Design of Digital Platforms

Steven Janssens, Pieter Maene en Kristof Mariën

13 december 2012

1 Overall Architecture

2 HW/SW Boundaries

The RSA algorithm is a basic and very often used algorithm for encryption and decryption of data. So it is important that the encryption and decryption is as fast as possible. The algorithm is standardized and will not change in the future. The only part of it that will change is the size of the inputs. Because of these facts we have chosen for a full hardware implementation.

From the previous section we know that a Montgomery multiplication takes about 1 second and a Montgomery exponentiation uses a lot of multiplications. So the multiplication must be done in hardware. Our hardware implementation takes about 1300 cycles. Assuming a clock frequency of about 5 MHz, this means a multiplication in hardware takes about 0,26 µs.

So the only choice that was left, was to do the exponentiation in *C* and call every time the Montgomery multiplication of the hardware. But doing this would cause a lot of overhead to transfer the data from the software to the hardware en back. So we decided to write the exponentation in *Gezel* as well.

3 HW/SW Interface

4 Performance Metrics

5 Synthesis Results

6 Test Strategy