[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 HAWK: The Lee Sedol Moment

002 Breaking China’s PQC candidates

SECTION

001

HAWK: THE LEE SEDOL MOMENT

MARCH 2016: ALPHAGO -VS- LEE SEDOL 9 DAN

HAWK – A PQC SIGNATURE SCHEME

HAWK [2, 3] was a NIST PQC Signature standardization (“On-Ramp”) candidate until July 29, 2026. Many saw HAWK as a successor algorithm to Falcon [4] (FIPS 206 / FN-DSA), although it is *based on different security foundations*.

Attractive: Fast signing & verification, 555-byte signatures, no floating point.

> QUOTE FROM NIST IR 8610, MAY 2026 [1]
>
> *NIST selected HAWK for the third round due to its strong performance and because its implementation only needs integer arithmetic operations. NIST encourages further analysis of HAWK’s security assumptions, particularly the smLIP problem within the specific structure of cyclotomic number fields.*

HAWK TIMELINE

- **2022.12.08**: Ducas, Postlethwaite, Pulles, van Woerden. *Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple* [3]. ASIACRYPT '22.
- **2026.05.14**: Hawk selected to 3rd round of NIST PQC Signature On-Ramp.
- **2026.06.25**: Nelson, Limbrey, Ling, Mendelsohn. *Cryptanalysis of HAWK: a Guessing Game* [5]. Authors conjecture a classical polynomial-time attack.
- **2026.07.05**: Saarinen. *HAWK "Guessing Game" is **not** Polynomial-Time* [7]. AI-Assisted implementation attempt/analysis. ("It's okay!")
- **2026.07.28**: Straznickas, Weis. *HAWK-n Key Recovery Reduces to SVP in Dimension n/2 + 1* [8]. – Anthropic's AI cryptanalysis announcement.
- **2026.07.29**: HAWK Withdrawn from the NIST Competition by its authors.

30 JULY 2026 – “LEE SEDOL” (BUT CONCLUSIONS VARY)

REACTIONS: CONG LING ON NIST PQC FORUM

Dear Colleagues,

This is a historic moment in cryptology: AI has beaten humans at cryptanalysis. We would like to share a few thoughts with the PQC community based on our own experience.

There are other dimension-reduction attacks on HAWK in literature. At Eurocrypt 2026, we proposed a dimension-halving algorithm for quaternion Ideal-SVP, which potentially implies that HAWK-n key recovery can be reduced to (cyclotomic) Ideal-SVP in dimension n.

Later, we proposed another guessing attack based on advanced number theory, under a few heuristic assumptions. However, one of these heuristics was soon found to be invalid by colleagues with the assistance of AI.

Apparently, we were outpaced by AI in both cases. A couple of lessons we have learned are: (a) humans can make mistakes; and (b) humans are slower than AI. Beyond cryptanalysis itself, the use of AI to check mathematical proofs is becoming an increasingly serious issue.

One can even imagine a crisis in cryptography: in the worst-case scenario, all human-designed cryptosystems are broken by AI. Whether or not that happens, a new era – Post-AI Cryptography – has arrived.

TWO KINDS OF "HARD PROBLEMS"

1. **Hard computational problems**: Instances of SAT, SVP, SD, MQ, $\cdots$
   (Seem exponentially hard even for quantum computers.)
2. **Hard "human" problems**: P $\neq$ NP, Riemann Hypothesis, $\cdots$
   ("Lots of people have tried" – for decades, centuries.)

2026: Computers / AIs are getting better at solving problems traditionally in (2).

Generally we want to prove (2) that a crypto algorithm is a hard instance (1). The hardness of (1) is studied in theoretical computer science, but the assessment of hardness of (2) – and some cryptography – has been more subjective.

Post-AI, we can have cryptography with better security evidence and proofs. Some machine-checked proofs may have to be beyond human comprehension.

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: A 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

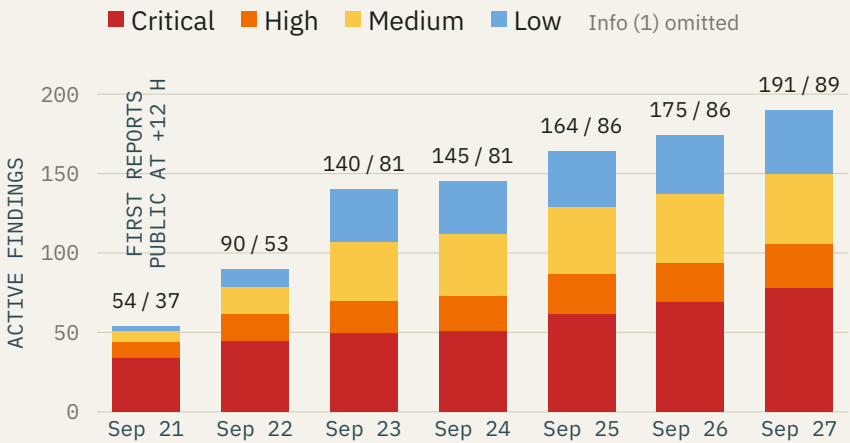
Sensitive (secret) variables are not used for branches, table lookups, non-constant time instructions.

