[un]prompted

The AI Practitioner Conference

Math Ability has Consequences — AI Cryptanalysis

Markku-Juhani O. Saarinen

Professor of Practice, Tampere University

Math Ability has Consequences

20261028-unp2-math-consequences

https://mjos.fi/doc/20261028-unp2-math-consequences.pdf

Markku-Juhani O. Saarinen

Tampere University, Finland

markku-juhani.saarinen@tuni.fi

TLP:CLEAR

CONTENTS

001 A Bad Year for McEliece

002 Breaking China’s PQC candidates

SECTION

001

A BAD YEAR FOR MCELIECE

CLASSIC MCELIECE

- **1978:** Robert McEliece (Caltech/JPL) publishes a 3-page technical report *"A Public-Key Cryptosystem Based On Algebraic Coding Theory"* [12].
- **1980s-2010s:** The McEliece cryptosystem is described in textbooks but rarely used due to much larger public keys (100s of kB) than RSA or Elliptic Curve Cryptography. Many "optimized" variants are proposed & broken.
- **2017** Daniel J. Bernstein, Tanja Lange & Coauthors submit a modern version **Classic McEliece** to the first round of the U.S. NIST PQC competition [7].
- **2020:** German Cyber agency BSI starts recommending Classic McEliece [5].
- **2025:** NIST says Classic McEliece won't be standardized by them [1].
- **2026:** In June Classic McEliece becomes an international ISO Standard [11].

★ July-August 2026 – "Lee Sedol" for AI in Cryptanalysis ★

BACK IN 2023-24: TII MCELIECE CHALLENGES

Two kinds of attacks: The best way to break one McEliece **secret message** is with Information Set Decoding (ISD ∼ exponential to the error weight).

Until 2025-26, to recover the **secret key** one would expect to do a brute force search on (n, m, t): Goppa-polynomial search × support-set search × trial cost:

$$\text{TII-n labels:}\quad \lambda_{\text{TII}} = \log_2\left(I(t, 2^m) \cdot \binom{2^m}{n} \cdot n^3 \right)$$

The Technology Innovation Institute (UAE) ran a McEliece challenge in 2023-24. TII offered cash prizes – the reward for TII-70 and above was $ 10,000 each.
https://github.com/ElenaKirshanova/tii_decoding_challenge

JULY 2026: NEW TII KEY RECOVERY RECORDS

My AI-discovered "HOVER" shortcut [16] for Hemmert's HOV key recovery [9] turned out to be quite effective against specific low-degree parameters:

Challenge	m	r	n	Wall Time	Memory	System
TII-252	10	11	1008	6 min 15 s	2.7 GiB	12-core laptop
TII-246	10	11	1009	3 min 11 s	2.7 GiB	12-core laptop
TII-240	10	11	1010	3 min 06 s	2.7 GiB	12-core laptop
TII-213	9	10	496	6 h 45 min	144 GiB	28-vCPU server
TII-129	9	9	509	4 h 30 min	80 GiB	28-vCPU server

Evidence (secret keys): https://github.com/mjosaarinen/tii-solved

Note: TII-83 was the "highest" challenge broken by the May 2024 deadline.

AUGUST 2026: HOLDOUT / GIJS: AI DISCLOSURE [8]

AI disclosure. Our main results emerged from the failed PIR attempt described above and were obtained through traditional human trial and error, without the use of AI. Still, AI was instrumental for many aspects of this work. OpenAI Codex (ChatGPT-5.6 Sol) was used to verify the results, analyze and improve concrete efficiency, draft some of the proofs, design and implement experiments, and help with literature review and other aspects of writing. Amazon Quick and Google AI harness were used for extra sanity checks.

AI played a more significant role in developing our key-recovery algorithm. The algorithm, inspired by the Sidelnikov–Shestakov algorithm, was proposed by the authors. ChatGPT-5.6 Sol then helped with the routine but tedious derivations of the structure of the interpolation coefficients. It also helped us quickly run the experiments measuring nullities, which were important for guiding the choice of parameters and gaining confidence in our conjectures.

