рівномірні і випадкові елементи.

Завдання: Визначити, чи є $c = ab$, або, чи $c \in Z_p$ випадковим рівномірним елементом.

Тобто, A за вхідні дані має (g, g^a, g^b, g^c), а на виході повинен отримати біт. Подія, при який A отримує одиницю, визначається, як $A(g, g^a, g^b, g^c) \to 1$. Тобто, A повинен вирішити наступне рівняння:

$$Adv^{DDH}(A) = |\Pr[A(g, g^a, g^b, g^c) \to 1] - \Pr[A(g, g^a, g^b, g^c) \to 1]|. \quad (16)$$

Говорять, що DDH-задачу в групі $\langle g \rangle$ є (ε, t)-складною, якщо для будь-якого A щонайбільше за час t, $Adv^{DDH}(A) \le \varepsilon$.

Далі дамо визначення декільком задачам для симетричного спарювання Типу 1, тоді, для даного типу $G = G_1 = G_2$, для позначення набору параметрів будемо використовувати (p, G, G, G_T, e). Нехай також, $G = \langle P \rangle$ і $G_T = \langle e(P, P) \rangle$. Також, припускається, що (p, G, G, G_T, e), а також генератори G і G_T та деякі інші параметри, в залежності від конкретної задачі, є відкритими параметрами.

Базовою складною задачею на білінійних відображеннях є білінійна задача Діффі – Гелмана, вперше запропонована Воне і Франкліним у [13].

4) BDH (BilinearDiffie-Hellman)

Вхідні дані: Набір (P, aP, bP, cP), де $a, b, c \in Z_p$ – рівномірні і випадкові елементи.

Завдання: Обчислити $e(P, P)^{abc}$.

Як і у випадку CDH-задачі, A повинен вирішити наступне рівняння:

$$Adv^{BDH}(A) = \Pr[A(P, aP, bP, cP) \to e(P, P)^{abc}] \quad (17)$$

Говорять, що DDH – задача у групі $\langle g \rangle$ є (ε, t)-складною, якщо для будь-якого A щонайбільше за час t, $Adv^{BDH}(A) \le \varepsilon$.

5) DBDH-задача (DecisionalBilinearDiffie-Hellman)

Вхідні дані: Набір (P, aP, bP, cP, Z), де $G = \langle P \rangle$, $a, b, c \in Z_p$ – рівномірні і випадкові елементи і $Z \in G_T$.

Завдання: Визначити, чи є $Z = e(P, P)^{abc}$, або, чи Z випадковим елементом G_T.

Тобто, A за вхідні дані має (P, aP, bP, cP, Z), а на виході повинен отримати біт. Подія, при який A отримує одиницю, визначається як $A(P, aP, bP, cP, Z) \to 1$. Тобто, A повинен вирішити наступне рівняння:

$$\begin{aligned} Adv^{DBDH}(A) = &|\Pr[A(P, aP, bP, cP, Z) \to 1 \mid Z = e(P, P)^{abc}] - \\ &- \Pr[A(P, aP, bP, cP, Z) \to 1 \mid Z - \text{випадкове}]|. \end{aligned} \quad (18)$$

Говорять, що DBDH-задача у (p, G, G, G_T, e) є (ε, t)-складною, якщо для будь-якого A щонайбільше за час t, $Adv^{DBDH}(A) \le \varepsilon$.

Як було відмічено раніше, якщо використовуються параметри (p, G, G, G_T, e) для спарювання Типу 1, тоді DDH-задача у G не є складною, для даних $(P, aP, bP, cP) \in G^4$, необхідно лише зробити перевірку $e(P, cP) \stackrel{?}{=} e(aP, bP)$, але це не означає, що CDH-задача у G теж не є складною. Фактично, на даний момент не існує методів розв'язання задачі CDH у G з використанням білінійного відображення e. Групи, для яких задача DDH є простою, але задача CDH – складною, називаються лакунарними групами Діффі – Геллмана, також існує відповідна лакунарна задача Діффі-Гелмана (GDH – gapDiffie-Hellman).

6) DLIN-задача (DecisionLinear)

Вхідні дані: Циклічна група $G = \langle P \rangle$ і набір (P, aP, bP, acP, bdP, Q).

