

Recursive double-size fixed precision arithmetic

C.Chabot, JG. Dumas, L. Fousse, P. Giorgi
{christophe.chabot,jean-guillaume.dumas,laurent.fousse}@imag.fr
pascal.giorgi@lirmm.fr

April 2, 2011

1 Introduction

This work is a part of the SHIVA (Secured Hardware Immune Versatile Architecture) project whose purpose is to provide a programmable and reconfigurable hardware module with high level of security. We propose a recursive double-size fixed precision arithmetic called RecInt. Our work can be split in two parts. First we developed a C++ software library with performances comparable to GMP ones. Secondly our simple representation of the integers allows an implementation on FPGA.

Concerning the software part, we remarked that most often the general purpose arbitrary precision GMP library is faster for cryptographic routines than special purpose libraries such as OpenSSL or Miracl. Then we found that GMP could be improved on very small precision. Our idea is to consider sizes that are a power of 2 and to apply doubling techniques to implement them efficiently: we design a recursive data structure where integers of size 2^k , for $k > k_0$ can be stored as two integers of size 2^{k-1} . Obviously for $k \leq k_0$ we use machine arithmetic instead (k_0 depending on the architecture). Our design makes use of C++ template mechanism so that we can define a generic doubling structure for large k and specialize it to machine arithmetic for small values of k . If some routines can be implemented faster for some specific sizes, the template mechanism allows also partial specializations of these routines. We provide a prototype implementation showing good performances on desktop PC's: the PALOALTO library¹.

Concerning the hardware part, our first works are based on the transformation of C++ sources to VHDL using dedicated softwares. We show that our first results are promising.

¹<https://www.ljkforge.imag.fr/projects/paloalto/>.

2 Recursive data structure

The main idea is to represent an element of size 2^k with two elements of size 2^{k-1} . We note $\text{RecInt}\langle k \rangle$ our recursive integer of size 2^k bits. That leads to a recursive structure with specializations for small sizes.

$$\left\{ \begin{array}{l} \text{RecInt}\langle k \rangle a \mapsto (\text{RecInt}\langle k-1 \rangle a.High, \text{RecInt}\langle k-1 \rangle a.Low) \\ \text{RecInt}\langle k_0 \rangle \text{ of size } 2^{k_0} \text{ called } \mathbf{limb}. \end{array} \right.$$

$$\text{where } a = a.High * 2^{2^{k-1}} + a.Low.$$

All these integers are unsigned, hence a $\text{RecInt}\langle k \rangle$ is capable to store any unsigned integer within the range $0..2^{2^k}$.

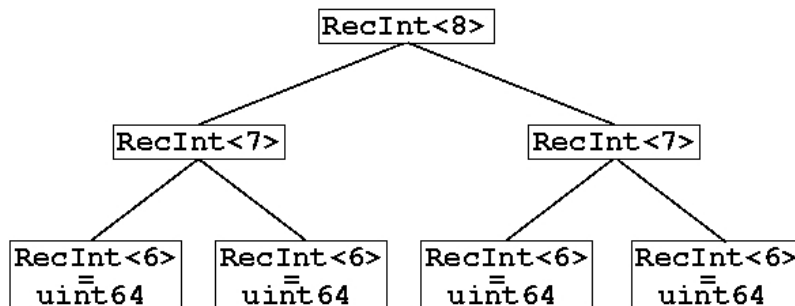


Figure 1: Recursive structure of a $\text{RecInt}\langle 8 \rangle$ in a 64 bits architecture.

3 Operations

Obviously all the classical arithmetic operations are provided. However we focus on specific ones.

3.1 Extending the word size

The idea is to provide a very fast arithmetic for integers of size a power of two which would mimic the behaviour of the word-size arithmetic: operations are correct modulo some 2^{2^k} . Indeed computing the remainder with such a modulus on a binary architecture comes to just keeping the correct number of bits.

