ENI6MA Paper Identity Proof

Signature proof — server-minted one-shot identity sheets
for mail, deeds, ballots, and notarized packages

Booklet serial: `BOOKLET-SERIAL-PENDING`

Circuit SHA-256:

`fd04da71e9c38cfdfa444b5505420908d710af8ff50cba3f88d66c8e079fab44`

Scan to open the circuit / validate landing

https://registry.eni6ma.net/circuits/SYNTHETIC-1

Each sheet in this signature proof is a blank-check paper identity: unique, circuit-bound, and spent after one use. Affix or enclose a sheet with the package you mail. The recipient validates against the enrolled circuit and learns only PASS or FAIL.

What these sheets are

This signature proof is not a password list and not a puzzle game.

Each page is a **server-minted one-shot paper identity sheet**. A sheet binds a unique timestamp tau and a unique nonce to an enrolled cryptographic circuit. You carry the booklet the way you would carry blank checks: unused sheets prove nothing until you intentionally spend one with a mailing or filing.

What you hold

- A **physical leaf** with a dice-labeled ceremony card and a SHA-256 footer.
- A **nonce** and tau that identify this leaf to the validator.
- A **circuit binding**: the sheet is only meaningful for the circuit whose SHA-256 appears on the cover of this booklet.

What you do not hold

- A reusable credential or shared secret you can type forever.
- A password, PIN, or recovery phrase.
- A certificate that anyone can photocopy into lasting authority.

When the sheet is validated, the nonce is burned. A spent sheet cannot authorize again. That is the product: paper that signs once, then dies.

Why a spent sheet is useless

Every sheet is minted with a unique tau (server timestamp) and a unique nonce. The enrolled circuit treats those values as a one-time reservation.

Unique and circuit-bound

- **Unique tau / nonce.** No two sheets in an honest mint share the same identity. A photocopy of a spent sheet still points at a burned nonce.
- **Circuit-bound.** Validation asks for the circuit SHA-256 (or the book QR on the cover) plus the sheet's tau / nonce. A sheet from another circuit does not validate here.
- **Burn-before-validate.** On submit, the nonce is marked spent before the PASS/FAIL check completes. There is no preview, no undo, and no second try with the same leaf.

Unforgeable in practice

Forging a fresh sheet means minting a new reservation against the enrolled circuit—something an outsider cannot do from paper alone. Replaying a used sheet fails because the ledger already recorded the burn. Wrong-circuit hashes fail closed. The validator returns only PASS or FAIL; it does not export a reusable credential.

How to use this signature proof

Carry this booklet sealed. When you need a signature proof for a real-world package, tear or cut one unused sheet and **affix or enclose** it with what you send.

Typical mailings

Package	How the sheet helps
Deed / title packet	Ties the physical mailing to a one-shot circuit validation
Ballot / absentee package	Gives the receiving clerk a PASS/FAIL check without a reusable credential
Contract courier	Proves the enclosed leaf was spent for this send, not a photocopy farm
Notarized package	Pairs wet-ink / notary practice with a spent cryptographic leaf

Pattern

1. Keep unused sheets sealed and logged.
2. Affix or enclose **one** sheet with the package.
3. Complete the dice ceremony on that sheet (see Instructions).
4. Mail or hand-deliver the package.
5. Recipient validates: circuit SHA-256 (or book QR) + sheet tau / nonce → PASS/FAIL.

You do not need a smartphone at mailing time unless you want an optional photo of the completed sheet for your own custody file.

Custody — treat blanks like blank checks

Unused sheets are valuable the way blank checks are valuable: anyone who controls an unused leaf can attempt to spend it. Treat the booklet accordingly.

Rules of custody

- Store the booklet dry, flat, and sealed when not in use.
- Log every sheet that leaves the booklet (date, package, recipient, tau / nonce).
- If the booklet is lost or stolen, **revoke** the remaining unused nonces with your circuit operator before an attacker can spend them.
- Never photograph or photocopy an *unused* sheet into shared drives.

Custody log (fill by hand)

Date	Sheet tau / nonce (short)	Package / purpose	Recipient	Spent?

Retain this log with the booklet cover. A spent sheet should appear here with “Spent = Y” and the mailing reference.

Physical safety and non-claims

Care of unused sheets

- Avoid humidity, spills, and prolonged sun on unused leaves.
- Do **not** laminate unused sheets; coatings can block pens and scanners and make custody inspection harder.
- Do not fold through the dice card or the SHA-256 footer if you can avoid it.
- Keep the booklet away from children and casual desk access—blank-check rules.

What this booklet is not claiming

- It does not replace local wet-ink, notary, or statutory mailing rules. Pair the sheet with whatever your jurisdiction already requires.
- It does not grant legal title by itself; it provides a one-shot cryptographic identity leaf bound to an enrolled circuit.
- It does not claim that a damaged or altered sheet will still validate.
- PASS/FAIL is the only validator outcome you should expect; there is no exported long-lived credential after a successful check.

If a sheet is damaged before use, retire it in the custody log and use another unused leaf. Do not attempt to reconstruct footer hashes by hand.

Instructions — before you mail

Complete these checks **before** you pull a sheet from the booklet.

Enrolled circuit

1. Confirm the **circuit SHA-256** on the cover matches the circuit your recipient (clerk, title agent, counterparty) expects to validate against.
2. Note the cover **book QR** — it points at the circuit / validate landing. Recipients may scan that QR instead of typing the hash.
3. Confirm your operator has not revoked this booklet's remaining nonces.

Sheet footer

Each identity sheet prints a **SHA-256** footer for the leaf. Before mailing:

- Read the footer; confirm it is intact and legible.
- Record the short form of tau / nonce in your custody log.
- Do not mark unused neighboring sheets.

Seal unused sheets

After removing one leaf, reseal or clip the remaining booklet so loose blanks cannot fall out. Treat every remaining page as an unspent blank check.

Sign and mail

Affix or enclose

1. Remove **one** unused sheet from the booklet.
2. Affix it to the package (sleeve, pouch, or designated enclosure) **or** enclose it loose inside the sealed mailing so the recipient can find it without destroying the legal papers.
3. Do not include extra unused sheets "just in case."

Complete the dice ceremony

Follow the dice-labeled card on the sheet:

1. Work each round in order using the printed dice faces as your ceremony guide.
2. Mark only on the sheet you are spending.
3. Keep marks clear; do not obscure the SHA-256 footer or the tau / nonce identifiers the validator will need.

Optional photo

For your own custody file, photograph the completed sheet before sealing the package. Store the photo with the custody log entry. This photo is evidence for *you*; it is not a substitute for the physical leaf in the mailing.

Mail

Seal the package per your usual deed / ballot / courier practice and send it. The cryptographic leaf travels with the package; validation happens on the receiving side.

Validate (recipient)

The validator answers only **PASS** or **FAIL**. There is no reusable token after a successful check.

What the recipient enters

1. **Circuit identity** — enter the cover **circuit SHA-256**, **or** scan the **book QR** on the cover (preferred when the booklet cover is present).
2. **Sheet identity** — enter the sheet's tau and nonce (from the leaf enclosed with the package).
3. Complete any ceremony inputs the validate page requests for that leaf.
4. Submit. Expect burn-then-validate: the nonce is spent, then PASS or FAIL.

Typical validate path

`/validate/<nonce_uuid>`

Replace `<nonce_uuid>` with the nonce printed on the sheet. If your operator publishes a different base URL, use that; the book QR on the cover is authoritative for this booklet's circuit landing.

Outcomes

Result	Meaning
PASS	Leaf matched the enrolled circuit ceremony; nonce is spent
FAIL	Leaf did not match; nonce is still spent — no retry on this sheet
Conflict / gone	Nonce already burned or expired — do not accept as fresh

Do not accept a photocopy in place of a sheet whose nonce is already spent.

