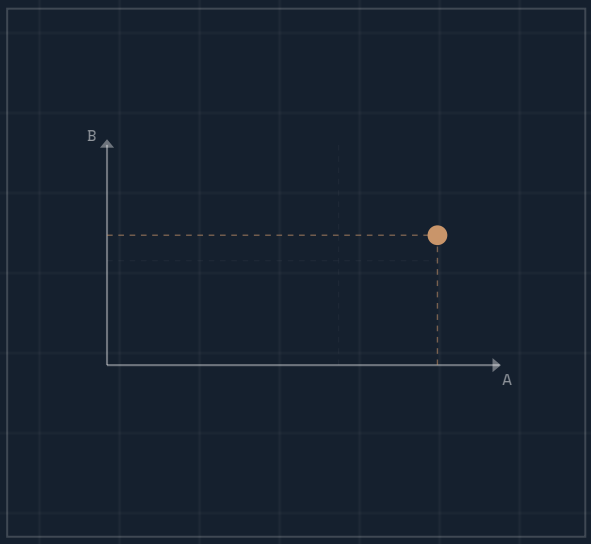
Linear Diophantine Systems & Post-Quantum Cryptography

The MRS Framework: From fundamental number theory to hybrid unbreakability.

Bilal el Issaoui | Amsterdam | 2026

A number is not a magical object, but a reference point in a perfectly calibrated system.

$$N = 19A + 9B$$



The Three Pillars of the (19, 9) System

Congruence

$19 \equiv 1 \pmod 9$

The anchor value A_0 = dr(N) provides absolute stability in the system.

Step Vector

$A \to A + 9, \quad B \to B - 19$

Each successive representation shifts exactly along this predictable axis.

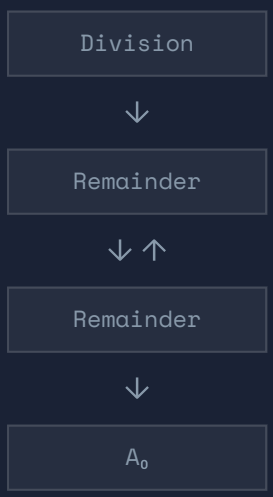
Euler Key

$\varphi(19) = 18 = 2 \times 9$

The mathematical coupling of the two bases, crucial for cryptographic synthesis.

The Efficiency Leap: Euclidean Algorithm vs. MRS

The Past: Euclidean Algorithm



Slow iterative process and back-substitution, initially yielding negative coordinates.

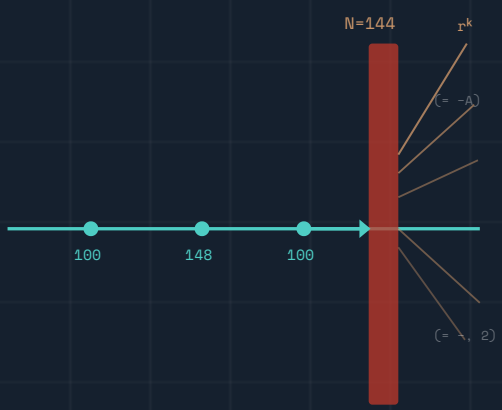
The Direct Route: MRS System

$$A_0 = N \pmod 9$$

$$R(N) = [(\lfloor N/19 \rfloor - dr(N)) / 9] + 1$$

One direct operation. Immediate result in positive coordinates. Superior computational efficiency.

The Frobenius Problem & Scale Invariance



For the standard system N ≥ 144 is required. What happens with smaller numbers?

The digital root is **scale invariant**. Multiplication merely appends a zero; the digit sum remains unchanged.

$$dr(N) = dr(10N) = dr(100N) = dr(10^k \times N) \quad \text{for all } k \geq 0$$

Extension I: The Scalability Waterfall

MACRO SCALE (k = 0)

N	k	$N' = 10^k \cdot N$	A_0	B_0	Verification
420	0	420	6	34	19 × 6 + 9 × 34 = 114 + 306 = 420 ✓

÷ 10

MESO SCALE (k = 1)

N	k	$N' = 10^k \cdot N$	A_0	B_0	Verification
42	1	420	0.6	3.4	19 × 0.6 + 9 × 3.4 = 11.4 + 30.6 = 42 ✓

