Cipher Crypto Performance Primitives

Особенности построения кроссплатформенной библиотеки криптографических примитивов "Шифр+" v2

ООО «Сайфер БИС»
Влад Ковтун
Андрей Охрименко

Актуальность

- Новые алгоритмы и математические теории (кривые Эдвардса, новые)
- Увеличение числа ядер CPU
- Развитие направлений:
  - Встраиваемые системы (IoT, Phones, Tablets, …)
  - Серверы (ARM64, MIPS64)
- Развитие различных аппаратных платформ:
  - x86, x86-64 (сервера и встраиваемые)
  - ARM, ARM64 (сервера и встраиваемые)
  - MIPS, MIPS64 (сервера и встраиваемые)
  - Power

Суть задачи

Программные платформ:

- Windows
- Linux
- MacOS
- Android
- iOS
- и другие

Компиляторы:

- Microsoft C++
- GCC
- CLang
- Intel C++

Улучшенная поддержка многопоточности на уровне ОС, языков программирования и компиляторов

Суть задачи

Поддержка различных алгоритмов:

- Международных
  - RSA, ECDSA, ECGDSA, EdCDSA
  - DES, TDES, AES
  - SHA-1, SHA-2, SHA-3
- Национальных (новые)
  - ДСТУ 7624:2014
  - ДСТУ 7564:2014
- Национальных (старые)
  - ГОСТ 28147-89
  - ГОСТ 34.311-95

Суть задачи

Поддержка различных расширений CPU:

- x86/x86-64
  - AES-NI
  - SSE/AVX/AVX2
  - CLMUL
  - ADX
  - Условные переходы без ветвлений
- ARM
  - Условные переходы без ветвлений
  - NEON
  - CLMUL

Предложенные решения

Языковые решения:

- Унифицированный и предсказуемый интерфейс
- Ссылки и минимизация указателей
- Шаблоны
- Разворачивание циклов
- Универсальные конструкции
- Безопасный код
- Умное управление памятью

Предложенные решения

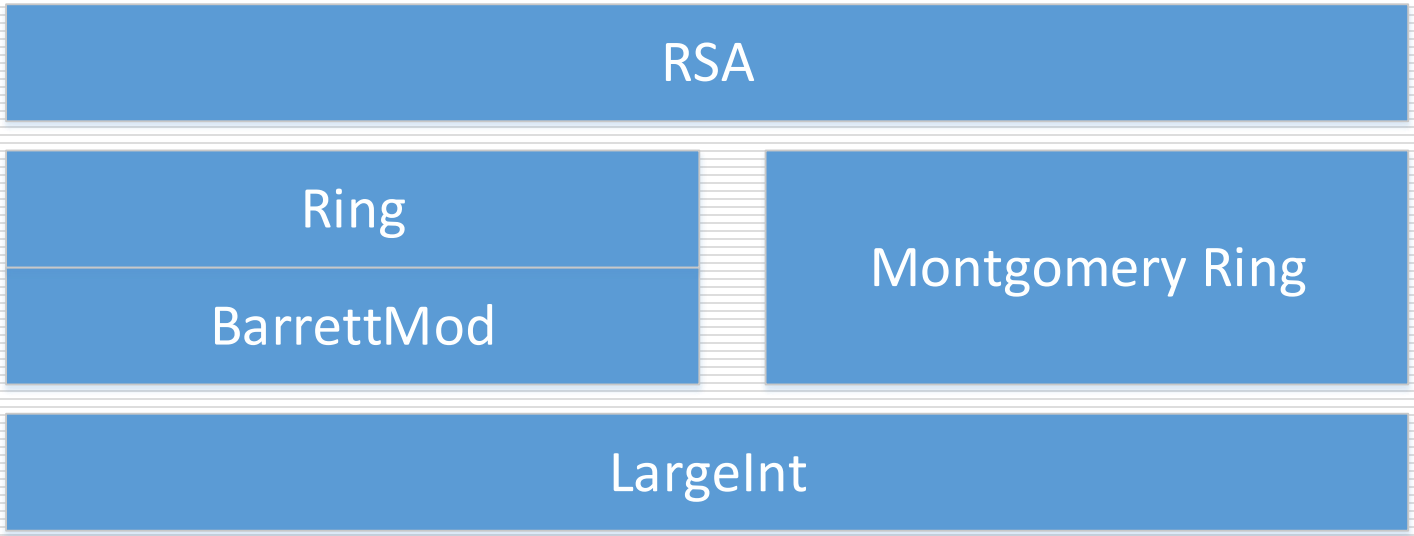
Языковые решения:

- Технология OpenMP
- Поддержка расширений CPU в RunTime
- Распараллеливание на уровне CPU

Архитектура. Предложенные решения

ДСТУ 4145:2002	
ECDSA, ECGDSA, ECKAS-DH, ECKAS-MQV	
EC over GF(2^m)	EC over GF(p_m)
Field GF(2^m)	Field GF(p_m)
Special Mod	BarrettMod
Polynomial	BigInt

Архитектура. Предложенные решения



Предложенные: Integers

Алгоритмические оптимизации:

- Выделены классы BigInt (до 512 бит) и LargeInt (более 512 бит)
- BigInt поддерживает принудительное развертывание циклов
- LargeInt поддерживает работу с большими блоками памяти, с циклами
- Умножение с отложенным переносом (возможность распараллеливать)

Предложенные: Integers

Алгоритмические оптимизации:

- Учет размера машинного слова
- Предвычисления для возведения в степень
- Учет изменения двоичной длины чисел при инвертировании

Предложенные: ModReduceInt

Алгоритмические оптимизации:

- Специфические алгоритмы для псевдо-Мерсена чисел
- Алгоритм Барретта, в общем виде, на основе операций умножения с отложенным переносом, с возможностью распараллеливания
- Арифметика Монтгомери
- Учет размера машинного слова

Предложенные: ModReducePoly

Алгоритмические оптимизации:

- Специфические алгоритмы для триномиалов и пентаномиалов
- Алгоритм с предвычислениями для произвольного модуля
- Учет размера машинного слова

Замеры производительности

БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ

Условия эксперимента #1

- CPU: Intel Core i7-6700HQ (4 cores, 8 threads, 2.6 GHz, 6 MB Smart Cache)
- RAM: 16 GB
- OS: Windows 10 x86-64
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #1 (x86)

	ECB	CTR	CFB	OFB	CBC	WRAP	MAC	WRAP-P	XTR	GCM	CCM
ГОСТ 28147-89	48.69	48.38	45.34	43.65	43.38	17.28	8.65	-	-	-	-
AES NI-128	2216.78	515.01	698.43	845.02	764.61	-	17.69	-	-	-	-
AES NI-192	1936.18	476.50	640.00	749.79	689.54	-	14.98	-	-	-	-
AES NI-256	1560.80	435.77	570.73	645.39	592.86	-	12.98	-	-	-	-
DES	57.88	55.02	56.82	61.77	58.31	-	6.24	-	-	-	-
TDES	21.61	21.79	21.91	22.56	22.26	-	2.24	-	-	-	-
ДСТУ 7624:2014 [128-128]	93.59	85.42	87.34	93.58	89.82	0.39	92.75	0.39	46.11	36.09	44.14
ДСТУ 7624:2014 [128-256]	66.22	64.05	64.31	66.51	65.39	0.35	66.19	0.36	38.87	31.139	32.91
ДСТУ 7624:2014 [256-256]	78.93	74.07	74.42	76.23	74.77	0.68	78.14	0.68	45.43	31.88	37.93
ДСТУ 7624:2014 [256-512]	61.77	58.97	60.57	60.80	62.51	0.65	61.80	0.65	39.78	28.99	29.54
ДСТУ 7624:2014 [512-512]	60.11	58.53	60.34	60.44	62.26	1.04	63.32	1.04	38.02	29.03	30.46

Производительность #1 (x64)