Workflow checklists

Ballot / absentee package

- ☐ Circuit SHA-256 confirmed with election office / operator
- ☐ One unused sheet logged and removed
- ☐ Dice ceremony completed on that sheet only
- ☐ Sheet affixed or enclosed with ballot package
- ☐ Unused booklet resealed
- ☐ Recipient validates with book QR or circuit hash + sheet tau / nonce

Deed / title packet

- ☐ Title agent knows which circuit to validate
- ☐ Sheet enclosed without obscuring recorded documents
- ☐ Custody log notes recording / courier ID
- ☐ Agent runs PASS/FAIL; refuses spent or wrong-hash leaves

Courier / contract

- ☐ Counterparty agrees on circuit in advance
- ☐ One sheet per send; no batch of blanks
- ☐ Optional sender photo filed with custody log
- ☐ Recipient validates before accepting the send as signed

Photocopy vs original

Item	Accept for validation?
Original unspent sheet in the package	Yes — then spend via validate
Photocopy of an **unspent** sheet	No — demand the physical leaf
Photocopy of a **spent** sheet	No — nonce already burned
Photo-only (no leaf)	No — unless your operator explicitly allows an evidence-only workflow

The original leaf is the object of custody. Photocopies are for sender records, not for minting

a second validation.

Failures and what to do

Failure	Likely cause	Action
Replay / conflict	Nonce already burned	Reject package as already spent; request a fresh sheet from sender
Wrong hash	Circuit SHA-256 does not match this booklet	Re-check cover hash / book QR; do not force another circuit
Damage	Footer or ceremony card unreadable	Sender retires sheet in custody log; remint/remail with a new leaf
Expiry	Operator TTL or revocation hit unused leaf	Confirm revocation list; issue replacement booklet if needed
Shoulder-surfing	Observer watched ceremony or photographed blanks	Treat exposed unused sheets as compromised; revoke and reissue

Hard rules

- Never retry validation on the same nonce hoping for a different outcome.
- Never “fix” a wrong circuit hash by editing the footer.
- If the booklet was exposed, revoke remaining blanks even if no sheet is known to be spent yet.

When in doubt, fail closed: do not treat the mailing as cryptographically signed until PASS is observed on the enrolled circuit.

Verifier card — tear-out checklist

For clerks, title agents, and receiving officers. Keep with the package file.

Before you accept

1. Confirm sender's booklet **circuit SHA-256** (or scan **book QR** on cover).
2. Locate the **original** identity sheet in the package (not a photocopy alone).
3. Read sheet tau and nonce; confirm footer SHA-256 is legible.
4. Open validate landing; enter circuit identity + sheet identity.
5. Submit once. Record **PASS** or **FAIL** below.
6. If PASS: file sheet with package evidence; mark spent in any local log.
7. If FAIL / conflict / gone: reject cryptographic claim; follow local procedure.

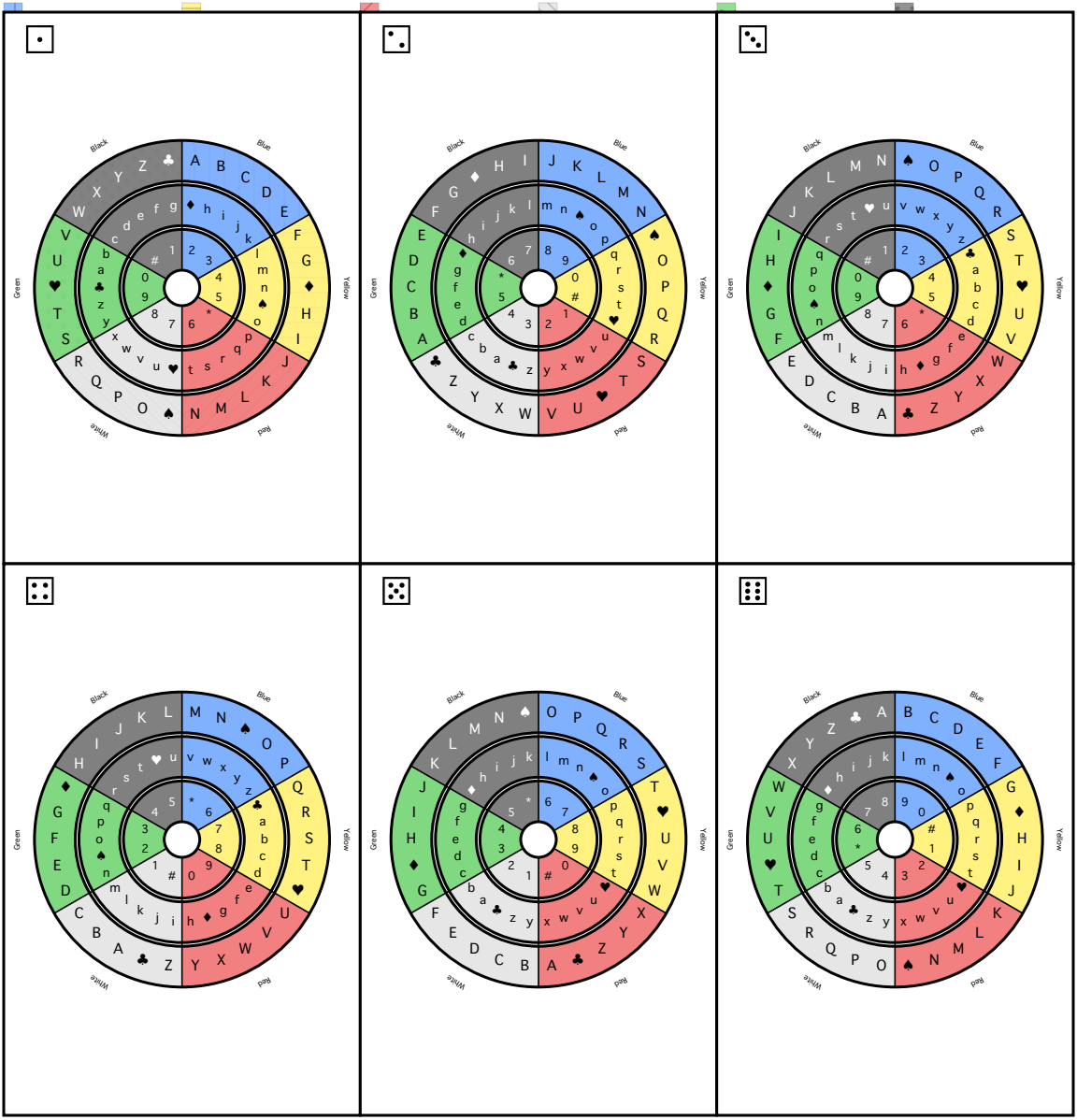
Result

- Date: _____
- Operator / clerk: _____
- Circuit (short): _____
- Sheet nonce (short): _____
- Outcome: □ PASS □ FAIL □ CONFLICT □ GONE
- Notes: _____