For instance, machine size arithmetic on a 32 bits architecture is done modulo 2^{2^5} , and modulo 2^{2^6} on a 64 bits architecture.

For truncated addition and subtraction, that comes to not keeping the carry (or the borrow).

When multiplying two integers of at most 2^k bits modulo 2^{2^k} , one does not need to compute the highest bits of the product as in the following figure.

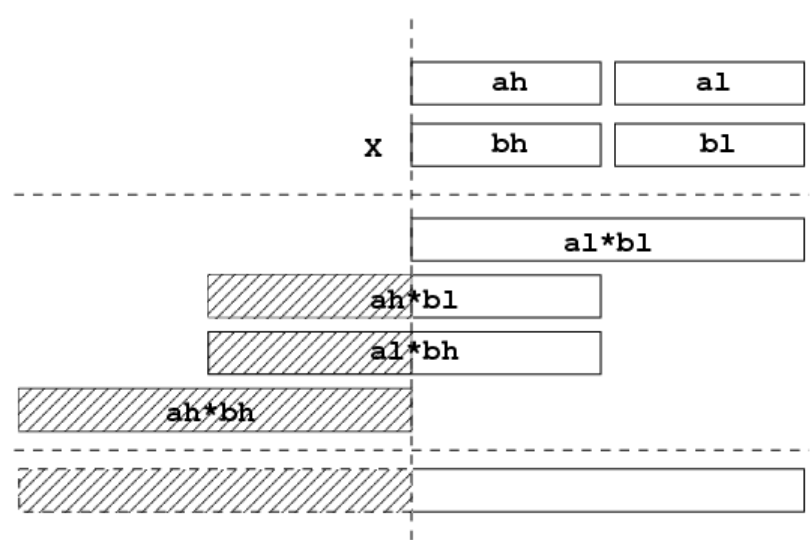


Figure 2: Truncated multiplication

Hence, one truncated multiplication of level k requires only 1 complete multiplication and 2 truncated multiplications of level $k - 1$ (instead of 4 complete multiplications for a naïve complete multiplication).

3.2 Recursive division

We use a recursive method for Euclidean division of integers described in [1]. This method uses two sub-algorithms dividing respectively 2 digits by 1 digit and 3 halves by 2. They allow then a recursive division of a s -digits integer by a r -digits integer with complexity $O(rs^{\log(3)-1} + r \log(s))$.

3.3 Montgomery modular multiplication

A naïve way of performing a modular multiplication is: performing a complete multiplication and then a modular reduction. However in the general case, this reduction is done with a division, which is time consuming. In the case there exists a radix R such that computations modulo R are inexpensive to process, Montgomery gives in [5] a method for performing a modular multiplication without trial division. Actually the complete multiplication is still performed but the reduction is done as following:

```

function REDC( $T$ )
   $m \leftarrow (T \bmod R)N' \bmod R$ 
   $t \leftarrow (T + mN)/R$ 
  if  $t \geq N$  then return  $t - N$  else return  $t$ .

```

where $0 < R^{-1} < N$ and $0 < N' < R$ satisfy $RR^{-1} - NN' = 1$.

This algorithm computes $\text{REDC}(T) = TR^{-1} \bmod N$ if $0 \leq T < RN$. Thus, $\text{REDC}((AR \bmod N)(BR \bmod N)) = ABR \bmod N$. This means that if we note $\bar{A} = AR \bmod N$ and $\bar{B} = BR \bmod N$ (called Montgomery representations of A and B), then $\text{REDC}(\bar{A}\bar{B}) = \overline{AB}$.

Hence, as long as we stay in Montgomery representation no division is required. In order to come back to the regular representation, one needs to perform a multiplication by R^{-1} modulo N .

In our case, if one wants to multiply two `RecInt<k>` A and B , $R = 2^{2^k}$. If A is a `RecInt<k+1>`,

- Reduction of A modulo R comes to take $A.Low$.
- Exact division of A by R comes to take $A.High$.