	ECB	CTR	CFB	OFB	CBC	WRAP	MAC	WRAP-P	XTR	GCM	CCM
ГОСТ 28147-89	44.65	40.07	40.59	41.34	40.72	16.31	8.17	-	-	-	-
AES NI-128	2282.95	542.41	805.42	955.98	805.042	-	17.93	-	-	-	-
AES NI-192	2124.97	509.86	692.34	768.31	695.34	-	17.63	-	-	-	-
AES NI-256	1738.53	469.59	645.39	768.63	695.34	-	14.92	-	-	-	-
DES	64.57	62.76	59.42	62.54	57.88	-	6.96	-	-	-	-
TDES	22.48	22.70	21.55	22.56	21.78	-	2.22	-	-	-	-
ДСТУ 7624:2014 [128-128]	128.22	126.22	124.24	135.24	130.24	0.71	131.24	0.71	70.71	57.45	62.51
ДСТУ 7624:2014 [128-256]	97.93	92.82	93.82	100.68	97.93	0.691	95.53	0.691	60.97	53.89	47.41
ДСТУ 7624:2014 [256-256]	128.12	122.22	128.64	130.24	128.22	1.32	133.58	1.32	61.89	46.48	65.12
ДСТУ 7624:2014 [256-512]	111.64	97.93	104.19	104.19	104.19	1.23	103.83	1.23	53.89	43.46	50.45
ДСТУ 7624:2014 [512-512]	120.22	112.63	120.22	120.24	120.22	1.95	120.92	1.95	62.51	41.67	57.89

Замеры производительности

ХЕШ-ФУНКЦИИ И КОДЫ АУТЕНТИФИКАЦИИ

Условия эксперимента #2

- CPU: Intel Core i7-6700HQ (4 cores, 8 threads, 2.6 GHz, 6 MB Smart Cache)
- RAM: 16 GB
- OS: Windows 10 x86-64
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #2 (x86)

	Хеш	HMAC	KMAC
ГОСТ 34.311-95	34.41	34.11	-
ДСТУ 7564:2014-256	67.70	66.63	67.14
ДСТУ 7564:2014-384	44.40	44.40	45.00
ДСТУ 7564:2014-512	44.23	43.87	44.10
SHA-1	325.52	332.44	-
SHA-224	140.76	140.76	-
SHA-256	138.27	139.51	-
SHA-384	88.27	88.27	-
SHA-512	88.27	87.78	-
SHA-512/224	87.29	87.29	-
SHA-512/256	89.29	87.29	-

Производительность #2 (x64)

	ECB	HMAC	KMAC
ГОСТ 34.311-95	34.87	34.49	-
ДСТУ 7564:2014-256	101.79	101.39	101.07
ДСТУ 7564:2014-384	75.62	76.10	76.40
ДСТУ 7564:2014-512	75.59	75.62	75.73
SHA-1	422.30	400.64	-
SHA-224	148.81	151.70	-
SHA-256	148.81	153.186	-
SHA-384	244.14	260.42	-
SHA-512	256.15	260.42	-
SHA-512/224	252.01	260.42	-
SHA-512/256	260.42	260.42	-

Замеры производительности

ЦИФРОВАЯ ПОДПИСЬ

Условия эксперимента #3

- CPU: Intel Core i7-6700HQ (4 cores, 8 threads, 2.6 GHz, 6 MB Smart Cache)
- RAM: 16 GB
- OS: Windows 10 x86-64

Условия эксперимента #3

- Размер данных: соответствует размеру ключа
- Единицы измерений: мс
- При постановке ЭЦП выполняется формирование предподписи, где выполняется:
  - Формирование E-параметра предподписи на основе **генератора ПСП встроенного в язык программирования**.
  - Формирование F-параметра на основе скалярного умножения.

Условия эксперимента #3

- Используется скалярное умножение в проективных координатах Лопеса-Дахаба и Монтгомери ladder.
- Рассматриваются кривые:
  - Согласно ДСТУ 4145:2002 и совместного приказа Министерства юстиции, Госспецсвязи 20.08.2012 №1236/5/453.