÷ 10

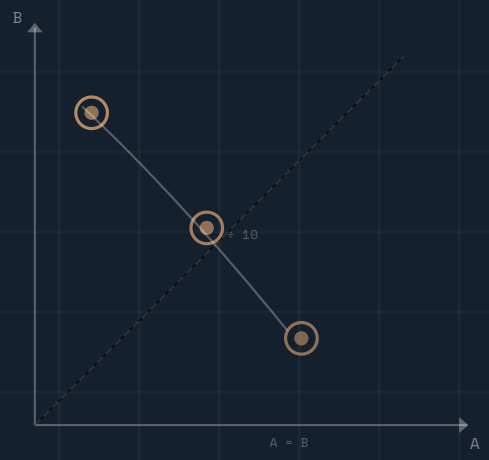
MICRO SCALE (k = 2)

N	k	$N' = 10^k \cdot N$	A_0	B_0	Verification
4.2	2	420	0.06	0.34	19 × 0.06 + 9 × 0.34 = 1.14 + 3.06 = 4.2 ✓

The proportional structure is always preserved. The mathematical anchor A_0 is simply the scaled digital root:

$dr^*(N) = dr(N) / 10^k$

Symmetry Cartography



Macro: N = 2520 → (90, 90)

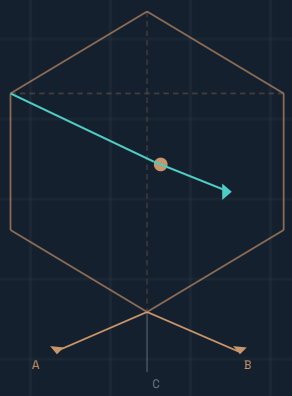
Meso: N = 252 → (9, 9)

Micro: N = 25.2 → (0.9, 0.9)

N	k	$N'=10^k \cdot N$	A_0	B_0	Verification
2520	0	2520	9	9	dr(2520)/1 = 9 → 90+90
252	1	2520	9	9	dr(252)/10 = 0.9 → 9+9
25.2	2	2520	9	9	dr(25.2)/100 = 0.09 → 0.9+0.9

Insight: Symmetry is a fundamental, scale-independent property of the MRS lattice. Points shift along a perfectly calculated axis.

Extension II: The Third Dimension (pA + qB + rC)

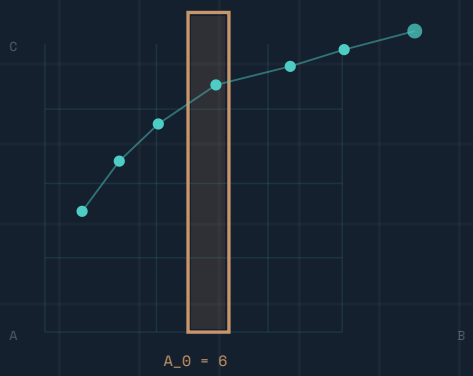


Rules

☑	$p \equiv 1 \pmod{q}$	The modular base property
☑	$\gcd(p, q) = 1$	Coprimality of p and q
☑	$r \mid q$	r divides q, so r and q are modularly compatible
☑	$p \equiv 1 \pmod{r}$	The modular property also holds for r

Conclusion: As long as these four mathematical rules hold, the new axis C never disturbs the fundamental anchor A_0.

The (19, 9, 3) System: The Canonical Extension

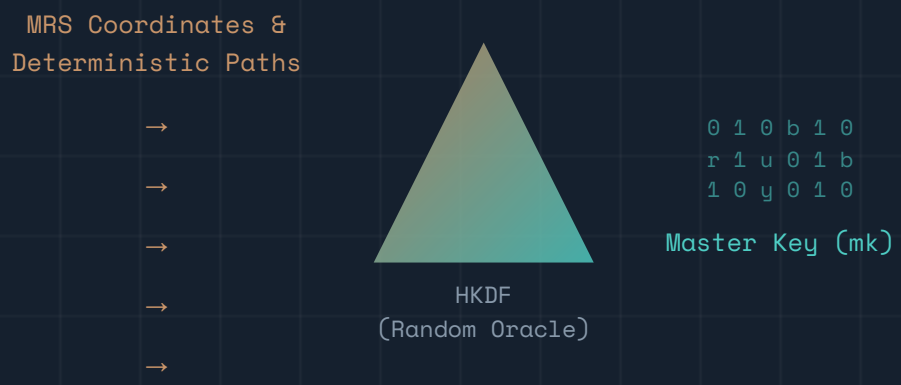


Case: N = 240

- Option 1: (6, 14, 0)
- Option 2: (6, 11, 9)
- Option 3: (6, 8, 18)

Insight: Axis C redistributes the remainder in steps of 3, while B compensates in steps of 9. The anchor A_0 remains unchanged, equal to the digital root (Theorem 3.2).