Hence REDC requires only 1 truncated multiplication and 1 complete multiplication.

4 C++ Library

This library depends on `gmp` (for machine word arithmetic). Hence if `gmp` is installed on your computer you can use our library by typing at the beginning of your C++ program:

```

#define __32bits // or __64bits depending on your processor
#include "recint.h"

```

4.1 Template recursive data structure

In order to simplify the development we chose to use a template recursive data structure with partial specialization. This specialization depends on the architecture.

- `RecInt<5>` \sim `uint32` in a 32 bits architecture.
- `RecInt<6>` \sim `uint64` in a 64 bits architecture.

First our library allows manipulation of fixed precision integers. Thus we define the template structure `RecInt<>` as following:

```

template <size_t k> struct RecInt {
    typedef RecInt<k+1> Father_t;
    typedef RecInt<k> Self_t;
    typedef RecInt<k-1> Half_t;

    // High = most significant part
    // Low = least significant part
    // *this == High * 2^(2^(k-1)) + Low
    Half_t High, Low;
};

template <> struct RecInt<LIMB_SIZE> {
    limb Value;
};

```

where `limb` represents the machine word.

4.2 Classical operations

Parameters of functions have been chosen to be passed by reference in order to avoid copying them at each call.

Functions that return a boolean are always of the following form:

```
template <class T> bool RI_is_equal_to(const T&, const T&);
```

All the other functions are void functions whose first parameters are the output values and the last ones, considered as `const` are the input ones:

```
template <class T> void RI_add(limb&, T&, const T&, const T&);
```

Classic functions are split into the following sections according to their use:

4.2.1 Operators

We define the following operators for basic arithmetic.

- Arithmetic operators: `+`, `-`, `*`;
- In place operators: `+=`, `-=`, `*=`;
- Increment and decrement operators: `++`, `--`;
- Comparison operators: `==`, `!=`, `<`, `>`;

4.2.2 Comparison functions

Comparison between `RecInt`:

- `char RI_comp(const RecInt<k>& a, const RecInt<k>& b)` returns +1 if $a > b$, 0 if $a == b$ and -1 if $a < b$.
- `bool RI_is_equal_to(const RecInt<k>& a, const RecInt<k>& b)` returns true if and only if $a == b$.
- `bool RI_is_greater_than(const RecInt<k>& a, const RecInt<k>& b)` returns true if and only if $a > b$.
- `bool RI_is_lower_than(const RecInt<k>& a, const RecInt<k>& b)` returns true if and only if $a < b$.

Comparison with a constant:

- `bool RI_is_equal_to_0(const RecInt<k>& a)` returns true if and only if $a == 0$.
- `bool RI_is_equal_to_1(const RecInt<k>& a)` returns true if and only if $a == 1$.
- `bool RI_is_equal_to_limb(const RecInt<k>& a, const limb& b)` returns true if and only if $a == b$.

4.2.3 Set functions

We provide a set of functions permitting to set a part of an integer or the whole integer to a specified value.

- `void RI_reset(RecInt<k>& a)` resets a to 0.
- `void RI_random(RecInt<k>& a)` sets a to a random value.
- `void RI_set_limb(RecInt<k>& a, const limb& b, const unsigned int& n)` sets the n^{th} limb of a to the value b (the 0^{th} limb is the least significant one).
- `void RI_set_const(RecInt<k>& a, const limb& b)` sets the 0^{th} limb of a to the value b .

4.2.4 Get functions

The following functions permit to get value(s) from an integer:

- `void RI_get_limb(limb& l, const RecInt<k>& a, const unsigned int& n)`: l is set to the value of the n^{th} limb of a .
- `void RI_get_limb0(limb& l, const RecInt<k>& a)`: l is set to the value of the least significant limb of a .

- void RI_get_limbn(limb& l, const RecInt<k>& a): l is set to the value of the most significant limb of a.
- void RI_copy(RecInt<k>& a, const RecInt<k>& b) copies the value of b into a.