Most importantly, an audit by ChatGPT identified a dimension gap that made our initial algorithm fail for binary Goppa codes and required changing the parameters. ChatGPT also helped run experiments to confirm the structure of the required interpolation coefficients for Goppa codes. We sent the resulting algorithm to Steve Weis from Anthropic, who was able (with the help of Claude) to successfully run our algorithm on small binary Goppa instances.

The authors verified the correctness and originality of all content.

HOLDOUT: COST AGAINST CLASSIC MCELIECE

Weis & Claude in August 2026: the interpolation relations also encode the hidden support. After removing local jet relations, their top-order blocks satisfy $V_{2,j} = \alpha_j^{s'-1} V_{1,j}$ (up to normalization and Frobenius conjugacy). Read off the α_j, recover the multipliers, and obtain an equivalent decoding key [18]. **Estimates:**

Parameter set	NIST Req [13]	ISD [3]	GIJS [8]	Weis [18]	Saarinen [14]
mceliece348864	143	151	114.2	94.3	126.8
mceliece460896	207	191	120.3	99.3	145.2
mceliece6688128	272	257	124.0	102.4	137.5
mceliece8192128	272	287	124.0	102.4	137.5

TII-253 ($m = 8, t = 9, n = 214$): two sparse kernels, ≈ 700 core-hours each [18].

SPECIAL HOLDOUT: TII-254 KEY RECOVERY

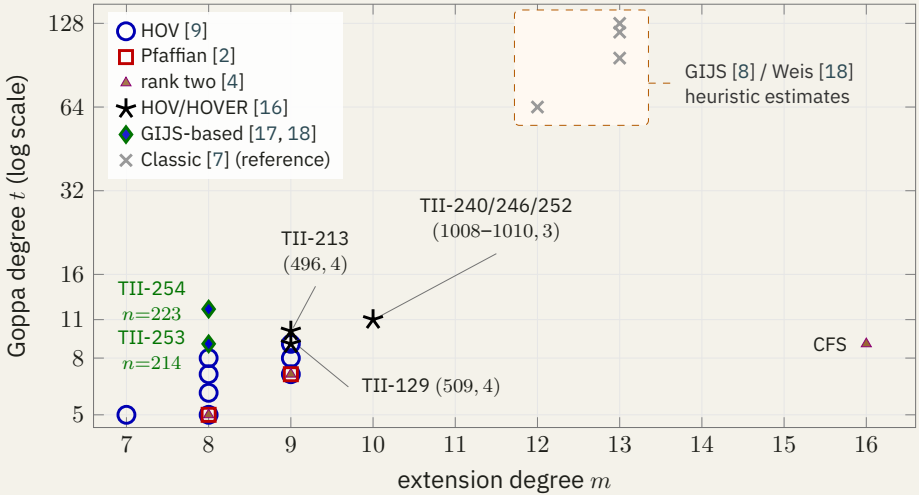
TII-254 $(m, t, n) = (8, 12, 223)$: hardest solved challenge so far [17].

I ran a human-directed, AI-operated algorithm improvement loop for 8 days.

TII-254-specific, 13-step process: Degree-6 holdout system; remove 4.8M provable "nuisance" directions (20.3M $\to$ 15.5M). Solve at two anchor columns: two 121-dim kernels. Their pair core splits as $80 = 64 + 16$; the common 64 is noise, and the $16 \cong \mathbb{F}_{2^8}^2$ has the support locators as its $\mathbb{F}_{2^8}$-lines.

Stage (per anchor)	Time	Hardware
Block Wiedemann sequence (width 512)	13.6 h	$1\times$ NVIDIA GH200
Polynomial-matrix basis	0.8–5.1 h	12–64 CPU threads
Kernel reconstruction	$\approx$2 h	$8\times$ GH200

CHARTING THE MCELIECE KEY RECOVERIES



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Hinweise zu aktuellen Entwicklungen um Classic McEliece

Stand: 29.09.2026

SEP 29, 2026: CURTAINS ON CLASSIC MCELIECE

Since 2020, Germany's cyber authority BSI has recommended Classic McEliece in its Technical Guideline TR-02102-1.

