QcBits:
constant-time small-key code-based cryptography

Tung Chou

Technische Universiteit Eindhoven, The Netherlands

February 26, 2016, PQCrypto, Fukuoka, Japan

QcBits:
constant-time small-key code-based cryptography

QcBits:
constant-time small-key code-based cryptography

"Using QC-MDPC codes"

QcBits:
constant-time small-key code-based cryptography

QcBits:
constant-time small-key code-based cryptography

"Timing-attack-resistant"

QcBits:

constant-time small-key code-based cryptography

QcBits:

constant-time small-key code-based cryptography

"The software: QC-MDPC + Bitslicing"

platform	key-pair	encrypt	decrypt	reference	scheme
Haswell	784 192	82 732	1 560 072	**(new) QcBits**	KEM/DEM
	14 234 347	34 123	3 104 624	ACMTECS 2015	McEliece
Cortex-M4	140 372 822	2 244 489	14 679 937	**(new) QcBits**	KEM/DEM
	63 185 108	2 623 432	18 416 012	PQCrypto 2016	KEM/DEM
	148 576 008	7 018 493	42 129 589	PQCrypto 2014	McEliece

Cycle counts for key-pair generation, encryption, and decryption for 80-bit pre-quantum security. Numbers in RED are non-constant-time. Numbers in BLUE are constant-time.

Step 1: syndrome computation

- Matrix view:

$$\left(\begin{array}{c|c} & \\ h^{(0)} & h^{(1)} \\ & \end{array} \right) \begin{pmatrix} e^{(0)} \\ \\ e^{(1)} \end{pmatrix} \in \mathbb{F}_2^n$$

Step 1: syndrome computation

- Matrix view:

$$\left(\begin{array}{c|c} h^{(0)} & h^{(1)} \end{array} \right) \begin{pmatrix} e^{(0)} \\ \\ e^{(1)} \end{pmatrix} \in \mathbb{F}_2^n$$

- Polynomial view:

$$h^{(0)} e^{(0)} + h^{(1)} e^{(1)} \in \mathbb{F}_2[x]/(x^n - 1)$$

Step 1: syndrome computation

- Matrix view:

$$\left(\begin{array}{c|c} h^{(0)} & h^{(1)} \end{array} \right) \begin{pmatrix} e^{(0)} \\ \\ e^{(1)} \end{pmatrix} \in \mathbb{F}_2^n$$

- Polynomial view:

$$h^{(0)} e^{(0)} + h^{(1)} e^{(1)} \in \mathbb{F}_2[x]/(x^n - 1)$$

- `PCLMULQDQ` or barrel shifter

Step 2: counting number of unsatisfied parity checks

- Matrix view:

$$\begin{pmatrix} s^{(0)} & s^{(1)} \end{pmatrix} \left(\begin{array}{c|c} h^{(0)} & h^{(1)} \end{array} \right) \in \mathbb{Z}^{2n}$$

Step 2: counting number of unsatisfied parity checks

- Matrix view:

$$\begin{pmatrix} s^{(0)} & s^{(1)} \end{pmatrix} \left(\begin{array}{c|c} & \\ h^{(0)} & h^{(1)} \\ & \end{array} \right) \in \mathbb{Z}^{2n}$$

- Polynomial view:

$$\left(\tilde{h}^{(0)} s^{(0)}, \ \tilde{h}^{(1)} s^{(1)} \right) \in (\mathbb{Z}[x]/(x^n - 1))^2$$

Step 2: counting number of unsatisfied parity checks

- Matrix view:

$$\begin{pmatrix} s^{(0)} & s^{(1)} \end{pmatrix} \left(\begin{array}{c|c} h^{(0)} & h^{(1)} \end{array} \right) \in \mathbb{Z}^{2n}$$

- Polynomial view:

$$\left(\tilde{h}^{(0)} s^{(0)}, \ \tilde{h}^{(1)} s^{(1)} \right) \in (\mathbb{Z}[x]/(x^n - 1))^2$$

- barrel shifter + bitslicing

www.win.tue.nl/~tchou/qcbits/