4.3 Arithmetic functions

The following classic operations will always output the full precision of the computation.

- void RI_add(limb& l, RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c):
 $a = b + c + l * 2^{2^k}$.
- void RI_add(limb& l, RecInt<k>& a, const RecInt<k>& b, const limb& c):
 $a = b + c + l * 2^{2^k}$.
- void RI_increment(limb& l, RecInt<k>& a): $a \leftarrow a + 1 + l * 2^{2^k}$.
- void RI_sub(limb& l, RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c):
 $a = b - c + l * 2^{2^k}$.
- void RI_sub(limb& l, RecInt<k>& a, const RecInt<k>& b, const limb& c):
 $a = b - c + l * 2^{2^k}$.
- void RI_decrement(limb& l, RecInt<k>& a): $a \leftarrow a - 1 + l * 2^{2^k}$.
- void RI_lmul(RecInt<k>& ah, RecInt<k>& al, const RecInt<k>& b, const RecInt<k>& c):
 $ah * 2^{2^k} + al = b * c$.
- void RI_lmul(limb& ah, RecInt<k>& al, const RecInt<k>& b, const limb& c):
 $ah * 2^{2^k} + al = b * c$.
- void RI_div(RecInt<k>& q, RecInt<k>& r, const RecInt<k>& a, const RecInt<k>& b):
q and r are respectively the quotient and the remainder in the Euclidean division of a by b: $a = b * q + r$ with $r < b$.
- void RI_div_quotient(RecInt<k>& q, const RecInt<k>& a, const RecInt<k>& b):
only the quotient q is output.
- void RI_div_remainder(RecInt<k>& r, const RecInt<k>& a, const RecInt<k>& b):
only the remainder r is output.
- void RI_square(RecInt<k>& ah, RecInt<k>& al, const RecInt<k>& b):
 $ah * 2^{2^k} + al = b^2$.
- void RI_gcd(RecInt<k>& g, const RecInt<k>& a, const RecInt<k>& b):
g is set to the Gcd of a and b.

- `void RI_ext_gcd(RecInt<k>& g, bool& su, RecInt<k>& u, bool& sv, RecInt<k>& v, const RecInt<k>& a, const RecInt<k>& b):` g is set to the Gcd of a and b with Bezout coefficients u and v respectively with sign su and sv ($su==0$ means that u is negative).

Addition and subtraction functions are provided with extended functions having suffixes `_in`, `_nc` or combined `_nc_in`.

The `_in` suffix means that the operation is made in place:

`void RI_add_in(limb& l, RecInt<k>& a, const RecInt<k>& b):` $a \leftarrow a+b$
and l is the carry.

The `_nc` suffix means that the carry (or borrow) is not output:

`void RI_sub_nc(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c):`
 $a \leftarrow b - c$.

4.4 Extending the word size

The following functions return results modulo 2^{2^k} :

- `void RI_add_nc(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c)`
returns a such that $a=b+c$ modulo 2^{2^k} .
- `void RI_sub_nc(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c)`
returns a such that $a=b-c$ modulo 2^{2^k} .
- `void RI_mul(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c)`
returns a such that $a=b*c$ modulo 2^{2^k} .

4.5 Modular operations

The PALOALTO Library allows manipulation of modular integers as well.

4.5.1 Modular operations on RecInt

Our library provides modular operations on classical `RecInt`. The user must specify the module n at each call of any operation. At the beginning of all functions, the input parameters are reduced modulo n . The outputs are also computed modulo n .

- `void RI_reduction(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& n):`
 $a \leftarrow b \bmod n$.
- `void RI_random_mod(RecInt<k>& a, const RecInt<k>& n):` a is set to a random value within the range $0..n-1$.
- `void RI_neg_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& n):`
 $a \leftarrow -b \bmod n$.