The January 2026 version still stated: *"The underlying mechanism, which is instantiated with binary Goppa codes, is about as old as the RSA mechanism and is therefore considered conservative and very thoroughly analysed."* [5]

On September 29, 2026 BSI revised their guidance:

"Classic McEliece should currently no longer be used in new developments or when planning new cryptographic applications." [6]

The BSI Classic McEliece security advisory [6] cites the same 2026 works as we did here [2, 4, 8–10, 18], including my works [16, 17].

SECTION

002

BREAKING CHINA’S PQC CANDIDATES

NGCC: CHINA'S OPEN PQC & HASH COMPETITION

Run by **ICCS** (Institute of Commercial Cryptography Standards). Follows the U.S. NIST model: public calls, fixed C API, KATs, open mailing lists.

Announced Feb 2025; calls Oct 2025; submissions Jun 30, 2026.

119 candidates (NIST PQC: 69 in 2017, SHA-3: 51 in 2008).

Submissions by Family & Category:

Family	Sign	KEM	KEX	Hash	Tot
Lattice	11	25	7	–	43
Code	5	15	1	–	21
Multivariate	6	–	–	–	6
Isogeny	3	1	1	–	5
Hash-based sig.	4	–	–	–	4
VOLE-in-the-head	4	–	–	–	4
Group action	1	–	–	–	1
Symmetric	–	–	–	35	35
Total	34	41	9	35	**119**

NGCC.DEV: ONE CRYPTOGRAPHER & CODING AGENTS

I have just a typical developer AI setup: OpenAI Codex (∼$200/month) and Claude Code (∼$100/month) on a 28-core cloud server, isolated Linux accounts, no sudo, no git write access. About 2.01 billion tokens in Sep 21–27.

AI uses tools: Python, SageMath, Rust, C, Lean, SAT solvers, lattice estimator…

Reference Literature: IACR ePrint, arXiv, proceedings (I have a large stash.)

Cross-vendor review ping-pong: Claude often reviews Codex and vice versa.

Source-only harness: 87,514 submitted files, including 471 prebuilt executables. Rule: *nothing shipped in a submission is ever executed*. Day one: 577 instances of 117 candidates built, 545 (94.5%) test their KATs byte for byte.

NGCC.DEV: GENERAL SECURITY AUDIT ITEMS

01 **Safety** Static-check submitted reference implementations (nothing very malicious found). Never execute shipped binaries, scripts or objects; build with our Makefiles, then isolate and time-limit tests.

02 **Evidence** Cite claim and source; reproduce a *witness* with a control. Tag research leads and proof gaps separately.

03 **Spec ↔ code** Compare the algorithm spec and its implementation: parameters, API headers, and Known-Answer Tests (KATs).

04 **Entropy Audit and Sensitivity Analysis** Trace DRBG use and randomness in keys, salts, nonces, and challenges, and internal variables.

PERHAPS THE BIGGEST “EXPERT” CONTRIBUTION

NGCC.DEV: BRIEFS AND CHECKLISTS

KEY ENCAPSULATION

Mutate ciphertexts. Check full re-encryption, rejection masks, and fallback binding to (pk, ct); probe FO failure/plaintext oracles.

SIGNATURES

Mutate message, signature, and length. Check verifier bypass, non-canonical encodings, and nonce or challenge entropy.

HASHES

Probe padding, zero extension, cross-digest relations, long-message bounds, and structural limits.

