SCHLOSS DAGSTUHL
Leibniz-Zentrum für Informatik

Quantum Cryptanalysis
Dagstuhl Seminar 13371
September 8–13, 2013

On quantum versions of the McEliece cryptosystem

Markus Grassl

joint work in progress with Fred Ezerman

National University of Singapore

The Main Goal

send *quantum* messages securely over a public quantum channel using some public key system

main references:

- Li Yang, Quantum public-key cryptosystem based on classical NP-complete problem, arXiv:quant-ph/0310076
- H. Fujita, Quantum McEliece public-key cryptosystem, *Quantum Information & Computation*, 12(3&4):181–202 (2012)
- Li Yang and Min Liang, A note on quantum McEliece public-key cryptosystem arXiv:1212.0725 [quant-ph]

Quantum Information

(pure) quantum state (qudit):

$|\psi\rangle \in \mathbb{C}^d$, normalized vector

quantum register:

$|\psi\rangle \in (\mathbb{C}^d)^{\otimes n} = \mathbb{C}^d \otimes \ldots \otimes \mathbb{C}^d$

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \{0,\ldots,d-1\}^n} \alpha_{\boldsymbol{x}} |\boldsymbol{x}\rangle = \sum_{\boldsymbol{x} \in \{0,\ldots,d-1\}^n} \alpha_{\boldsymbol{x}} |x_1, x_2, \ldots, x_n\rangle$$

in particular if $d = p^m = q$, use $\mathbb{F}_q^n$ to label the basis states

operations/errors:

$$X^\alpha = \sum_{x \in \mathbb{F}_q} |x + \alpha\rangle\langle x| \qquad \text{and} \qquad Z^\beta = \sum_{y \in \mathbb{F}_q} \omega_p^{\mathrm{tr}(\beta y)} |y\rangle\langle y|$$

$$\omega_p = \exp(2\pi i/p)$$

Quantum One-Time Pad

[P. O. Boykin & V. Roychowdhury, Optimal encryption of quantum bits, PRA **67**, 042317 (2003)]

informationally secure encryption of a quantum state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$:

- requires a private key with $m = 2n \log_2 d$ bit
- use the key k to choose (uniformly) one out of 2^m unitary matrices U_k that form a basis of the $d^n \times d^n$ matrices

$$\sum_k U_k |\psi\rangle\langle\psi| U_k^{-1} = \alpha \cdot I$$

- local operations $X^{a_1} Z^{b_1} \otimes \ldots \otimes X^{a_n} Z^{b_n}$ are sufficient

- does not require quantum storage, only simple local processing
- use any system for the key distribution (first generate/send the classical key, then the quantum message)
- does not allow to detect an eavesdropper

A First Proposal

[L. Yang, Quantum public-key cryptosystem based on classical NP-complete problem, quant-ph/0310076]

Let $G \in \mathbb{F}_q^{k \times n}$ be the public key of a classical McEliece system, and pick a random vector $\boldsymbol{e} \in \mathbb{F}_q^n$ of weight t.

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} |\boldsymbol{x}\rangle$$

$$\rightarrow \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} |\boldsymbol{x}G\rangle \qquad \text{encoding}$$

$$\rightarrow \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} |\boldsymbol{x}G + \boldsymbol{e}\rangle \qquad \text{artificial error}$$

Cryptanalysis I

Decoding/attacking the cipher state

$$|\psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}\rangle \longmapsto |\Psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}G + \boldsymbol{e}\rangle$$

- syndrome computation $\sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}G + \boldsymbol{e}\rangle|\boldsymbol{e}H^t\rangle \Longrightarrow$ classical decoding
- operators $X^{a_1} \otimes \ldots \otimes X^{a_n}$ commute with the error $\boldsymbol{e}$
  $\Longrightarrow$ measurement of $|\psi\rangle$ in X-basis is possible
- for $i \in \{1, \ldots, k\}$, let $\boldsymbol{b} \in \mathbb{F}_q^n$ be orthogonal to all rows $\boldsymbol{g}_j$, $j \neq i$ of G, and $\boldsymbol{b} \cdot \boldsymbol{g}_i = 1$
  $\Longrightarrow$ measurement of $Z^{b_1} \otimes \ldots \otimes Z^{b_n}$ on $|\Psi\rangle$ yields Z-measurement of the i-th qubit of $|\psi\rangle$ if $\boldsymbol{b} \cdot \boldsymbol{e} = 0$ ($\mathrm{tr}(\boldsymbol{b} \cdot \boldsymbol{e}) = 0$ suffices)

