SOLILOQUY: A Cautionary Tale

P. Campbell
M. Groves
D. Shepherd

CESG

Outline

We describe SOLILOQUY, a lattice-based primitive designed at CESG in 2007.

SOLILOQUY has several nice properties; in particular the public key is very compact for a lattice system.

We believe that SOLILOQUY is classically secure but were surprised to discover a potential quantum attack.

We sketch this attack, which we believe may be the first on a lattice-based PKC scheme.

Conclusions and further research.

SOLILOQUY

Some mathematical background

Let n be a prime and ζ a primitve n^{th} root of unity.

Let $K = \mathbb{Q}(\zeta)$ be the n^{th} cyclotomic field and $\mathcal{O} = \mathbb{Z}[\zeta]$ its ring of integers. Elements of $\mathcal{O}$ are monic polynomials of the form $\alpha = \sum_{i=1}^{n} a_i \zeta^i \in \mathcal{O}$.

For primes $p \equiv 1 \bmod n$ the principal ideal $p\mathcal{O}$ decomposes into a product of prime ideals $p\mathcal{O} = \prod_{i=1}^{n-1} \mathcal{P}_i$.

The prime ideals $\mathcal{P}_i$ are conjugates with norm $N(\mathcal{P}_i) = p$ and $Gal(K/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^{\times}$. They have a simple two-element representation $\mathcal{P} = p\mathcal{O} + (\zeta - c_i)\mathcal{O}$, where the c_i are n^{th} roots of unity in $GF(p)$.

We will be interested in the value $c = 2^{(p-1)/n} \mod p$ and its prime ideal $\mathcal{P} = p\mathcal{O} + (\zeta - c)\mathcal{O}$.

Public and private keys

A candidate private key will be a “small” ring element $\alpha = \sum_{i=1}^{n} a_i \zeta^i \in \mathcal{O}$.

These are generated randomly (by sampling the coefficients from a discrete Gaussian distribution) and tested until we find an α such that $p = N(\alpha)$ is prime and $c \not\equiv 1 \bmod p$. Conjugate to get into the required form $\alpha\mathcal{O} = p\mathcal{O} + (\zeta - c)\mathcal{O}$.

Then set the SOLILOQUY private key to be α and its corresponding public key to be p.

The crypto primitive

For crypto applications we will want to define maps to encrypt and decrypt data.

We encode a ring element ϵ (plaintext or ephemerals) into an integer z (ciphertext) using the public key p:

$$\epsilon := \sum_{i=0}^{n-1} e_i \zeta^i \mapsto \sum_{i=0}^{n-1} e_i c^i \bmod p =: z$$

We can recover a “small” ϵ from z and the private key α by simply rounding:

$$\epsilon = z - \lceil z\alpha^{-1} \rfloor \cdot \alpha.$$

SOLILOQUY as a GGH-type lattice scheme

Private / public lattice basis matrices with $H = HNF(C)$:

$$C = \begin{bmatrix} a_0 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & & a_{n-3} & a_{n-2} \\ \vdots & & \ddots & \\ a_1 & & a_{n-1} & a_0 \end{bmatrix}, H = \begin{bmatrix} 1 & 0 & \dots & 0 & -c^{n-1} \\ 0 & 1 & & 0 & -c^{n-2} \\ \vdots & & \ddots & & \\ 0 & 0 & & 1 & -c \\ 0 & 0 & & 0 & p \end{bmatrix}$$

Since α is small, C will be a reduced basis for the lattice and decryption is Babai's rounding algorithm.

The public key H can be reconstructed from just p, which is very compact for a lattice cryptosystem.

(Note: Smart-Vercauteren also used this HNF construction in their 2009 FHE scheme.)

Security

The security of SOLILOQUY can be analysed via the difficulty of two well known hard problems.

CVP. Classical CVP security via LBR is well understood. There is no known significant (exponential) quantum speed-up.

PIP: Given a representation of a principal ideal $\mathcal{I}$ of $\mathcal{O}$, compute a small generator α of $\mathcal{I}$. The known (at that time) classical and quantum algorithms are only practical for number fields of small, fixed degree.

