Представление целых чисел с отложенным переносом

Общие сведения

Владислав Ковтун
Андрей Охрименко
Александр Стокипный

Содержание

- Актуальность
- Существующие представления
- Общее описание подхода
- Операции над числами
- Выводы

Введение

Цель: повышение производительности операций над целыми числами для криптографических преобразований

Объект: процесс представления целых чисел

Предмет: операции над целыми числами

Актуальность

<table>
<tr><td>Криптопреобразования</td><td colspan="2">Зашифровывание/ расшифровывание</td><td colspan="2">Формирование и проверка цифровой подписи</td><td colspan="2">Обмен ключами</td></tr>
<tr><td rowspan="2">Арифметика в поле целых чисел</td><td>Сложение</td><td>Вычитание</td><td>Умножение</td><td>Возведение в квадрат</td><td colspan="2">Сдвиг</td></tr>
<tr><td colspan="2">Возведение в степень</td><td colspan="2">Приведение по модулю</td><td>Деление</td><td>Инвертирование</td></tr>
<tr><td>Команды CPU</td><td colspan="6">mov, mul, shr, shl, add, sub …</td></tr>
</table>

Математические задачи

- Факторизация большого числа.
- Дискретный логарифм (ДЛ) в поле целых чисел и в поле полиномов.
- ДЛ в группе точек эллиптической кривой.
- ДЛ в якобиане дивизоров гиперэллиптической кривой.
- Поиск кратчайшего вектора в Эвклидовом пространстве.

Криптосистемы

- RSA
- DSA
- ECDSA
- ECKAS-DH
- NTRU

Представление целых чисел

- позиционные
- непозиционные
- смешанные

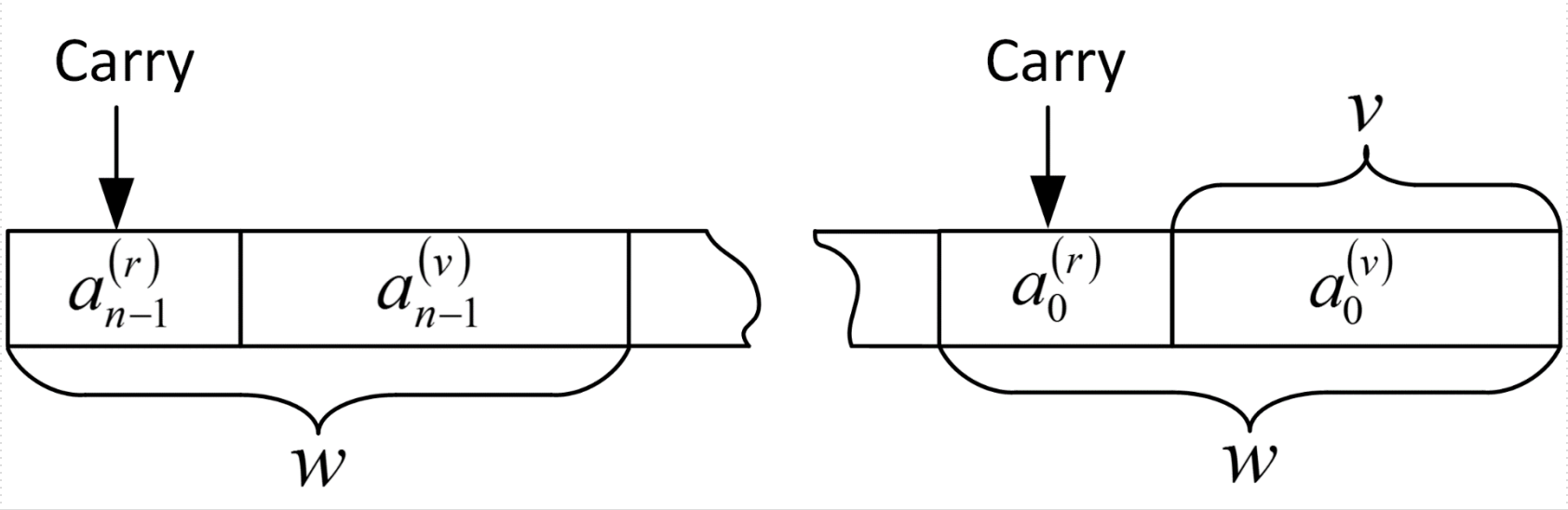
Представление целых чисел

- Двоичное представление (binary form)
- Двоичное представление со знаком (signed-digit binary)
- Non-adjacent form (NAF)
- Представление в системе остаточных классов (Residue Number System)
- Представление в частотной области (frequency domain)

