Montgomery Reduction

Cybersecurity Specialization
-- Hardware Security

Montgomery Reduction

- Let R>N be two integers and gcd(N,R)=1. For $0 \le T < NR$, the *Montgomery reduction* of T modulo N w.r.t. R is defined as $TR^{-1} \pmod N$.
- Montgomery reduction algorithm
  - $m = T \times (-N^{-1}) \pmod R$
  - $t = (T + mN)/R$
  - if ($N \le t$)
  - $\quad t = t - N$
- Claim: $t = TR^{-1} \pmod N$
  - $tR = T \pmod N$
  - $0 \le t < N$

$tR = T + mN = T \pmod N$

$0 \le m < R \rightarrow 0 \le mN < NR$

$0 \le T+mN < 2NR$

$0 \le (T+mN)/R < 2N$

$TR^{-1} = (T + T(-N^{-1}) \pmod R)N)/R \pmod N$

Computing a x b (mod N)

- Pick R, s.t. R > N, gcd (R,N) = 1
- Compute
  - N^{-1} (mod R)
  - a' = aR (mod N), b' = bR (mod N)
  - $c' = (a'b')R^{-1}$ (mod N)
  - $c = c'R^{-1}$ (mod N)
- Claim: c ≡ a x b (mod N)
  - $c'R^{-1} \equiv (a'b')R^{-1}R^{-1} \equiv (a'R^{-1})(b'R^{-1}) \equiv ab$ (mod N)
- If $R=2^k$, xR, ÷R, mod R are trivial
  - an option to implement modular exponentiation

$TR^{-1} = (T + T(-N^{-1}) \text{ (mod R)}N)/R$ (mod N)

Example: 68 x 57 (mod 109)

- a = 68, b = 57, N = 109
- Pick R = 128 = 2^7
- $N^{-1} = 101$, $-N^{-1} = 27$ (mod 128)
  - 109 x 101 ≡ (128-19) x (128-27) ≡ 19 x 27 ≡ 513 ≡ 1
- a' ≡ aR ≡ 68 x 128 ≡ 8704 ≡ 93 (mod 109)
- b' ≡ bR ≡ 57 x 128 ≡ 7296 ≡ 102 (mod 109)
- c' ≡ (93x102 + 93x102x27(mod 128)x109)/128
  ≡ 22784/128
  ≡ 178
  ≡ 69 (mod 109)

$TR^{-1} = (T + T(-N^{-1}) \text{ (mod R)}N)/R$ (mod N)

Example: 68 x 57 (mod 109)

- $a = 68$, $b = 57$, $N = 109$
- $R = 128 = 2^7$, $-N^{-1} = 27 \pmod{128}$
- $a' \equiv aR \equiv 93 \pmod{109}$
- $b' \equiv bR \equiv 102 \pmod{109}$
- $c' \equiv (a'b')R^{-1} \equiv 69 \pmod{109}$
- $c \equiv (69 + 69 \times 27 \pmod{128} \times 109)/128$
  $\equiv 7808/128$
  $\equiv 61 \pmod{109}$
- $68 \times 57 \equiv 3876 \equiv 61 \pmod{109}$

$TR^{-1} = (T + T(-N^{-1}) \pmod{R}N)/R \pmod{N}$