Cryptology Annual News Update and Vignette

Bill Ricker
for BLU.org
Sept 17, 2025

1. Cryptology News Bulletins
2. Post Quantum Cryptograpy update
3. Historic Vignette: AF is Midway / Midway is low on Water
4. Bibliography

1 Cryptology News Bulletins 2024-09 to 2025-09

“**Abundance of Caution**” is C-suite lingo for “*Oopsie, oh flying squirrel*”

Let’s Encrypt: short-lived certificates &c

- LetsEncrypt Dec. editorial announced automatically renewable 6-day server TLS certificates, using the same automation used for the free 90-day certs.
  - Slashdot hated it;
  - Schneier liked it.
  - First issued Feb. 2025.
  - It was approximately LE’s 10th anniversary.

In other news

- Now issuing IP Address certificates,
- Turned off
  - Online Certificate Status Protocol (OCSP)
    (in favor of Revocation Lists only)
  - Expiration Notification as renewal automation has spread, reducing their retained PII;
- announced phased shutdown of RFC 6962 Certificate Transparency Logs (in favor of Static Certificate Transparency API); timed to allow browsers to catch up.

UK NCSC advice on ‘Advanced Cryptography’

UK white paper Schneier & friends comments

Advanced := *Beyond* protecteding **data at rest** and **data in motion**; allowing some **processing** of protected data.

Their examples:

- Homomorphic encryption
- Private information retrieval
- Multiparty computation
- Zero-knowledge proofs
- Private set intersection revealing your whole list
- Attribute-based encryption attributes

key takeaways are

- Don’t roll your own security code (per usual)
- these techniques are immature so get best help

NIST revised password rules

NIST SP 800-63 Digital Identity Guidelines includes passwords. This is officially only applicable to Federal information systems, but constitutes a best practice for the rest of us to be aware of.

Schneier on 2024 draft’s password rules

Attacks only get better: GPU assisted Brute Force

'GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA: Brute Force Cryptanalysis of KASUMI, SPECK, and TEA3.'

These are actual wireless communications protocols' keys.

This research shows that *some* key-sizes are within brute-force *now* with state-actor scale (e.g. Top500) clusters of GPUs or hypothetical specialized hardware, and others may be in range by 2050.

Schneier &c

NOTES

Venona-level persistence-play is already in play[1]. Today's cellphone intercepts may be cracked in the future. For the highest priority, investigators may be willing to dedicate a cluster for a year to get the session-key for a previously recorded conversation. And it will only get more affordable.

---

[1] see the ♳ Review: Forward Secrecy slide in 2, and BLU 2018 footnotes below

What to use instead of PGP, FB IM, …

Updating our prior discussions (in 2019[2], 2021[3], and 2022[4]):

Nov. 2024: What To Use Instead of PGP

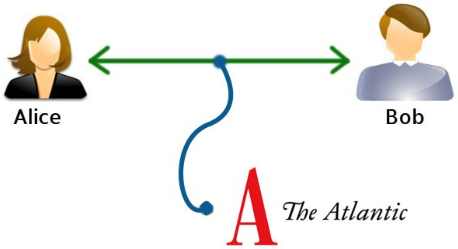
Nice discussion by use-case by a cryptologist who finds vulns. By Use Case is important, as the flaws in PGP/GPG usage largely come from trying to be the one Swiss Army Knife to pound all nails.

Apr.2025: Neiman Lab: How to leak to a journalist

tl;dr:

- SecureDrop
- Signal
- Whistle blower support services

But even with Signal secure group messages, OpSec requires you not add the *wrong* person from your Contacts!



[2] 2019 what to use, initial suggestions by use-case;
[3] 2021 what to use, 2019♳ with added caveat Keybase sold to Zoom;
[4] 2022 what to use, 2019♳ with a governmental PGP use failure;

2 What’s up with Post Quantum Cryptography?

Review: What's Quantum Computing?

♳ Reprises (♳) and updates last major PQC status update Sept 2022 which is excerpted below with recycled "♳ Review" markings.

Quantum Superposition when used for computing.

- QC measured in "**qubits**" not bits
- 30% True, 70% False.