TIMING SIDE-CHANNELS

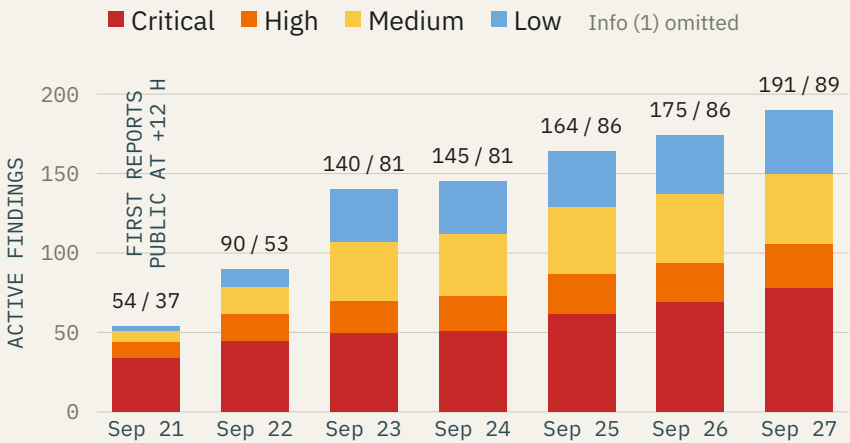
Sensitive (secret) variables are not used for branches, table lookups, non-constant time instructions.

NGCC.DEV: VULNERABILITY CLASSIFICATION

Critical	A violation of primary NGCC security requirements. *EUF-CMA (signatures), IND-CCA2 (KEMs), collisions, preimages,...*
High	A serious failure or well-supported attack path, short of a complete primary break.
Medium	A security-relevant defect or leak without demonstrated recovery or forgery.
Low	Narrow robustness, availability, or API impact; no cryptographic break shown.
Info	A tracking or out-of-model observation, without a candidate-specific break.

CUMULATIVE, LABELS: FINDINGS / REPORTS [15]

NGCC.DEV: 191 FINDINGS IN FIRST SEVEN DAYS

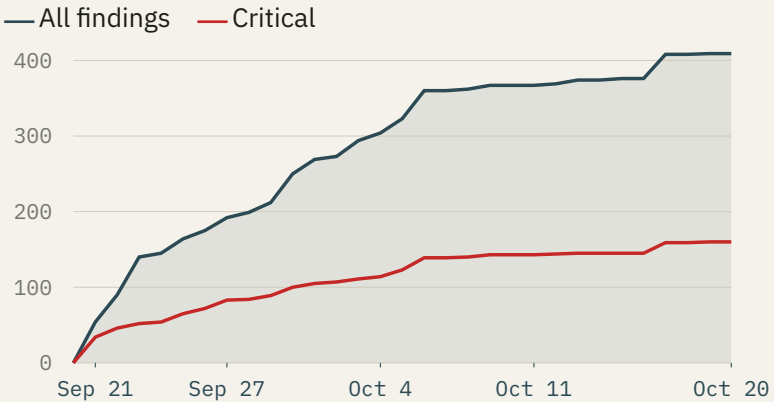


NGCC.DEV: FIRST WEEK BREAKDOWN [15]

		Scope			Category			
Severity	**Des.**	**Impl.**	**S.-c.**	**Sign**	**KEM**	**KEX**	**Hash**	**Total**
Critical	32	46	0	35	24	5	14	78
High	14	13	1	11	12	2	3	28
Medium	24	9	11	14	18	4	8	44
Low	6	17	17	9	13	2	16	40
Info	0	1	0	0	0	0	1	1
Total	76	86	29	69	67	13	42	**191**
My project + AI	24	59	27	30	45	12	23	**110**
Others + AI	10	9	1	15	5	0	0	20
Human / unknown	42	18	1	24	17	1	19	61

Status: 167 Confirmed, 10 Probable, 10 Leads, 4 Proof gaps.

NGCC.DEV: THE FIRST MONTH



OCT 20

409

active findings

160

Critical

110

candidates with findings

Current reports include one first-week finding added after the paper snapshot.