Завдання: Визначити, чи є $(c+d)P=Q$, або, чи є Q випадковим рівномірним елементом G, який також є незалежним від інших елементів.

Задачі, що описані у даній статті, мають фіксоване число елементів G, відповідно, нестатичні задачі мають змінне число елементів G. Фактичне число елементів далі буде позначатися параметрами h і q.

7) BDHE-задача (BilinearDiffie-HellmanExponent)

Вхідні дані: Набір $(P,aP,a^2P,\ldots,a^{h-1}P,a^{h+1}P,\ldots,a^{2h}P,Q)$, де, $a\in Z_p$, $Q\in G$ – випадкові елементи і $G=\langle P\rangle$.

Завдання: Обчислити $e(P,Q)^{a^h}$.

8) DBDHE-задача (DecisionalBilinearDiffie-HellmanExponent)

Вхідні дані: Набір $(P,aP,a^2P,\ldots,a^{h-1}P,a^{h+1}P,\ldots,a^{2h}P,Q,Z)$, де, $a\in Z_p$, $Q\in G$ – випадкові елементи і $Z\in G_T$.

Завдання: Визначити, чи є $Z=e(P,Q)^{a^h}$, або, чи є Z випадковим рівномірним елементом G_T, який також є незалежним від інших елементів.

9) BDHI-задача (BilinearDiffie-Hellmaninversion)

Вхідні дані: Набір $(P_1,\ldots,P_h)$, де $P_i=a^iP$ для деякого випадкового $a\in Z_p$.

Завдання: Обчислити $e(P,P)^{1/a}$.

10) DBDHI-задача (DecisionalBilinearDiffie-Hellmaninversion)

Вхідні дані: Набір $(P_1,\ldots,P_h,Z)$, де $P_i=a^iP$ для деякого випадкового $a\in Z_p$ і $Z\in G_T$.

Завдання: Визначити, чи є Z еквівалентним $e(P,P)^{1/a}$, або, чи є Z випадковим рівномірним елементом G_T, який є незалежним від a.

11) wDBDHI-задача(WeakDecisionalBilinearDiffie-HellmanInversion)

Вхідні дані: Набір $(Q,P_1,\ldots,P_h,Z)$, де $P_i=a^iP$ для деякого випадкового $a\in Z_p$, $Q\in G$ – випадковий елемент, $Z\in G_T$.

Завдання: Визначити, чи є Z еквівалентним $e(P,P)^{1/a}$, або, чи є Z випадковим рівномірним елементом G_T, який є незалежним від a.

12) wDBDHI* – задача(друга версія попередньої задачі)

Вхідні дані: Набір $(Q,P_1,\ldots,P_h,Z)$, де $P_i=a^iP$ для деякого випадкового $a\in Z_p$, $Z\in G_T$, $Q\in G$ – випадковий елемент.

Завдання: Визначити, чи є Z еквівалентним $e(P,Q)^{h+1}$, або, чи є Z випадковим рівномірним елементом G_T, який є незалежним від a.

Обчислювальні версії останніх двох задач є еквівалентними над лінійно-часовим зведенням і за допомогою алгоритму рішення даних задач можна вивести алгоритм для обчислювальної версії важко зведеної BDHI-задачі [14].

13) q-ABDHE-задача (TruncatedDecisionalAugmentedBilinearDiffie-HellmanExponent)

Вхідні дані: Набір $(Q,\alpha^{q+2}P',P,\alpha P,\alpha^2P,\ldots,\alpha^qP,\alpha^{q+2}P,\ldots,\alpha^{2q}P)$.

Завдання: Обчислити $e(P,Q)^{\alpha^{q+1}}$.

Існує декілька версій цієї задачі:

а) Скорочена версія

Вхідні дані: Набір $(Q,\alpha^{q+2}Q,P,\alpha P,\alpha^2P,\ldots,\alpha^qP)$.

Завдання: Обчислити $e(P,Q)^{\alpha^{q+1}}$.

б) Вирішальна (decision) версія, запропонована Джентрі[15]

Вхідні дані: Набір $(Q,\alpha^{q+2}Q,P,\alpha P,\alpha^2 P,\ldots,\alpha^q P,Z)$.

Завдання: Визначити,чи є $Z=e(P,Q)^{\alpha^{q+1}}$, або, чи є Z випадковим рівномірним елементом G_T.