The only known photo of Schrodinger's cat.

♳ Review: Kinds of Quantum Hardware

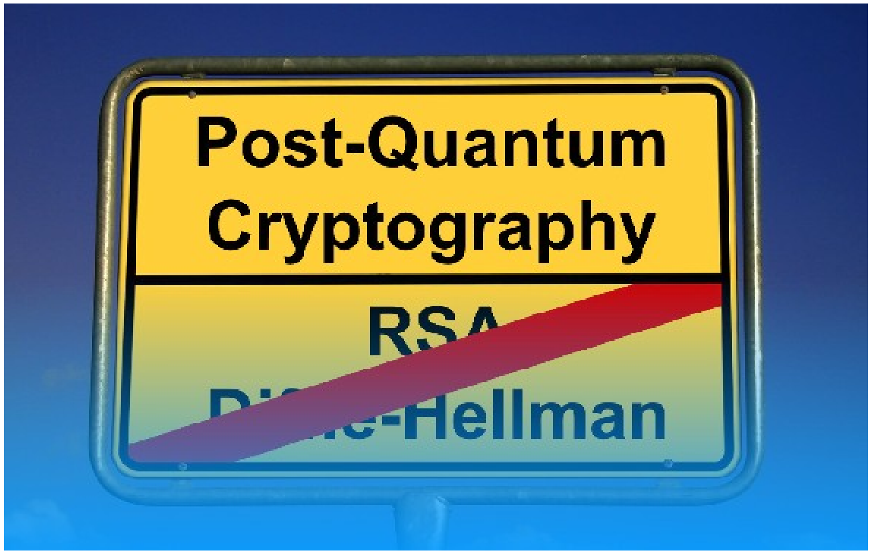
- Quantum Annealing - big qubit counts, great for optimization problems

but not cryptology. (?yet? well maybe ...) _Not general purpose._

- Quantum Circuit/Logic - small numbers of qubits so far.

In theory, algorithms for these hardware types can use non-deterministic parallelism to evade classical performance limits, and in particular, could allow factoring fast enough to be dangerous, provided big enough quantum circuits can be made to work.

♳ Review: We’re discussing PQC before QC?



Yes !

- Quantum Cryptography
  - theoretically using entangled quantum states
  - to create an encryption
  - or an anti-eaves-droppable connection
- Quantum Crypt**analysis**
  - Using Quantum Computing to defeat classical PKI encryption
- Post Quantum Cryptography
  - new classical encryptions that can resist Quantum Cryptanalysis,
  - so read as Ready for post-**(**Quantum-Computing**)** Cryptography.

Review: What’s the problem?

♳

- Unbreakable ciphers aren’t always unbreakable, for always.
- QC *could theoretically* break most PKI
  - Schor’s Algorithm / Grover’s / VQF
  - discrete log as well as prime factoring, even elliptic curves
- **2024-01-05** Improving Shor’s Algorithm
  - “Thirty Years Later, a Speed Boost for Quantum Factoring” (Quanta)
  - Oded Regev’s paper on arXive
  - and another team already reduced the memory penalty of the speed improvement arXiv

---

2025 GOOGLE WILLOW QC

(Hype, not yet dangerous)

BBC: Google unveils ‘mind-boggling’ quantum computing chip

MSN: Google’s Willow quantum chip breakthrough is hidden behind a questionable benchmark

See caveats on Wikipedia [5]:

> Per Google company’s claim, Willow is the first chip to achieve below threshold quantum error correction.[1][2] However, a number of critics have pointed out several limitations:

(*quoted at length in notes*)

---

[5] Wikipedia 2025-08-08

Review: Generalization of Forward Secrecy

♳ * Classical “Forward Secrecy” property requires tha old messages not broken by *later* loss/compromise of host key

- Generalized: old saved messages not broken by later breakthroughs either.
- Realistic threat?
  - ○ Saved messages have been decrypted with later breakthrus before.
  - ○ VENONA + GEE 1940s [6]
  - ○ NSA Utah Data farm, 2013

[6] see BLU Sept 2018 Venona footnote above

Review: NIST Post-Quantum Cryptography Standards

♳

> The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. – **NIST**

Review: NIST PQC Competition

♳

National Institute of Standards & Technology started a multi-round competition, similar to with AES and SHA3 competitions