- `void RI_add_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c, const RecInt<k>& n): $a \leftarrow b + c \bmod n$.`
- `void RI_sub_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c, const RecInt<k>& n): $a \leftarrow b - c \bmod n$.`
- `void RI_mul_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c, const RecInt<k>& n): $a \leftarrow b * c \bmod n$.`
- `void RI_mul_mod(RecInt<k>& a, const RecInt<k>& b, const limb& c, const RecInt<k>& n): $a \leftarrow b * c \bmod n$.`
- `void RI_square_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& n): $a \leftarrow b^2 \bmod n$.`
- `void RI_exp_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c, const RecInt<k>& n): $a \leftarrow b^c \bmod n$.`
- `void RI_exp_mod(RecInt<k>& a, const RecInt<k>& b, const limb& c, const RecInt<k>& n): $a \leftarrow b^c \bmod n$.`
- `void RI_inv_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& n): $a \leftarrow b^{-1} \bmod n$.`
- `void RI_div_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& c, const RecInt<k>& n): $a \leftarrow b * c^{-1} \bmod n$ if c is invertible modulo n .`
- `bool RI_is_quadratic_residue(const RecInt<k>& a, const RecInt<k>& n)` returns `true` if and only if a is a quadratic residue modulo n .
- `void RI_square_root_mod(RecInt<k>& a, const RecInt<k>& b, const RecInt<k>& n):` a is such that $a^2 = b \bmod n$.

The `neg`, `add` and `sub` functions are extended with the suffix `_in` (in place operation) as for the classic operations. Note that the `_nc` suffix does not make any sense in this situation.

4.5.2 RecIntMod type

A special type is provided for modular operations. `RecIntMod<>` is basically a `RecInt<>` provided with a module p declared as a `static RecInt<>` of the same size. Furthermore we guarantee that such elements are always reduced modulo p . Actually we guarantee that all inputs and outputs of functions manipulating `RecIntMod<>` are reduced modulo p (that is to say within the range $0..p - 1$).

```
template <size_t k> struct RecIntMod {
    typedef RecInt<k> RecIntk;

    static RecIntk p;
    RecIntk Value;
};
```

Two functions allowing the conversion from `RecIntMod<>` to `RecInt<>` and vice versa are available: `Convert_to_RecInt(RecInt<k>&, RecIntMod<k>)` and `Convert_to_RecIntMod(RecIntMod<k>&, RecInt<k>)`.

4.5.3 Modular operations on `RecIntMod`

The same operations as in last section are applicable to `RecIntMod<>` integers. However the module `p` must be initialized before any arithmetic operation with the following function:

```
void RI_init_module(const RecInt<k>& p)
```

Since the module is declared as `static`, one has to initialize it only once before any computation. If done so, we guarantee that any `RecIntMod<>` integer will be always reduced modulo `p` throughout the program. Note that the user is allowed to change the module a posteriori, but the reduction modulo the new module will not be guaranteed anymore.

The user can get the module back by using:

```
void RI_get_module(RecInt<k>& p)
```

Once the module has been initialized, the user can use the operations presented in *Modular operations on `RecInt`* section, since they are overloaded for a use with `RecIntMod`.

5 C++ library Performances

In order to evaluate the performance of the PALOALTO prototype, we used GMP's assembly routine for double machine word arithmetic (e.g. `umul_ppmm` defined in the GMP [3] file `longlong.h`, multiplying two integers and generating their two-word product).

Using these assembly routines and the recursive data structure detailed above, we were able to get the performance of the following tables for fixed precision operations with recursive data structures.

For these performance comparisons we use the GMPbench suite [4].

