Які критерії оцінки можуть бути застосовані для оцінки криптографічної стійкості ЕЦП та порядок їх застосування?

Критерії та показники оцінки властивостей і якості криптографічних перетворень типу ЦП, що ґрунтуються на еліптичних кривих

На світовому рівні ЦП вже набув дуже широкого розповсюдження в системах електронних документів та електронного документообігу, електронній пошті, платіжних системах, електронному врядуванні, електронній звітності, електронній торгівлі тощо. Зрозуміло, що при недостатньому рівні захищеності успішна реалізація загроз і атак може призвести до надзвичайно критичних ситуацій і подій, коли електронні документи та електронні дані будуть викривлені, підмінені, знищені тощо, особливо в процесі архівного зберігання значний час. Тому як дослідження, так і оцінка ЦП на різних етапах життєвого циклу ЦП – від розроблення до модифікації та виведення з дії, а також як наслідок застосування на різних етапах життєвого циклу даних є важливими задачами. Першими постають задачі визначення та вибору критеріїв і показників оцінки ЦП.

Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь [329], тобто, по суті, будемо розуміти мірило оцінки. Наші попередні дослідження дозволили зробити висновок, що порівняння криптографічних кривих можна здійснити з використанням двох сукупностей критеріїв: безумовних та умовних [110]. З урахуванням попереднього досвіду [12], оцінку криптоперетворень типу ЦП рекомендується виконувати у 2 етапи. На першому етапі перевіряється їх відповідність безумовним критеріям, а на другому отримуються відповідні оцінки з використанням умовних критеріїв. Саме за рахунок використання умовних критеріїв і з’являється можливість порівняти різні криптографічні перетворення типу ЦП за інтегральним критерієм.

Надалі під відповідністю безумовним критеріям будемо розуміти той факт, що експертні оцінки за безумовними критеріями є позитивними, тобто вони задовольняються (справджуються).

6.7.1. Безумовні критерії оцінки криптографічних перетворень типу ЦП, що ґрунтуються на еліптичних кривих

До безумовних критеріїв будемо відносити ті критерії, виконання яких для криптографічних перетворень типу ЦП в групі точок ЕК є обов'язковим, тобто безумовними.

Аналіз стану застосування [4–19, 31–67, 105–111], досвід розробки й оцінки властивостей криптоперетворень типу ЦП в групі точок ЕК [42–61, 63, 52], досягнуті результати при практичному розв'язанні задач криптоаналізу та реалізації різних атак [11–14, 105–111] дозволили в якості основних вибрати безумовні, що наведені в п.6.3.3.

Безумовні критерії оцінки ЕЦП

До безумовних критеріїв відноситимемо ті критерії, виконання яких для ЕЦП, заснованих на криптографічних перетвореннях у групі точок ЕК, є обов'язковим.

Проведений аналіз стану застосування еліптичних кривих [15, 16, 34], розробки й оцінки властивостей криптографічних перетворень у групі точок ЕК [30–37], досягнуті результати в практичному вирішенні завдань криптоаналізу та реалізації різних атак [99] дозволяють як основні вибрати такі безумовні критерії оцінки [див. 3.1]:

1) надійність математичної бази, у сенсі практичної відсутності можливостей здійснювати атаки типа «універсальне розкриття» за рахунок недосконалості математичного апарату групи точок еліптичних кривих або слабкостей, які можуть бути закладені за рахунок специфічних властивостей загальних параметрів і ключів (критерій $W_{\delta 1}$);

2) практична захищеність криптографічних перетворень у групі точок ЕК від силових і аналітичних атак, яка досягається за рахунок вибору розмірів загальних параметрів і ключів (критерій $W_{\delta 2}$);

3) реальна захищеність від усіх відомих і потенційно можливих криптоаналітичних атак, де під захищеністю розуміють той факт, що всі відомі криптоаналітичні атаки типу «повне розкриття» мають експоненціальну