Two-fold Encryption

[Li Yang and Min Liang, A note on quantum McEliece public-key cryptosystem arXiv:1212.0725]

1. encrypt the state $|\psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}\rangle \longmapsto |\Psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}G + \boldsymbol{e}\rangle$

2. apply a Fourier transformation $H^{\otimes n}$ (additive group of $\mathbb{F}_q$)

$$H^{\otimes n}|\Psi\rangle = H^{\otimes n} \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}G + \boldsymbol{e}\rangle = (Z^{e_1} \otimes \ldots \otimes Z^{e_n})H^{\otimes n} \sum_{\boldsymbol{x}\in\mathbb{F}_q^k} \alpha_{\boldsymbol{x}}|\boldsymbol{x}G\rangle$$

$$= (Z^{e_1} \otimes \ldots \otimes Z^{e_n}) \sum_{\boldsymbol{y}\in\mathbb{F}_q^n} \beta_{\boldsymbol{y}}|y\rangle = |\Psi'\rangle$$

3. encrypt the state $|\Psi'\rangle$ using another (classical) McEliece instance

$$|\Psi''\rangle = (Z^{e_1} \otimes \ldots \otimes Z^{e_n}) \sum_{\boldsymbol{y}\in\mathbb{F}_q^n} \beta_{\boldsymbol{y}}|\boldsymbol{y}G' + \boldsymbol{e'}\rangle$$

Using Quantum Codes

[H. Fujita, Quantum McEliece public-key cryptosystem, QIC, 12(3&4):181–202 (2012)]

private key:

- quantum (stabilizer) code $\mathcal{C} = [\![n, k, d \geq 2t+1]\!]_q$ with an efficient decoding algorithm for at least t errors
- scrambling of the code using a permutation π of the n qudits

public key:

- standard form of the scrambled quantum code $\mathcal{C}^\pi$ that allows efficient encoding, given as a stabilizer matrix of size $(n-k) \times n$ over $\mathbb{F}_{q^2}$
- encode a quantum state $|\psi\rangle \in (\mathbb{C}^q)^{\otimes k}$ and introduce random errors $X^a Z^b$ at t random positions

Cryptanalysis II

- there are $\binom{n}{t}(q^2-1)^t$ errors of weight t
- syndrome-based decoding of additive/$\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^2}$
- (classical) decoding only needs to find the "closest coset"
- decoding quantum codes is also NP-hard
  [M.-H. Hsieh and F. Le Gall, NP-hardness of decoding quantum error-correction codes, PRA 83, 052331 (2011)]
- measuring *logical* operators is possible if they commute with the error

Using CSS Codes

[H. Fujita, Quantum McEliece public-key cryptosystem, QIC, 12(3&4):181–202 (2012)]

private key:

- a CSS code $\mathcal{C} = [\![n, k = k_1 - k_2, d \geq 2t+1]\!]_q$ based on nested classical codes $C_2 < C_1 = [n, k_1, d_1 \geq 2t_1 + 2]_q$ with $C_2^\perp = [n, n-k_2, d_2^\perp \geq 2t_2 + 1]_q$ with efficient decoding algorithms for C_1 and $C_2^\perp$.
- scrambling of the code using a permutation π of the n qudits

public key:

- generator matrix $G_1 = \binom{G_2}{G_{12}}$ for C_1^π with G_2 generating C_2^π
- $$|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} |\boldsymbol{x}\rangle \longmapsto \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} \sum_{\boldsymbol{y} \in \mathbb{F}_q^{k_2}} |\boldsymbol{y}G_2 + \boldsymbol{x}G_{12}\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^k} \alpha_{\boldsymbol{x}} |C_2 + \boldsymbol{x}G_{12}\rangle$$
- add t_1 random X-errors and t_2 random Z-errors

