

Cauldron Me Crazy

Kansas K.A.R. 111-23-25 · eInstant Cert Pack v1

Issued: 2026-05-15T21:45:36.567492Z · Authority: Multi.Bingo iLottery RGS
Signing key: Ed25519 · ID d651f1b9f793f40d

Math validation

Pool size	1,000,000
RTP @ unit denom	88.0025%
Top prize (max denom)	\$20,000
Bonus engine	generic_bonus

1. Game specification (Kansas K.A.R. 111-23-25)

Cauldron Me Crazy is an instant lottery game governed by Kansas K.A.R. 111-23-25. Finite-pool model with 1,000,000 shares per pool. The bit-exact payable below has been imported from the K.A.R. (j) odds table.

Prize formula: $\text{prize_cents} = \text{multiplier} \times \text{denom_cents} \times \text{tickets_purchased}$

2. Paytable (41 tiers)

Multiplier	Count in pool	Odds (1 in)
x4000.0	1	1,000,000.00
x3000.0	1	1,000,000.00
x2000.0	1	1,000,000.00
x1000.0	1	1,000,000.00
x500.0	5	200,000.00
x450.0	2	500,000.00
x400.0	5	200,000.00
x350.0	2	500,000.00
x300.0	5	200,000.00
x275.0	2	500,000.00
x250.0	5	200,000.00
x200.0	5	200,000.00
x175.0	10	100,000.00
x150.0	10	100,000.00
x125.0	10	100,000.00
x100.0	25	40,000.00
x90.0	75	13,333.33
x80.0	75	13,333.33
x75.0	75	13,333.33
x70.0	25	40,000.00
x65.0	25	40,000.00
x60.0	25	40,000.00
x55.0	25	40,000.00
x50.0	25	40,000.00
x45.0	500	2,000.00
... (16 more)		

3. Pool architecture

Each pool consists of 1,000,000 shares. Pool generation: RGS service `multibingo-rng:9443` provides the server seed (RNG_STRICT=true, no local fallback). Paytable counts written into array, shuffled with `mulberry32(SHA-256(server_seed))` Fisher-Yates. Pool audit_hash chained via Ed25519 signature. Tickets consumed sequentially; outcome = multiplier at position in shuffled array.

4. Audit chain (K.A.R. h)

Daily Merkle root signed with Ed25519 (key ID `d651f1b9f793f40d`). Leaves = ticket_hash + pool_hash. Persisted in WORM-locked PG row + audit blob to disk (S3 Object Lock in prod). Each day's row stores `prev_root_sha256` forming a hash chain.

5. Verifier endpoints

```
GET /api/ilottery/games/CAULDRON_ME_CRAZY/paytable
GET /api/ilottery/games/CAULDRON_ME_CRAZY/config?jur=GLI-SANDBOX
POST /api/ilottery/games/CAULDRON_ME_CRAZY/open-pool
POST /api/ilottery/games/CAULDRON_ME_CRAZY/play
POST /api/ilottery/vector/replay (game_code=CAULDRON_ME_CRAZY)
GET /api/ilottery/verify/:ticket_id
GET /api/ilottery/merkle/proof/:ticket_id
GET /api/ilottery/audit/public-key
```

6. Test vectors v1

URL: https://kobowlotto.com/mathforge/ilottery/gdd/cauldron_me_crazy/vectors_v1.json
600 vectors × 5 denoms = 3,000 prize data points (6 tiers × 100 each).

7. Operator Ed25519 public key

```
-----BEGIN PUBLIC KEY-----
MCowBQYDK2VwAyEAU2k0zXnm09QHDuKlSEQYUAFeACAEOTUceEuiRGLSiXs=
-----END PUBLIC KEY-----
```