Jeremy Barthélemy
ECE 645

Montgomery Multiplication
Pseudocode: Architecture 2

Pseudocode below is based on the Multiple-Word Radix-2 Montgomery Multiplication Algorithms found in the Huang IEEE paper.

Note, ${}_{i=0}\sum^{n-1} I$ signifies the sum from i=0 to i=(n-1) of I.

<u>General Algoithm:</u>

Input:

odd M; $n = \lfloor \log_2 M \rfloor + 1$; word size w, $e = \lceil (n+1)/w \rceil$,

$X = {}_{i=0}\sum^{n-1} x_i{*}2^i$, $Y = {}_{j=0}\sum^{e-1} Y^{(j)}{*}2^{w*j}$, $M = {}_{j=0}\sum^{e-1} M^{(j)}{*}2^{w*j}$ with $0 \le X,Y < M$

Output:

$Z = {}_{j=0}\sum^{e-1} S^{(j)}{*}2^{w*j} = MP(X,Y,M) \equiv X*Y*2^{-n} \pmod M$, $0 \le Z < 2M$

S = 0; /*initialize all words of S*/

for i = 0 **to** n-1 **do**

  $q_i = (x_i{*}Y) \oplus S_0^{(0)}$;

  $(C^{(1)},S^{(0)}) = x_i{*}Y^{(0)} + q_i{*}M^{(0)} + S^{(0)}$;

  for j = 1 **to** e **step** 1 **do**

    $(C^{(j+1)}, S^{(j)}) = C^{(j)} + x_i{*}Y^{(j)} + q_i{*}M^{(j)} + S^{(j)}$;

    $S^{(j-1)} = (S_0^{(j)},S^{(j-1)}_{w-1..1})$;

  $S^{(e)} = 0$;

return Z = S;

<u>Computation in Task D</u>:

Input:

x_i, $Y^{(0)}$, $M^{(0)}$, $S_0^{(1)}$, $S^{(0)}_{w-1..1}$

Output:

q_i, $C^{(1)}$, $S^{(0)}_{w-1..1}$

$qi = (x_i{*}Y_0^{(0)}) \oplus S_1^{(0)}$;

$(CO^{(1)}, SO^{(0)}_{w-1}, S^{(0)}_{w-2..0}) = (1, S^{(0)}_{w-1..1}) + x_i{*}Y^{(0)} + q_i{*}M^{(0)}$;

$(CE^{(1)}, SE^{(0)}_{w-1}, S^{(0)}_{w-2..0}) = (0, S^{(0)}_{w-1..1}) + x_i{*}Y^{(0)} + q_i{*}M^{(0)}$;

if $S_0^{(1)} = 1$ **then**

  $C^{(1)} = CO^{(1)}$;

  $S^{(0)}_{w-1..1} = (SO^{(0)}_{w-1}, S^{(0)}_{w-2..1})$;

else

  $C^{(1)} = CE^{(1)}$;

  $S^{(0)}_{w-1..1} = (SE^{(0)}_{w-1}, S^{(0)}_{w-2..1})$;

Computation in Task E:

Input:

$q_i, x_i, C^{(j)}, Y^{(j)}, M^{(j)}, S_0^{(j+1)}, S^{(j)}_{w-1..1}$

Output:

$C^{(j+1)}, S^{(j)}_{w-1..1}, S_0^{(j)}$

$(CO^{(j+1)}, SO^{(j)}_{w-1}, S^{(j)}_{w-2..0}) = (1, S^{(j)}_{w-1..1}) + C^{(j)} + x_i{*}Y^{(j)} + q_i{*}M^{(j)};$
$(CE^{(j+1)}, SE^{(j)}_{w-1}, S^{(j)}_{w-2..0}) = (1, S^{(j)}_{w-1..1}) + C^{(j)} + x_i{*}Y^{(j)} + q_i{*}M^{(j)};$
if $S_0^{(j+1)} = 1$ **then**
    $C^{(j+1)} = CO^{(j+1)};$
    $S^{(j)}_{w-1..1} = (SO^{(j)}_{w-1}, S^{(j)}_{w-2..1});$
else
    $C^{(j+1)} = CE^{(j+1)};$
    $S^{(j)}_{w-1..1} = (SE^{(j)}_{w-1}, S^{(j)}_{w-2..1});$

Computation in Task F:

Input:

$q_i, x_i, C^{(e-1)}, Y^{(e-1)}, M^{(e-1)}, S^{(e-1)}_{w-1..1}, C_0^{(e)}$

Output:

$C^{(e)}, S^{(e-1)}_{w-1..1}, S_0^{(e-1)}$

$(C^{(e)}, S^{(e-1)}) = (C_0^{(e)}, S^{(e-1)}_{w-1..1}) + C^{(e-1)} + x_i{*}Y^{(e-1)} + q_i{*}M^{(e-1)};$