_____

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052854

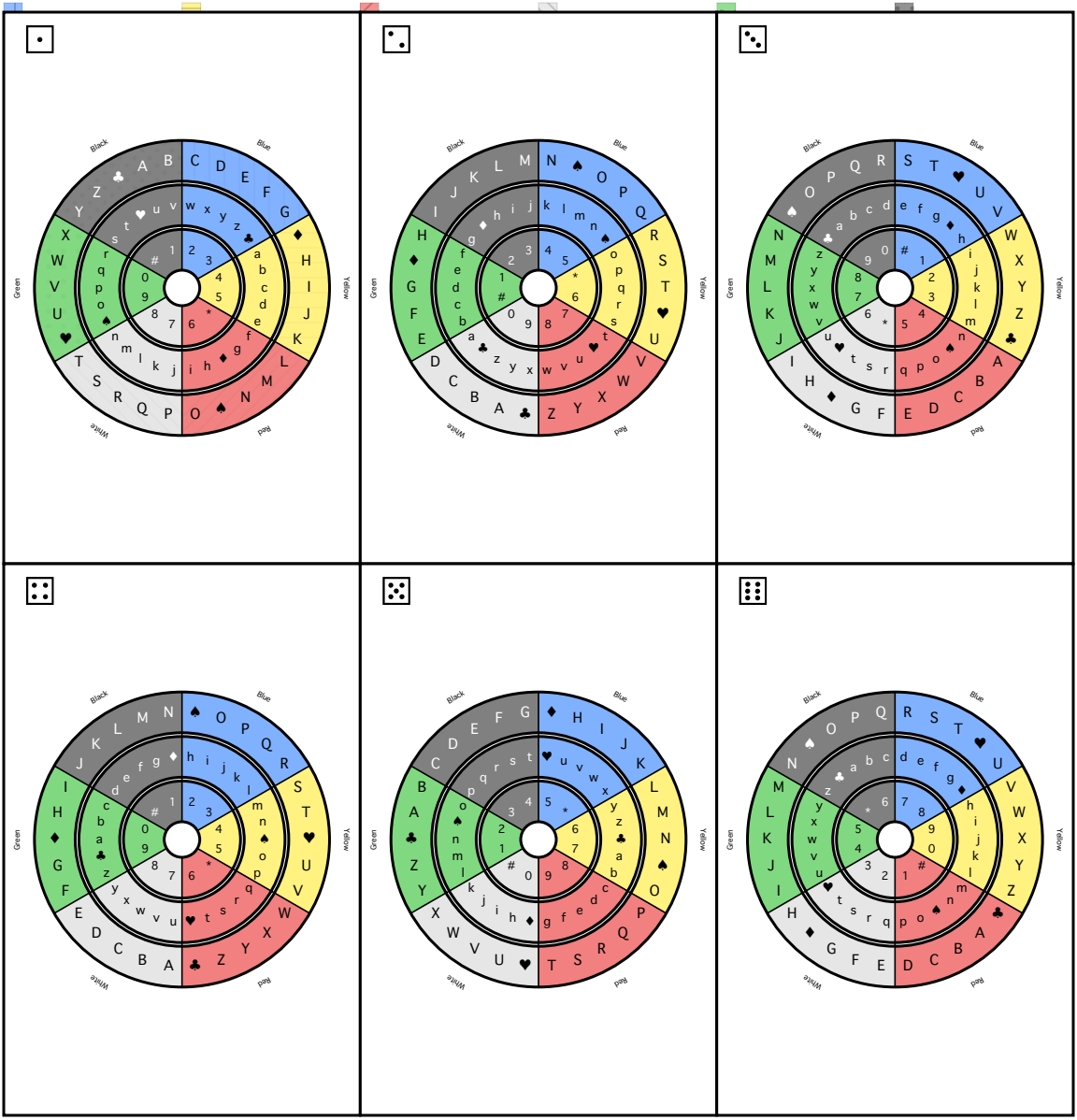


τ: 1785533985052854 | sha256(τ): 57c2b6bc

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052855

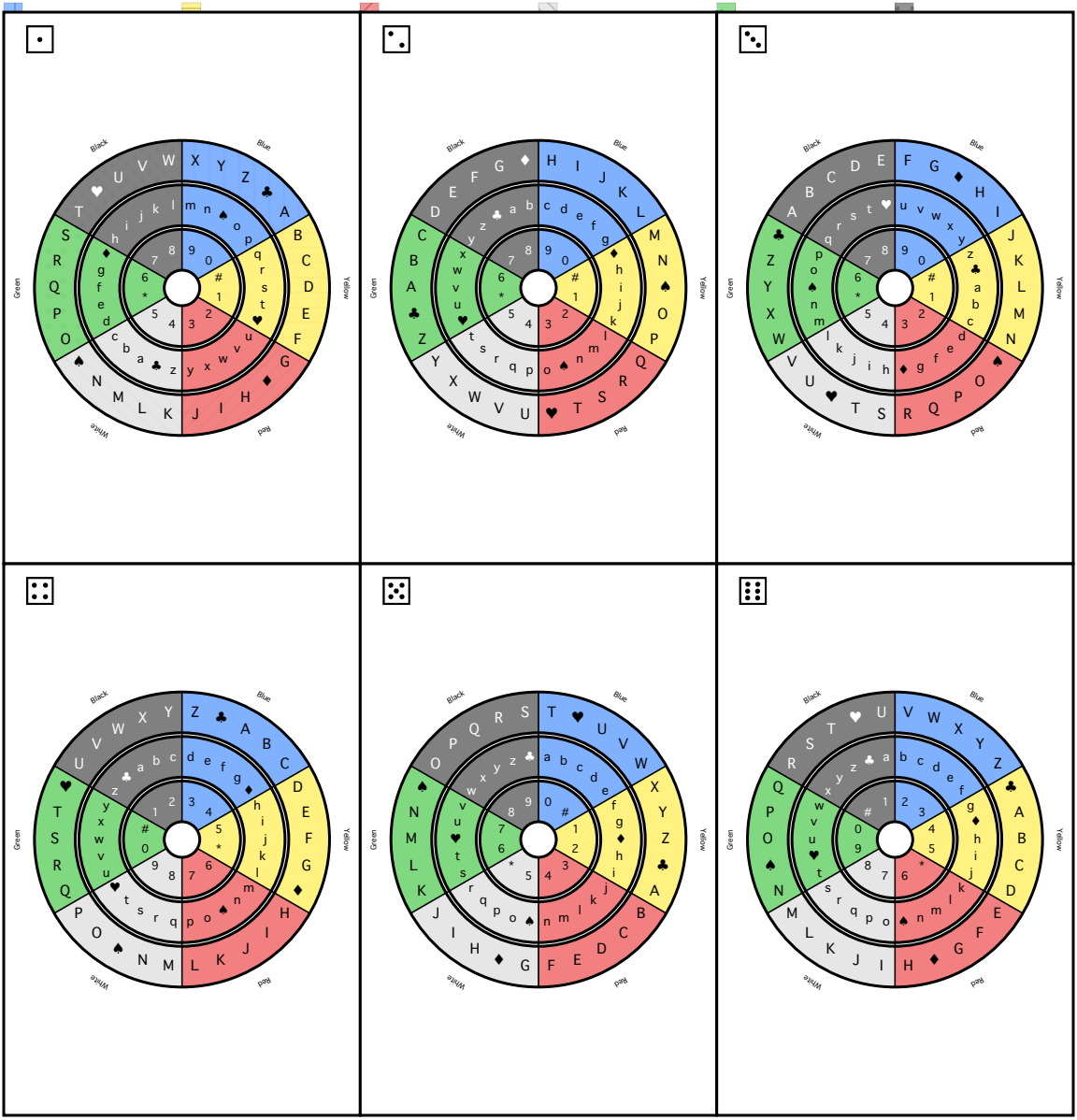


τ: 1785533985052855 | sha256(τ): 58ee2b16