- NIST announcement

- NIST Q&A
- Schneier on PQC

Review: Quantum Cracking 2023

♳

- **RSA2048 in play or not?** - Chinese academic paper claiming 2k bit RSA within range of current gen NON-fault-tolerant QC, no great surprise given Qubits available and theoretical algorithm size. Schor and Schneier unconvinced - does it actually converge w/o FT? Schneier 2023-01
- Schneier “You Can’t Rush PQC Standards”
- Quantum resistant hybrid-signing FIDO2 keys for 2FA
- **Side-Channel Attack against CRYSTALS-Kyber**

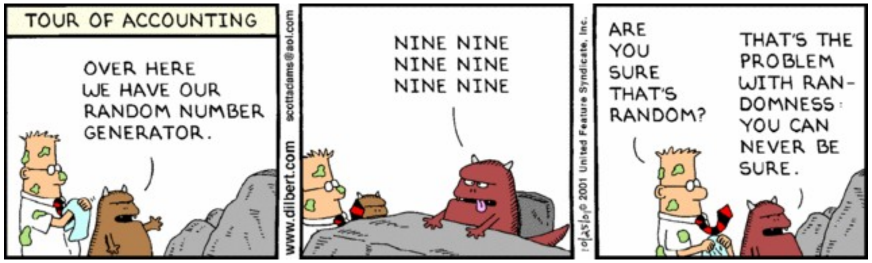
  [2023.02.28] CRYSTALS-Kyber is one of the public-key algorithms currently recommended by NIST as part of its post-quantum cryptography standardization process. Researchers have just published a side-channel attack’using power consumption’against an implementation of the algorithm that was supposed to be resistant against that sort of attack. The algorithm is not ‘broken’ or ‘cracked’’despite headlines to the contrary’this is just a side-channel attack. What makes this work really interesting is that the researchers used a machine-learning model to train the system to exploit the side channel.

OTOH as seen in TETRA:BURST, a side-channel attack can be used to extract key or algorithm from a piece of equipment that falls into opponent lab.

Review: Known weaknesses

♳

- breaks eliminated 62 of 69 entrants in Rounds 1 to 4
- including the two front-runners, Rainbow and SIKE
- 7 remain, will they survive?
- FALCON would be compromised by a lack-of-randomness in salt, or failure to salt, as repeating same key and hash again gives too much information.


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

Isn't non-random or uniformly-blank Salt an unlikely failure?

TL;DR ***No. It's happened.*** (*see in notes*)

NIST PQC Timeline (updated)

- 2022-04-28 How to Prepare Your PKI for Quantum Computing (April 28, 2022)
- 2023-03-03 Post-Quantum Cryptography Conference (Friday March 3, 2023 - Ottawa, Canada)
- 2023-08 FRN RFC Draft Standards FIPS 203, 204, 205.
- 2024-04 Fifth PQC Standardization Conference
- 2024-08-15 FIPS Standards; `FIPS Allowed`: NIST announced finalized PQC standards for 3 of 4 “winners” (3 more to come)
  - FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
    - proposed as “CRYSTALS-Kyber”
    - general encryption (payload symmetric key encapsulation), for data in motion
    - August 2024
  - FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)
    - proposed as “CRYSTALS-Dilithium”
    - Digital Signatures, authentication
    - August 2024
  - FIPS 205: Stateless Hash-Based Digital Signature Standard (ML-DSS; SLH-DSA)
    - proposed as Spincs+
    - Digital Signatures, authentication
    - August 2024
- 2024-10-24 PQDSS Round 2 starts
- 2025-03-11 future FIPS 207 HQC-KEM selected from PQKEM round 4.
- 2025-08-28 FIPS 206 Draft (FN-DSA) submitted
- ….. you are here …..
- 2025-09-24 ’ Sixth PQC Standardization Conference *the week after this annual talk, so expect more news soon!* Conference page has Agenda; already has 2 sessions on Cryptanlysis of PQDSS Round 2.
- 2025/26 FIPS certification for the PQC algorithms; `FIPS Approved`.
- …. and eventually, FIPS disapproval/phase-out/banishment of non-PQC legacy algorithms …

NIST PQC

2025 NIST PQC FIPS 206 FN-DSA draft

A year ago, NIST finalized 3 FIPS PQC standards and selection of several PQC algorithms (1 KEM, 2 DSA). Since then, a few more have progressed through the process.

