**Рівномірна вибірка Гауса та її застосування для схеми підпису Falcon**

**Дерев’янко Я.А., Горбенко І.Д. …**

**Анотація:**

Вибірка Гауса для цілих чисел є ключовим інструментом у криптографії на основі решітки, але виконання вибірки у типовий, ефективний спосіб з доведеною захищеністю виявилось напрочуд складним завданням. Представлений у даній роботі відбірник є надзвичайно простим, і саме ця простота дозволила зробити його простим у впровадженні, доказово захищеним, портативним, ефективним та доказово стійким проти часових атак. Нещодавно його було впроваджено у схему ЕП Falcon.

**Ключові слова:**

Криптографія, заснована на алгебраїчних решітках, Вибірка Гауса, рівномірна вибірка.

**1. Вступ**

Використання відбірника Гауса не уникнути для певних ситуацій, наприклад,відбір проб: його проведення з іншими розподілами є поки не вирішеним питанням, за винятком одиничних випадків (вибірка з широкого класу розподілів), які спричиняють зростання складності до на виході, що, в свою чергу, призводить до зменшення рівня безпеки. Тому, важливо прийти до відбірників Гауса над цілими числами, які були б не тільки ефективними, але й доказово захищеними, стійкими до часових атак та загалом простими в реалізації.

**2 Відбірник**

Основне припущенням в даному випадку - вважати, що всі стандартні відхилення обмежені і що центр знаходиться в [0, 1]. А отже, позначаючи верхню та нижню межі на стандартному відхиленні як , ми представляємо алгоритм, який відбирає розподіл для будь-якого та .

Алгоритм вибірки називається , він описаний в Алгоритмі 1.

Далі також вводиться алгоритм, позначений як . Він виконує вибірку відкидання (Алгоритм 2) Таким чином, за допомогою цієї конструкції можна вивести наступне твердження.

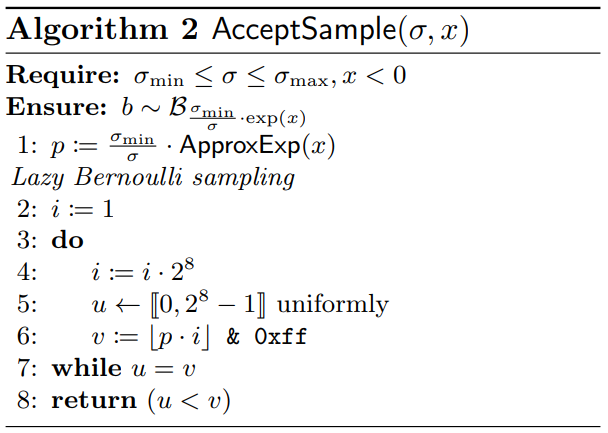
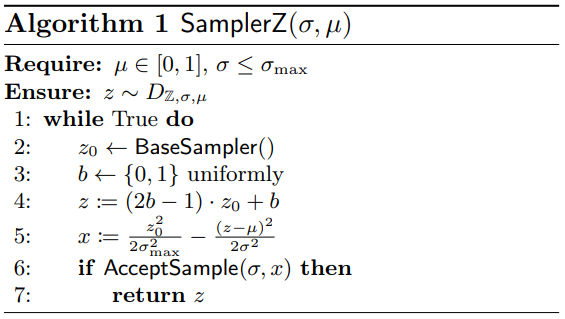


Рис. 2.1 – Алгоритми та

**Твердження 6 (Правильність).** Припустимо, що всі рівномірні розподіли є досконалими і що та exp, тоді будова (в алгоритмах 1 та 2) така, що .

Для практичних реалізацій неможливо отримати ідеальні розподіли. Можливо лише отримання та exp.

**4 Доказ захищеності**

**Теорема 7 (Безпека SamplerZ).** Припустимо, що має λ-бітову захищеність від задачі пошуку. Тепер розглянемо копію останньої криптосистеми, позначеної , де єдиною відмінністю є застосування . Якщо дотримано дві наступні умови:

тоді, буде мати (λ-2)-бітову захищеність від задачі пошуку.

Для отримання конкретних числових значень ми припускаємо, що для вихідної схеми заявлено 256 бітів захищеності, таким чином для реальної реалізації необхідно 254 біта захисту. Тоді для реалізації Falcon числові значення будуть наступними:

**5 Аналіз опору часовим атакам**

У цьому розділі показується, що Алгоритм 1 є стійким проти часових атак. Спочатку доводиться технічна лема, яка показує, що кількість ітерацій у циклі while Алгоритму 1 (майже) незалежна від

**Лема 8.** Нехай і нехай , є стандартними відхиленнями, такими що . Нехай . Кількість ітерацій циклу while у відповідає геометричному закону параметра

Далі показується, що Алгоритм 1 є абсолютно рівномірним(ізохронним) відносно та статистично ізохронним (для відхилення Рені) щодо .

**Теорема 9.** Нехай , нехай , є стандартними відхиленнями, такими що , і нехай константа в (0, 1). Припустимо, що елементарні операції {+, -, ×, /} над цілими числами та числами з плаваючою крапкою є рівномірними(ізохронними). Час роботи Алгоритму 1 слідує за розподілом так, що:

для деякого розподілу , незалежного від його вхідних даних та вихідних - .

**Наслідок 10**. Розглянемо зловмисника , який робить запитів підпису щодо алгоритму підпису, який використовує . Припустимо, що зламує захист, вирішуючи задачу пошуку з імовірністю успіху для деякого . Вивчення часу роботи кожного виклику не збільшує ймовірність успіху більш ніж на постійний коефіцієнт.

**Вплив коефіцієнта масштабування.** Коефіцієнт масштабування ≤ є вирішальним для того, щоб зробити пробовідбірник рівномірним(ізохронним), оскільки він декорелює час роботи від . Однак це також впливає на , оскільки можна легко показати, що пропорційний коефіцієнту масштабування. Тому бажано зробити його якомога меншим. Максимальне значення коефіцієнта масштабування фактично залежить від криптографічної схеми, в якій використовується відбірник. Для випадку схеми підпису Falcon і вплив коефіцієнта масштабування обмежений.

**Висновки**

Отже, як вже було сказано, Вибірка Гауса для цілих чисел є ключовим інструментом у криптографії на основі решітки, тому важливо прийти до відбірників Гауса над цілими числами, які були б не тільки ефективними, але й доказово захищеними, стійкими до часових атак та загалом простими в реалізації.. У даній роботі було розглянуто одна з реалізації відбірника, який є простим в реалізації, майже не відрізняється від стандартного відбірника Гауса, забезпечує рівномірність(ізохронність) вибірки, а також є несприятливим до часових атак. При цьому, реалізація з даним відбірником є лише на 22% повільнішою, що все ще дозволяє алгоритму ЕП Falcon в такій реалізації бути конкурентоспроможним.