The Bridge: From Structure to Entropy



The complex yet fully predictable paths of the MRS chain form a perfect, hidden source of entropy.

```
mk <@ RO.get(encode_chain chain ++ hkdf_context);
```

We use mathematical predictability internally to generate absolute cryptographic chaos (security) externally.

The Hybrid Problem: Quantum vs. Classical

Quantum Threat

Shor's algorithm breaks RSA/ECC in polynomial time.

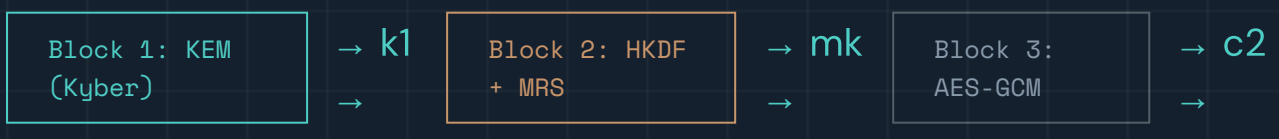
New Post-Quantum solutions (such as Kyber) are robust, but relatively young in their adoption cycle.

Classical Symmetry

AES-GCM is extremely fast, globally proven, and intrinsically quantum-resistant (Grover only requires doubling the key size, e.g. AES-256).

The Synthesis: A hybrid KEM design combines the best of both worlds. The embedding of the mathematical MRS layer forms an unbreakable, additional shield.

System Architecture: MRS_AUTH_KEM_Hybrid



Block 1

KEM (Kyber)

Task: Key encapsulation (k1). Formally IND-CCA2 secure against adaptive quantum attacks.

Block 2

HKDF + MRS

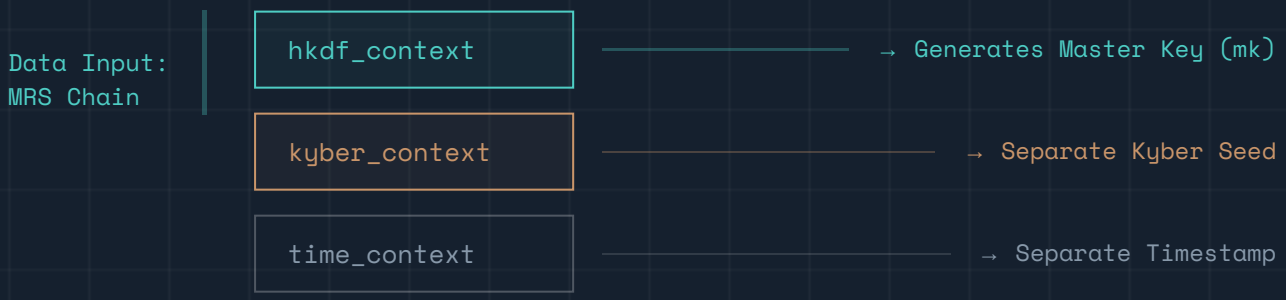
Task: Key derivation from the deep mathematical MRS chain (mk). Modelled as a Random Oracle.

Block 3

AES-GCM

Task: Authenticated Encryption with Associated Data (AEAD). IND-CPA secure. Produces ciphertext (c2): Message + Tag + Nonce.

Domain Separation: Collision Prevention in the Random Oracle




```
(*
=============================================
*)
(* 3. HKDF via Random Oracle *)
(* *)
(* We reuse the HKDF_RO interface from *)
(* MRS_AUTH_Part2. *)
(* The master key mk is derived from the *)
(* MRS chain: *)
(*  mk = RO.get(encode_chain chain *)
(*          ++ hkdf_context) *)
(* Via a separate context this is domain- *)
(* separated from the Kyber seed derivation *)
(* and the timestamp derivation. *)
(*
=============================================
*)
```

```
op hkdf_context : bytes.
(* domain separation for master
key derivation *)

axiom
hkdf_context_distinct_kyber :
  hkdf_context <>
kyber_context.
axiom
hkdf_context_distinct_time :
  hkdf_context <> time_context.
axiom
hkdf_context_distinct_chain :
  hkdf_context <>
chain_context.

(* Domain sep: all four context
strings unique *)
lemma hkdf_domain_sep (ch : int
list) :
```

Different processes cannot mathematically corrupt one another.