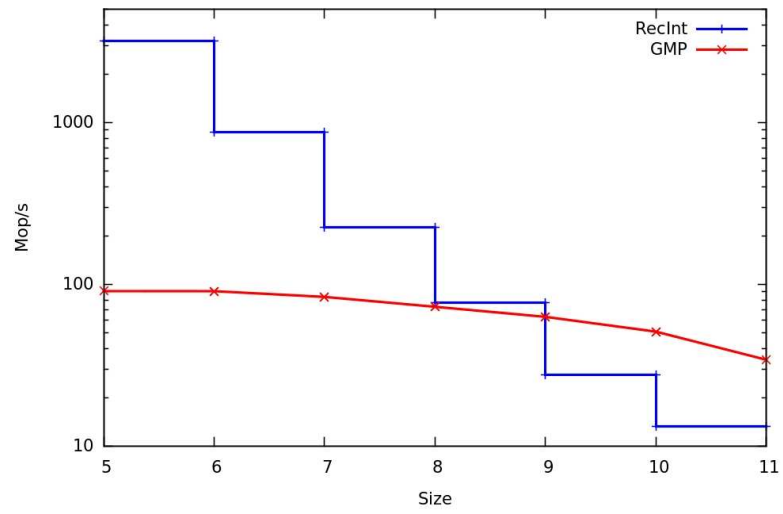


Figure 3: Fixed precision addition with RecInt versus GMP-5.0.1, gcc 4.4.0, Xeon X5482, 3.2GHz, in millions of arithmetic operations per second.

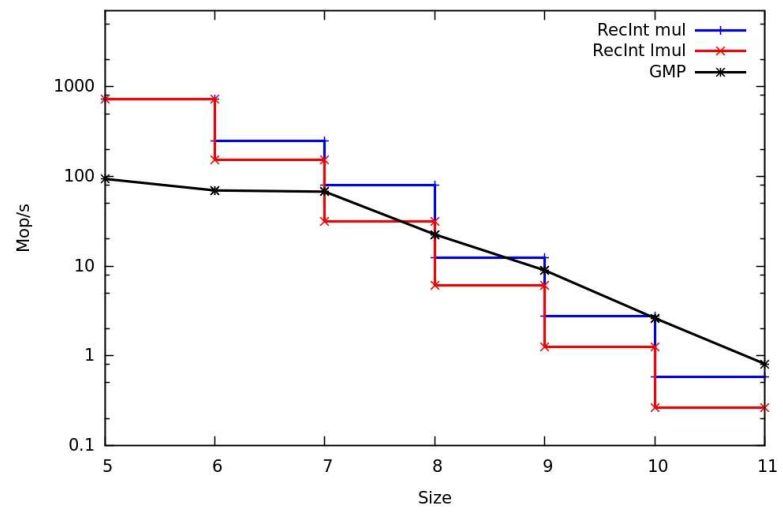


Figure 4: Fixed precision complete and truncated multiplications with RecInt versus GMP-5.0.1, gcc 4.4.0, Xeon X5482, 3.2GHz, in millions of arithmetic operations per second.

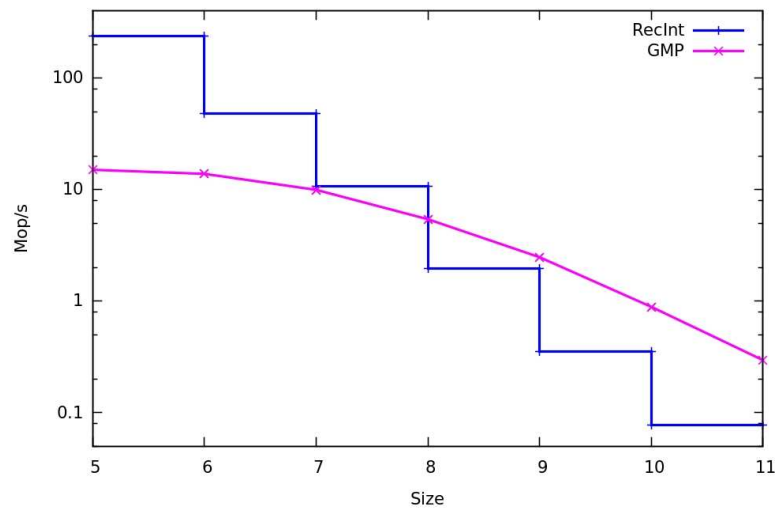


Figure 5: Fixed precision modular multiplication with RecInt versus GMP-5.0.1, gcc 4.4.0, Xeon X5482, 3.2GHz, in millions of arithmetic operations per second.

