$R_q = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n+1\rangle$

$n = 2^k$, $q \equiv 1 \bmod 2n$

Shared small $s(x) \in R_q$

random $a(x)$

random small $e(x)$

$m(x) \leftrightarrow$ bitstring

$e(m) =$

$(c_0(x), c_1(x)) =$

$(a s + 2e + m, -a)$

$d(c_0, c_1) = c_0 + c_1 s \bmod 2$

New scheme

$\vec{c} = (c_0, \ldots, c_d) \in R_q^{d+1}$

$\vec{c} + \vec{c}' = (c_0, \ldots, c_d) + (c_0', \ldots, c_{d'}')$

$= (c_0 + c_0', c_1 + c_1', \ldots, c_d + c_d', c_{d+1}', \ldots, c_{d'}')$

$\vec{c} = c_0 + c_1 v + c_2 v^2 + \cdots + c_d v^d \in R_q[v]$

$\mathbb{Z}/q\mathbb{Z}[x]/\langle x^n+1\rangle[v]$

$\mathbb{Z}[x,v]/\langle q, x^n+1\rangle$

$d(\vec{c}) = \langle \vec{c} | \vec{s} \rangle = \vec{c}(s)$

plugging s in for v.

$\vec{s} = (1, s, s^2, \ldots, s^d)$

Prop: if $e(m) = \vec{c}$ and $e(m') = \vec{c}'$, then $d(c \times c') = m m'$ as long as the error is small.

Pf/ $e(m) = \vec{c} = (c_0 + c_1)$

$= (as + 2e + m, -a)$

$= as + 2e + m - aV$

$e(m') = \vec{c}' = (c_0' + c_1')$

$= (a's + 2e' + m', -a')$

$= a's + 2e' + m' - a'V$

$c \times c' = (as + 2e + m - aV)(a's + 2e' + m' - a'V)$

$= aa's^2 + as2e' + asm' - aa'sV$
$+ 2ea's + 4ee' + 2em' - 2ea'V$
$+ ma's + 2me' + mm' - ma'V$
$+ -aa'sV - 2e'aV - amV + aa'V^2$

$= mm' + asm' + a'sm + aa's^2$
$+ 2(ea's + 2ee' + em' + e'as + e'm)$
$- (as + 2e + m)a'V - (a's + 2e' + m')aV + aa'V^2$

$= mm' + asm' + a'sm + aa's^2$
$+ 2(ea's + 2ee' + em' + e'as + e'm)$
$- aa's^2 - 2ea's - ma's - a'as^2 - 2e'as - m'as + aa's^2$

$= mm' + 2(em' + e'm + 2ee') \equiv mm' \bmod 2.$

Last Time:

$s = x^3 - x^2 + 2x$

$m = x^3 + x$

$c = (-x^3 + 2x^2 + 7x - 2) + (-3x^2 - 7x + 5)v$

$m' = x^2 + x$

$c' = (-8x^3 - 5x^2 - 3x + 6) + (-4x^3 + 5x^2 - 2x)v$

$cc' = (8x + 10x^2 + 3x^3)$

$+ (15 + 3x + 11x^2 + 15x^3)v$

$+ (11 + 2x + 14x^2 + 13x^3)v^2$

$d(cc') = 8x + 10x^2 + 3x^3$

$+ (15 + 3x + 11x^2 + 15x^3)(x^3 - x^2 + 2x)$

$+ (11 + 2x + 14x^2 + 13x^3)(x^3 - x^2 + 2x)^2$

$= 8x + 10x^2 + 3x^3$

$+ 15x^3 - 15x^2 + 30x + 3x^4 - 3x^3 + 6x^2$

$+ 11x^5 - 11x^4 + 22x^3 + 15x^6 - 15x^5 + 30x^4$

$-11x \quad +11 \qquad -15x^2 \quad +15x \quad -13$

$+ (11 + 2x + 14x^2 + 13x^3)(x^6 + x^4 + 4x^2 - 2x^5 - 4x^4 - 4x^3)$

$-x^2 \quad -x \qquad +2x \quad +4$

$= 8x + 10x^2 + 3x^3 + 15x^3 - 15x^2 + 13x$

$-3 - 3x^3 + 6x^2 - 11x + 11 + 5x^3 - 15x^2 + 15x - 3$

$+ (11 + 2x + 14x^2 + 13x^3)(4 + x + 3x^2 - 4x^3)$

$$= 8x + 10x^2 + 3x^3 + 15x^3 - 15x^2 + 13x$$
$$-3 - 3x^3 + 6x^2 - 11x + 11 + 5x^3 - 15x^2 + 15x - 3$$
$$+ (11 + 2x + 14x^2 + 13x^3)(4 + x + 3x^2 - 4x^3)$$

$$= 5 + 8x + 3x^3 + 3x^3$$
$$+ (44 + 11x + 33x^2 - 44x^3$$
$$+ 8x + 2x^2 + 6x^3 - 8x^4 + 8$$
$$+ 56x^2 + 14x^3 + 42x^4 - 56x^5 + 56x$$
$$- 42$$
$$+ 52x^3 + 13x^4 + 39x^5 - 52x^6)$$
$$- 13 \qquad + 39x \qquad - 52x^2$$

$$= 2 + 122x + 42x^2 + 31x^3 = 2 + 3x + 6x^2 - 3x^3$$

Should get

$$-4x^3 + 5x^2 + 3x - 1$$

$$\equiv x^2 + x + 1 \mod 2$$

(0 111)

$$(x^3 + x)(x^2 + x) = x^5 + x^4 + x^3 + x^2$$

$$= x^3 + x^2 - x - 1$$

$$= x^3 + x^2 + x + 1 \mod 2$$

(1111)

This is somewhat homomorphic encryption.

how for prod of 2 cs

maybe not for 1000 cs.

Gentry et al. (2009): Bootstrapping.

encrypt key inside message

and compress

can fit decryption + 1 more ring operation inside allowed # of operations.

by repeating / repeatedly encrypting

when I run out of error,

can do calcs as big as I want.

Not Practical.

Yet.