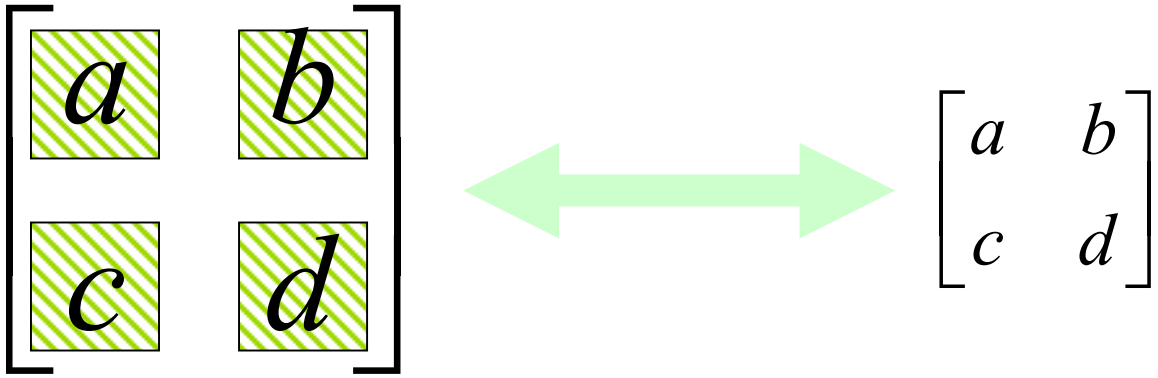
NTRUSign Introduced

December 2001

Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joe Silverman, William Whyte

Polynomial Ring

- $a(x) \in Z[X] / X^N - 1$
- $a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{N-1}X^{N-1}$



NTRU Lattice

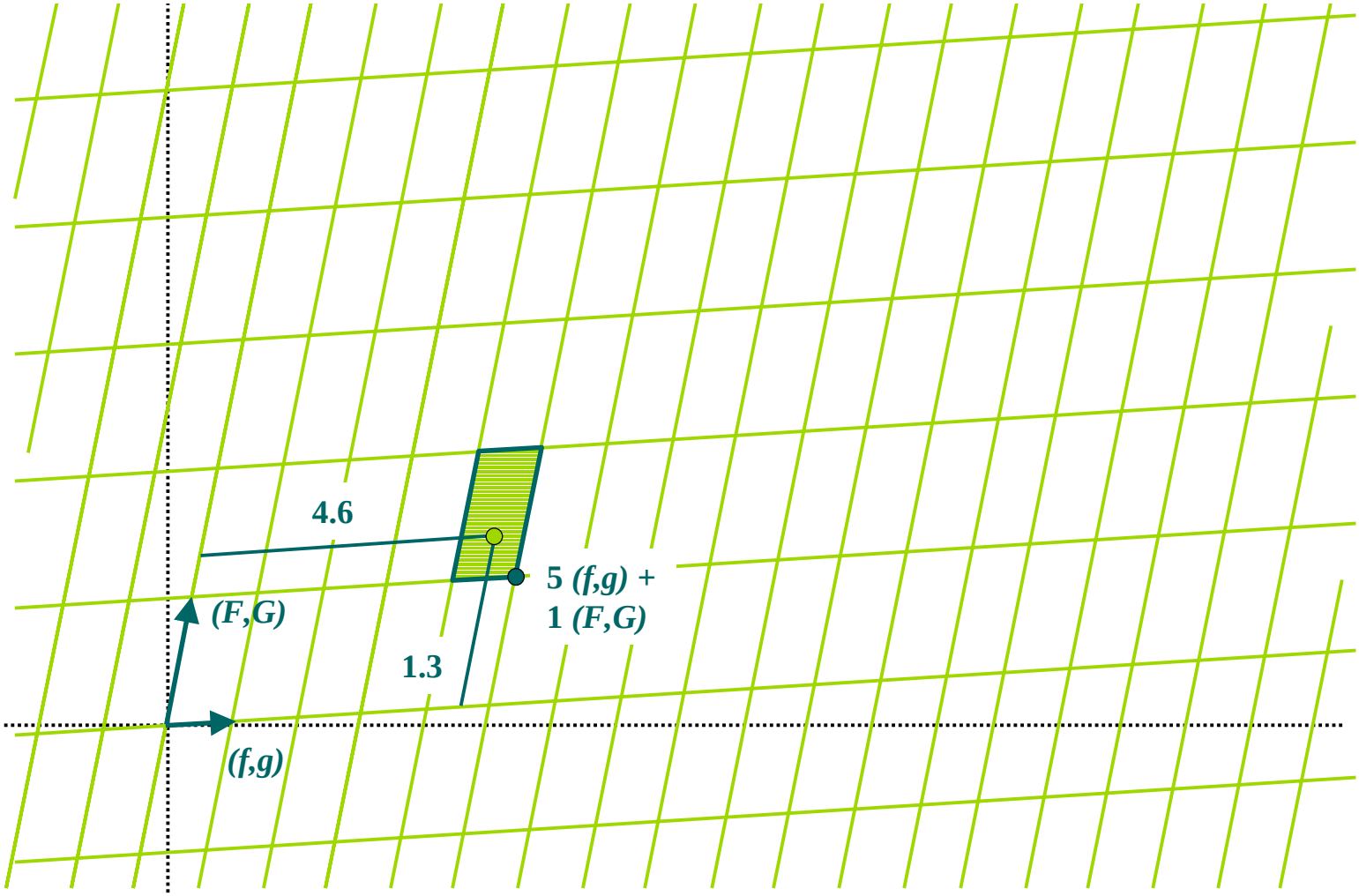
$$L_{NTRU} = \begin{bmatrix} 1 & h \\ 0 & q \end{bmatrix}$$

