Optimizing Multi-Scalar Multiplication (for Off-chain Transactions Optimization)

Doktorantas: Saulius Grigaitis

Prelimenarus disertacijos pavadinimas: Blokų grandinių spartinimas naudojant negrandinines transakcijas

Numatomas studijų laikas: 2018 – 2026 (akademinės atostogos 2021-2026)

Vadovas: dr. Igoris Belovas

Tyrimo objektas:

Blokų grandinių protokolai orientuoti į spartesnį transakcijų vykdymą.

Tyrimo tikslas:

Tobulinti ir modifikuoti esamus blokų grandinių protokolus, siekiant didinti transakcijų pralaidumą.

Planuojami rezultatai

- Atlikti blokų grandinių protokolų analitinę apžvalgą
- Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su transakcijų pralaidumo didinimu blokų grandinių protokoluose
- Pasiūlyti patobulinimus egzistuojantiems blokų grandinių protokolams siekiant padidinti transakcijų pralaidumą
- Pasiūlytų patobulinimų pagrindu realizuoti prototipą
- Eksperimentiškai ištirti patobulintas protokolų versijas ir jų savybes palyginti su pradiniais protokolais

Plano vykdymo suvestinė

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse		Nacionalinėse		Su citav. rodikliu			Be citav. rodiklio		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė	Planas	Įvykdyta	Būklė
I (2018/2019)			1	1[3]				0	1[1]	Publikuota
II (2019/2020)	1					1[6]	Publikuota			
III (2020/2021)	1	2[4,5]			1	1[7]	Publikuota	0	1[2,]	Publikuota
IV (2025/2026)					1					
Iš Viso	2	2	1	1	2	2	0	0	0	0

Mokslinių tyrymų etapai

	Darbo pavadinimas	Atlikimo terminai	Pastabos
1.	Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje): 1.1. Atlikti blokų grandinių tinklų analitinę apžvalgą. 1.2 Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su blokų grandinių spartinimu naudojant negrandinines (angl. *off-chain*) transakcijas.	2018 m. spalio mėn. – 2019 m. spalio mėn.	Atspausdinta apžvalginė publikacija šios dalies pagrindu.
2.	Mokslinio tyrimo vykdymas:		Fokusuojamasi į simuliatorių tyrimus, kurie leistų įvertinti protokolų patobulinimus našumo atžvilgiu. Nustatyta, kad tinkamų simuliatorių naujos kartos PoS protokolams nėra.
	2.1. Tyrimo metodikos sudarymas: 2.1.1. Tyrimo metodikos išsikeltam uždaviniui spręsti parinkimas; 2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.	2019 m. lapkričio mėn. - 2020 m. sausio mėn.	
	2.2. Teorinis tyrimas: 2.2.1. Sričių, kuriose tikslinga spartinti blokų grandines negrandininėmis transakcijomis identifikavimas; 2.2.2. Blokų grandinių spartinimo naudojant negrandinines transakcijas tyrimas; 2.2.3. Blokų grandinių spartinimo naudojant negrandinines transakcijas modelio sukūrimas ar testavimas.	2020 m. vasario mėn. – 2020 m. spalio mėn.	

Mokslinių tyrimų etapai

	2.3. Empirinis tyrimas: 2.3.1. Blokų grandinių spartinimo naudojant negrandininęs transakcijas pritaikymas 2.2.1 uždavinyje identifikuotoms praktinėms sritims. 2.3.2. El. komercijai pritaikyto blokų grandinių sprendimo, naudojančio negrandininęs transakcijas, tyrimas ir tobulinimas.	2020 m. lapkričio mėn. – 2021 m. gegužės mėn.	Atspausdinta publikacija šios dalies pagrindu. Tolesni tyrimai fokusuojasi į optimizavimą kriptografijos algoritmų (KZG10 ir kt.), kurie įgalina didinti transakcijų našumą duomenų *shardingo* pagalba
	2.4. Gautų rezultatų analizė, apibendrinimas, išvadų parengimas: 2.4.1. Gautų rezultatų analizė; 2.4.2. Rezultatų apibendrinimas, esminių rezultatų išskyrimas; 2.4.3. Išvadų parengimas.	2021 m. birželio mėn. – 2021 m. spalio mėn.	
3.	Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų ir kt.) parengimas: 3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas; 3.2. Analitinės disertacijos dalies parengimas; 3.3. Teorinės disertacijos dalies parengimas; 3.4. Eksperimentinės disertacijos dalies parengimas; 3.5. Bendrųjų išvadų formulavimas.	2021 m. lapkričio mėn. – 2022 m. gegužės mėn.	Planas nusikėlė 4 metams dėl akademinių atostogų į 2025-2026. Pasiūlyta nauja šeima algoritmų konkrečiai mokslinei problemai - multi-skaliarinei daugybai, kuri naudojama tiek ir KZG10

