SOLILOQUY
and cyclic structure in lattice cryptography

Bristol April 13th – 14th, 2015

dan.shepherd@cesg.gsi.gov.uk

SOLILOQUY

SOLILOQUY
and cyclic structure in lattice cryptography

- The design, knapsacks, cyclic lattices
- Features and weaknesses
- Can the design be rescued?
- Cryptography with *bi*-cyclic lattices

[Campbell, Groves, S, 2014]

SOLILOQUY
and cyclic structure in lattice cryptography

Key Encapsulation

share a secret value

use straightforward number-theory

quantum-safe

Motivating example : Cocks-RSA,
depends on hardness of factorising large composites,
but known not to be quantum-safe [Shor '94]

SOLILOQUY
and cyclic structure in lattice cryptography

Integer Knapsacks

subset-sum

n ‘rocks’ r_i and a modulus p

a (discrete) distribution for ‘error’ e

$$S = \Sigma\, e_i.r_i \quad (\mathrm{mod}\ p)$$

secret trapdoor?

SOLILOQUY
and cyclic structure in lattice cryptography

49677538431172

96790521832932

19693780780716

...

94867590111780

80437018419267

$p = 106801446087337$

SOLILOQUY
and cyclic structure in lattice cryptography

-1	0	0	...	0	0	49677538431172
0	-1	0	...	0	0	96790521832932
0	0	-1	...	0	0	19693780780716
						...
0	0	0	...	-1	0	94867590111780
0	0	0	...	0	-1	80437018419267
0	0	0	...	0	0	106801446087337
						29704705035121

SOLILOQUY
and cyclic structure in lattice cryptography

-1	0	0	...	0	0	49677538431172
0	-1	0	...	0	0	96790521832932
0	0	-1	...	0	0	19693780780716
						...
0	0	0	...	-1	0	94867590111780
0	0	0	...	0	-1	80437018419267
0	0	0	...	0	0	106801446087337
0	-1	1	...	0	0	0

SOLILOQUY
and cyclic structure in lattice cryptography

$$S = \Sigma\, e_i.r_i \quad (\mathrm{mod}\ p)$$

$$S = e \quad (\mathrm{mod}\ \Lambda)$$

SOLILOQUY
and cyclic structure in lattice cryptography

Public key compression:

$$
\begin{array}{cccccccl}
-1 & 0 & 0 & \ldots & 0 & 0 & c^{1} & \pmod{p} \\
0 & -1 & 0 & \ldots & 0 & 0 & c^{2} & \pmod{p} \\
0 & 0 & -1 & \ldots & 0 & 0 & c^{3} & \pmod{p} \\
 & & & & & & \ldots & \\
0 & 0 & 0 & \ldots & -1 & 0 & c^{35} & \pmod{p} \\
0 & 0 & 0 & \ldots & 0 & -1 & c^{36} & \pmod{p} \\
\underline{0} & \underline{0} & \underline{0} & \underline{\ldots} & \underline{0} & \underline{0} & \underline{\quad} & \underline{p \qquad .}
\end{array}
$$

$$S = \Sigma\, e_i.c^i \pmod{p}$$

SOLILOQUY
and cyclic structure in lattice cryptography

The lattice is cyclic:

$$
\begin{matrix}
1 & -c^{-1} & 0 & \ldots & 0 & 0 & 0 \\
0 & 1 & -c^{-1} & \ldots & 0 & 0 & 0 \\
0 & 0 & 1 & \ldots & 0 & 0 & 0 \\
 & & & \ldots & & & \\
0 & 0 & 0 & \ldots & 1 & -c^{-1} & 0 \\
0 & 0 & 0 & \ldots & 0 & 1 & -c^{-1} \\
0 & 0 & 0 & \ldots & 0 & 0 & p
\end{matrix}
$$

SOLILOQUY
and cyclic structure in lattice cryptography

If m is a prime number...

fix attention to the hyperplane $\Sigma e_i = 0$,

and the relevant lattice becomes an ideal.

$n = \varphi(m)$

$K = Q[\zeta]$, m^{th} cyclotomic field, degree n

$O = Z[\zeta]$, its ring of integers

$\Lambda = (\zeta - c).O + p.O$

Structure of m^{th} cyclotomic field:

m can be any small integer

K has Galois group (Z/mZ)*, order n

- These are morphisms of the form $\zeta \rightarrow \zeta^j$
- Complex conjugation "†" is $\zeta \rightarrow \zeta^{-1}$

"Trace" means sum over Galois group

SOLILOQUY
and cyclic structure in lattice cryptography

The field K naturally has a Q-bilinear form:

$$\mathrm{Trace}[\, x.y^{\dagger} \,]$$

So really it is an Inner Product Space.