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 [6]

NGCC.DEV: 191 FINDINGS IN FIRST SEVEN DAYS

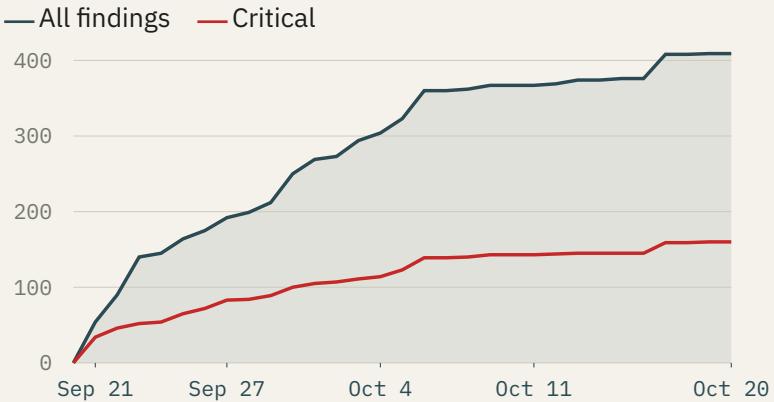


NGCC.DEV: FIRST WEEK BREAKDOWN

		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).

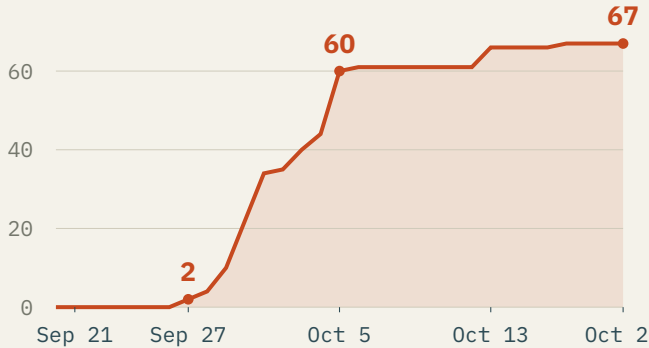
From day five, Codex-assisted signature breaks by Martin Feussner (Bergen): key recovery or forgery for Shuttle, Sigurd, ATLAS-128, Lynxer, SQIsignTriangle.

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

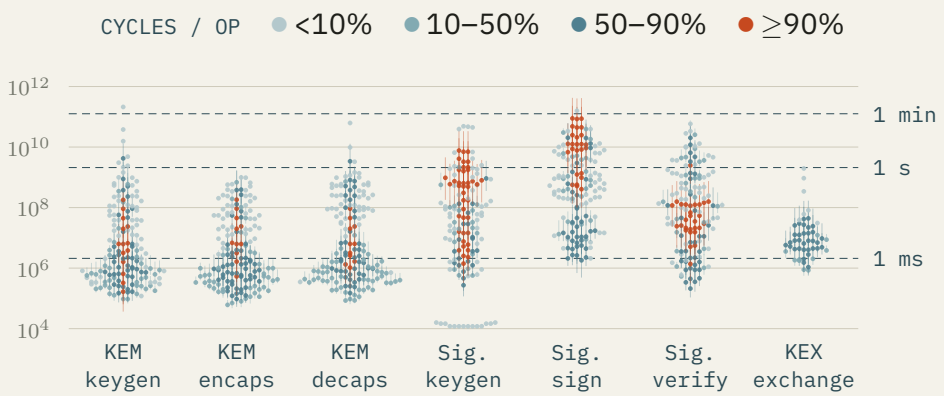
⇓

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.

HASH/XOF MAY LARGELY SET PUBLIC-KEY PERFORMANCE

NGCC.DEV: PERFORMANCE TRIALS [6]



403 / 959 operations spend at least half their cycles in ICCS placeholder helpers.

END OF TALK!

QUESTIONS

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

REFERENCES (1)

[1] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, 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 Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process". Interagency or Internal Report NIST IR 8610. National Institute of Standards and Technology, May 2026, p. 38. DOI 10.6028/NIST.IR.8610.

[2] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. "HAWK version 1.1 (February 5, 2025)". Feb. 2025. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/hawk-spec-round2-web.pdf.

[3] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. "Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple". In: *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13794. Lecture Notes in Computer Science. Springer, 2022, pp. 65–94. DOI 10.1007/978-3-031-22972-5_3. URL: https://eprint.iacr.org/2022/1155.

REFERENCES (2)

[4] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU (Specification v1.2 — 01/10/2020)”. Oct. 2020. URL: https://falcon-sign.info/falcon.pdf.

[5] Ben Nelson, Joshua Limbrey, Cong Ling, and Andrew Mendelsohn. “Cryptanalysis of HAWK: a Guessing Game”. Cryptology ePrint Archive, Paper 2026/1318. June 2026. URL: https://eprint.iacr.org/2026/1318.

[6] 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.

[7] Markku-Juhani O. Saarinen. “HAWK “Guessing Game” is not Polynomial-Time”. Cryptology ePrint Archive, Paper 2026/1377. July 2026. URL: https://eprint.iacr.org/2026/1377.

[8] Zygimantas Straznickas and Stephen A. Weis. “HAWK-n Key Recovery Reduces to SVP in Dimension $n/2 + 1$”. Cryptology ePrint Archive, Paper 2026/1593. 2026. URL: https://eprint.iacr.org/2026/1593.