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052856

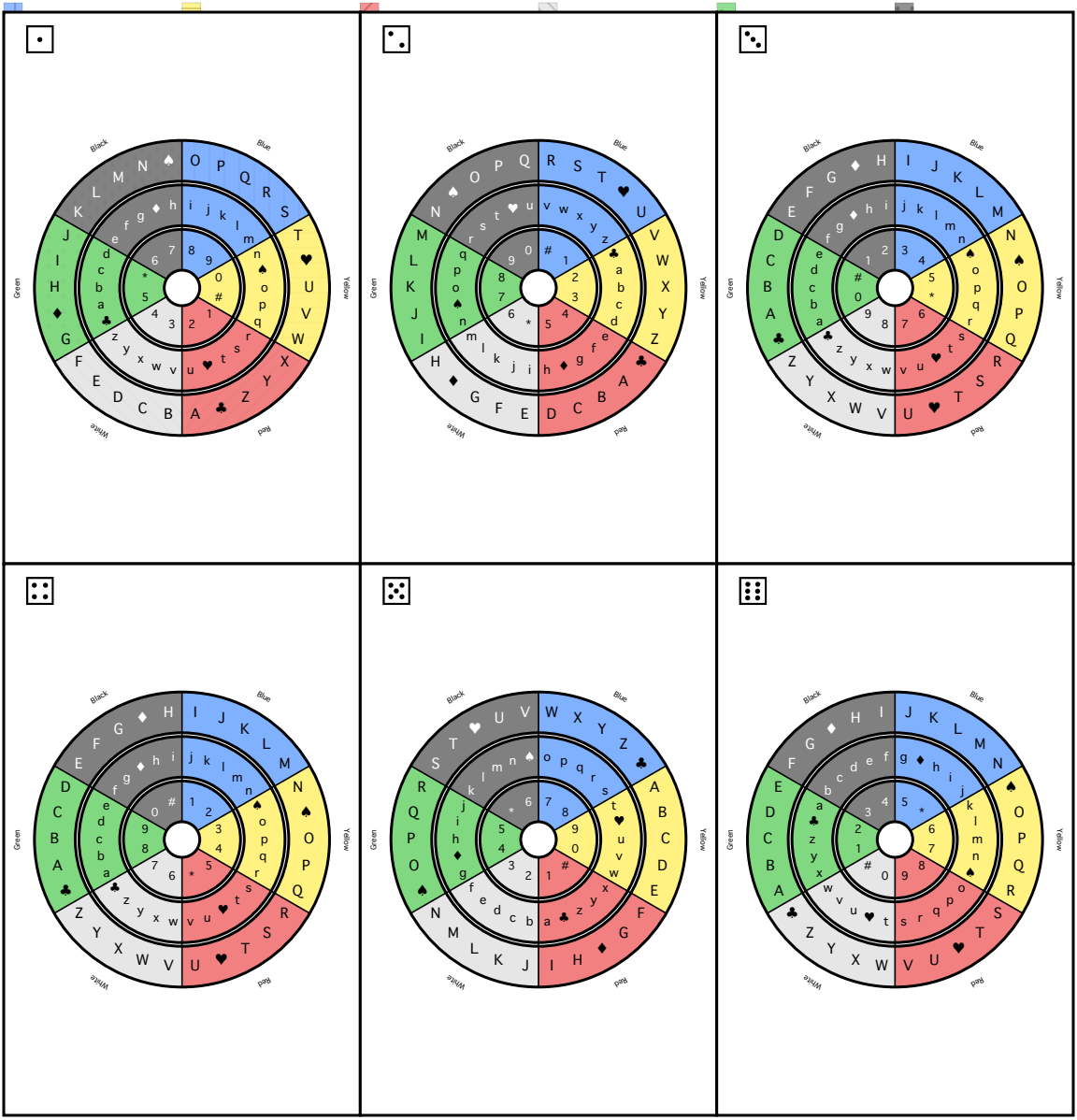


τ: 1785533985052856 | sha256(τ): 46e0b6ad

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052857

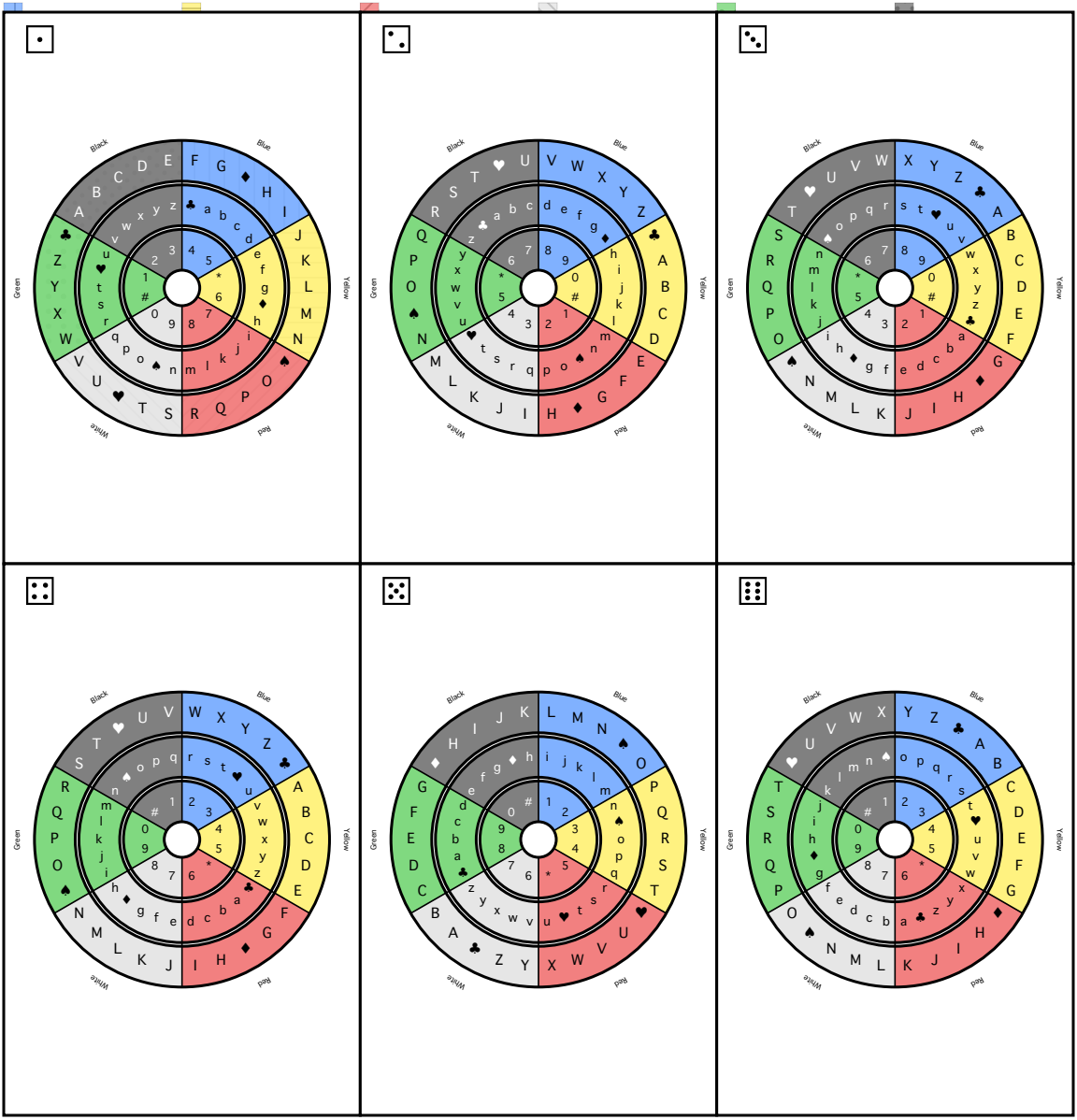


τ: 1785533985052857 | sha256(τ): 3ef7b045

