Status report — Slovakia

Secure implementation of post-quantum cryptography
SPS Project Number: 984520
2nd meeting

Otokar Grošek Pavol Zajac

Institute of Computer Science and Mathematics
Slovak University of Technology

This project is supported by
NATO Science for Peace and Security Programme

Outline

McEliece calculator

- NTL based C++ implementation of MECS by M. Repka;
- Basic functions (KeyGen, Enc, Dec) + support for various measurements;
- Suitable for education and research.

Bitpunch: standalone McEliece implementation

Team project, SW adaptation of (Shoufan et.al, 2009).

What was achieved:

- Standalone McEliece implementation in C without external libraries;
- Parametric, modular, extensible;
- Suitable for research experiments.

Bitpunch: standalone McEliece implementation

What still needs more work:

- Better APIs, integration with other crypto libraries;
- "Schoolbook" implementation means slow speed;
- Unit-testing framework;
- Lightweight version for microprocessors;
- SCA countermeasures.

Comparison of MECS SW implementations

Tested implementations:

1. MECS Calculator by M. Repka
2. Bitpunch MECS by F. Uhrecky et.al.
3. Flea 0.1.1, HyMES adaptation by F. Strenzke, `www.cryptosource.de`
4. Java BouncyCastle McEliecePKCS class, `www.bouncycastle.org`

Testing platform:

CPU	Intel Core i5-2430M CPU @ 2.40GHz $\times$ 4
RAM	2 $\times$ 4GB DDR3 1333MHz
OS	Ubuntu 14.04.1 LTS, Linux 3.13.0-34-generic
GCC	4.8.2 (Ubuntu 4.8.2-19ubuntu1)

Comparison of MECS SW implementations

MECS parameters: $m = 11$, $t = 50$, $n = 2048$, $k = 1498$

	KeyGen [ms]	Enc [μs]	Dec [ms]	Library Size	
				Shared [kB]	Static [kB]
Calculator	1395	124	36.6	92 (+2MB)	116 (+4MB)
Bitpunch	866	62	3.9	64	96
Flea wo.H	46	34	0.6	160	232
Flea w. H	44	34	0.2		
BouncyCastle	1096	201	8.6	583 (whole BC 3MB)	

New results in Lee codes

- P. Horak, O. Grošek: A new approach towards the Golomb-Welch conjecture.
- A different view of Lee Codes using homomorphisms.
- New theoretical results:
  - the non-existence of linear $PL(n, 2)$ codes for $n \leq 12$;
  - the first quasi-perfect Lee codes for dimension $n = 3$;
  - for fixed n, there are only finitely many quasi-perfect Lee codes over Z.
- Application to MECS is an open question...

Construction of matrices with row and column weight $n/2$

- WIP: T. Fabšic, K. Nemoga, O. Grošek and P. Zajac
- How to efficiently construct non-singular matrices with row and column weight exactly $n/2$?
- How many of them do exist?
- At first, we restrict ourselves to circulant matrices...

Circulant matrices with row weight $n/2$

Lemma

Let $n = 0 \pmod 4$. Every circulant $(n \times n)$-matrix over $\mathbb{Z}_2$ with $\frac{n^2}{2}$ ones is non-invertible.

Are there other similar impossibility results?

Circulant matrices with row weight $n/2$, $n = 2 \pmod 4$

- Express circulant matrices as polynomials...
- Consider $c(x) = q(x) + b^2(x) + x^s b^2(x)$, where:
  - $q(x) = x^{n-2} + x^{n-4} + \cdots + x^2 + 1$.
  - $b(x) \in \mathbb{Z}_2[x]$, $\deg(b(x)) < n/2$
  - $\gcd(b(x), q(x)) = 1$
  - $s \in \mathbb{Z}_n$, $\gcd(s, n) = 1$
- The construction defines a set A of circulant invertible matrices with row weight $n/2$, $|A| = 2 \times \psi(x^{\frac{n}{2}} + 1) \times \phi(n)$

Connection to MECS

- Special class of scrambling matrices...
- Possible generalizations for use in construction and analysis of QC-codes, especially QC-MDPC codes