- FIPS 206 draft submitted Falcon / FN-DSA
  - FN-DSA (Falcon, also DSA) was scheduled for finalization later in 2024 but has only just been submitted as draft standard August, 2025
    > Nov 7, 2024 Falcon (to be renamed FN-DSA) seems much better than SLH-DSA and ML-DSA if you look only at the numbers in the table. There is a catch though. For fast signing, Falcon requires fast floating-point arithmetic, which turns out to be difficult to implement securely. CloudFlare

“Securely” presumably is regarding **timing**.

Cryptographic math wants to be not only one-way functions but (in a world where encryption is often on a shared CPU) not only fixed time but also fixed tempo, to avoid side-channel (power, CPU%, memory access pattern, …) disclosure of key bits or key correlatives.

2024-OCT NIST PQC DSA Round 2

- Round 2 DSA candidates, October 2024: 14 new candidates (looking for diversity) ♳
    - CROSS Codes and Restricted Objects Signature Scheme
    - LESS Linear Equivalence Signature Scheme
    - SQIsign
    - HAWK
    - Mirath (MIRA+MiRitH)
    - MQOM MQ on my Mind
    - PERK
    - RYDE
    - SDitH Syndrome Decoding in the Head
    - MAYO
    - QR-UOV
    - SNOVA
    - UOV Unbalanced Oil and Vinegar
    - FAEST

2025 future FIPS-207 selected Hamming Quasi-Cyclic (HQC, KEM)

- *selected* from fourth round candidates
- “backup for ML-KEM”, “different math”
- Key-Encapsulation Mechanism (KEM), for data in motion
- selected March 2025; targetting draft standard 2026, final FIPS 2027
- this selection sidelines the other fourth-round contenders BIKE (close), Classic McEliece (deferred pending ISO; huge keys), SIKE (broken).
- HQC had the simplest hardness assumptions.

2024/2025 Related NIST

Random Bits

NIST SP 800-90A PRE-DRAFT Call for Comments: **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**

- requesting comments on draft Rev.1 prior to producing Rev.2

AES 256 (2025)

c/o ___

Dec. 2024: NIST proposed a 256-bit block variant of AES with a static 256-bit key size.

Public comments were open until January 25, 2025.

NIST PR

3 History Vignette - Midway is low on water

Or,

AF is MIDWAY

The Battle of Midway was won miles away, weeks before, in a bunker in Hawaii. □⦶

Historic Context

Battle of Midway wasn’t a surprise landing after-all.

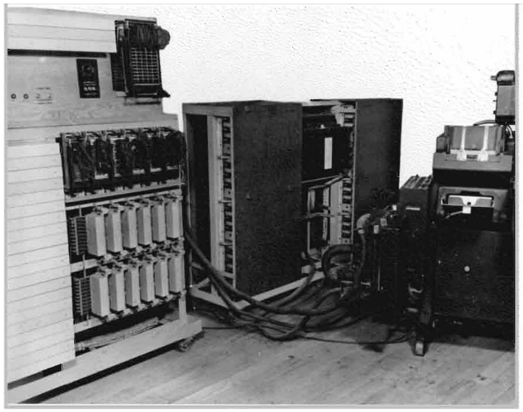
- Spring 1942, months after Pearl Harbor
- Decodes show IJN planning next offensive against “AF”
  - various two-letter codes AH, AK, … were Hawaiin islands
  - AF should be nearby if consistent
  - inferred must be Midway Is., but not conclusive
- strategem to prove it: feed a Known Plain Text to IJN listeners and hope they send it in code being read
  - Midway sends LOW ON WATER in the clear (as if not considered secret)
  - IJN sends AF LOW ON WATER in JN-25b, intercepted & decrypted.
- USN carriers ambush IJN carriers

Revenge of Pearl Harbor Navy

Only after Pearl Harbor attack was Station HYPO, Navy Cryptological unit there, assigned to the suddenly higher priority “JN-25b” IJN operational code.

