BIG QUAKE

(BInary Goppa QUAsi–cyclic Key Encapsulation)

M. Bardet, E. Barelli, O. Blazy, R. Canto-Torres, A. Couvreur,
P. Gaborit, A. Otmani, N. Sendrier and J.-P. Tillich

INRIA, CNRS, École Polytechnique, Université de Limoges, Université de Rouen

NIST 1st standardization workshop, April 2018

Outline

1. Presentation
2. Security
3. Suggested parameters

General presentation

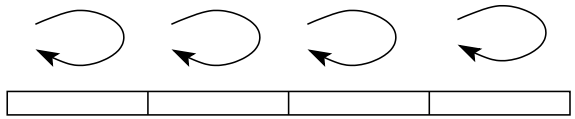
BIG QUAKE is a public key encryption scheme based on quasi–cyclic Goppa codes.

- based on binary Goppa codes (unbroken since 1978);

General presentation

BIG QUAKE is a public key encryption scheme based on quasi–cyclic Goppa codes.

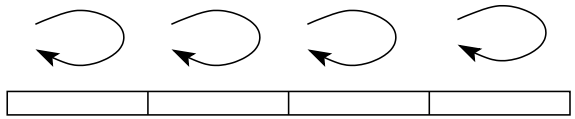
- based on binary Goppa codes (unbroken since 1978);
- uses quasi–cyclicity to reduce the key size:



General presentation

BIG QUAKE is a public key encryption scheme based on quasi–cyclic Goppa codes.

- based on binary Goppa codes (unbroken since 1978);
- uses quasi–cyclicity to reduce the key size:

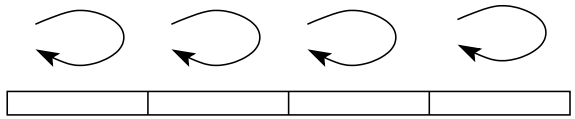


  - The cost of message recovery attack is mostly unchanged;

General presentation

BIG QUAKE is a public key encryption scheme based on quasi–cyclic Goppa codes.

- based on binary Goppa codes (unbroken since 1978);
- uses quasi–cyclicity to reduce the key size:

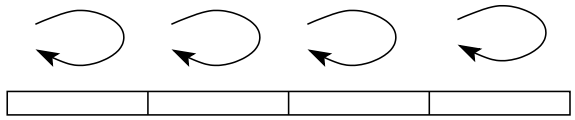


  - The cost of message recovery attack is mostly unchanged;
  - The cost of key-recovery attacks is reduced but remains significantly above that of message recovery attacks.

General presentation

BIG QUAKE is a public key encryption scheme based on quasi–cyclic Goppa codes.

- based on binary Goppa codes (unbroken since 1978);
- uses quasi–cyclicity to reduce the key size:



  - The cost of message recovery attack is mostly unchanged;
  - The cost of key-recovery attacks is reduced but remains significantly above that of message recovery attacks.
  - $\Rightarrow$ Same security as classic McEliece but with shorter keys (size divided by a factor between 3 and 19).

Semantic security

BIG QUAKE is proved to be OW IND–CPA in the Random Oracle Model under the following assumptions:

- Decoding ℓ–quasi–cyclic (ℓ–QC) codes is hard;
- Distingushing ℓ–QC Goppa codes from arbitrary ℓ–QC codes is hard.

Known attacks

Definition

Let $\mathscr{C}$ be an ℓ–QC code, we denote by $\mathscr{C}^{\sigma_\ell}$ the code:

$$\mathscr{C}^{\sigma_\ell} \stackrel{\text{def}}{=} \{\boldsymbol{c} \in \mathscr{C} \mid \sigma_\ell(\boldsymbol{c}) = \boldsymbol{c}\}$$

where σ_ℓ denotes the ℓ–blockwise cyclic shift.

Proposition

Let $\mathscr{C}$ be an ℓ–QC Goppa code, then $\mathscr{C}^{\sigma_\ell}$ is a Goppa code (whose length and dimension are divided by ℓ).

Security with respect to known attacks

- **Message recovery attacks.** We chose our parameters to resist to any known variant of ISD.
- **Key recovery attacks**. Our parameters are computed in order to resist to:

[1] J.-C. Faugère, V. Gauthier–Umaña, A. Otmani, L. Perret, J.-P. Tillich. *A distinguisher for High–rate McEliece Cryptosystems*. IEEE ITW 2011.

Security with respect to known attacks

- **Message recovery attacks.** We chose our parameters to resist to any known variant of ISD.
- **Key recovery attacks**. Our parameters are computed in order to resist to:
  - Brute force search on $\mathscr{C}^{\sigma_\ell}$ combined with Sendrier's *Support Splitting Algorithm*.

[1] J.-C. Faugère, V. Gauthier–Umaña, A. Otmani, L. Perret, J.-P. Tillich. *A distinguisher for High–rate McEliece Cryptosystems*. IEEE ITW 2011.