"Every number has a length,
Every ideal is a lattice"

Nice feature that ideals of cyclotomic fields (Galois extensions) are naturally lattices; there is no need to construct an embedding, or worry about bases.

SOLILOQUY
and cyclic structure in lattice cryptography

Trapdoor – how to decode?

α in O “random” private key

$\Lambda = \alpha.O = (\zeta - c).O + p.O$; so $p = \mathrm{Norm}(\alpha)$

The public key forms a Principal Ideal.

(E.g. m prime) Decoding trivial for e in O if

- $\Sigma e_i = 0$;
- $\Sigma|e_i|. < n / \max_{ij} \mathrm{Trace}[(\zeta^i-\zeta^j)/\alpha]$

SOLILOQUY
and cyclic structure in lattice cryptography

"SOLILOQUY"

public key is <u>one</u> number,
consisting of <u>one</u> prime,
to be 'factored' in a (fixed) cyclotomic ring;
underlying lattice is an O-module,
free on <u>one</u> generator

Cf [Smart, Vercauteren, 2010]

CESG

SOLILOQUY
and cyclic structure in lattice cryptography

H I M R

Features:

- ✓ Meets my requirements for ‘simplicity’
- ✓ Triviality in the class group ensures that no quantum attack can take advantage of that particular abelian group
- ❖ Doesn’t have any proper security proof
- ❖ In the same way that RSA may be easier than factoring, so breaking SOLILOQUY may be easier than finding a generator for Λ
- ➢ Does finding a (any) generator for Λ actually break the crypt?
- ➢ Is the design quantum-safe?

Maximal Real Subfield:

There is an efficient classical algorithm for recovering α in O from $\alpha.\alpha^\dagger$ in the maximal real subfield O^+, so we may as well focus on the smaller-dimension problem of recovering $\alpha.\alpha^\dagger$. [Howgrave-Graham, Syzdlo, 2004]

Every unit of O has the form $\zeta^j.\xi$, where ζ is the root of unity and ξ in O^+ is real (at least when m is a prime power).

O^+ has class number h^+ which is "probably" 1 (PID).

[Washington, 1996]

SOLILOQUY
and cyclic structure in lattice cryptography

Log-unit lattice:

The (real) units of O form a multiplicative group.

Focus on the torsion-free part (don't distinguish ξ, $-\xi$, $\zeta^j.\xi$).

Their logs form an additive group, a lattice of rank n/2-1.

The (logs of the) <u>cyclotomic units</u> constitute a sublattice (but in fact the whole lattice if $h^+=1$).

This has a well-known easily found 'nice' basis, with a near-orthogonal parallelepiped fundamental domain.

Cf [Cramer, Ducas, Peikert, Regev, 2015]

(Real) Cyclotomic Units (case m prime):

(It gets messier if m is not at least a prime power.)

- -1 generates 2-torsion part;
- A basis for torsion-free part is given by

$$\frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$$

for a in {2,3,...,(m-1)/2}.