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052858

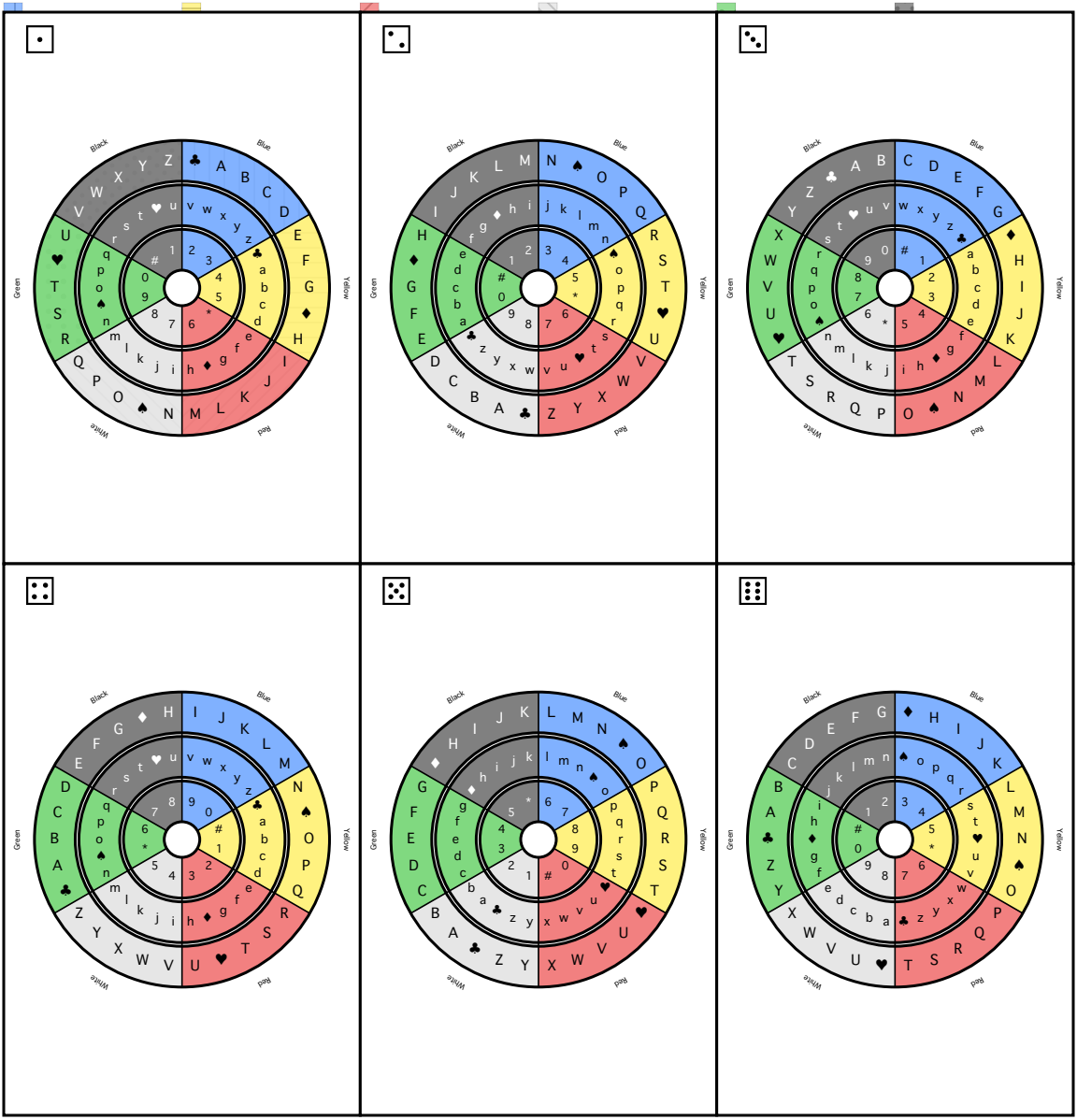


τ: 1785533985052858 | sha256(τ): 0df6a7ab

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052859

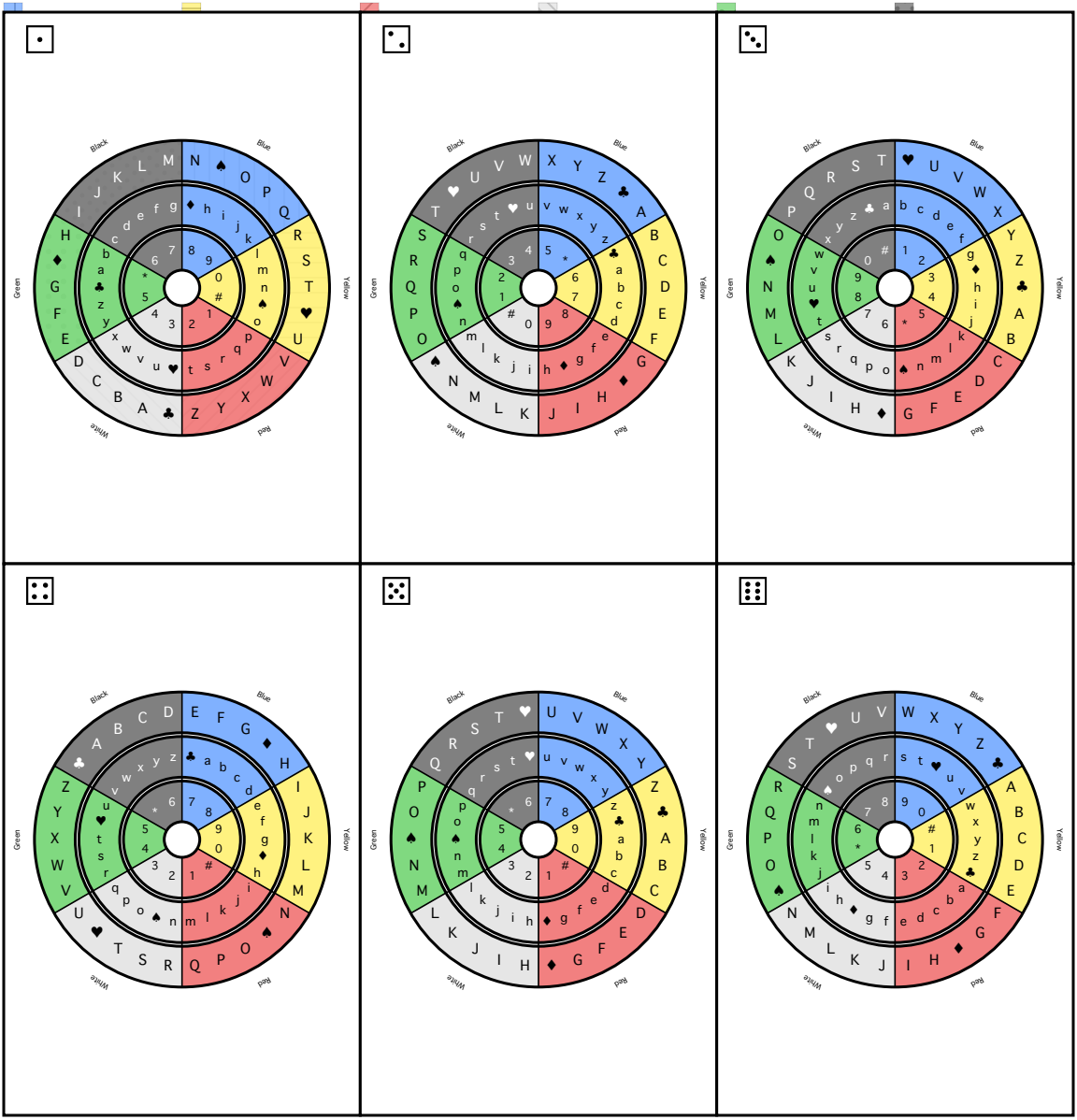


τ: 1785533985052859 | sha256(τ): a4a13485

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052860