Mokslinių tyrimų etapai

			schemoje, tiek ir labai plačiai kitur (pvz. parašų verifikavime). Šiuo metu yra parengta 60% disertacijos.
4.	Daktaro disertacijos parengimas ir svarstymas padalinyje	2022 m. birželio mėn. (planas nusikėlė į 2026)	
5.	Daktaro disertacijos gynimas	2022 m. rugsėjo mėn. (planas nusikėlė į 2026)	

Bendruosius gebėjimus stiprinančios veiklos

Dalyko pavadinimas	Data	Programos trukmė val.	Programos apimtis kreditais ECTS	Trumpas turinio aprašas
R įvadas	2019-10-30	8	1,25	Šie mokymai supažindina su statistinės bei grafinės analizės programa R. Pristatomi R naudojimo principai ir galimybės, pateikiami atskiri atvejai ir pavyzdžiai. Mokymų pradžioje sudaroma galimybė paruošti savo kompiuterius darbui su R.
LATEX	2019-06-15	8	1,25	Šiame dalyke studentai supažindinti su teksto redagavimo programa LaTeX. 1. Instaliavimas ir paruošimas darbui; 2. Preambulė; 3. Teksto redagavimas; 4. Formulės ir specialūs simboliai; 5. Paveikslėliai ir lentelės; 6. Nuorodos ir bibliografija; 7. Aplinkos; 8. Pateiktys.
Pedagoginė veikla			1	Nuo 2019 mokslo metų rudens semestrais dėstau savo parengtą kursą „Blokų grandinių technologijos“ Vadovavau ir šiuo metu vadovauju bakalauro ir magistro darbams.

Kito pusmečio planas (2026)

- Pabaigti rengti disertaciją;
- Pagal vėliausius tyrimų rezultatus pabaigti rengti publikaciją;

KZG10 Polynomial Commitments: Trusted Setup

A common (not desired) requirement for Zero Knowledge schemes;

KZG10 needs prover and verifier to know $[s^i]_1$ and $[s^i]_2$ for $i = 0, \ldots, n-1$;

Secret s must be not be known to anybody and it's computation too hard to recover it from the given trusted setup;

Secure Multiparty Computation (MPC) is a secure way to generate Trusted Setup if at least single party is honest;

KZG10 Polynomial Commitments: Commitment

KZG10 polynomial commitment is a polynomial evaluated at secret s that nobody knowns:

$$[p(s)]_1 = [\sum_{i=0}^{n} p_i s^i]_1 = \sum_{i=0}^{n} p_i [s^i]_1 \tag{2}$$

The probability that any another polynomial has the same commitment at unknown secret s equals to the degree of polynomial (not higher than trusted setup size) divided by elliptic curve group order. Let's say for the trusted setup of size 2^{26} and elliptic curve order 2^{256} the probability is $2^{26}/2^{256} = 2^{-230}$.

Multi-Scalar Multiplication: Pippenger Example

$$S_{n,r} = \sum_{i=1}^{n} a_i P_i$$

When *r* is small we group elements by scalar:

$S_{12,4} = 2P_1 + 3P_2 + 3P_3 + 2P_4 + 1P_5 + 1P_6 + 3P_7 + 2P_8 + 2P_9 + 3P_{10} + 1P_{11} + 3P_{12}$ – 37 group operations

$S_{12,4} = 1 \cdot (P_5 + P_6 + P_{11}) + 2 \cdot (P_1 + P_4 + P_8 + P_9) + 3 \cdot (P_2 + P_3 + P_7 + P_{10} + P_{12}) = 1S_1 + 2S_2 + 3S_3$.

$1S_1 + 2S_2 + 3S_3 = S_3 + (S_3 + S_2) + (S_3 + S_2 + S_1)$ – this needs only 4 group operations + 9 group operations for each subsum.

Multi-Scalar Multiplication: Pippenger (large scalars)