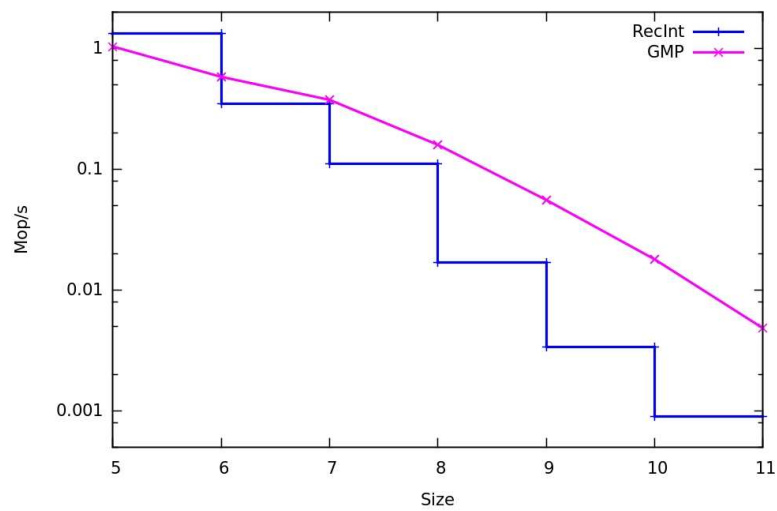


Figure 6: Fixed precision modular exponentiation with RecInt versus GMP-5.0.1, gcc 4.4.0, Xeon X5482, 3.2GHz, in millions of arithmetic operations per second.

The step shape of RecInt curves is explained by the fact that we use a `RecInt<k>` for all integers with size within the range $2^{k-1} - 1..2^k$.

Results obtained with RecInt are comparable to those with GMP. However, RecInt appears to be more efficient for small fixed precision.

6 Towards FPGA implementation

We present here the first attempts towards an implementation on a real FPGA. Inside SHIVA project, we need to provide basic arithmetic modules in order to be used in a RSA or Elliptic curve based encryption scheme. In order to build these modules, since our C++ library is already written, we chose to use a dedicated software transforming C++ source into VHDL called GAUT [2]. The creation of VHDL program can be split in the following steps:

- Compilation of C++ source and creation of the corresponding graph.
- Compilation of the library containing the needed operations.
- Synthesizing of the VHDL program and estimation of performances.

Here are some simulations of a modular exponentiation on a Virtex 5. We made the output flow vary in order to check the effect on the required size on the FPGA.

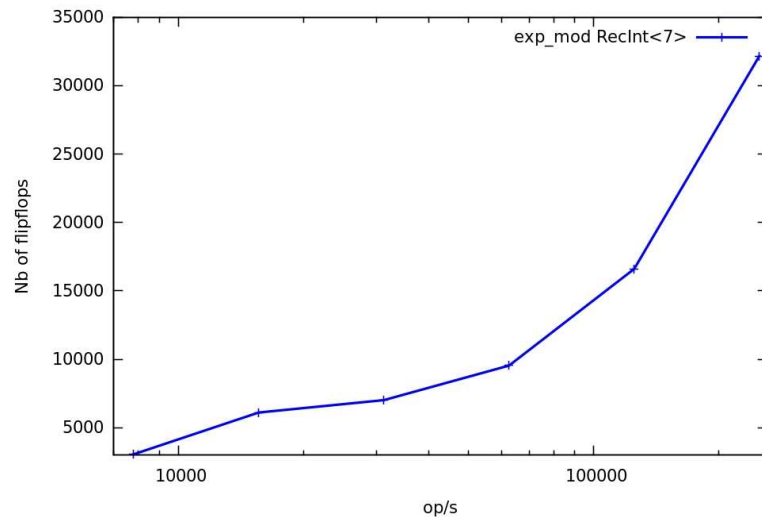


Figure 7: 128 bits words.