складність I_{ec}, а критерієм незахищеності – субекспоненціальний I_{ce} (критерій $W_{\delta 3}$);

4) статистична безпечність криптографічного перетворення в групі точок ЕК, під якою розуміють статистичну незалежність результату криптографічного перетворення, тобто виходу від входу (критерій $W_{\delta 4}$);

5) теоретична захищеність криптографічного перетворення, у якому використовуються загальні параметри з відповідними властивостями й довжинами, при яких не існують аналітичні атаки, складність яких менше, ніж складність атаки типу «повне розкриття» (критерій $W_{\delta 5}$);

6) відсутність слабких особистих ключів, при яких складність криптоаналітичних атак типу «повне розкриття» й «універсальне розкриття»

менше, ніж складність атаки «повне розкриття» для інших особистих ключів (критерій $W_{\delta 6}$);

7) прийняті складності прямого $I_{\text{пр}}$ та зворотного $I_{\text{зв}}$ криптографічних перетворень, коли вони мають поліноміальний характер і не перевищують допустимих величин $I_{\text{пр}}'$ і $I_{\text{зв}}'$ (критерій $W_{\delta 7}$).

Як результат інтегральним безумовним критерієм відбору є логічне значення так/ні (1/0), що обчислюється на основі значень часткових безумовних критеріїв

$$(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}) \in (1,0). \qquad (3.132)$$

У цілому функцію відповідності ЕЦП для вказаних умов можна записати у вигляді

$$f_{фв}(\ ) = \mathrm{W}_{\delta 1} \wedge \mathrm{W}_{\delta 2} \wedge \mathrm{W}_{\delta 3} \wedge \mathrm{W}_{\delta 4} \wedge \mathrm{W}_{\delta 5} \wedge \mathrm{W}_{\delta 6} \wedge \mathrm{W}_{\delta 7},$$

де символ «^» позначає операцію кон'юнкції булевих змінних. Зрозуміло, що функції відповідності ЕЦП відповідають вимогам, якщо

$$f_{фв}(\ ) \in (0,1).$$

Таким чином, інтегральний критерій дозволяє лише встановити факт відповідності чи не відповідності такого ЕЦП безумовним вимогам.

3.8.3. Умовні критерії оцінки ЕЦП

Якісне та кількісне порівняння криптографічних перетворень у групі точок ЕК можна здійснити, використовуючи безпосередньо метод аналізу ієрархій.

Виберемо як умовні критерії оцінки ЕЦП такі часткові критерії (табл. 3.10).

Таблиця 3.10

Умовні часткові критерії оцінки ЕЦП

	Критерії	Позначення
	Можливість та умови вільного поширення й застосування міжнародного або національного стандарту криптографічних перетворень у групі точок еліптичної кривої в Україні з урахуванням нормативно-правових актів України на експорт, імпорт і обмеження на його застосування	W_{y1}
	Рівень довіри до міжнародного або національного стандарту криптографічного перетворення в групі точок еліптичної кривої, що визначається результатами досліджень і степенем поширення застосування та визнання в різних державах і міжнародно визнаних системах	W_{y2}
	Перспективність застосування міжнародного або національного стандарту в Україні з урахуванням визнання та застосування перспективних інформаційно-телекомунікаційних систем та інформаційних технологій тощо	W_{y3}
	Тимчасова та просторова складності апаратної, апаратно-програмної та програмної реалізацій засобів ЕЦП та управління й сертифікації ключів тощо	W_{y4}
	Можливість і умови застосування стандартів з різними значеннями загально-системних параметрів і ключів, методами виготовлення та обслуговування сертифікатів відкритих ключів тощо	W_{y5}
	Степінь гнучкості ЕЦП з точки зору використання в різних додатках, за різних вимог та обмежень, у різних умовах, степінь уніфікації та стандартизації тощо	W_{y6}
	Рівень захищеності при реалізації різних видів загроз, за різних умов здійснення криптоаналітичних атак і відхилення властивостей загальних параметрів від визначених тощо	W_{y7}