Операции с переносом

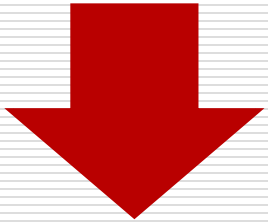
- Сложение
- Вычитание
- Умножение
- Возведение в квадрат
- Деление и приведение по модулю
- Мультипликативное инвертирование
- Возведение в степень

Delayed Carry Form (DCF)



Delayed Carry Form (DCF)

$$a = \{a_{n-1}, \ldots, a_1, a_0\}$$



$$d_{\mathrm{DCF}} = \{d_{m-1}, \ldots, d_1, d_0\}_{\mathrm{DCF}}$$

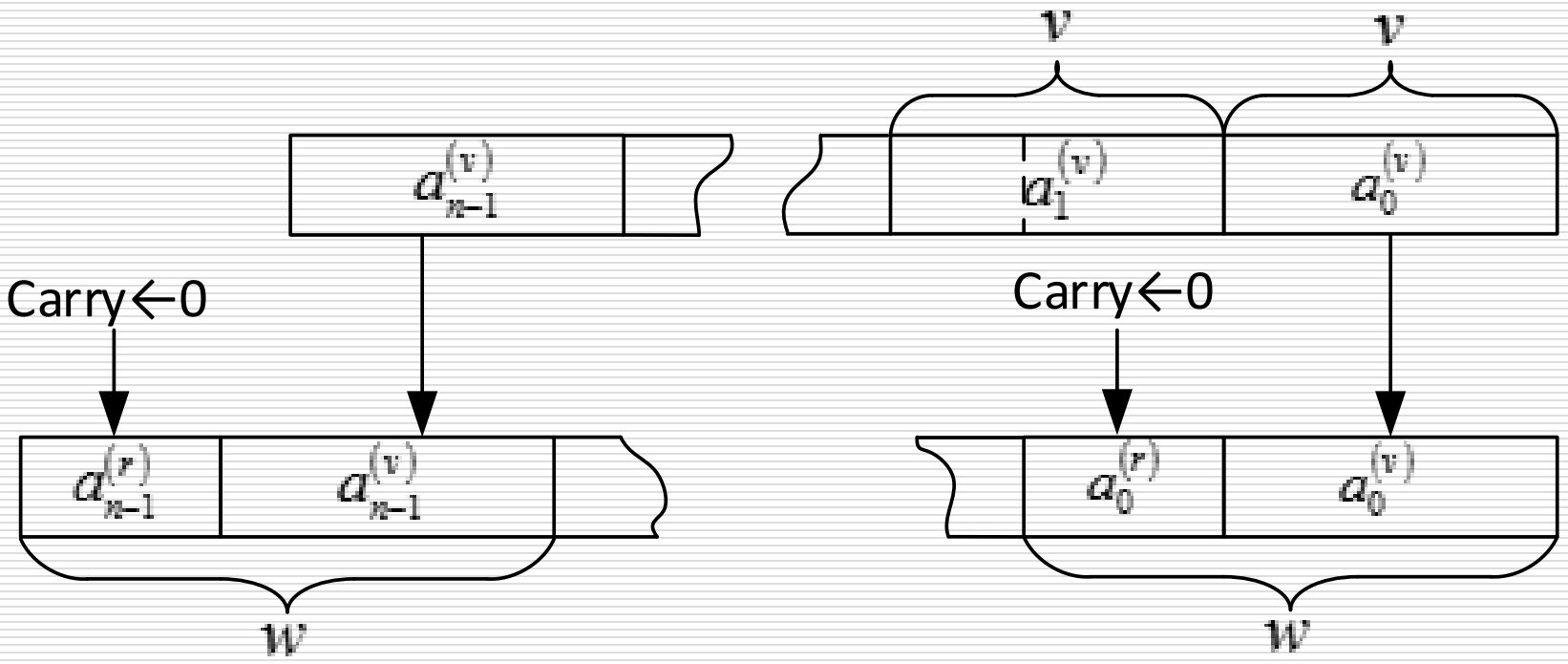
Delayed Carry Form (DCF)