When *r* is large we break down each scalar:

$$a_i = \sum_{j=0}^{h-1} a_{ij} q^j,\ 0 \le a_{ij} < q,\ h = \lceil \log_q r \rceil$$

$$S_j := a_{1,j} P_1 + a_{2,j} P_2 + \cdots + a_{n,j} P_n\ (0 \le j \le h-1)$$

$$S_{n,r} = \sum_{i=1}^{n} a_i P_i = \sum_{i=1}^{n} \left(\sum_{j=0}^{h-1} a_{ij} q^j \right) P_i = \sum_{j=0}^{h-1} q^j \left(\sum_{i=1}^{n} a_{ij} P_i \right)$$

$$= \sum_{j=0}^{h-1} q^j S_j,$$

Multi-Scalar Multiplication: BGMW

Points are fixed for KZG10 (and many other applications of MSM) so we can precompute $q^j P_i$

$$a_i = \sum_{j=0}^{h-1} a_{ij} q^j,\ 0 \le a_{ij} < q,\ h = \lceil \log_q r \rceil$$

$$S_j := a_{1,j} P_1 + a_{2,j} P_2 + \cdots + a_{n,j} P_n\ (0 \le j \le h-1)$$

$$S_{n,r} = \sum_{i=1}^{n} a_i P_i = \sum_{i=1}^{n} \left(\sum_{j=0}^{h-1} a_{ij} q^j \right) P_i = \sum_{i=1}^{n} \sum_{j=0}^{h-1} a_{ij} \cdot q^j P_i$$

This requires at most *nh* + *q* – *3* group operations.

Construction I

Precompute pairs P_i+P_j (in addition to BGMW) for indices

$$i, j \in \bigcup_{d=0}^{\frac{nk}{tw}-1} \{dt, dt+1, \ldots, (d+1)t-1\}, \quad i \neq j,$$

where w denotes the window size in bits, n is the MSM size, k is the scalar size in bits, and t is the chunk size

Construction II

- Variant I + Booth indexes
- Precompute pairs $P_i + P_j$ and $P_i - P_j$ (in addition to BGMW) for indices

$$i, j \in \bigcup_{d=0}^{\frac{nk}{tw}-1} \{dt, dt+1, \ldots, (d+1)t-1\}, \quad i \neq j,$$

where w denotes the window size in bits, n is the MSM size, k is the scalar size in bits, and t is the chunk size

Construction III

- Construction II + triples.
- Precompute pairs $P_i + P_j + P_m$, $-P_i + P_j + P_m$, $P_i - P_j + P_m$,$P_i + P_j - P_m$,in addition to Construction II) for indices

$$i, j, m \in \bigcup_{d=0}^{\frac{nk}{tw}-1} \{dt, dt+1, \ldots, (d+1)t-1\}, \quad i \neq j,\ i \neq m,\ j \neq m.$$

where w denotes the window size in bits, n is the MSM size, k is the scalar size in bits, and t is the chunk size

Experiments: Rust-kzg library

- Implemented in Rust (high performance and safety);
- Contains test suites and benchmarks;
- Used by some real world projects and scientists;
- Over 40 students involved;
- Opensource (Apache 2.0 license).

Construction I

Table 3.1: MSM size 2^1 Fixed-Window vs. Construction I

Fixed Window			Construction I				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
7	12.29 KB	0.0912	7	1	10.66 KB	0.0925	-1.46%
8	24.58 KB	0.0861	4	1	18.43 KB	0.0472	45.14%
9	49.15 KB	0.0848	4	3	42.62 KB	0.0430	49.36%
10	98.30 KB	0.0816	3	5	89.76 KB	0.0368	54.90%
11	196.61 KB	0.0802	3	10	166.56 KB	0.0337	57.98%
12	393.22 KB	0.0792	3	19	300.96 KB	0.0306	61.32%
13	786.43 KB	0.0755	3	50	723.36 KB	0.0281	62.74%
14	1.57 MB	0.0761	3	50	723.36 KB	0.0281	63.05%
15	3.15 MB	0.0760	3	50	723.36 KB	0.0281	62.99%
16	6.29 MB	0.0709	3	50	723.36 KB	0.0281	60.36%

Construction I

Table 3.6: MSM size 2^6 Fixed-Window vs. Construction I

Fixed Window			Construction I				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
12	12.58 MB	0.5244	5	1	10.18 MB	0.5787	-10.36%
13	25.17 MB	0.4866	6	3	25.10 MB	0.4904	-0.77%
14	50.33 MB	0.4566	6	6	49.87 MB	0.4689	-2.69%
15	100.66 MB	0.4360	6	12	94.70 MB	0.4562	-4.64%
16	201.33 MB	0.3920	6	25	186.71 MB	0.4462	-13.82%
17	402.65 MB	0.3938	6	43	363.66 MB	0.4432	-12.54%
18	805.31 MB	0.3698	6	43	363.66 MB	0.4432	-19.84%
19	1.61 GB	0.3514	6	43	363.66 MB	0.4432	-26.12%
20	3.22 GB	0.3318	6	43	363.66 MB	0.4432	-33.58%
21	6.44 GB	0.3320	6	43	363.66 MB	0.4432	-33.51%

