Исследование возможностей фреймворка winterfell для создания эффективного по вычислительным ресурсам доказательства выполнения SHA-256

Воронов М. С., Николайчук А. К.

Программист, Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: michail.vms@gmail.com, Antyartem1@yandex.ru

Научный руководитель *— Воронов М. С.*

Цель работы исследовать фреймворк Winterfell для построения STARK-доказательств, доказать свойства его функциональности (в частности, формульные оценки размера доказательства в зависимости от параметров протокола), реализовать на его основе доказательство выполнения SHA-256 и проверить теоретические выводы на этом примере.

В работе изучена архитектура Winterfell: представление вычисления в виде таблицы вычислений, разбиение на основной и вспомогательный сегменты в Randomized AIR (алгебраическое промежуточное представление), интерполяция столбцов в полиномы, переходные и граничные ограничения, построение композиционного полинома, низкостепенное расширение полиномов и протокол FRI (Fast Reed–Solomon IOP of Proximity). Выведены формулы для размера компонент доказательства (Merkle proofs, FRI proof, OOD frame и др.) и асимптотики полного размера.

Теорема 1. *Полный размер доказательства вычисления выражается как сумма компонент:*

$$|\pi| = |\mathcal{C}| + |\mathcal{M}| + |\mathcal{O}| + |\mathcal{Q}_T| + |\mathcal{Q}_C| + |\mathcal{F}| + |\nu_{pow}|. \tag{1}$$

Здесь $\mathcal{C}$ контекст (метаданные протокола), $\mathcal{M}$ коммитменты (корни дерьев Меркла полиномов таблицы, композиции и слоёв FRI), $\mathcal{O}$ внедоменные значения, $\mathcal{Q}_T$ и $\mathcal{Q}_C$ ветки деревьев Меркла для проверок композиционного и табличных полиномов, $\mathcal{F}$ доказательство FRI, ν_{pow} nonce для proof-of-work. Основной вклад в размер дают $\mathcal{F}$ (FRI proof) и $\mathcal{Q}_T$ (trace queries); заметный вклад $\mathcal{Q}_C$ (constraint queries). При фиксированных параметрах протокола размер доказательства растёт логарифмически по длине таблицы вычислений: $|\pi| = O(Q \cdot \log(n))$.

Реализована схема доказательства корректности вычисления SHA-256 в Winterfell. Для этого введена виртуальная машина, в которой битовые операции выражаются в терминах арифметики конечного поля по простому модулю и задаются переходными ограничениями AIR; измерены размеры доказательств при различных параметрах. Для реализации SHA-256 при длине строки $n = 2^{20}$ измеренный размер доказательства составил около 119 KB.

Ключевые параметры протокола: Q число запросов проверяющего, ρ коэффициент расширения домена, η коэффициент свёртки FRI, R максимальная степень остатка FRI, λ_{grind} параметр proof-of-work. Уровень безопасности оценивается эвристикой $\lambda_{\text{conj}} \approx \min\{\log_2(\rho) \cdot Q + \lambda_{\text{grind}},\ \text{field\_bits},\ \text{collision\_resistance}\} - 1$: каждый дополнительный запрос даёт примерно $\log_2(\rho)$ бит безопасности, grinding добавляется аддитивно и почти не увеличивает размер доказательства. Теоретические оценки согласуются с экспериментами по декомпозиции доказательства и масштабированию при изменении параметров.

Литература

1. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint 2018/046.
2. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. IACR ePrint 2017/134.
3. Ben-Sasson E., Goldberg L., Kopparty S., Saraf S. DEEP-FRI: Sampling Outside the Box Improves Soundness. IACR ePrint 2019/336.
4. Haböck U., Kohlweiss M., Riabzev M. Basefold: Efficient Field-Agnostic Polynomial Commitment Schemes from Foldable Codes. IACR ePrint 2022/1216.
5. Winterfell Documentation: `https://github.com/facebook/winterfell`