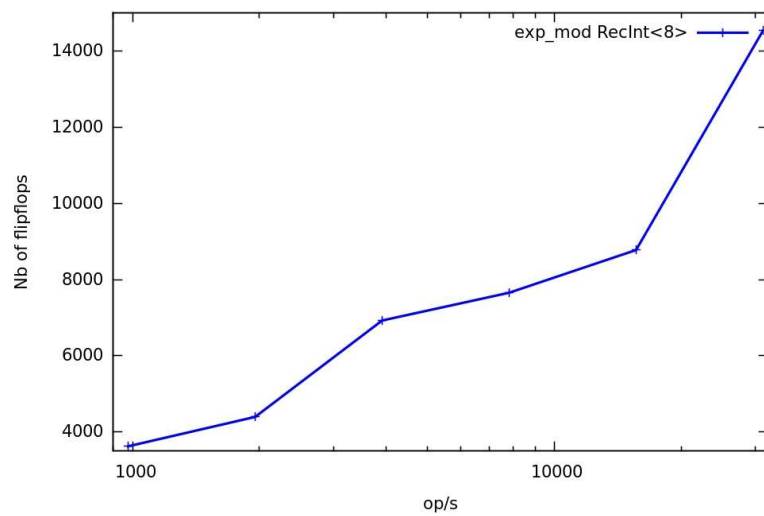


Figure 8: 256 bits words.

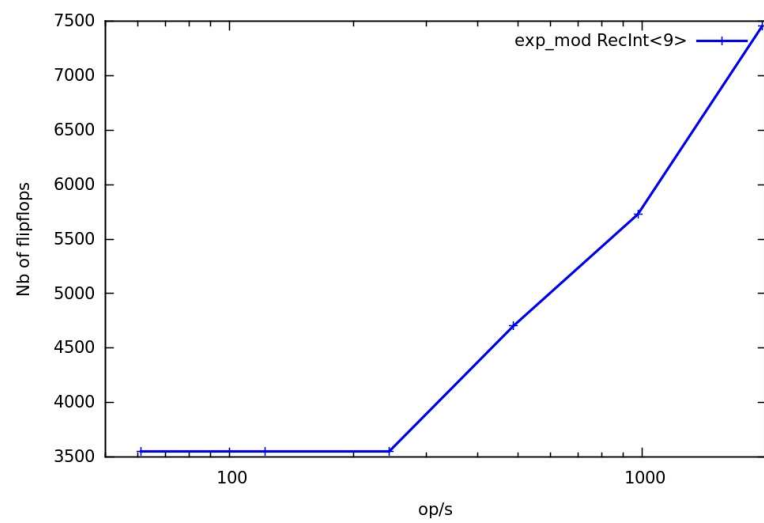


Figure 9: 512 bits words.

We notice that required size can be significantly reduced if we accept a lower output flow.

These results have been obtained without significant modifications on the C++ source. Thus they are not optimal but rather promising.

Further work will consist in optimizing C++ source in order to make it more adapted to VHDL synthesizing.

References

- [1] C. Burnikel, J. Ziegler, "Fast recursive division", MPI Informatik research report, October 1998.
- [2] "GAUT - High-Level Synthesis tool From C to RTL", <http://www-labsticc.univ-ubs.fr/www-gaut/>
- [3] "The GNU Multiple Precision Arithmetic Library", <http://gmplib.org>.
- [4] "The GNU Multiple Precision Arithmetic Library bench suite", <http://gmplib.org/gmpbench.html>
- [5] P.L. Montgomery, "Modular multiplication without trial division", In Mathematics of computation, Volume 44, Number 170, April 1985, pp. 519-521.