Cipher Crypto Performance Primitives on ARM

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 платформы:

- Raspbian OS
- Asus Tinker OS

Компиляторы:

- GCC
- CLang

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:

- ARMv6 (Broadcom BCM2835) 32-bit
  - Условные переходы без ветвлений
- ARM v7 (Rockchip RK3288) 32-bit
  - Условные переходы без ветвлений
- ARM v8 (Rockchip RK3288) 64-bit
  - NEON
  - CLMUL

Предложенные решения

Языковые решения:

- Унифицированный и предсказуемый интерфейс
- Ссылки и минимизация указателей
- Шаблоны
- Разворачивание циклов
- Универсальные конструкции

Предложенные решения

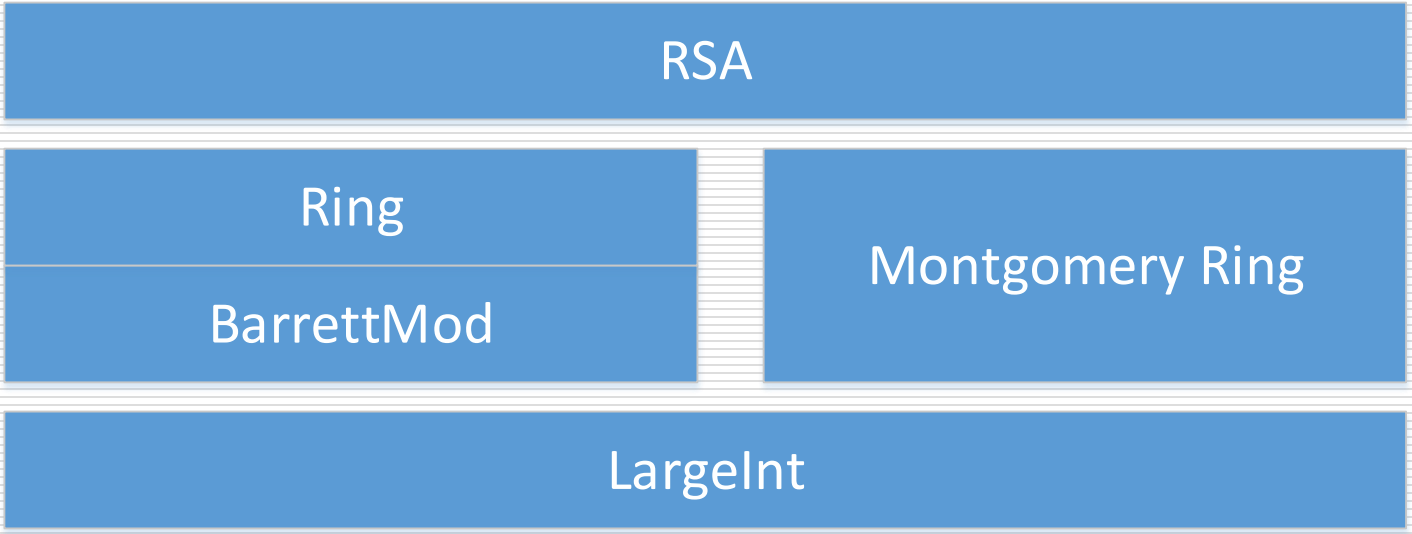
Языковые решения:

- Безопасный код
- Умное управление памятью
- 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

Предложенные: Integers

Алгоритмические оптимизации:

- Умножение с отложенным переносом (возможность распараллеливать)
- 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 (ARM v6)

- CPU: Broadcom BCM2835, ARM v6-l (ARM1176JZ-F), 1 cores, 800 MHz
- RAM: 512 MB
- HDD: 16 GB SD card
- OS: Raspbian OS
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #1 (ARM v6)

	ECB	CTR	CFB	OFB	CBC	KW	MAC	KW-P	XTS	GCM	CCM
ГОСТ 28147-89	7.81	7.32	7.12	7.48	7.59	-	-	-	-	-	-
AES NI-128	6.76	5.99	5.72	6.07	6.52	-	6.64	-	-	-	-
AES NI-192	5.90	5.05	4.98	5.59	5.65	-	5.79	-	-	-	-
AES NI-256	4.93	4.44	4.03	4.78	4.72	-	4.84	-	-	-	-
DES	4.95	4.05	3.55	5.08	4.62	-	5.81	-	-	-	-
TDES	2.12	1.84	1.66	2.03	1.93	-	0.21	-	-	-	-
ДСТУ 7624:2014 [128-128]	3.74	3.26	3.54	3.68	3.64	0.049	3.82	0.049	1.19	2.07	1.73
ДСТУ 7624:2014 [128-256]	2.67	2.39	2.55	2.63	2.61	0.053	3.11	0.053	1.24	1.89	1.44
ДСТУ 7624:2014 [256-256]	3.00	2.71	2.76	2.91	2.91	0.095	3.03	0.095	1.33	1.62	1.41
ДСТУ 7624:2014 [256-512]	2.34	2.15	2.18	2.28	2.29	0.091	2.36	0.091	1.16	1.41	1.11
ДСТУ 7624:2014 [512-512]	2.10	1.82	1.87	1.99	2.03	0.015	2.14	0.015	1.07	1.09	0.96