We believed for several years that since SOLILOQUY used large degree fields it should be quantum resistant.

Outline of a quantum attack

Some simplifying assumptions

Likely true for our specific situation but not in general: We know the generators for the unit group. We can recover α from *any* generator of $\alpha\mathcal{O}$. It is enough to recover $\alpha \cdot \alpha^*$ in the ring of integers $\mathcal{O}' = \mathbb{Z}[\zeta + \zeta^{-1}]$ of $K' = \mathbb{Q}(\zeta + \zeta^{-1})$.

We thus re-cast the problem as: Given a generating set $u_1, \ldots, u_{r-1}$ of the unit group $\mathcal{O}^\times$ recover any generator of the principal ideal $\alpha\mathcal{O}$ in the ring of integers $\mathcal{O}$ of a totally real field of degree r.

This special case turns out to be tractable. Our approach is similar the work of Hallgren and co-authors on unit groups and related number-theoretic problems.

SOLILOQUY as a hidden lattice problem

The embedding $\log(\omega) = (\log(|\sigma_0(\omega)|), \ldots, \log(|\sigma_{r-1}(\omega)|))$ maps $\mathcal{O}^\times$ to a rank $r-1$ lattice $\Lambda = \log(\mathcal{O}^\times)$. Encode α as the rank r lattice: $\Lambda_\alpha = \begin{bmatrix} -1 & \log(\alpha) \\ 0 & \Lambda \end{bmatrix}$.

Hide Λ_α by defining a function $F : \mathbb{Z} \times \mathbb{R}^r \to \mathbb{R}^r$, such that $F(k, v) = F(k', v')$ iff $(k, v) \equiv (k', v') \bmod \Lambda_\alpha$.

Restrict the input domain to $G \subset \mathbb{Z} \times \mathbb{R}^r$ where

$$G = \left\{ (k, v) \in \mathbb{Z} \times \mathbb{R}^r : \sum_{i=0}^{r-1} v_i = -k \log(N(\alpha.\mathcal{O})) \right\}$$

and set

$$F(k, v) = \exp(v) \cdot (\alpha\mathcal{O})^k.$$

The quantum algorithm

1**. For an input $(k, v) \in G$ compute a "quantum fingerprint" $\psi_{(k,v)}$ representing the lattice $F(k, v)$.

2**. Discretise and bound G and form the superposition

$$\sum_{(k,v)\in G} |k, v, 0\rangle \mapsto \sum_{(k,v)\in G} \left|k, v, \psi_{(k,v)}\right\rangle$$

3. Take a QFT over G and measure the third register to obtain an approximate basis for the dual lattice Λ_α^*.

4. Iterate the previous steps to produce many samples close to Λ_α^*.

5. Use classical LBR to compute an approximate basis for Λ_α and hence α. (Requires sufficient precision.)

Fingerprints and binning

Lattice fingerprints

Our “quantum fingerprint” will be a model for the superpositon of the short vectors in a given lattice.

Let B be a Gram-Schmidt lattice basis matrix in $\mathbb{R}^n$ and let $l \in \mathbb{R}$ be some fixed length. We use an ‘enumeration’ map $\phi : [0, l) \quad \rightarrow \quad \mathbb{Z}^n$ depending on n, B, and l, which can be inverted at integer points (to facilitate reversible quantum computation).

Let $C_n(B, l) := \{\ \phi(x)\ :\ x \in [0, l) \cap \mathbb{Z}\ \}$. This is a discretised model for $E_n(\rho) := Ball_{n,\rho} \cdot B^{-1}$ in the sense that that it fits within an ellipsoid $E_n(\rho + \varepsilon)$ and covers all the integer points in $E_n(\rho - \varepsilon)$.

$$E_n(\rho - \varepsilon) \cap \mathbb{Z}^n \subseteq C_n(B, l) \quad \subseteq \quad E_n(\rho + \varepsilon) \cap \mathbb{Z}^n.$$

Let O be the isometry between the Gram-Schmidt and the “natural” bases for the lattice. Then $\mathbf{v} \in C_n(B, l)$ indexes $\mathbf{v} \cdot B$, a short vector in the Gram-Schmidt basis corresponding to the natural vector $\mathbf{v} \cdot B \cdot O$.