NGCC.DEV: THE CRITICAL BUG ZOO

- **Verifier bypass** UVW returns success on failed signatures; any forgery passes.
- **Broken FO check** Amoeba compares only every fourth ciphertext byte; tampering leaks the secret key.
- **Randomness misuse** Galas and VDOO skip the RNG and repeat keys; 14 schemes reset the DRBG as a XOF or KDF.
- **Missing challenge binding** Chinith omits $\tilde{a}_0$ from the challenge; anyone can sign under any public key.
- **Index bugs** CEDRUS+C uses only tree 0 (four few-time keys); MORNING-ATLAS repeats masks, exposing the key after two signatures.
- **Bits vs. bytes** CreTAKE's 512-bit secret has only 64 bits of entropy.
- **Hash padding** Mixed bit ordering makes the empty string collide with seven zero bits.
- **Ciphertext aliases** OAEP-NTRU accepts alternate ciphertext bytes for the same key: a one-query IND-CCA break.

NGCC.DEV: DESIGN BREAKS FROM THE FIRST WEEK

Here the security issue is in the **specification / design**. It is often difficult to draw a line between a “design oversight”, and a “new cryptanalytic attack.”

Through day four, most **design attacks** came from human researchers (some AI-assisted): Tins witness by $\mathbb{F}_2$ elimination; Facto-DSA-128 forgery in 6.4 s; full-round MoFang hash collisions (Tsinghua).

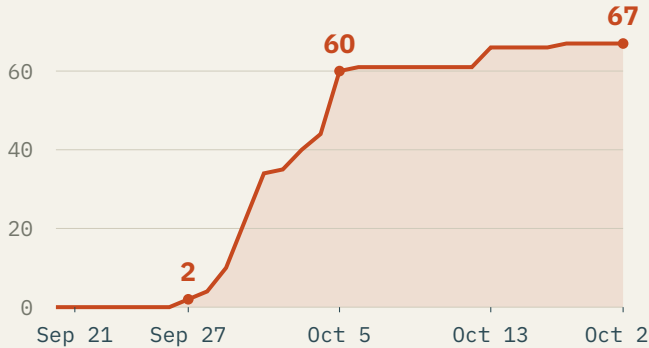
From day five, Codex-assisted signature breaks by Martin Feussner (Bergen): key recovery or forgery for Shuttle, Sigurd, ATLAS-128, Lynxer, SQIsignTriangle.

Of the 81 findings by others, 20 disclosed AI: OpenAI models (10), Chinese Doubao and Xuanzhi CryptoLLM (2), unnamed (8). Later a lot of GLM 5.3.

Still human: Scope, evidence, disclosure, and the decision to publish.

NGCC.DEV: THE CHINESE WAVE & SLOP DROPS

Cumulative findings with named model assistance



OCT 13 BATCH

□□□□□□
□□□□□

11 .md reports
162 observations

⇓

5 new IDs
3 findings + 2 Info

Credited to: Doubao, Xuanzhi, GLM 5.3, kimi-k3. Oct 13: other claims overlapped or did not meet criteria.

END OF TALK!

QUESTIONS

https://mjos.fi/doc/20261028-unp2-math-consequences.pdf

REFERENCES (1)

[1] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. “Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process”. Interagency or Internal Report NIST IR 8545. National Institute of Standards and Technology, Mar. 2025, p. 34. DOI 10.6028/NIST.IR.8545.

[2] Magali Bardet, Axel Lemoine, and Jean-Pierre Tillich. “An Attack on the CFS Scheme and on TII McEliece Challenges”. In: *Advances in Cryptology - CRYPTO 2026 - 46th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-20, 2026, Proceedings, Part IV*. Ed. by Nadia Heninger and Mike Rosulek. Vol. 16803. Lecture Notes in Computer Science. Springer, 2026, pp. 380–412. DOI 10.1007/978-3-032-35398-6_13. URL: https://eprint.iacr.org/2026/430.

REFERENCES (2)

[3] Daniel J. Bernstein and Tung Chou. “CryptAttackTester: high-assurance attack analysis”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VI*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14925. Lecture Notes in Computer Science. Full version is available as IACR ePrint Report 2023/940. Springer, 2024, pp. 141–182. DOI 10.1007/978-3-031-68391-6_5. URL: https://eprint.iacr.org/2023/940.