Условия эксперимента #1 (ARM v7)

- CPU: Rockchip RK3288, ARM v7-a (Cortex-17), 4 cores, 1.8 GHz
- RAM: 2 GB LPDDR3
- HDD: 16 GB SD card
- OS: Asus Tinker OS
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #1 (ARM v7)

	ECB	CTR	CFB	OFB	CBC	KW	MAC	KW-P	XTS	GCM	CCM
ГОСТ 28147-89	29.46	28.95	29.29	29.33	29.06	-	-	-	-	-	-
AES NI-128	73.03	68.16	72.24	72.91	72.28	-	71.61	-	-	-	-
AES NI-192	59.30	56.17	58.90	60.71	60.80	-	61.78	-	-	-	-
AES NI-256	52.35	49.41	52.63	53.34	52.99	-	53.63	-	-	-	-
DES	31.89	30.49	31.91	36.24	31.40	-	36.20	-	-	-	-
TDES	12.82	12.60	12.89	13.54	12.89	-	1.35	-	-	-	-
ДСТУ 7624:2014 [128-128]	30.53	29.77	30.95	30.86	30.71	0.13	31.23	0.13	8.97	16.72	15.11
ДСТУ 7624:2014 [128-256]	22.25	21.79	22.40	22.37	22.12	0.13	0.13	0.13	8.14	12.90	10.90
ДСТУ 7624:2014 [256-256]	22.04	21.42	21.88	21.97	21.81	0.26	21.77	0.26	14.70	10.59	10.56
ДСТУ 7624:2014 [256-512]	17.00	16.53	16.64	16.87	16.90	0.24	17.00	0.24	12.56	9.29	8.41
ДСТУ 7624:2014 [512-512]	17.99	17.56	17.79	17.85	17.88	0.37	18.06	0.37	13.05	8.49	8.80

Замеры производительности

ХЕШ-ФУНКЦИИ И КОДЫ АУТЕНТИФИКАЦИИ

Условия эксперимента #2 (ARM v6)

- CPU: Broadcom BCM2835, ARM v6-l (ARM1176JZ-F), 1 cores, 800 MHz
- RAM: 512 MB
- HDD: 16 GB SD card
- OS: Raspbian OS
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #2 (ARM v6)

	Hash	HMAC	KMAC
ГОСТ 34.311-95	4.24	4.24	-
ДСТУ 7564:2014-256	1.63	1.63	1.63
ДСТУ 7564:2014-384	0.86	0.86	0.86
ДСТУ 7564:2014-512	0.86	0.86	0.86
SHA-160	24.74	24.85	-
SHA-224	17.48	17.52	-
SHA-256	17.57	17.56	-
SHA-384	2.05	2.05	-
SHA-512	2.05	2.05	-
SHA-513	2.06	2.06	-
SHA-514	2.05	2.05	-

Условия эксперимента #2 (ARM v7)

- CPU: Rockchip RK3288, ARM v7-a (Cortex-17), 4 cores, 1.8 GHz
- RAM: 2 GB LPDDR3
- HDD: 16 GB SD card
- OS: Asus Tinker OS
- Число повторов 1 млн.
- Размер данных: 16 кБ
- Единицы измерений: МБ/с

Производительность #2 (ARM v7)

	Hash	HMAC	KMAC
ГОСТ 34.311-95	19.82	19.81	-
ДСТУ 7564:2014-256	13.57	13.70	13.71
ДСТУ 7564:2014-384	8.79	8.72	8.79
ДСТУ 7564:2014-512	8.79	8.79	8.79
SHA-160	146.69	146.71	-
SHA-224	81.78	81.80	-
SHA-256	81.80	82.01	-
SHA-384	25.35	25.35	-
SHA-512	25.35	25.35	-
SHA-513	25.35	25.35	-
SHA-514	25.35	25.35	-

Замеры производительности

ЦИФРОВАЯ ПОДПИСЬ

Условия эксперимента #3 (ARM v6)

- CPU: Broadcom BCM2835, ARM v6-l (ARM1176JZ-F), 1 cores, 800 MHz
- RAM: 512 MB
- HDD: 16 GB SD card
- OS: Raspbian OS

Условия эксперимента #3 (ARM v7)

- CPU: Rockchip RK3288, ARM v7-a (Cortex-17), 4 cores, 1.8 GHz
- RAM: 2 GB LPDDR3
- HDD: 16 GB SD card
- OS: Asus Tinker OS