Construction II

Table 3.7: MSM size 2^1 Fixed-Window vs. Construction II

Fixed Window			Construction II				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
7	12.29 KB	0.0924	8	1	12.29 KB	0.0911	1.47%
8	24.58 KB	0.0862	4	1	24.58 KB	0.0435	49.56%
9	49.15 KB	0.0847	4	2	49.15 KB	0.0402	52.53%
10	98.30 KB	0.0814	4	4	98.30 KB	0.0360	55.73%
11	196.61 KB	0.0805	4	8	196.61 KB	0.0318	60.48%
12	393.22 KB	0.0787	4	16	393.22 KB	0.0292	62.95%
13	786.43 KB	0.0757	4	32	786.43 KB	0.0279	63.13%
14	1.57 MB	0.0762	4	64	1.57 MB	0.0273	64.20%
15	3.15 MB	0.0760	4	64	1.57 MB	0.0273	64.10%
16	6.29 MB	0.0706	4	64	1.57 MB	0.0273	61.38%

Construction II

Table 3.11: MSM size 2^5 Fixed-Window vs. Construction II

Fixed Window			Construction II				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
11	3.15 MB	0.3524	8	1	3.15 MB	0.3761	-6.72%
12	6.29 MB	0.3262	5	1	5.11 MB	0.3151	3.39%
13	12.58 MB	0.3090	6	3	12.48 MB	0.2735	11.48%
14	25.17 MB	0.2880	6	6	24.87 MB	0.2648	8.06%
15	50.33 MB	0.2808	6	10	40.21 MB	0.2630	6.33%
16	100.66 MB	0.2542	6	23	91.32 MB	0.2588	-1.79%
17	201.33 MB	0.2525	6	43	181.76 MB	0.2577	-2.06%
18	402.65 MB	0.2408	6	43	181.76 MB	0.2577	-7.01%
19	805.31 MB	0.2273	6	43	181.76 MB	0.2577	-13.40%
20	1.61 GB	0.2156	6	43	181.76 MB	0.2577	-19.55%

Construction III

Table 3.13: MSM size 2^1 Fixed-Window vs. Construction III

Fixed Window			Construction III				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
9	49.15 KB	0.0848	3	1	33.02 KB	0.0475	43.95%
10	98.30 KB	0.0816	4	2	98.30 KB	0.0399	51.18%
11	196.61 KB	0.0802	2	2	196.61 KB	0.0375	53.23%
12	393.22 KB	0.0792	3	3	314.88 KB	0.0346	56.34%
13	786.43 KB	0.0755	3	4	583.68 KB	0.0320	57.64%
14	1.57 MB	0.0761	3	6	1.38 MB	0.0287	62.25%
15	3.15 MB	0.0760	4	10	2.88 MB	0.0269	64.58%
16	6.29 MB	0.0709	4	14	5.57 MB	0.0254	64.21%
17	12.58 MB	0.0747	4	17	8.29 MB	0.0246	67.10%
18	25.17 MB	0.0728	4	22	14.49 MB	0.0241	66.95%
19	50.33 MB	0.0708	4	41	40.68 MB	0.0236	66.73%
20	100.66 MB	0.0683	4	46	51.90 MB	0.0236	65.46%
21	201.33 MB	0.0709	4	64	132.66 MB	0.0231	67.43%
22	402.65 MB	0.0677	4	64	132.66 MB	0.0231	65.90%
23	805.31 MB	0.0703	4	64	132.66 MB	0.0231	67.16%
23	805.31 MB	0.0703	4	64	132.66 MB	0.0231	67.16%

Construction III

Table 3.16: MSM size 2^4 Fixed-Window vs. Construction III

Fixed Window			Construction III				Comparision
w	Precomp.	Time	w	chunks	Precomp.	Time	
14	12.58 MB	0.1918	5	1	12.46 MB	0.1834	4.40%
15	25.17 MB	0.1851	4	1	15.34 MB	0.1722	7.00%
16	50.33 MB	0.1677	6	2	42.30 MB	0.1700	-1.37%
17	100.66 MB	0.1696	5	2	52.08 MB	0.1562	7.93%
18	201.33 MB	0.1624	5	3	116.91 MB	0.1472	9.36%
19	402.65 MB	0.1536	6	6	390.49 MB	0.1412	8.09%
20	805.31 MB	0.1451	6	8	670.17 MB	0.1384	4.63%
21	1.61 GB	0.1513	6	12	1.44 GB	0.1356	10.36%
22	3.22 GB	0.1392	6	15	2.33 GB	0.1345	3.38%
23	6.44 GB	0.1413	6	21	4.83 GB	0.1334	5.56%
24	12.88 GB	0.1325	6	21	4.83 GB	0.1334	-0.73%

Further Research

- Complete implementation and benchmarking of a few more variants (further reduce buckets by one bit, overlapping chunks).