- $h = g/f \bmod q$
- so $(f, g) \in L_{NTRU}$
  - know small vector, but not entire basis

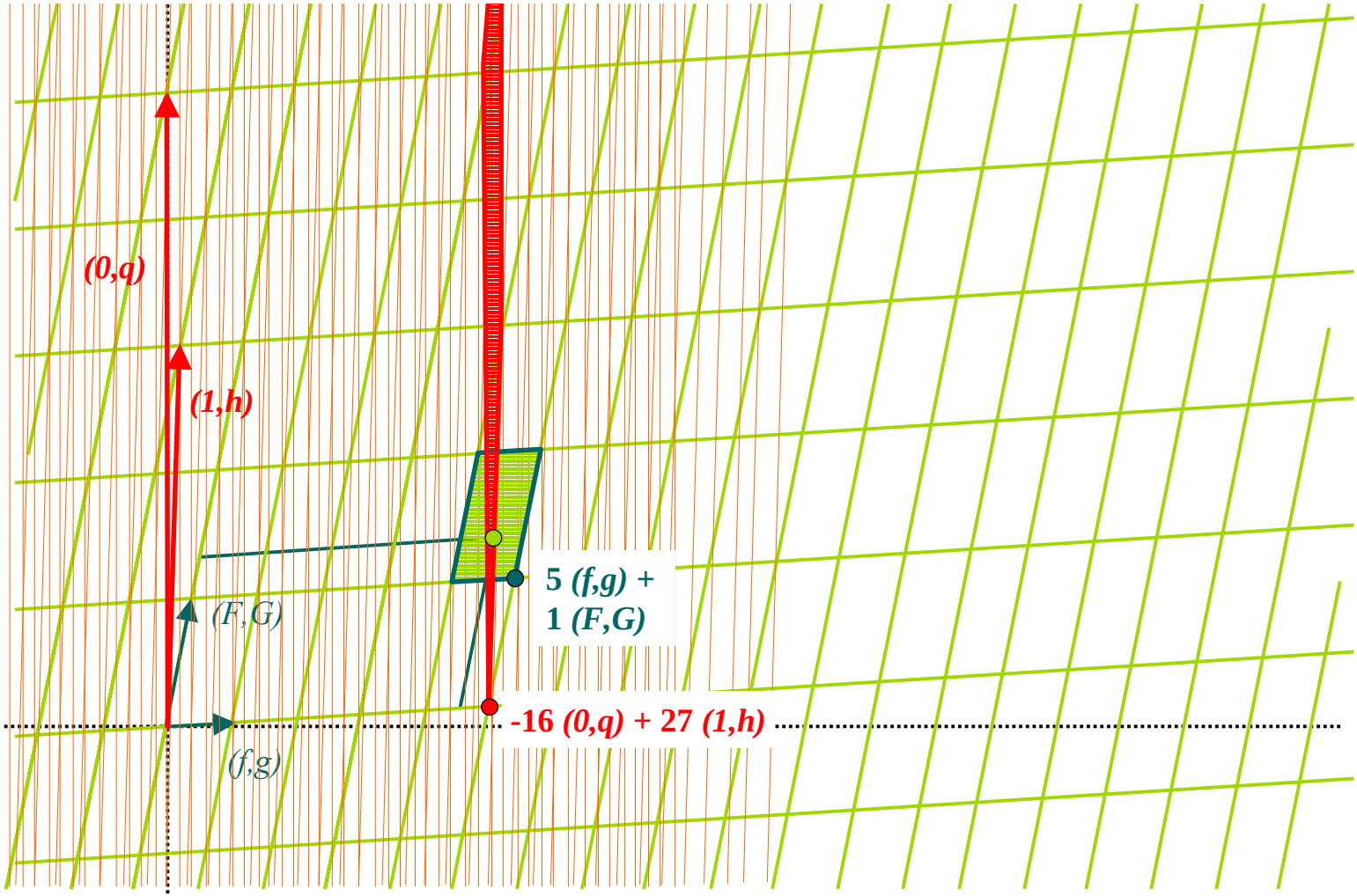
NTRUSign Overview

- Lattice described by public key *h*
- Signer knows complete good basis for the lattice derived from two short polynomials *f*, *g*
- Signing:
  - Given message digest *m*, find (*s*, *t* = *s h*), a point in NTRU lattice very close to
    (0, *m*).
  - Signature is *s*.
- Verification:
  - Check that (*s*, *s h*) is very close to (0, *m*)

NTRUSign in pictures



NTRUSign in pictures



Keygen (1): Finding a Unimodular Matrix

- Want to find a,b s.t.

$$\det \begin{bmatrix} f & g \\ a & b \end{bmatrix} = 1.$$

- i.e. $fb - ag = 1 \bmod X^N-1$
- Solve using resultants:
  - $\alpha_1 f + \beta_1(X^N-1) = \boldsymbol{R}_1$
  - $\alpha_2 g + \beta_2(X^N-1) = \boldsymbol{R}_2$
  - $u \boldsymbol{R}_1 + v \boldsymbol{R}_2 = 1$
  - $u \alpha_1 f + v \alpha_2 g = 1 \bmod X^N-1$

Keygen (2): Producing the NTRU Lattice

$$\det\begin{bmatrix} f & g \\ a & b \end{bmatrix} = 1$$

$$\det\begin{bmatrix} f & g \\ qa & qb \end{bmatrix} = q$$

$$\det\begin{bmatrix} f & g \\ F & G \end{bmatrix} = q$$

Keygen (3): Making F, G small

$$x \boxed{f} = (q\ a)$$

$$x = (q\ a) \boxed{\alpha_1} \frac{1}{\boldsymbol{R}_1}$$

- For $N = 251$, typically $||f, g|| = 11$, $||F, G|| = 45$

Signing & Verification

- Use full basis $\begin{pmatrix} f & g \\ F & G \end{pmatrix}$, inverse $\frac{1}{q}\begin{pmatrix} G & -g \\ -F & f \end{pmatrix}$
- message $\xrightarrow{hash}$ (0, *m*)
- If basis for entire lattice is ***B***, then signing is:
  (*s*, *t*) = ***B*** * round (***B***$^{-1}$ * (0, *m*))
- Transmit *s*.
- Verifying:
  - calculate *t* = *s***h* mod *q*.
  - make sure ||*s*||, ||*m*-*t*|| are small (< NormBound)

Security Analysis

- Direct forgery = solving appr-CVP in NTRU lattice
- Transcript analysis:
  - No chosen message attack in RO model by definition
    - RO maps H(m) to $\{-q/2, q/2\}^N$.
  - If message was random within ball of radius $\mathrm{NormBound}$, transcript could not leak information
  - Transcript is

    $$s = d * f + D * F \quad \text{where}$$

    - *d, D* are $\{-1/2, 1/2\}^N$
    - *d, D* slightly constrained: *s* must have integer coefficients.
  - In low dimension, leaks information about geometry of lattice; in high dimension, appears to require impractically long transcripts ($> 10^9$).
    - Further details to appear in next version of preprint

Performance of New Scheme (provisional)

- NTRUSign-251 on 800Mhz Pentium III Win 2k Visual C++ (no assembler)
  - 2000 sigs/sec
  - 3300 verifications/sec
- Compare:
  - RSA 1024 (MIRACL, Mike Scott)
    - Sign: 105/sec, Verify: 2200/sec
  - ECC over GF (2^{163}) (Hankerson, Hernandez, Menezes)
    - Random curves: 616 point multiplies/sec, ~ 616 signs/sec, ~528 verifies/sec
    - Koblitz curves: 1025 point multiplies/sec, ~ 1025 signs/sec, ~880 verifies/sec
- on 16 MHz 8051 without coprocessor
  - < 200ms for 1 signature
  - < 180ms for 1 verification
  - RSA 420 ms for signature ***with*** coprocessor; ECC 120 ms for signature ***with*** coprocessor

Further information

- Preprint available from http://www.ntru.com
- New Challenge problems also posted