$$d_{\mathrm{DCF}} = \{d_{m-1}, \ldots, d_1, d_0\}_{\mathrm{DCF}}$$

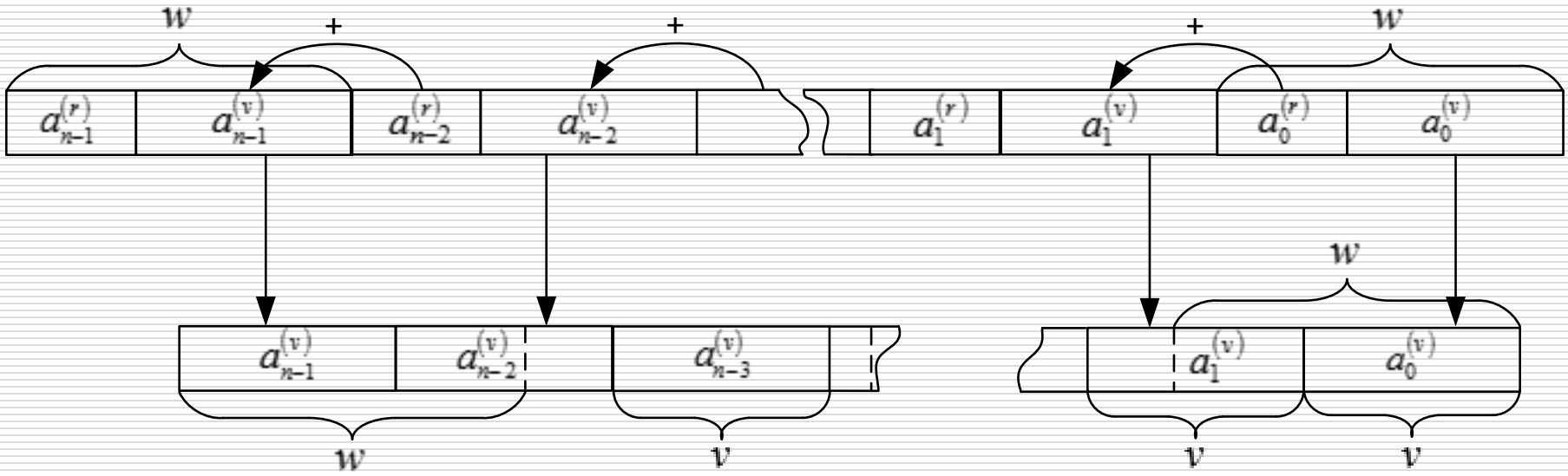
$$d_i^{(w)} = a_i^{(r)} \parallel a_i^{(v)}$$

$$m = \frac{n \cdot w}{v} = \frac{n \cdot w}{w - r}$$

Преобразование двоичного числа к DCF представлению



Преобразование DCF-числа к двоичному представлению



Условия применения операций

№	Название алгоритма	Обозначение	Вход 1	Вход 2	Выход
1	Преобразование целых чисел из двоично-непрерывной формы в DCF-форму	B2D	BF	–	DCF
2	Преобразование целых чисел из DCF-формы в двоично-непрерывную форму	D2B	DCF	–	BF
3	Сложение чисел в DCF-форме	AddD	DCF	DCF	DCF
4	Смешанное сложение целых чисел в двоично-непрерывной форме и DCF-форме, результат в DCF-форме	AddMxBD	DCF	BF	DCF
		AddMxBB	BF	BF	DCF

Условия применения операций

№	Название алгоритма	Обозначение	Вход 1	Вход 2	Выход
5	Вычитание чисел в DCF-форме	SubD	DCF	DCF	DCF
6	Смешанное вычитание чисел в DCF-форме	SubMxDB	DCF	BF	DCF
		SubMxBD	BF	DCF	DCF
		SubMxBD	BF	BF	DCF
7	Сдвиг влево	ShlD	DCF	–	DCF
8	Смешанный сдвиг влево	ShlBD	BF	–	DCF