Далі, дамо визначення декільком задачам для спарювання Типу 2. Для визначення структури крупи на еліптичній кривій будемо використовувати спарювання Вейля. Для даного $N=\#E(F_q)$, якщо N не має квадратних коефіцієнтів, тоді структура групи $E(F_q)$ є ізоморфною до Z/NZ. Якщо r^2 ділиться на N, тоді повинна існувати точка порядку r^2, або дві незалежні точки порядку r. Для спарювання Вейля можуть існувати тільки дві незалежні точки, такі, що r ділиться $(q-1)$.

14) ECDDH-задача (TheEllipticCurveDecision Diffie-Hellman)

Вхідні дані: Набір точок P_1,P_2,P_3,P_4 у $E(K)[r]$, такі, що $P_2=[\lambda]P_1$, для деякого λ.

Завдання: Визначити, чи є $P_4=[\lambda]P_3$.

В загальному випадку ця задача на білінійних відображеннях може бути вирішена наступним чином. Якщо $e(P_1,P_3)\neq 1$, тоді достатньо перевірити рівняння $e(P_1,P_4)=e(P_2,P_3)$.

Жу і Нгуєн [16] запропонували алгоритм який працює, в тому числі, і на суперсингулярні кривій, що розв'язує вирішальну версію задачі Диффі – Гелмана на спарюваннях за поліноміальний час, але, вважається, що обчислювальна (computational) задача Діффі – Гелмана має рівень стійкості, що дорівнює задачі дискретного логарифмування. Тому, вважається, що ECDDH дійсно менш важка задача за ECCDH.

15) BDH-задача (Bilinear Diffie-Hellman)

Вхідні дані: Точки P, $Q=\psi([c]P)$, $P_1=[a]P$, $P_2=[b]P$ такі, що $e(P,Q)\neq 1$.

Завдання: Обчислити $e([ab]P,Q)$.

Вважається, що BDH-задача є більш важкою за ECDH- задачу (EllipticCurveDiffie-Hellman), а також за задачу Діффі – Гелмана над кінцевими полями. Так, якщо маємо DH-оракул над E, вхідними даними для обчислення $[ab]P$ є (P,P_1,P_2), необхідно обчислити $e([ab]P,Q)$. Якщо маємо DH-оракул над кінцевим полем, обчислюємо $h_1=e(P,Q)$, $h_2=e(P_1,Q)=h_1^a$, $h_3=e(P_2,Q)=h_1^b$, і на вхід оракула подаємо (h_1,h_2,h_3), тоді в результаті отримаємо $h_1^{ab}=e([ab]P,Q)$.

16) DBDH-задача (DecisionBilinear Diffie-Hellman)

Вхідні дані: Точки P, Q такі, що $e(P,Q)\neq 1$, $P_1=[a]P$, $P_2=[b]P$ і g.

Завдання: Визначити, чи є $g\overset{?}{=}e([ab]P,Q)$.

Дана DBDH-задача не є складнішою за вирішальну версію задачі Діффі – Гелмана над кінцевим полем.

У роботі [5] було показано, що можна ефективно розв'язати задачу Діффі – Гелмана над двома циклічними групами G і H простого порядку r, таких, що $G\times G\to H$, де $H\subset F_{q^k}^*$ – прообраз підгрупи, якщо існує ефективно обчислювальний гомоморфізм з H до G.

Існує ще декілька обчислювальних задач[17], що засновані на спарюваннях, в даній статті були наведені лише основні задачі, що частіше за інші використовуються в криптографічних системах на ідентифікаційних даних.

Висновок

Наведено класифікацію та аналіз основних обчислювальних задач на білінійних відображеннях, а також визначення та основні математичні відомості, що необхідні для розумінні даних задач.

Стійкість BDH-задач над еліптичною кривою $E(F_q)$, а також над кінцевим полем F_{q^k}, залежить від стійкості задачі Діффі – Гелмана. Найчастіше, для криптографічних перетворень, що засновані на білінійних відображеннях, використовується підгрупа над $E(F_q)$ достатньо великого простого порядку r. Мінімальним рівнем безпеки для наведених задач є $r > 2^{160}$ і $q^k > 2^{1024}$. Взагалі ефективність криптосистеми залежить від особливостей побудування усієї схеми, але, чим менше значення приймає q, тим швидше виконуються арифметичні операції над кривою $E(F_q)$. Тому необхідно, щоб параметр q приймав найменше значення, тоді основним параметром безпеки буде виступати k, яке повинне приймати якомога більші значення. Найчастіше обирається точки на $E(F_q)$, для яких $q \approx 2^{170}$, і еліптичні криві зі вкладеним ступенем $k = 6$, тобто $q^k \approx 2^{1024}$.