Operational Flow: Encryption to Decryption

1. Generate KEM key pair (pk, sk). → `pk (Public Key)`
2. Encapsulate session key k1 via KEM → c1. → `c1 (Encapsulated k1)`
3. Build the complex mathematical MRS chain for number N. → `MRS Chain`
4. HKDF: Derive master key mk from the generated chain. → `mk (Master Key)`
5. The Crux: Combine keys → $k_{combined} = k1 \oplus mk$
6. Encrypt the original message with AES-GCM under k_combined → c2. → `c2 (Message + Tag + Nonce)`
7. Transmission: Send (pk, c1, c2) over the open network. → (pk, c1, c2) 🌐

The Formal Security Proof: Game Hopping

Game 0: The Real Protocol

k1 → mk → KEM ⊕ AES-GCM

$k_{combined}$ = k1 ⊕ mk

c2 = AES-GCM(…, $k_{combined}$)

→

Game 1: Replace KEM Key with Random (k_r)

k_r (random) ⊕ MRS chain → AES-GCM

→

Game 2: Replace Combined Key with Random

k_r' (random) → AES-GCM

→

Game 3: Replace AES Ciphertext with Random

Random ciphertext (c_r)

Mechanism: In Game 3 the attacker's success probability is exactly 50%. By calculating the mathematical distance (advantage) between Game 0 and Game 3, we prove the absolute security of the protocol.

The Formal Proof: The IND-CCA2 Battlefield

What is the power of the Adversary?
- Full and unrestricted access to the public key.
- Access to a Decryption Oracle: may decrypt any arbitrary ciphertext.

The Single Exception: The Oracle refuses to decrypt the specific challenge ciphertext (c1^).

```
module DecOracle (K : KEM) = {
  var sk : skey
  var c_star : cipher
  var queries : cipher fset
  proc init(s : skey, c : cipher) =
{
    sk <- s; c_star <- c; queries <-
fset0;
  }
}
```

The Goal: The attacker must distinguish with probability greater than 50% whether the challenge message is real or random noise.

Proof Step 1: Reduction to Kyber KEM

Replace k1 with k_r. This difference is mathematically tightly bounded by the IND-CCA2 advantage of the underlying KEM. As long as the KEM is secure, the attacker is blind to this replacement.

```
(* Game 1: replace k1 with a fresh random key k_r *)
(* Observation: k_combined = k1 XOR mk. If k1 is uniform and *)
(*  independent of mk, then k_combined is also uniform. *)
(* But we want to use the KEM security, so we replace *)
(*  k1 directly with a random value k_r. *)
(* This is justified by the IND-CCA2 property of K: *)
(*  the adversary cannot distinguish enc(pk).k1 from random. *)
(* Formally: |Pr[Game0] - Pr[Game1]| is bounded by the KEM advantage. *)
```

Proof Step 2: The Power of XOR (Exact Equivalence)

$$k_{combined} = k_r \oplus mk$$

1. Because in Game 1 k_r is fully random (uniform), the XOR operation functions here as an infallible One-Time Pad.

2. $|Pr[Game\ 1] - Pr[Game\ 2]| = 0$. This transition is mathematically exact.

Result: The key is transformed into pure random noise without any loss of security guarantees.

Proof Step 3: Reduction of AES-GCM

Game 2

Encrypted message (c2)

Game 3

```
01001010 11010010
10110101 00101101
11001010 01010011
```

Random ciphertext (c_rand)

With a fully random key from the previous step, security now rests entirely on the **IND-CPA** strength of **AES-GCM**. In **Game 3** there is absolutely no remaining relation to the original data. The attacker's success probability has collapsed to a pure guess (exactly 50%).

The Conclusion: A Formally Proven Fortress

$$\text{Attacker's Advantage} \leq 2 \times \text{negl}(\lambda)$$

The security margin is absolute. Through the XOR architecture, the system forces the attacker to simultaneously break both Post-Quantum Kyber and the deep cryptographic MRS chain in order to succeed.

```
(* Corollary: summary of security guarantees *)
(* *)
(* The MRS_AUTH_KEM protocol is IND-CCA2 secure under: *)
(* 1. The KEM (Kyber) is IND-CCA2 secure *)
(* 2. HKDF is modelled as a Random Oracle *)
(* 3. AES-GCM is IND-CPA secure *)
(* *)
(* The security margin is 2·negl(λ) ≤ negl(λ). *)
```

Order in numbers dictates absolute chaos for the adversary.

...unmatched international security.

B. el Issaoui | Mathematical Research Amsterdam | 2026