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 (ARM v6)

ДСТУ 4145:2002	B-163	B-167	B-173	B-179	B-191	B-233	B-257	B-307	B-367	B-431
Генерация личного ключа	0.110	0.090	0.094	0.095	0.104	0.150	0.183	0.230	0.321	0.424
Генерация открытого ключа	4.003	3.993	4.322	4.730	4.971	9.632	12.411	18.125	27.180	41.649
Формирование предподписи	3.888	3.960	4.287	4.541	4.931	9.565	12.352	18.237	27.097	41.568
Постановка	3.929	3.996	4.333	4.583	4.979	9.652	12.393	18.293	27.188	41.703
Проверка*	8.088	8.176	8.866	9.349	10.131	19.527	25.302	37.144	54.846	83.708

Производительность #3 (ARM v7)

ДСТУ 4145:2002	B-163	B-167	B-173	B-179	B-191	B-233	B-257	B-307	B-367	B-431
Генерация личного ключа	0.02	0.026	0.026	0.027	0.028	0.038	0.045	0.056	0.073	0.095
Генерация открытого ключа	0.801	0.833	0.892	0.960	1.018	1.926	2.462	3.439	5.424	8.139
Формирование предподписи	0.812	0.829	0.899	0.959	1.014	1.916	2.456	3.474	5.425	8.121
Постановка	0.815	0.830	0.900	0.965	1.017	1.921	2.458	3.479	5.437	8.127
Проверка*	1.678	1.707	1.855	1.979	2.073	3.9246	5.005	7.047	11.048	16.354

Условия эксперимента #4

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

Производительность #4 (ARM v6)

ECDSA	P-192	P-224	P-256	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация личного ключа	0.102	0.129	0.167	0.336	0.611	0.087	0.150	0.197	0.379	0.707
Генерация открытого ключа	5.648	8.642	17.734	42.661	69.121	3.875	9.518	14.532	35.698	83.110
Постановка	5.689	9.004	17.601	42.786	71.015	3.995	9.720	14.753	36.118	84.151
Проверка	11.350	18.176	35.614	85.497	142.564	8.210	19.729	29.794	72.569	169.488

Производительность #4 (ARM v7)

ECDSA	P-192	P-224	P-256	P-384	P-512	B-163	B-233	B-283	B-409	B-571
Генерация личного ключа	0.027	0.034	0.042	0.078	0.138	0.023	0.038	0.049	0.086	0.159
Генерация открытого ключа	1.253	2.080	4.069	9.444	17.012	0.812	1.893	2.938	6.863	15.991
Постановка	1.312	2.099	4.009	9.892	17.885	0.834	1.926	2.980	6.968	16.209
Проверка	2.725	4.305	8.303	19.889	35.890	1.716	3.931	6.021	14.151	32.682

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 (ARM v6)

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 личного ключа	0.074	0.101	0.128	0.165	0.239	0.335	0.560	0.085	0.148	0.194	0.379	0.707
Генерация открытого ключа	21.051	35.403	52.172	74.246	124.627	208.53	464.422	22.991	54.283	116.284	223.225	742.20
Постановка	10.61	17.813	26.11	37.573	63.18	104.46	233.01	3.917	9.580	14.532	35.67	83.446
Проверка	21.042	36.158	53.929	76.641	128.04	213.10	465.207	8.157	19.626	29.856	72.205	168.68

Производительность #5 (ARM v7)

ECGDSA	P-160	P-192	P-224	P-256	P-320	P-384	P-512
Генерация личного ключа	0.020	0.029	0.034	0.041	0.059	0.078	0.124
Генерация открытого ключа	4.890	7.874	11.568	17.25	34.7961	58.5892	131.965
Постановка	2.432	3.932	6.011	8.761	17.137	28.745	65.310
Проверка	5.068	8.073	12.158	18.431	34.386	58.102	128.884

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 (ARM v6)

RSA	512	1024	1536	2048	3072	4096	7168	8192
Генерация личного ключа*	277.691	4491.37	9746.33	14531.4	201523	132912	972956	14210000
Постановка	15183	101788	323812	736399	2434000	5667000	13350000	20290000
Проверка	2738.15	9995.8	21074.2	37441.5	83558.9	144786	431266	576799

* - очень медленный генератор ПСП

Производительность #6 (ARM v7)

RSA	512	1024	1536	2048	3072	4096	7168	8192
Генерация личного ключа	99.567	1205.23	5249.22	10680.5	33216.4	70008.1	480783	1421000
Постановка	3865.59	29627.6	94864.1	218616	731126	1682000	8729000	1300000
Проверка	583.05	2208.88	4676.45	8078.7	18177.5	31412.1	94289.5	123745

Дальнейшие направления

- Поддержка распараллеливания для ряда режимов блочных шифров
- 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