Условия применения операций

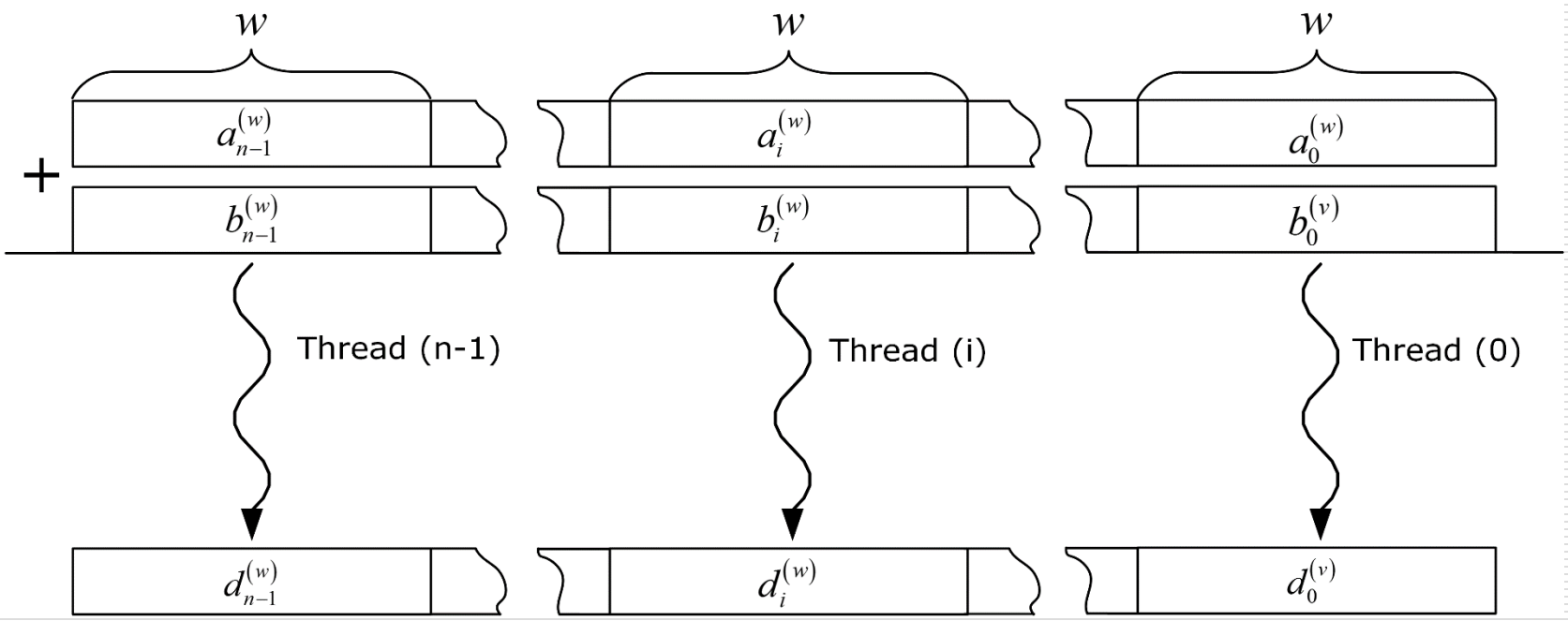
№	Название алгоритма	Обозначение	Вход 1	Вход 2	Выход
9	Сдвиг вправо	ShlD	DCF	–	DCF
10	Смешанный сдвиг вправо	ShlBD	BF	–	DCF
11	Умножение чисел	MulMxBD	BF	BF	DCF
12	Возведение в квадрат	SqrMxBD	BF		DCF

Аналитическая оценка избыточности

$$R(d_{DCF}) = w \cdot n \cdot \left(\frac{w}{v} - 1\right)$$

Длина блока для отложенного переноса, бит	Разрядность машинного слова		Избыточность, число слов		Длина числа в DCF, число слов	
	32 bits	64 bits	32 bits	64 bits	32bits	64bits
8	+	+	$n/3$	$n/7$	$4n/3$	$8n/7$
16	+	+	$n/2$	$n/3$	$3n/2$	$4n/3$
24	+	+	$3n$	$3n/5$	$4n$	$8n/5$
32	–	+	–	n	–	$2n$

Схема распараллеливания



Выводы

- Применение DCF в арифметических операциях умножения, возведения в квадрат и приведение по модулю позволило до 3-х раз повысить их производительность на современных процессорах (32- и 64-разрядных), что, в свою очередь, существенно повысило производительность криптосистемы в целом.
- Кроме прямого увеличения производительности арифметических операций, появляется возможность выполнения операции в два и более параллельных потока, что дает возможность повысить их производительность до 10 раз, с ростом двоичной длины чисел до 16 тыс. бит

Выводы

- В качестве дальнейших перспектив, интересна адаптация предложенных алгоритмов арифметических операций на вычислительных системах GPGPU для реализации криптографических преобразований

Вопросы?

Спасибо за внимание!

ООО «САЙФЕР БИС»

Андрей Охрименко

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