SOLILOQUY
and cyclic structure in lattice cryptography

'Nice' basis for log-unit lattice given by

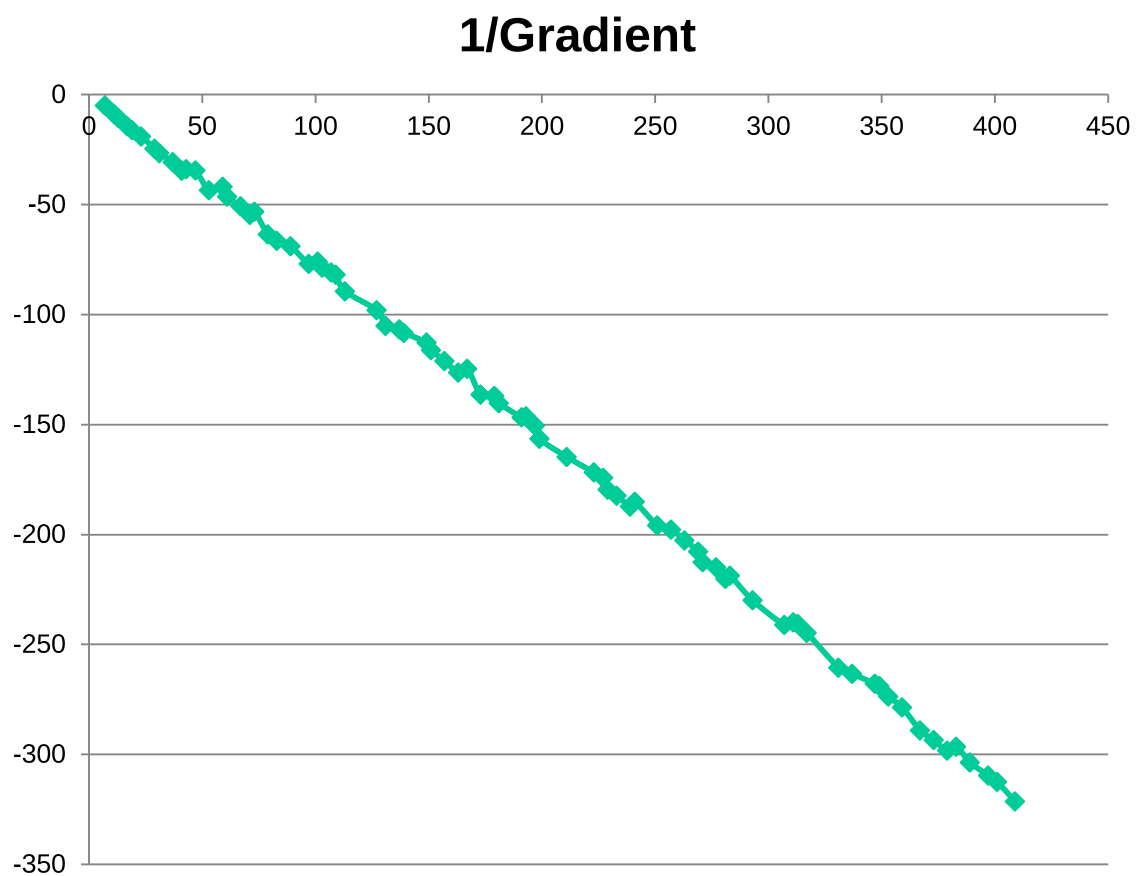
$$\log_e \left| \frac{\sin(2ab\pi/m)}{\sin(2b\pi/m)} \right|$$

for b in [1..(m-1)/2], a in [2..(m-1)/2].

Examine the Gram-Schmidt cuboid fundamental domain of this basis, for increasing (prime) m:

- Follows the Geometric Series Assumption
- <u>Shortest side length</u> of cuboid <u>grows</u>

SOLILOQUY
and cyclic structure in lattice cryptography



SOLILOQUY
and cyclic structure in lattice cryptography

SOLILOQUY
and cyclic structure in lattice cryptography

- Assume (for example) that α is chosen from a (discrete) *Gaussian distribution*...
- Then the (n) coefficients of α are (approximately) *independent Normal*,
- So the (n/2) coefficients of $\alpha.\alpha^\dagger$ are *independent Exp*,
- So the coefficients of $\mathrm{Log}(\alpha.\alpha^\dagger)$ are *independent Gumbel*,
- Projected onto the span of the log-unit lattice (rank n/2-1), $\mathrm{Log}(\alpha.\alpha^\dagger)$ has coefficients with *constant* variance, independent of dimension n, and independent of variance of original Gaussian.
- $\mathrm{Log}(\alpha.\alpha^\dagger)$ lies in log-unit FD with probability 99.99999....%

- Find any gen of $(\zeta - c).\mathcal{O} + p.\mathcal{O}$
- Find any gen of $((\zeta+\zeta^{-1})-(c+c^{m-1})).\mathcal{O}^{+} + p.\mathcal{O}^{+}$

The Principal Ideal Problem is

efficiently solved

using a quantum algorithm!

[Eisenträger, Hallgren, Kitaev, Song, 2014]

[Campbell, Groves, S, 2014]

[Biasse, Song, (work in progress)]

SOLILOQUY
and cyclic structure in lattice cryptography

Can the design be rescued?

- Choose $\Lambda = \alpha.\mathcal{O}$, but with secret key γ in Λ <u>not</u> a generator
- Choose Λ <u>not</u> principal, but with some 'good' secret key γ in Λ

In any case, γ (and not α) would now provide the good quality parallelepiped for decoding.