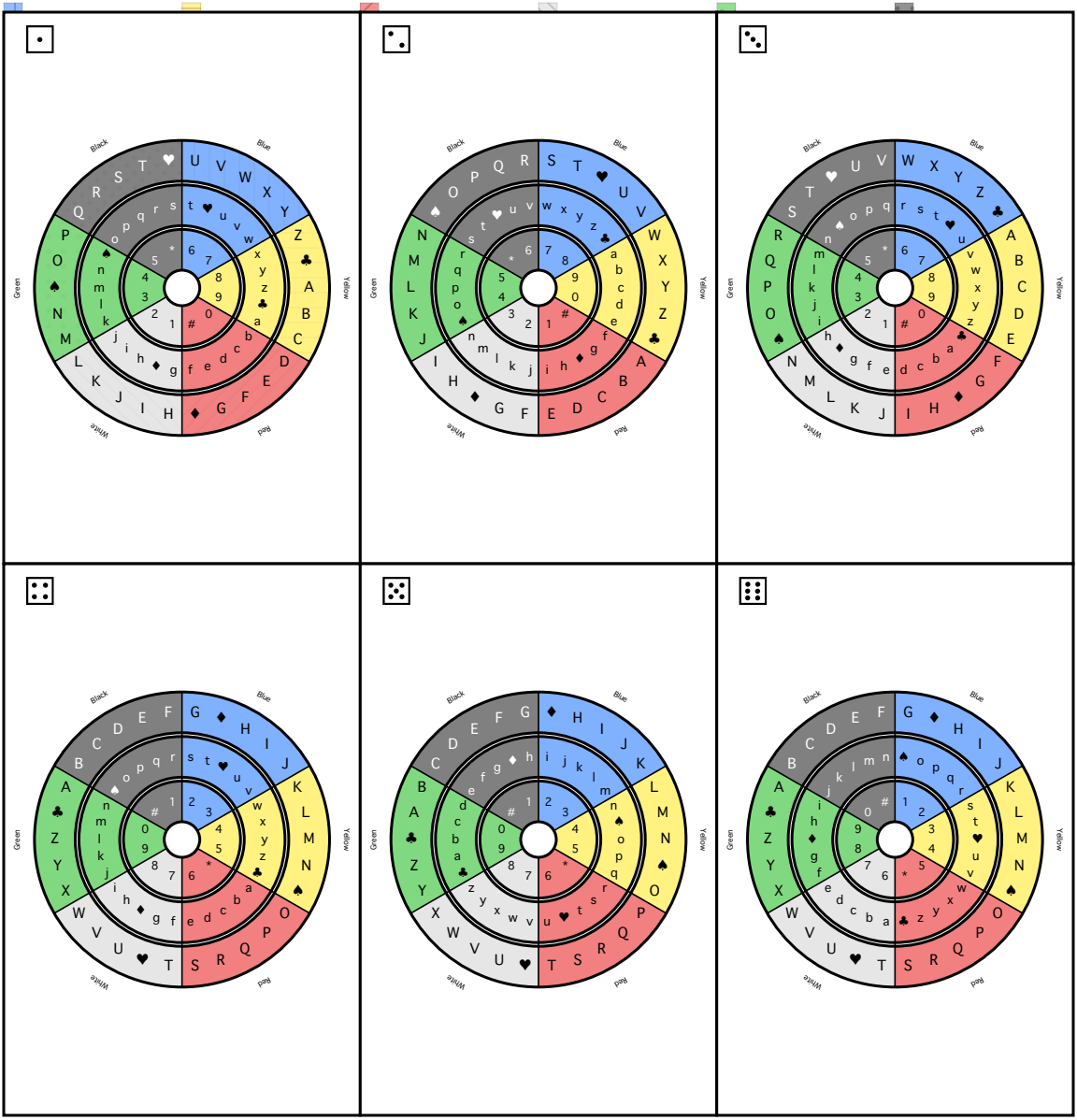


τ: 1785533985052860 | sha256(τ): 06f919d4

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052861

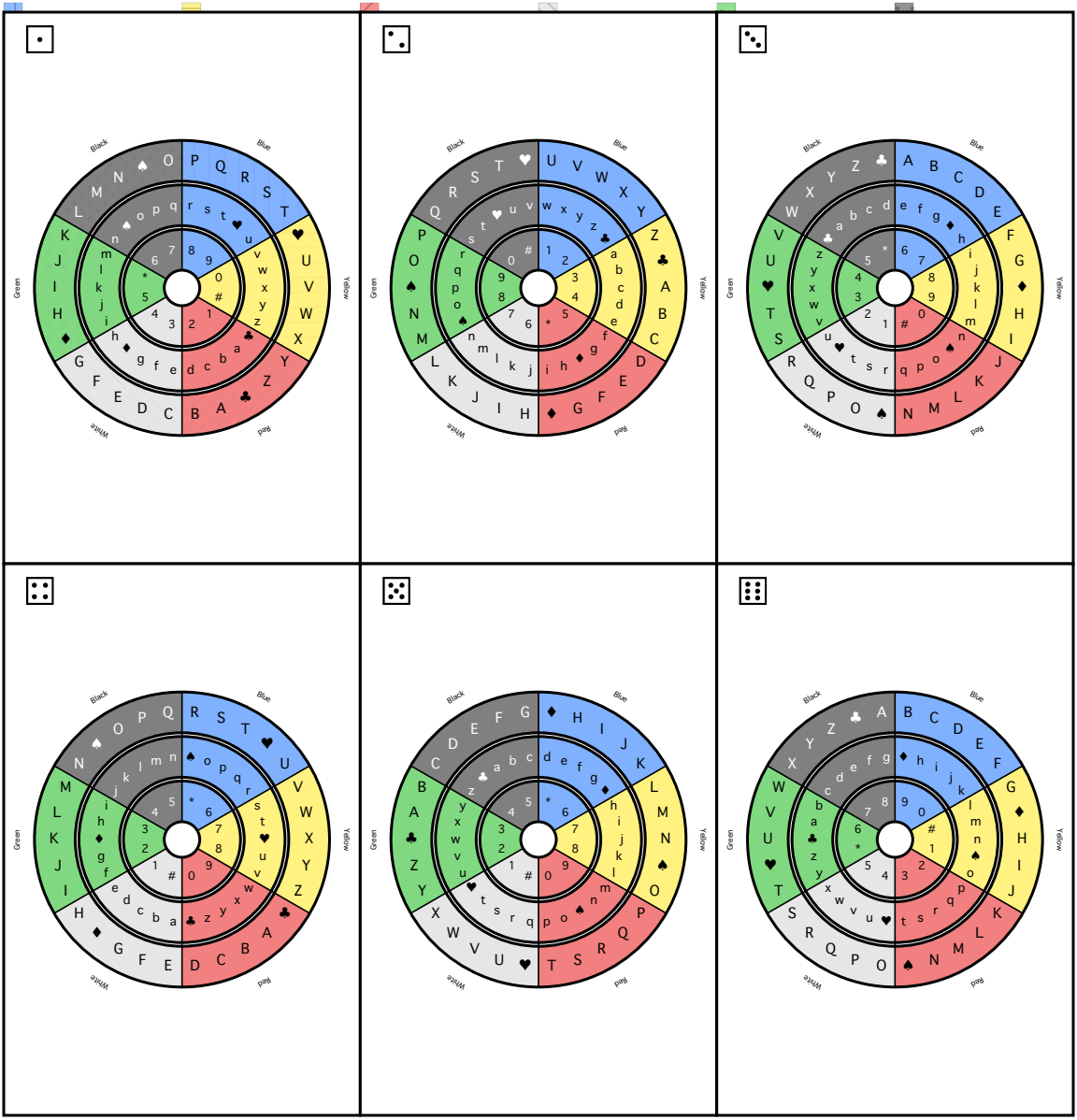


τ: 1785533985052861 | sha256(τ): fbdcd16f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052862