Производительность #3 (x86)

ДСТУ 4145:2002	B-163	B-167	B-173	B-179	B-191	B-233	B-257	B-307	B-367	B-431
Генерация открытого ключа	0.336	0.354	0.395	0.423	0.445	0.724	0.93	1.45	2.568	3.540
Формирование предподписи	0.349	0.369	0.401	0.426	0.46	0.754	0.935	1.388	2.570	3.550
Постановка	0.366	0.372	0.403	0.429	0.461	0.765	0.937	1.435	2.576	3.559
Проверка*	0.367	0.378	0.428	0.456	0.482	0.792	0.999	1.489	2.882	3.851

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Производительность #3 (x64)

ДСТУ 4145:2002	B-163	B-167	B-173	B-179	B-191	B-233	B-257	B-307	B-367	B-431
Генерация открытого ключа	0.21	0.224	0.246	0.240	0.260	0.571	0.748	0.952	1.414	2.081
Формирование предподписи	0.217	0.226	0.248	0.244	0.264	0.576	0.762	0.956	1.428	2.151
Постановка	0.228	0.228	0.252	0.259	0.267	0.58	0.764	0.995	1.44	2.159
Проверка*	0.237	0.248	0.259	0.258	0.285	0.536	0.785	1.041	1.527	2.292

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Условия эксперимента #4

- Используется скалярное умножение в проективных координатах Лопеса-Дахаба и Монтгомери ladder.
- Рассматриваются кривые:
  - NIST FIPS 186-3

Производительность #4 (x86)

ECDSA	P-192	P-224	P-256	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация открытого ключа	0.470	0.709	1.351	3.093	5.352	0.354	0.751	1.095	2.947	7.975
Постановка	0.479	0.726	1.382	3.159	5.451	0.356	0.758	1.102	2.96	8.093
Проверка*	0.532	0.756	1.489	3.434	5.789	0.402	0.781	1.148	3.108	8.54

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Производительность #4 (x64)

ECDSA	P-192	P-224	P-256	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация открытого ключа	0.148	0.386	0.558	1.053	1.301	0.215	0.56	0.895	1.94	3.948
Постановка	0.156	0.398	0.564	1.055	1.281	0.218	0.567	0.901	1.967	4.007
Проверка*	0.168	0.424	0.613	1.16	1.409	0.235	0.605	0.967	2.084	4.23

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Условия эксперимента #5

- Используется скалярное умножение в проективных координатах Лопеса-Дахаба и Монтгомери ladder.
- Рассматриваются кривые:
  - NIST FIPS 186-3
  - RFC 5639 (Brainpool). Кривые над полями GF(p), где p-простое число общего вида.

Производительность #5 (x86)

ECGDSA	P-160	P-192	P-224	P-256	P-320	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация открытого ключа	1.487	2.461	3.672	5.193	9.413	17.10	34.66	2.09	4.78	9.837	20.0	66.21
Постановка	0.741	1.228	1.837	2.572	4.765	8.63	18.43	0.394	0.778	1.167	3.151	8.42
Проверка*	0.817	1.33	2.017	2.874	5.094	8.64	19.57	0.419	0.84	1.278	3.406	8.992

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Производительность #5 (x64)

ECGDSA	P-160	P-192	P-224	P-256	P-320	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация открытого ключа	0.542	0.67	1.083	1.17	2.00	2.98	6.33	1.195	2.696	5.63	10.69	30.68
Постановка	0.279	0.314	0.561	0.6	0.954	1.56	3.24	0.209	0.579	0.877	1.846	3.871
Проверка*	0.295	0.371	0.608	0.669	1.066	1.75	3.457	0.242	0.613	0.944	2.065	4.153

* - при проверке ЭЦП, каждое скалярное умножение выполняется в отдельном потоке.

Условия эксперимента #6

- При генерации ключей использовался генератор ПСП из ДСТУ 4145:2002 на основе ГОСТ 28147-89
- Используется возведение в степень на основе предвычислений w-NAF с использованием арифметики Монтгомери.
- Для генерации простых чисел p и q используется алгоритм Рабина-Миллера, где число испытаний равно 50.
- Для наглядности, приводятся значения для публичной экспоненты e=65537.