We use another lattice to partition up natural space into cells or “bins”. Vector $\mathbf{v} \cdot B \cdot O$ will be replaced by the label $\mathbf{u}$ of its bin, reducing precision by a carefully-chosen scaling factor q. Define *Simple binning* as:

$$\mathbf{u} = \theta_B(\mathbf{v}) := \lceil q \cdot \mathbf{v} \cdot B \cdot O \rfloor.$$

(The *Randomised* variant $\theta_{R,\mathbf{w},B}(\mathbf{v}) := \lceil q \cdot \mathbf{v} \cdot B \cdot O \cdot R + \mathbf{w} \rfloor$ is preferable, because over many random choices R and $\mathbf{w}$, the likelihood of two vectors going into the same bin depends *only* on their separation relative to q.)

Our (simple) quantum fingerprint generator computes

$$|k,v\rangle\,|0\rangle \;\mapsto\; \frac{1}{\sqrt{\lceil l\rceil}}\sum_{x=0}^{\lceil l\rceil-1}|k,v\rangle\left|\theta_{B(k,v)}(\phi(x))\right\rangle$$

The pure state

$$\left|\psi_{(k,v)}\right\rangle \;:=\; \frac{1}{\sqrt{\lceil l\rceil}}\sum_{x=0}^{\lceil l\rceil-1}\left|\theta_{B(k,v)}(\phi(x))\right\rangle$$

is called the (simple) *quantum fingerprint* of (k,v).

The coherent randomised version is:

$$\left|\psi'_{(k,v)}\right\rangle \;:=\; \frac{\sum_R\sum_{\mathbf{w}}\sum_{x=0}^{\lceil l\rceil-1}|R\rangle\,|\mathbf{w}\rangle\left|\theta_{R,\mathbf{w},B(k,v)}(\phi(x))\right\rangle}{\sqrt{\#_R\cdot\#_{\mathbf{w}}\cdot\lceil l\rceil}}$$

The fingerprint structure allows us to define a *fidelity* between two different descriptions

$$Fid(\ (k,v),(k,v)'\ )\ \ :=\ \left\langle \psi'_{(k,v)} \mid \psi'_{(k,v)'} \right\rangle .$$

A fidelity of 1 would indicate that $C(B,l)\cdot B\cdot O$ and $C(B',l)\cdot B'\cdot O'$, activate exactly the same set of bins (for every $R,\mathbf{w}$ binning strategy) and so lattices must be very similar, or identical. When the two lattices are ‘essentially different’, there is no reason to expect significant overlap in any region, and so the fidelity should be small.

The idea is that, for correctly chosen (l,q), the numerical instablity arising from computing $F(k,v)$ is removed by the binning strategy, as (real, infinite) $F(k,v)$ is replaced with (discrete, bounded) $\psi_{(k,v)}$.

Open questions and conclusions

We abandoned the development of SOLILOQUY in early 2013 and are not recommending it for any real-world applications.

However there are several interesting ideas presented here which might benefit from further study:

* A compact public key for lattice PKC. See also Smart-Vercauteren's application to FHE.

* This may be the first quantum attack on a lattice-based PKC protocol. However ours is a very special case (cyclotomics) that does not easily generalise.

* Other approaches to lattice fingerprints are possible. Hallgren et. al. have recently suggesed using multiple Gaussian sampling.

Conclusion

We have outlined one approach to lattice fingerprints which we believe could be combined with a quantum PIP algorithm to give an attack on SOLILOQUY.

Designing quantum-safe cryptography is difficult. It took us several years to develop SOLILOQUY and several more to assess its potential quantum resistance.

At this time, when many novel types of quantum-safe cryptography are being proposed, the work of ETSI and others will be very important in ensuring these receive a thorough and independent assessment.