Cryptanalysis III

- separate decoding of X- and Z-errors
  $\Longrightarrow \binom{n}{t_i}(q-1)^{t_i}$ errors of weight t_i (compared to $\binom{n}{t}(q^2-1)^t$)
- decoding CSS codes is also NP-hard [Fujita]
- potentially smaller public key:
  generator matrix of size $k_1 \times n$ over $\mathbb{F}_q$ compared to a
  stabilizer matrix of size $(n-k) \times n$ over $\mathbb{F}_{q^2}$ (or $(n-k) \times 2n$ over $\mathbb{F}_q$)
- Fujita proposes to use CSS codes based on binary expansion of generalised Reed-Solomon (GRS) codes, as there are efficient decoding algorithms for the codes and their duals

Encrypting Classical Messages

[H. Fujita, Quantum McEliece public-key cryptosystem, QIC, 12(3&4):181–202 (2012)]

- use the first qubit as a flag to indicate quantum/classical messages
- instead of encoding a message $\boldsymbol{m} \in \mathbb{F}_q^k$ as basis state $|\boldsymbol{m}\rangle$, pick a random string $\boldsymbol{r} \in \mathbb{F}_q^k$ and encode m_i in the basis $\mathcal{B}_{r_i}$, where $\mathcal{B}_j$ are MUBs; for qubits: $|\boldsymbol{r}\rangle \otimes (H^{r_1}|m_1\rangle) \otimes \ldots \otimes (H^{r_k}|m_k\rangle)$

- there is some chance to measure the flag qubit correctly
- when classical messages are encoded as basis states, phase errors can be ignored (but might yield information about eavesdropping)
- the proposed randomized encoding doubles the message length, but now phase errors have some effect

Scrambling CSS Codes

in addition to permutations, we can apply local Clifford operations to the code

- CSS-structure is hidden to the attacker
- structural attack is potentially harder
- separate decoding of X- and Z-errors is no longer obvious

Open Problems:

1. Given a stabilizer code, decide whether it is a scrambled CSS code.
2. Given a scrambled CSS code, unscramble it.

Detecting CSS Codes

- general stabilizer matrix

$$S = (S_X | S_Z) \in \mathbb{F}_q^{(n-k)\times 2n} \quad \text{with } S_X S_Z^t - S_Z S_X^t = 0$$

- stabilizer matrix of a CSS code

$$S = \left(\begin{array}{c|c} S_X & 0 \\ 0 & S_Z \end{array} \right)$$

- transformation $S \mapsto TSP$ with $T \in \mathrm{GL}(n-k, q)$ and $P \in \mathrm{SL}(2, q)^n \rtimes S_n$, $\mathrm{SL}(2, q)$ acts on corresponding columns in S_X and S_Z
- for qubits, $6^n \times n!$ transformations P, but permutations can be ignored

Conclusions

- more or less straight-forward quantum analogue of McEliece's system
- some analysis of the security parameters exists (see [Fujita])

open questions:

- optimized decoding algorithms for quantum codes/non-binary codes
- complexity of detecting/descrambling CSS codes
- quantum attacks on classical/quantum McEliece
- detailed comparison of quantum McEliece with, e. g., classical McEliece and quantum one-time pad
- two-fold encoding and CSS encoding yield similar quantum circuits; are the schemes equivalent?

Further References

quantum one-time pad

- A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, Private Quantum Channels, Proceedings FOCS 2000, 547–553.
- F. Brandão and J. Oppenheim, Quantum One-Time Pad in the Presence of an Eavesdropper, Physical Review Letters **108**, 040504 (2012).
- D. W. Leung, Quantum Vernam Cipher, Quantum Information & Computation, 2(1):14–34 (2002).
- M. Mosca, A. Tapp, and R. de Wolf, Private Quantum Channels and the Cost of Randomizing Quantum Information, arXiv quant-ph/0003101.

quantum codes

- M. Grassl, M. Rötteler, and Th. Beth, Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes, International Journal of Foundations of Computer Science (IJFCS), Vol. 14, No. 5 (2003), pp. 757–775.