Security with respect to known attacks

- **Message recovery attacks.** We chose our parameters to resist to any known variant of ISD.
- **Key recovery attacks**. Our parameters are computed in order to resist to:
  - Brute force search on $\mathscr{C}^{\sigma_\ell}$ combined with Sendrier's *Support Splitting Algorithm*.
  - Distinguisher [FGOPT 11][1] on $\mathscr{C}$ and $\mathscr{C}^{\sigma_\ell}$.

[1] J.-C. Faugère, V. Gauthier–Umaña, A. Otmani, L. Perret, J.-P. Tillich. *A distinguisher for High–rate McEliece Cryptosystems*. IEEE ITW 2011.

Security with respect to known attacks

- **Message recovery attacks.** We chose our parameters to resist to any known variant of ISD.
- **Key recovery attacks**. Our parameters are computed in order to resist to:
  - Brute force search on $\mathscr{C}^{\sigma_\ell}$ combined with Sendrier's *Support Splitting Algorithm*.
  - Distinguisher [FGOPT 11][1] on $\mathscr{C}$ and $\mathscr{C}^{\sigma_\ell}$.
  - Attacks based on polynomial systems solving (conservative analysis).

[1] J.-C. Faugère, V. Gauthier–Umaña, A. Otmani, L. Perret, J.-P. Tillich. *A distinguisher for High–rate McEliece Cryptosystems*. IEEE ITW 2011.

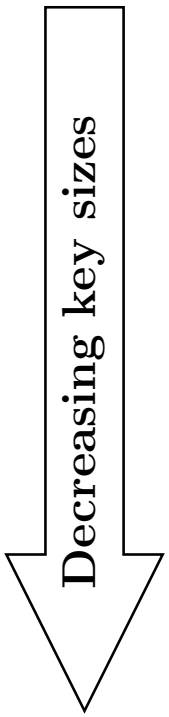
Security with respect to known attacks

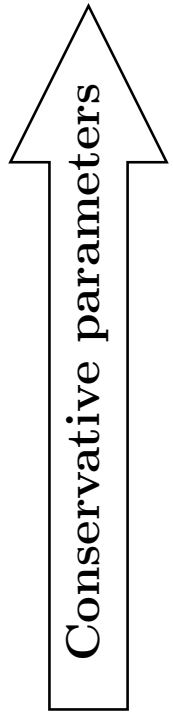
- **Message recovery attacks.** We chose our parameters to resist to any known variant of ISD.
- **Key recovery attacks**. Our parameters are computed in order to resist to:
  - Brute force search on $\mathscr{C}^{\sigma_\ell}$ combined with Sendrier's *Support Splitting Algorithm*.
  - Distinguisher [FGOPT 11][1] on $\mathscr{C}$ and $\mathscr{C}^{\sigma_\ell}$.
  - Attacks based on polynomial systems solving (conservative analysis).
  - Additional cautions : ℓ primitive modulo 2 to limit the number of intermediary codes that an attacker can compute.

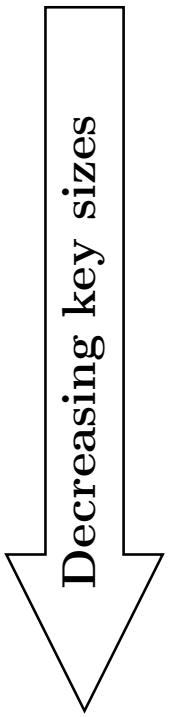
[1] J.-C. Faugère, V. Gauthier–Umaña, A. Otmani, L. Perret, J.-P. Tillich. *A distinguisher for High–rate McEliece Cryptosystems*. IEEE ITW 2011.

Suggested parameters

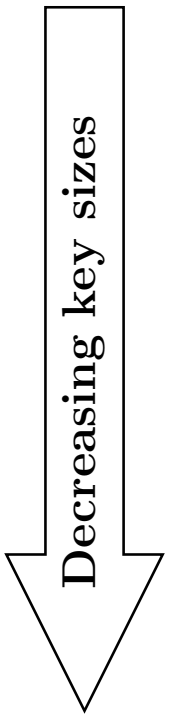
Security Level	m	Length	Dimension	ℓ	Public key size (kBytes)
1	12	3510	2418	13	25.3
3	18	7410	4674	19	84.1
5	18	10070	6650	19	149.6


Decreasing key sizes


Conservative parameters

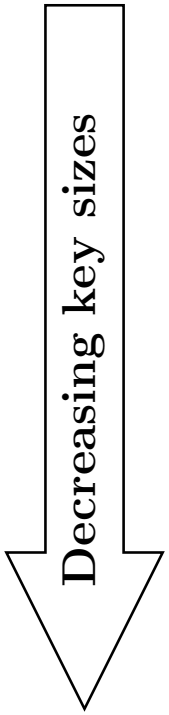


Classic McEliece, NTS KEM



Classic McEliece, NTS KEM

DAGS



Classic McEliece, NTS KEM

BIG QUAKE

DAGS

Thanks for your attention!