- Find a cyclotomic field with an 'unpleasant' unit group.

I believe there aren't any...

What about *bi*-cyclic lattices?

Defn: A cyclic/bi-cyclic/tri-cyclic lattice is an O-module, free on 1/2/3 generators.

Example: $(f \quad g)$ in $\begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}$

q is a system parameter; h (mod q) is the public key;
g in coset f.h + q.O is secret.
Cf NTRU, Ring-LWE, etc.

CESG

SOLILOQUY
and cyclic structure in lattice cryptography

H I M R

Method:

Try to reduce the bi-cyclic case to the cyclic case.

Technique:

Embed Λ into a ring O' larger than O, so that it becomes an O'-module free on one generator.

Detail:

Choose non-square r in coset $h^2 + q.O$ and let $O' = O[\sqrt{r}]$.

SOLILOQUY
and cyclic structure in lattice cryptography

Keeping track of data:

$$\alpha_{\pm} := g \pm f\sqrt{r} \ \text{ in } \ O'$$

$$\beta := \alpha_{+}.\alpha_{-} = g^2 - r.f^2 \ \text{ in } \ q.O$$

$$\Lambda \rightarrow \Lambda_{\pm} := (h \pm \sqrt{r}).O + q.O$$

$$\alpha_{\pm}.O' \leq \Lambda_{\pm} \leq O'$$

CESG

SOLILOQUY
and cyclic structure in lattice cryptography

H I M R

SOLILOQUY

- Ring is O
- Ring is fixed and 'simple'
- $\Lambda = (\zeta - c).O + p.O$
- $\mathrm{Norm}(\Lambda) = p$
- $\Lambda = \alpha.O$
- α generates Λ
- PIP : $\Lambda \rightarrow \alpha$
- Simpler attack recovers $\alpha.\alpha^{\dagger}$ first

NTRU etc

- Ring is $O' = O[\sqrt{r}]$
- Ring 'contains' public key
- $\Lambda_{+} = (h + \sqrt{r}).O + q.O$
- $\mathrm{Norm}(\Lambda_{+}) = q$
- $\Lambda_{+} \geq \alpha_{+}.O'$
- α_{+} does <u>not</u> generate Λ_{+}
- Need to guess $\Lambda_{+}:\alpha_{+}.O'$
- Suffices to guess $\Lambda_{+}.\Lambda_{-}:\alpha_{+}.\alpha_{-}.O'$ but same as guessing β

SOLILOQUY
and cyclic structure in lattice cryptography

"Rescued" SOLILOQUY

- γ in Λ is 'short'
- Ring is fixed for all users
- Λ prime but not principal
- Norm(γ) a composite
- Modulus p (large) depends on private key
- Key generation not practical

NTRU etc

- α_+ in Λ_+ is 'short'
- Ring chosen depending on private key
- Λ_+ not principal
- Norm(α_+) irrelevant
- Modulus q (small) fixed in advance for all users
- Key generation efficient

SOLILOQUY
and cyclic structure in lattice cryptography

Conclusions

- Consider lattice crypt in algebraic setting as well as usual geometric cryptanalysis
- SOLILOQUY (and similar FHE schemes) not quantum-safe
- Quantum PIP solver implements “Shor’s algorithm” in context of an abelian subgroup hidden in a <u>continuous</u> group (no “security through continuity” argument!)
- To “rescue” SOLILOQUY, design something bi-cyclic
- Bi-cyclic lattices seem to offer superior security, while still compressing the public key; consider tri-cyclic lattices, etc.

SOLILOQUY
and cyclic structure in lattice cryptography

?

SOLILOQUY
and cyclic structure in lattice cryptography

How does the quantum PIP algorithm work? (Sketch)

Control-space variables k (one dimension)
and $\underline{v}$ (n/2-1 dimensions)

$$k,v \rightarrow k,v, \text{Fingerprint}((\Lambda.\Lambda^{\dagger})^k * \text{Exp}(\underline{v}))$$

This 'hides' the subgroup given by

$$\begin{matrix} 1 & -\text{Log}(\alpha.\alpha^{\dagger}) \\ 0 & \text{Log}(\xi) \end{matrix}$$

Analysis of the QFT yields the units ξ and the generator $\alpha.\alpha^{\dagger}$.