Для криптографічних систем на білінійних відображеннях основними питаннями є: як знайти підходящу еліптичну криву і як швидко обчислити $e(P,Q)$, тому важливим завданням є аналіз обчислювальних задач на решітках, а також об'єднаної математики алгебраїчних решіток і білінійних відображень, що, на наш погляд, дозволить прискорити криптографічні перетворення та покращити показники стійкості криптографічних систем на ідентифікаторах.

Список літератури:1. *Sanjit Chatterjee, Palash Sarkar*. Identity-Based Encryption / Springer Science + Business Media, LLC.– 2011. – P.29-30, 44-48, 125-135. 2. *J.H. Silverman*. The Arithmetic of Elliptic Curves / GTM.– Vol.106.– Springer-Verlag.– 1986. 3. *D. Lorenzini*. An Invitation to Arithmetic Geometry / AMS, Graduate Studies in Mathematics.– Vol.106.– 1993. 4. *Ишмухаметов, Ш.Т.* Методы факторизации натуральных чисел : учеб. пособие / Казанский университет. – 2011. – С.100-114. 5. *Ian F. Blake, GadielSeroussi, Nigel P. Smart.* Advances in Elliptic Curve Cryptography / London Mathematical Society Lecture Note Series. 317. – Cambridge University Press.– 2005.– P.183-211. 6. *S. Lichtenbaum*. Duality theorems for curves over p-adic fields / Inventiones Math.– Vol. 7.– 1969.– P.120–136. 7. *G. Frey, H.-G. Ruck.* A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves / Math.Comp. – Vol. 62.– 1994.– P.865–874. 8. *G. Frey, M. Muller, H.-G. Ruck.* The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems // IEEE Trans. Inf. Theory. – Vol. 45.– 1999.– P.1717–1719. 9. *F. Hess.* A note on the Tate pairing of curves over finite fields / Arch. Math.– Vol. 82.– 2004.– P.28–32. 10. *R. Balasubramanian, N. Koblitz*. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm / J. Cryptology.– Vol. 11.– 1998.– P.141–145. 11. *T. Garefalakis*. The generalised Weil pairing and the discrete logarithm problem on elliptic curves / In S. Rajsbaum, edit. – Lecture Notes in Computer Science LATIN 2002 «Theoretical Informatics». – Vol.2286.– Springer-Verlag.– 2002.– P.118–130. 12. *Steven D. Galbraith, Kenneth G. Paterson, Nigel P. Smart*. Pairings for cryptographers / Discrete Applied Mathematics.– Vol. 156(16).– 2008.– P.3113–3121. 13. *Dan Boneh, Matthew K. Franklin*. Identity-based encryption from the Weil pairing / SIAM J. Comput.– Vol. 32(3).– 2003.– P.586–615. 14. *Dan Boneh, Xavier Boyen, Eu-Jin Goh*. Hierarchical identity based encryption with constant size ciphertext / In Ronald Cramer, edit. – Lecture Notes in Computer Science «Annual International Conference on the Theory and Applications of Cryptographic Techniques». – Vol.3494.– Springer.– 2005.– P.440–456. 15. *Craig Gentry*. Practical identity-based encryption without random oracles / In Serge Vaudenay, edit. – Lecture Notes in Computer Science «Annual International Conference on the Theory and Applications of Cryptographic Techniques». – Vol. 4004.– Springer.– 2006.– P.445–464. 16. *A. Joux, K. Nguyen*. Separating Decision Diffie–Hellman from Diffie–Hellman in cryptographic groups / J. Cryptology.– 2003.– P.239–248. 17. *A. Joux.* The Weil and Tate pairings as building blocks for public key cryptosystems / In C. Fieker, D.R. Kohel, edit. – ANTS-5 «Algorithmic Number Theory».– Vol.2369.– Springer.– 2002.– P.20–32.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.09.2012