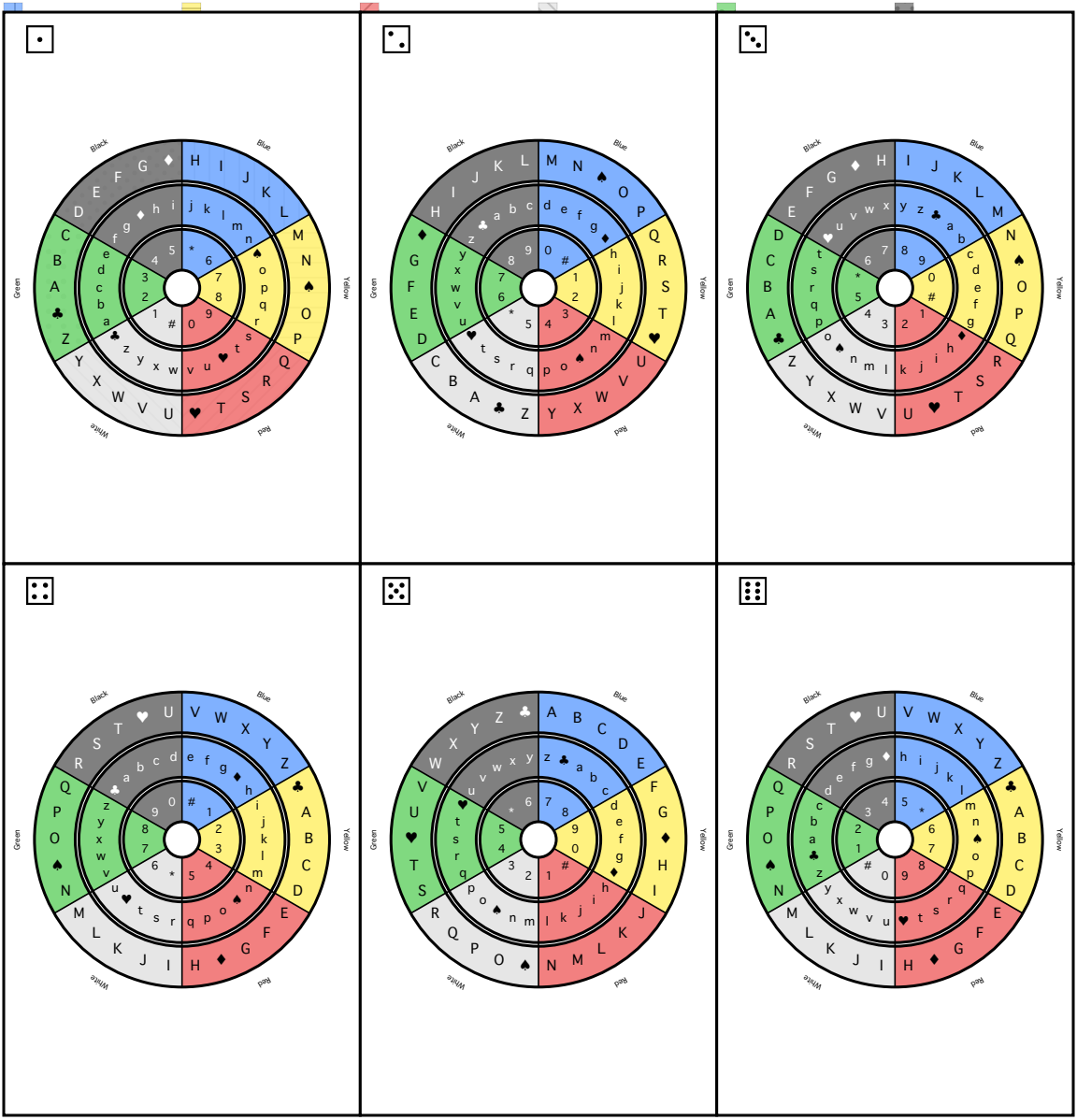


τ: 1785533985052862 | sha256(τ): ac013d45

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052863

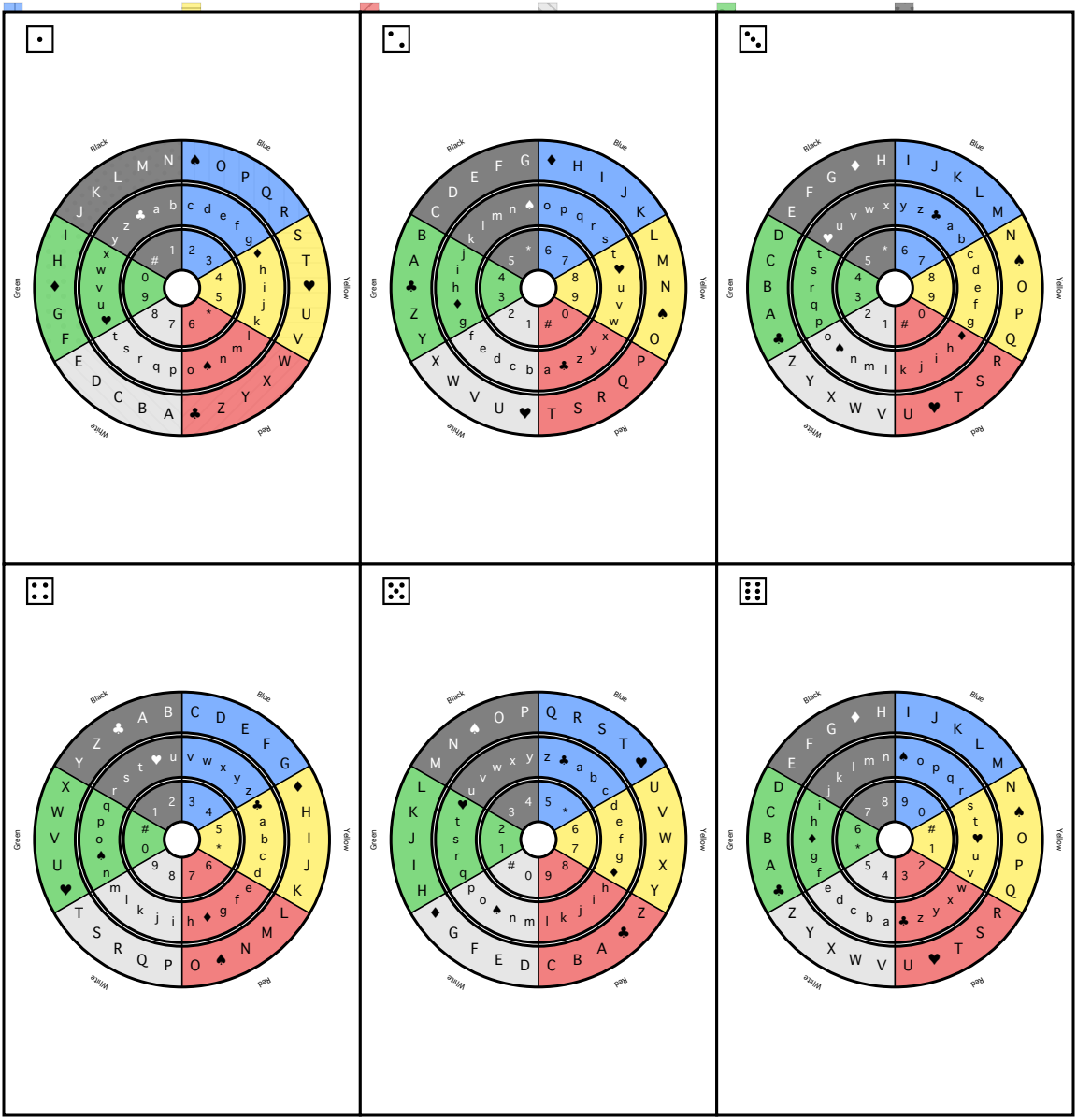


τ: 1785533985052863 | sha256(τ): f810780c

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052864

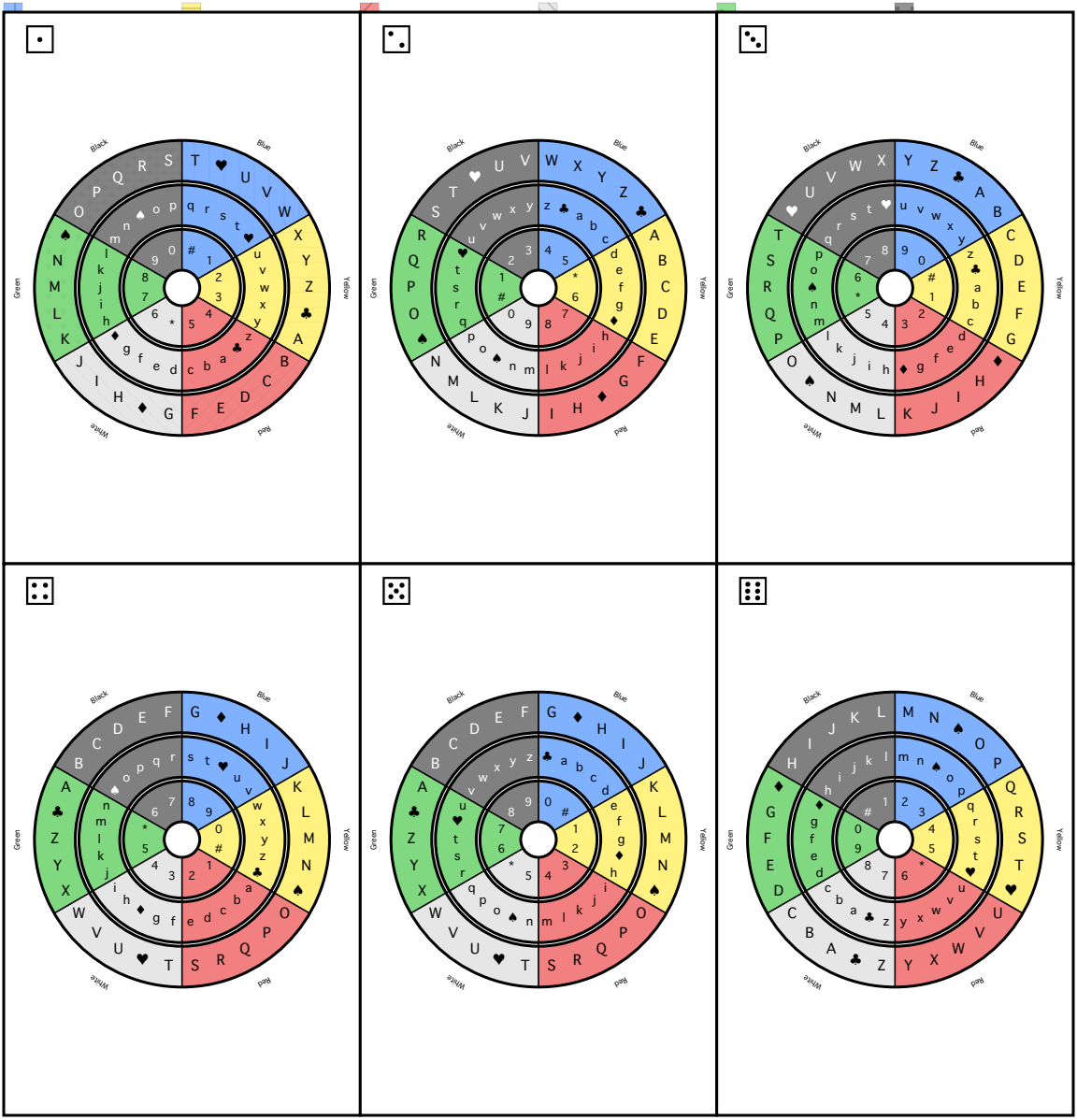


τ: 1785533985052864 | sha256(τ): 6616b4d3

