Code-Based Cryptography

McEliece Cryptosystem

I. Márquez-Corbella

informatiques mathématiques

2. McEliece Cryptosystem

1. Formal Definition
2. Security-Reduction Proof
3. McEliece Assumptions
4. Notions of Security
5. Critical Attacks - Semantic Secure Conversions
6. Reducing the Key Size
7. Reducing the Key Size - LDPC codes
8. Reducing the Key Size - MDPC codes
9. **Implementation**

eBATS: ECRYPT Benchmarking of PK Systems

eBATS: ECRYPT Benchmarking of Asymetric Systems

D. J. Bernstein and T. Lange (editors)
eBACS: ECRYPT Benchmarking of Cryptographic Systems.
http://bench.cr.yp.to, accessed 7 March 2015.

eBATS: ECRYPT Benchmarking of PK Systems

Measures PK system:

- ➜ Keys size
- ➜ Time of `KeyGen`
- ➜ Time of `Encrypt`
- ➜ Time of `Decrypt`

eBATS: ECRYPT Benchmarking of Asymetric Systems

D. J. Bernstein and T. Lange (editors)
eBACS: ECRYPT Benchmarking of Cryptographic Systems.
http://bench.cr.yp.to, accessed 7 March 2015.

eBATS: ECRYPT Benchmarking of PK Systems

Include **7 PK encryption schemes**:

1. `McEliece` implementation (2^{80} Security)
   By **B. Biswas** and **N. Sendrier**
2. `NTRU` implementation (2^{256} Security)
   By **M. Etzel**
3. Five sizes of `RSA` (starting with 2^{80} Security)

Measures PK system:

- ➜ Keys size
- ➜ Time of `KeyGen`
- ➜ Time of `Encrypt`
- ➜ Time of `Decrypt`

eBATS: ECRYPT Benchmarking of Asymetric Systems

D. J. Bernstein and T. Lange (editors)
eBACS: ECRYPT Benchmarking of Cryptographic Systems.
http://bench.cr.yp.to, accessed 7 March 2015.

McEliece is an interesting candidate

eBATS behchmarking:

- **Fastest Encryption:** `RSA1024 - McEliece`
- **Fastest Decryption:** `NTRU - McEliece`

McEliece is an interesting candidate

eBATS behchmarking:

- **Fastest Encryption:** `RSA1024 - McEliece`
- **Fastest Decryption:** `NTRU - McEliece`

➢ **Advantages of McEliece:** McEliece provide:

- **Extremely** fast **encryption**
- **Reasonably** fast **decryption**

McEliece is an interesting candidate

eBATS behchmarking:

- **Fastest Encryption:** `RSA1024 - McEliece`
- **Fastest Decryption:** `NTRU - McEliece`

➢ **Advantages of McEliece:** McEliece provide:

- **Extremely** fast **encryption**
- **Reasonably** fast **decryption**

✗ **Main Drawback:** Large Key size

But **QC-MDPC** codes allows **compact key representation**

- Provide Public key of 4800 bits for 2^{80} security
- No attacks or implementations are known.

Recent Results

				cycles/block		
m	**t**	**Public Key Size**	**Sec.**	**Encryption**$^{(*)}$	**Decryption**$^{(*)}$	**Decryption**$^{(*)}$ **(McBits)**
11	40	88440	95	25K	189K	29K
12	50	262200	120	47K	300K	60K

- $*$ Intel Xeon 3.4Ghz, single processor
- $*$ Intel Core 3.4Ghz, 4-core

AES: 10-20 cycles/byte

$100\text{Kcycles} \sim 30\mu\text{s}$

D. Bernstein, T. Chou and P. Schwabe
McBits: Fast Constant-Time Code-Based Cryptography.
CHES 2013, LNCS, Vol. 8086, 2013, pp 250-272.

B. Biswas and N. Sendrier
McEliece Cryptosystem Implementation: Theory and Practice.
Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

Software implementation

McEliece scheme has been implemented on several platforms:

1. **CPU**

B. Biswas and N. Sendrier

McEliece Cryptosystem Implementation: Theory and Practice.

Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

Software implementation

McEliece scheme has been implemented on several platforms:

1. **CPU**

   

   B. Biswas and N. Sendrier

   McEliece Cryptosystem Implementation: Theory and Practice.
   Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

2. **GPU**

   

   T. Howenga

   Efficient Implementation of the McEliece Cryptosystem on Graphics Processing Units.
   Master's thesis, Ruhr-University Bochum, Germany, 2009.

Software implementation

McEliece scheme has been implemented on several platforms:

1. **CPU**

   

   B. Biswas and N. Sendrier

   McEliece Cryptosystem Implementation: Theory and Practice.
   Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

2. **GPU**

   

   T. Howenga

   Efficient Implementation of the McEliece Cryptosystem on Graphics Processing Units.
   Master's thesis, Ruhr-University Bochum, Germany, 2009.

Software implementation

McEliece scheme has been implemented on several platforms:

1. **CPU**

   

   B. Biswas and N. Sendrier

   McEliece Cryptosystem Implementation: Theory and Practice.
   Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

2. **GPU**

   

   T. Howenga

   Efficient Implementation of the McEliece Cryptosystem on Graphics Processing Units.
   Master's thesis, Ruhr-University Bochum, Germany, 2009.

3. **FPGA**

   

   T. Eisenbarth, T. Güneysu, S. Heyse and C. Paar.

   MicroEliece: McEliece for Embedded Devices.
   CHES 2009, LNCS, Vol. 5747, 2009, pp 49-64.

   

   A. Shoufan, T. Wink, G. Molter, s. Huss and F. Strentzke.

   A Novel Procesor Architecture for McEliece Cryptosystem and FPGA Platforms
   ASAP 2009, pp 98-105.

Software implementation

McEliece scheme has been implemented on several platforms:

1. **CPU**

   

   B. Biswas and N. Sendrier

   McEliece Cryptosystem Implementation: Theory and Practice.
   Post-Quantum Cryptography, LNCS, Vol. 5299, 2008, pp 47-62.

2. **GPU**

   

   T. Howenga

   Efficient Implementation of the McEliece Cryptosystem on Graphics Processing Units.
   Master's thesis, Ruhr-University Bochum, Germany, 2009.

3. **FPGA**

   

   T. Eisenbarth, T. Güneysu, S. Heyse and C. Paar.

   MicroEliece: McEliece for Embedded Devices.
   CHES 2009, LNCS, Vol. 5747, 2009, pp 49-64.

   

   A. Shoufan, T. Wink, G. Molter, s. Huss and F. Strentzke.

   A Novel Procesor Architecture for McEliece Cryptosystem and FPGA Platforms
   ASAP 2009, pp 98-105.

4. **Small Embedded devices (8-bit micro controllers)**

   

   T. Eisenbarth, T. Güneysu, S. Heyse and C. Paar.

   MicroEliece: McEliece for Embedded Devices.
   CHES 2009, LNCS, Vol. 5747, 2009, pp 49-64.

Engineering

But ... there is still work to do!

Engineering

But ... there is still work to do!

1. Semantic Security Layer is mandatory

Engineering

But ... there is still work to do!

1. Semantic Security Layer is mandatory
2. Evaluation of Side-Channel attacks

Engineering

But ... there is still work to do!

1. Semantic Security Layer is mandatory
2. Evaluation of Side-Channel attacks
3. Protection against timing attacks

Engineering

But ... there is still work to do!

1. Semantic Security Layer is mandatory
2. Evaluation of Side-Channel attacks
3. Protection against timing attacks
4. Resistance of McEliece against fault injection attacks

Code-Based Cryptography

1. Error-Correcting Codes and Cryptography
2. McEliece Cryptosystem
3. **Message Attacks (ISD)**
4. Key Attacks
5. Other Cryptographic Constructions Relying on Coding Theory