УДК 003.26

ОБЗОР И АНАЛИЗ ПРОВЕРЯЕМЫХ ФУНКЦИЙ ЗАДЕРЖКИ, ОСНОВАННЫХ НА ИЗОГЕНИЯХ, ДЛЯ ПРИМЕНЕНИЯ В ПРОТОКОЛАХ РАСПРЕДЕЛЁННОЙ ГЕНЕРАЦИИ СЛУЧАЙНОСТИ

Кожевникова А. С.[1], Давыдов В. В.[1,2]
Научный руководитель – канд. техн. наук, доцент Давыдов В. В.[1,2]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
[2]Университет ИТМО
kaspost7@gmail.com, vadimdavydov@outlook.com

Работа выполнена в рамках государственного задания (проект FSER-2025-0003).

Введение

На сегодняшний день ряд криптографических протоколов, таких как электронная лотерея, электронное голосование, выбор лидера в протоколе Proof-of-Stake и многие другие, используют публично проверяемую случайность. Концепция криптографического «маяка случайности» была предложена М. Рабином в 1983 году как публичный источник, периодически публикующий случайно выбранные, непредсказуемые и, в то же время, проверяемые значения [1]. Существуют источники случайности, основанные на физических процессах (например, бросок кубика или подбрасывание монетки), позволяющие обеспечить уверенность в непредвзятости полученных результатов, однако, на физические процессы можно повлиять, а также их достаточно трудно проверить. В качестве альтернативы применяются централизованные криптографические генераторы случайности (Random Beacons), реализуемые доверенной стороной и публикующие псевдослучайные значения. Однако их существенными недостатками являются абсолютное доверие к источнику, а также отсутствие у пользователей возможности проверить корректность генерации. Для устранения указанных недостатков были предложены распределённые протоколы генерации случайности (Distributed Random Beacons, DRB), в которых итоговое случайное значение совместно формируется несколькими участниками [2].

Основная часть

К одному из способов распределённой генерации случайности можно отнести подход, основанный на использовании проверяемой функции задержки (Verifiable Delay Function, VDF) [2] на объединённых входных секретных данных каждого участника. Концепция VDF впервые была описана Боне и соавторами в 2018 году [3]. Большинство известных практических конструкций VDF основаны на классических криптографических предположениях теории чисел, при этом, в связи с активным развитием квантовых компьютеров, актуальной является разработка постквантовых VDF. В протоколах распределённой генерации случайности при достаточно большой задержке ни один участник не может определить выходное значение до завершения вычисления VDF и, следовательно, не может выбрать своё значение так, чтобы предвзято повлиять на результат. Данный подход устраняет проблему последнего раскрывающего.

В данной работе формализованы дополнительные свойства (с основными свойствами можно ознакомиться в [3]) для проверяемых функций задержки в контексте их использования в протоколах распределённой генерации случайности. Были введены следующие свойства:

1) *Отсутствие доверенной стороны*: параметры VDF должны генерироваться без участия доверенной стороны и без дополнительной информации, знание которой позволяет существенно ускорить вычисление функции.

2) *Справедливость*: время вычисления функции честным участником должно быть близко к предположительно минимальному времени, необходимому атакующему.

3) *Устойчивость к ускорителям*: никакая программная или аппаратная реализация не обеспечивает существенного ускорения вычислений.

4) *Непредсказуемость выхода относительно входных значений*: при сговоре участники не смогут на основе своих вкладов предопределить или существенно повлиять на выход VDF.

С учётом указанных требований были рассмотрены современные VDF, основанные на задачах поиска изогений между суперсингулярными эллиптическими кривыми. В работе приводится краткий сравнительный обзор рассматриваемых VDF с точки зрения сформулированных требований. Схема, приведённая в [4], обладает предполагаемой устойчивостью к ускорителям, так как анализ современных алгоритмов вычисления изогений показывает, что, хотя и существуют алгоритмические оптимизации вычисления изогений [5], существенного ускорения на данный момент не известно. При этом схема требует наличия доверенной стороны для генерации параметров, что является её существенным недостатком. Схема, предложенная в [6], относится к классу weak VDF и не удовлетворяет свойству справедливости, так как допускает параллельные вычисления со стороны честного участника. В работе [7] предложена функция задержки без доверенной стороны при генерации параметров, но авторы отмечают возможность распараллеливания этапа генерации доказательства.

Выводы

В работе исследовано применение проверяемых функций задержки в протоколах распределённой генерации случайности. Сформулированы дополнительные требования к VDF, необходимые для их корректного применения в DRB-протоколах. В рамках предложенных требований проанализированы современные постквантовые VDF, основанные на задачах поиска изогений между суперсингулярными эллиптическими кривыми, и оценена возможность их практического использования в DRB. Проведённый анализ показал, что схема [7] представляется наиболее перспективной для применения.

Литература

1. Rabin M. O. Transaction protection by beacons //Journal of Computer and System Sciences. – 1983. – Т. 27. – №. 2. – С. 256-267.

2. Raikwar M., Gligoroski D. Sok: Decentralized randomness beacon protocols // Australasian Conference on Information Security and Privacy. – Cham : Springer International Publishing, 2022. – С. 420-446.

3. Boneh D. et al. Verifiable delay functions // Annual international cryptology conference. – Cham : Springer International Publishing, 2018. – С. 757-788.

4. De Feo L. et al. Verifiable delay functions from supersingular isogenies and pairings //International Conference on the Theory and Application of Cryptology and Information Security. – Cham : Springer International Publishing, 2019. – С. 248-277.

5. Bernstein D. J. et al. Faster computation of isogenies of large prime degree //Open Book Series. – 2020. – Т. 4. – №. 1. – С. 39-55.

6. Decru T., Maino L., Sanso A. Towards a quantum-resistant weak verifiable delay function //International Conference on Cryptology and Information Security in Latin America. – Cham : Springer Nature Switzerland, 2023. – С. 149-168.

7. Chavez-Saab J., Rodríguez-Henríquez F., Tibouchi M. Verifiable isogeny walks: Towards an isogeny-based postquantum VDF // International Conference on Selected Areas in Cryptography. – Cham : Springer International Publishing, 2021. – С. 441-460.