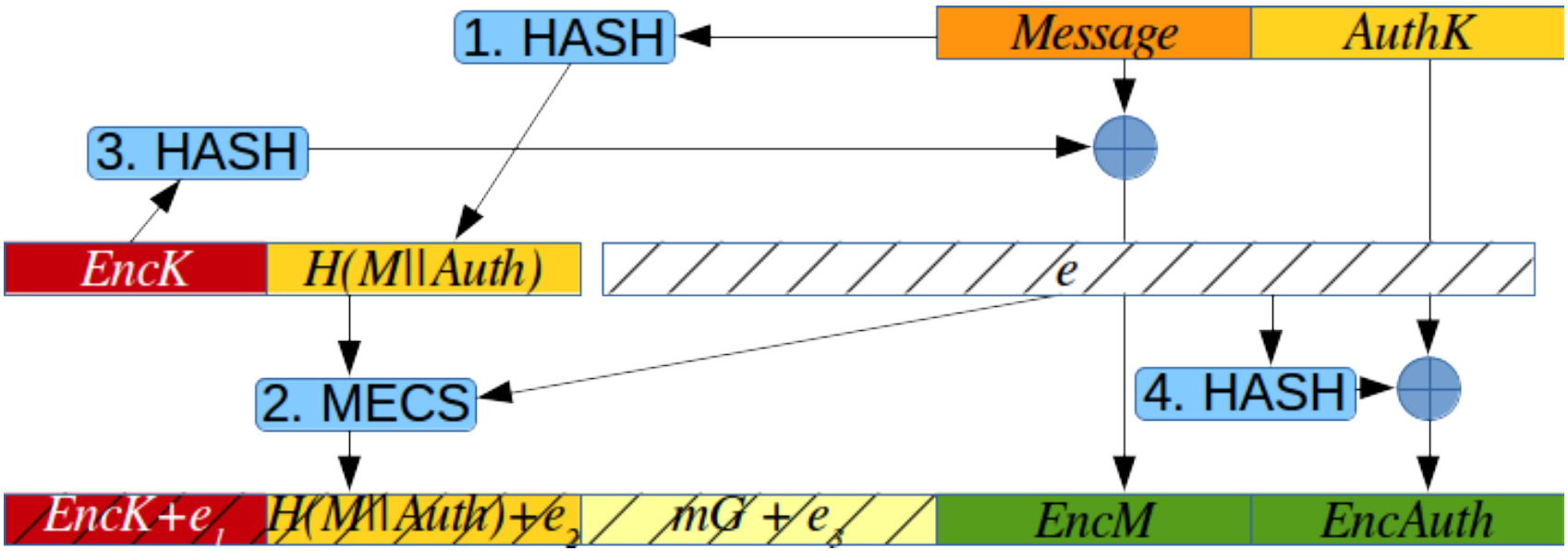
Overview of the MECS

- WIP: M.Repka and P. Zajac
- Goal: State of the art in secure implementation of MECS (from the engineering point-of-view)
- A lot of open questions...
- Standardisation required:
  - Parameters and security levels;
  - APIs for basic MECS, CCA2-conversions, and hybrid cryptosystems;
  - Support for code and algorithmic variants (e.g. resend API for MDPC codes? list decoding?);
  - ...

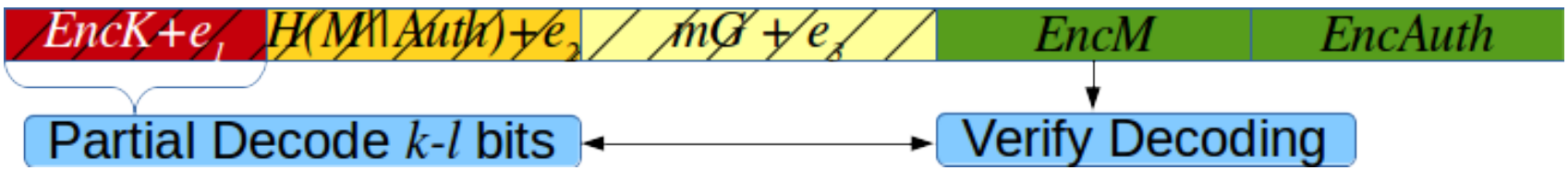
A flaw in some CCA2 conversions

- P. Zajac: A note on CCA2-protected McEliece cryptosystem with a systematic public key, `http://eprint.iacr.org/2014/651`
- An observation based on problem with implementing (Shoufan et.al, 2009): unspecified parameter *l* (hash length).
- Counterintuitive property: Longer hash leads to a less secure system.

Pointcheval variant with systematic matrix



Attack



"Brute forcing" *EncK*:

$$2^{H(t/n)(k-l)}$$

instead of expected 2^{k-l}.

Publicity and Training

"Best Practices in Cryptology and Information Security" Course
Bratislava, June 25 - 27, 2014

Summary

- Implementations: MECS Calculator, Bitpunch MECS;
- Research:
  - New theoretical results in Lee codes;
  - Study of cyclic matrices with row weight $n/2$;
  - Study of SW and security engineering aspects of MECS;
- Training: "Best Practices in Cryptology and Information Security".