Производительность #6 (x86)

RSA	512	1024	1536	2048	3072	4096	7168	8192	15360	16384
Генерация личного ключа*										
Постановка	1.356	9.879	32.053	74.012	169.96	576.57	3001.7	4378	-	34195
Проверка	0.329	1.295	3.574	5.156	8.657	20.58	62.98	77.56	-	313.26

* - очень медленный генератор ПСП

Производительность #6 (x64)

RSA	512	1024	1536	2048	3072	4096	7168	8192	15360	16384
Генерация личного ключа*	13.0	70.0	383.0	345.0	3391.0	2803.0	42947	129166	699716	-
Постановка	0.239	1.536	5.005	12.237	27.28	95.33	486.67	711.88	-	5573.6
Проверка	0.086	0.379	0.77	1.291	2.107	4.84	14.807	19.09	-	77.69

* - очень медленный генератор ПСП

Замеры производительности

IPHONE 4S

Условия эксперимента

- Device: iPhone 4S
- CPU: Apple A5 (ARM Cortex-A9)
- RAM: 256 MB
- Алгоритмы:
  - БСШ:
    - ДСТУ 7624:2014 256/256
    - ГОСТ 28147-89
    - AES-256
  - ЭЦП:
    - ДСТУ 4145:2002+ДСТУ 7564:2014
    - ECDSA+SHA-256

Цифровая подпись. ДСТУ4145. Условия эксперимента #7

- Хеш-функция: ДСТУ 7564:2014-256
- Размер данных: 10 байт
- Единицы измерений: мс
- При постановке ЭЦП ДСТУ 414:2002 выполняется формирование предподписи, где выполняется:
  - Формирование E-параметра предподписи на основе генератора ПСП описанного в ДСТУ 4145:2002 на основе ГОСТ 2847-89.
  - Формирование F-параметра на основе скалярного умножения.

Цифровая подпись. ДСТУ4145. Условия эксперимента #7

- Используется скалярное умножение в проективных координатах Лопеса-Дахаба и Монтгомери ladder.
- Рассматриваются кривые:
  - Согласно ДСТУ 4145:2002 и совместного приказа Министерства юстиции, Госспецсвязи 20.08.2012 №1236/5/453.

Цифровая подпись. ECDSA. Условия эксперимента #8

- Хеш-функция: SHA-256
- Размер данных: 10 байт
- Единицы измерений: мс
- При постановке ЭЦП ECDSA выполняется формирование псвдослучайного параметра на основе генератора ПСП описанного в ДСТУ 4145:2002 на основе ГОСТ 2847-89.

Цифровая подпись. ECDSA. Условия эксперимента #8

- Используется скалярное умножение в проективных координатах Лопеса-Дахаба и Монтгомери ladder.
- Рассматриваются кривые:
  - NIST FIPS 186-3 (над простым полем)

Цифровая подпись. Производительность #7 и #8

	ДСТУ 4145:2002 (#6)			ECDSA (#7)		
	B-163	B-257	B-431	P-192	P-384	P-521
Генерация открытого ключа	7	8	9	7	8	10
Постановка	10	18	37	10	39	68
Проверка	13	26	68	15	68	118

Симметричное шифрование. Условия эксперимента #9

- Блочные шифры:
  - ГОСТ 28147-89
  - ДСТУ 7624:2014 256/256
  - AES-256
- Режим: CTR
- Размер данных: 1 блок
- Единицы измерений: мс

Симметричное шифрование. Производительность #9

Алгоритм	CTR	
	Зашифровать	Расшифровать
ГОСТ 28147-89	35	35
AES-256	36	37
ДСТУ 7624:2014 [256-256]	37	37

Дальнейшие направления

- Поддержка распараллеливания для ряда режимов блочных шифров
- Поддержка технологии CUDA для платформы x86/x86-64 для ассиметричных алгоритмов
- Расширение перечня поддерживаемых инструкций для различных архитектур CPU
- Поддержка кривых Эдвардса и Монтгомери из списка Бернштейна: http://safecurves.cr.yp.to/equation.html

Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Влад Ковтун
Андрей Охрименко

email:vk@cipher.kiev.ua, ao@cipher.kiev.ua
www: http://cipher.kiev.ua