- 3rd edition codebook per IJN records, but version “b” in USN records
- 5 digit code-words (code-groups) per word or phrase encoded
- superenciphered by additive key
- codebook versions reissued periodically
- key table booklets (of 50,000 5-digit random nubmers) reissued more often
- Some progress already made by other stations

Processing Encicode to find, strip Additive key

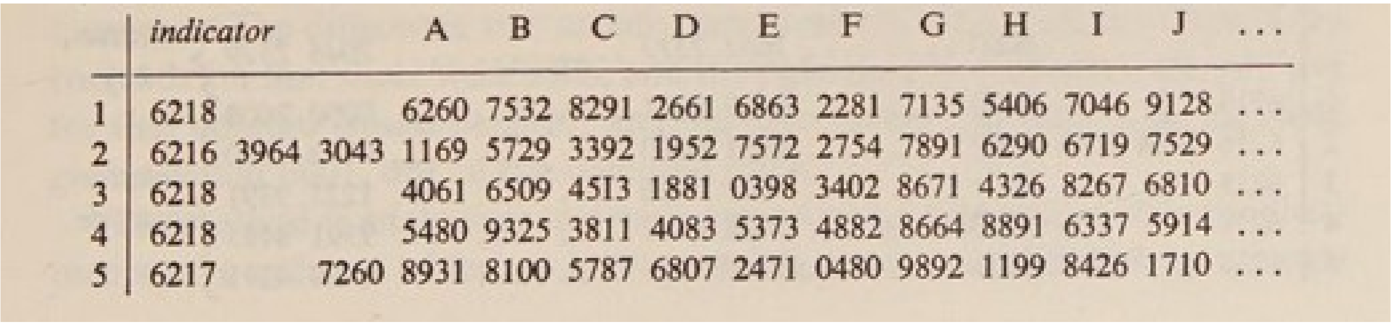


(~~TS//SI~~) Slide Run

- Using IBM 405 Tabulators
- Keypunch leading 16 × 5 figure groups per 80 column cards
- Search for coincidences, and common differences
- also for common prefixes of message
- statistical tests; common adjacencies; index of differences seen.
- also cards for known placode groups' Kana (and translation?) to produce (partial) decrypts
- Encicode : — portmanteau of enciphered code, the numeric or alphabetic codegroup as protected by a superencipherement. (Coined by WFF himself!) See
- for historical reasons, Pearl Harbor HYPO had dedicated IBM tabulators in the bunker (SCIF) and space to add crew

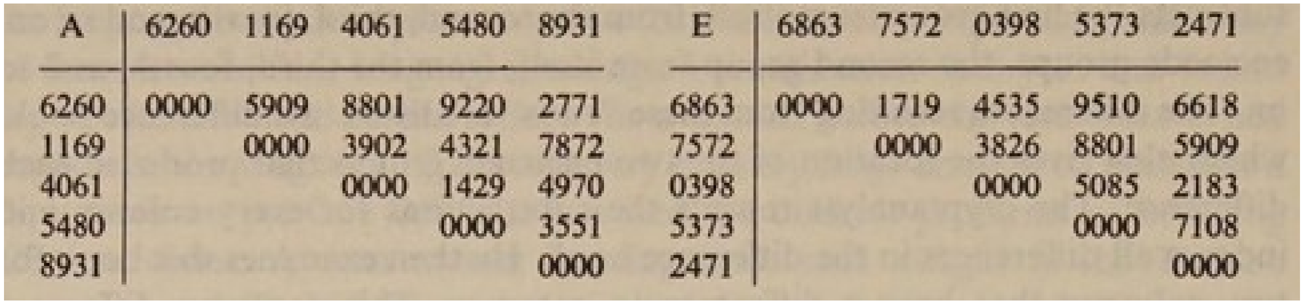
Method of Differences

- Calculate (and index and record!) the **differences** of all the encicode groups in a message.
- Using Indicator or Kappa/Chi tests, align messages using common key in depth



	indicator			A	B	C	D	E	F	G	H	I	J	. . .
1	6218			6260	7532	8291	2661	6863	2281	7135	5406	7046	9128	. . .
2	6216	3964	3043	1169	5729	3392	1952	7572	2754	7891	6290	6719	7529	. . .
3	6218			4061	6509	4513	1881	0398	3402	8671	4326	8267	6810	. . .
4	6218			5480	9325	3811	4083	5373	4882	8664	8891	6337	5914	. . .
5	6217		7260	8931	8100	5787	6807	2471	0480	9892	1199	8426	1710	. . .