[4] Pierre Briaud, Axel Lemoine, Hugues Randriambololona, and Jean-Pierre Tillich. “A Heuristic Subexponential Attack on the McEliece Cryptosystem”. Cryptology ePrint Archive, Paper 2026/1232. 2026. URL: https://eprint.iacr.org/2026/1232.

[5] BSI. “Cryptographic Mechanisms: Recommendations and Key Lengths”. Technical Guideline TR-02102-1. Bundesamt für Sicherheit in der Informationstechnik, Jan. 2026, p. 92. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf.

[6] BSI. “Notes on recent developments concerning Classic McEliece”. Security Advisory. Sept. 2026. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Notes_Classic_McEliece.pdf.

REFERENCES (3)

[7] Classic McEliece Team. “Classic McEliece: conservative code-based cryptography: guide for security reviewers”. Document of official Classic McEliece web site. Oct. 2022. URL: https://classic.mceliece.org/mceliece-security-20221023.pdf.

[8] Ashrujit Ghoshal, Yuval Ishai, Aayush Jain, and Nuozhou Sun. “Quasipolynomial Cryptanalysis of the McEliece Cryptosystem (or: PIR Meets McEliece)”. Cryptology ePrint Archive, Paper 2026/1630. Aug. 2026. URL: https://eprint.iacr.org/2026/1630.

[9] Tobias Hemmert. “Key Recovery for the McEliece Cryptosystem Using Higher-Order Vanishing”. Cryptology ePrint Archive, Paper 2026/1339. 2026. URL: https://eprint.iacr.org/2026/1339.

[10] Tobias Hemmert and Andreas Wiemers. “Distinguishing Goppa Codes Using Higher-Order Vanishing”. In: *Advances in Cryptology – CRYPTO 2026. 46th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–20, 2026, Proceedings, Part IV*. Ed. by Nadia Heninger and Mike Rosulek. Vol. 16803. Lecture Notes in Computer Science. Springer, 2026, pp. 191–223. DOI 10.1007/978-3-032-35398-6_7. URL: https://eprint.iacr.org/2025/1661.

[11] ISO. “Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers – Amendment 2”. en. Standard ISO/IEC 18033-2:2006/Amd 2:2026. International Organization for Standardization, 2026. URL: https://www.iso.org/standard/86890.html.

REFERENCES (4)

[12] Robert J. McEliece. “A Public-Key Cryptosystem Based on Algebraic Coding Theory”. Progress Report DSN PR 42-44. Deep Space Network, 1978, pp. 114–116. URL: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

[13] NIST. “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”. NIST Call for PQC Standardization Candidates. Dec. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[14] Markku-Juhani O. Saarinen. “Bit Operation Cost of “Holdout” Key-Recovery Attacks Against Classic McEliece”. Cryptology ePrint Archive, Paper 2026/1786. Sept. 2026. URL: https://eprint.iacr.org/2026/1786.

[15] Markku-Juhani O. Saarinen. “Chinese NGCC Algorithms: The First Week of AI Cryptanalysis”. Cryptology ePrint Archive, Paper 2026/2266. Oct. 2026. URL: https://eprint.iacr.org/2026/2266.

[16] Markku-Juhani O. Saarinen. “HOVER: Higher-Order Vanishing Endomorphism Recovery”. Ed. by Aslan Askarov, Abhishek Vaish, and Christian Damsgaard Jensen. Nov. 2026. URL: https://eprint.iacr.org/2026/1778.

REFERENCES (5)

[17] Markku-Juhani O. Saarinen. “Two-Anchor Holdout/Hermite: Solving the TII-254 McEliece Key Recovery Challenge”. Cryptology ePrint Archive, Paper 2026/1986. Sept. 2026. URL: https://eprint.iacr.org/2026/1986.

[18] Stephen A. Weis. “Improving GIJS Key Recovery for Classic McEliece”. Cryptology ePrint Archive, Paper 2026/1984. Sept. 2026. URL: https://eprint.iacr.org/2026/1984.