5 messages in depth



A	6260	1169	4061	5480	8931	E	6863	7572	0398	5373	2471
6260	0000	5909	8801	9220	2771	6863	0000	1719	4535	9510	6618
1169		0000	3902	4321	7872	7572		0000	3826	8801	5909
4061			0000	1429	4970	0398			0000	5085	2183
5480				0000	3551	5373				0000	7108
8931					0000	2471					0000

Difference runs on columns A and E.

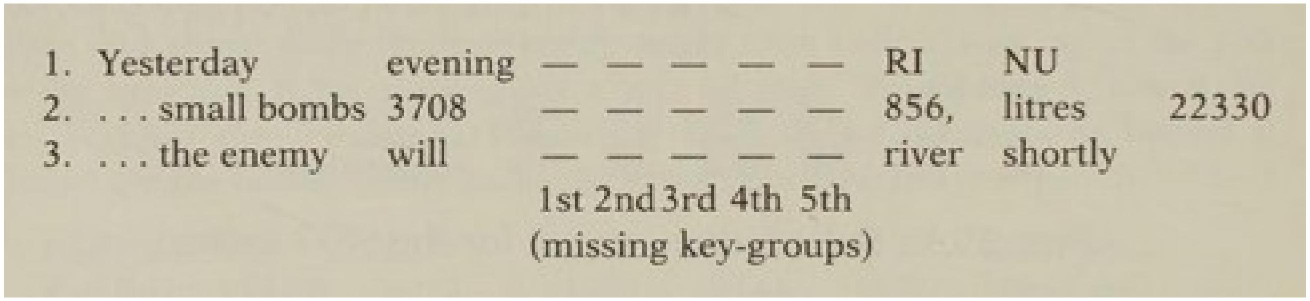
- note `8801` and `5909` are common differences between columns A and E.
- (full differences would show more such)
- subtracting relative difference from all of the column produces relative key and relative placode groups.

Book-Breaking

- Can follow stripping, or can lead stripping.
- first: recover code-groups for stereotyped beginning and end of message
- second: code-groups used for numerals and spelling non-coded-words broken as simple cipher
- already known groups plus context of message (from, to, when, length, military situation) suggest values for first group in a gap
- if a One Part Code, the code and plain-text values are in numeric=alphabetic order, so adjacency is a big hint
- cross-riff messages in depth
  - which may solve gaps in Additive key-book as well
  - assuming a group in a gap from context implies a difference, which will imply code-groups for messages in depth; do they make all sense too?

Using a Depth

Example from Hinsley & Stripp:



1.	Yesterday	evening	—	—	—	—	—	RI	NU	
2.	. . . small bombs	3708	—	—	—	—	—	856,	litres	22330
3.	. . . the enemy	will	—	—	—	—	—	river	shortly	
			1st	2nd	3rd	4th	5th			
			(missing key-groups)							

Stripp-298-depth

Works like an N-dimensional Cross-word puzzle … but with cells being codewords representing words or phrases, and connections being same-offsets in codeword sequence.

4 Bibliography & Footnotes

Section 4 - Bibliography is in the Notes version of files. It doesn't fit well in slides.

The **YouTube** of this presentation will be linked on BLU.org along with these slides and extended notes *etc* as 2025-sep as per usual.

Prior talks in this series - most talks have slides &/or YouTube attached, sometimes extras.
Alas the YouTube audio pre-pandemic wasn't great, BLU will need a donation of a wireless clip-on mike if we ever return to Hybrid/In-Person meetings. Or we all need to wear a wired or BT headset while presenting in person?