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052865

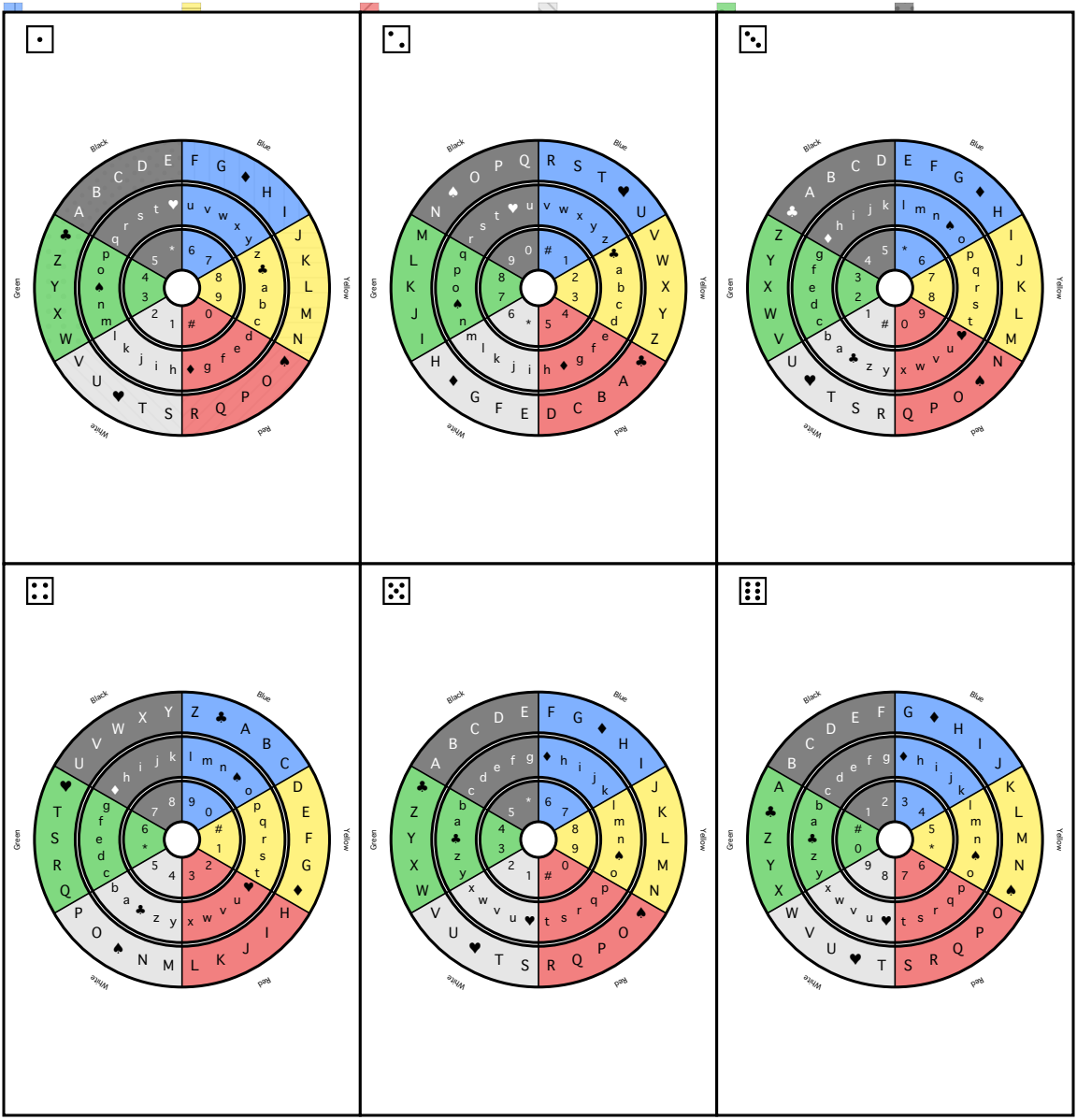


τ: 1785533985052865 | sha256(τ): 432ffcbc

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052866

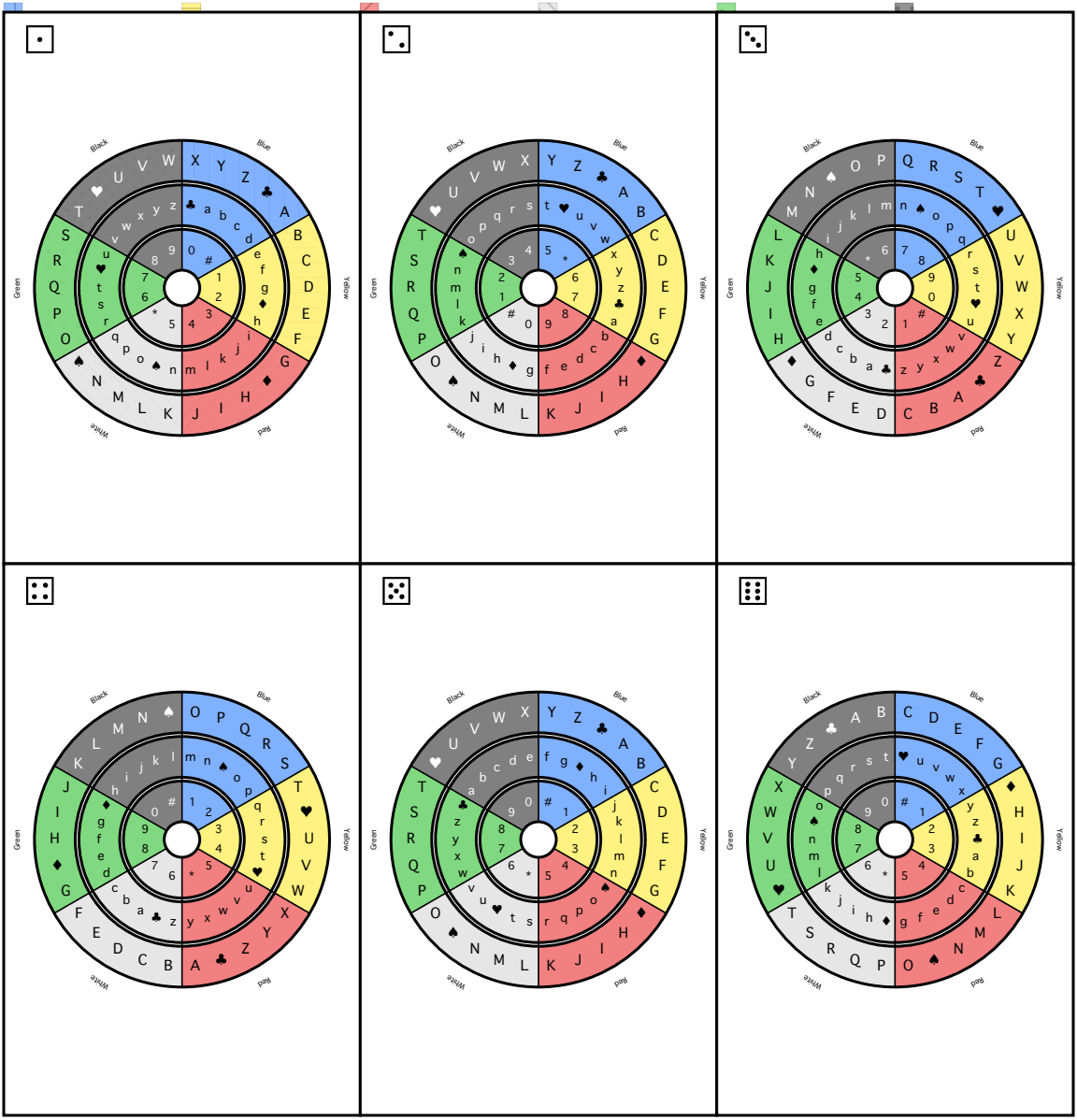


τ: 1785533985052866 | sha256(τ): f8b5e05f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052867

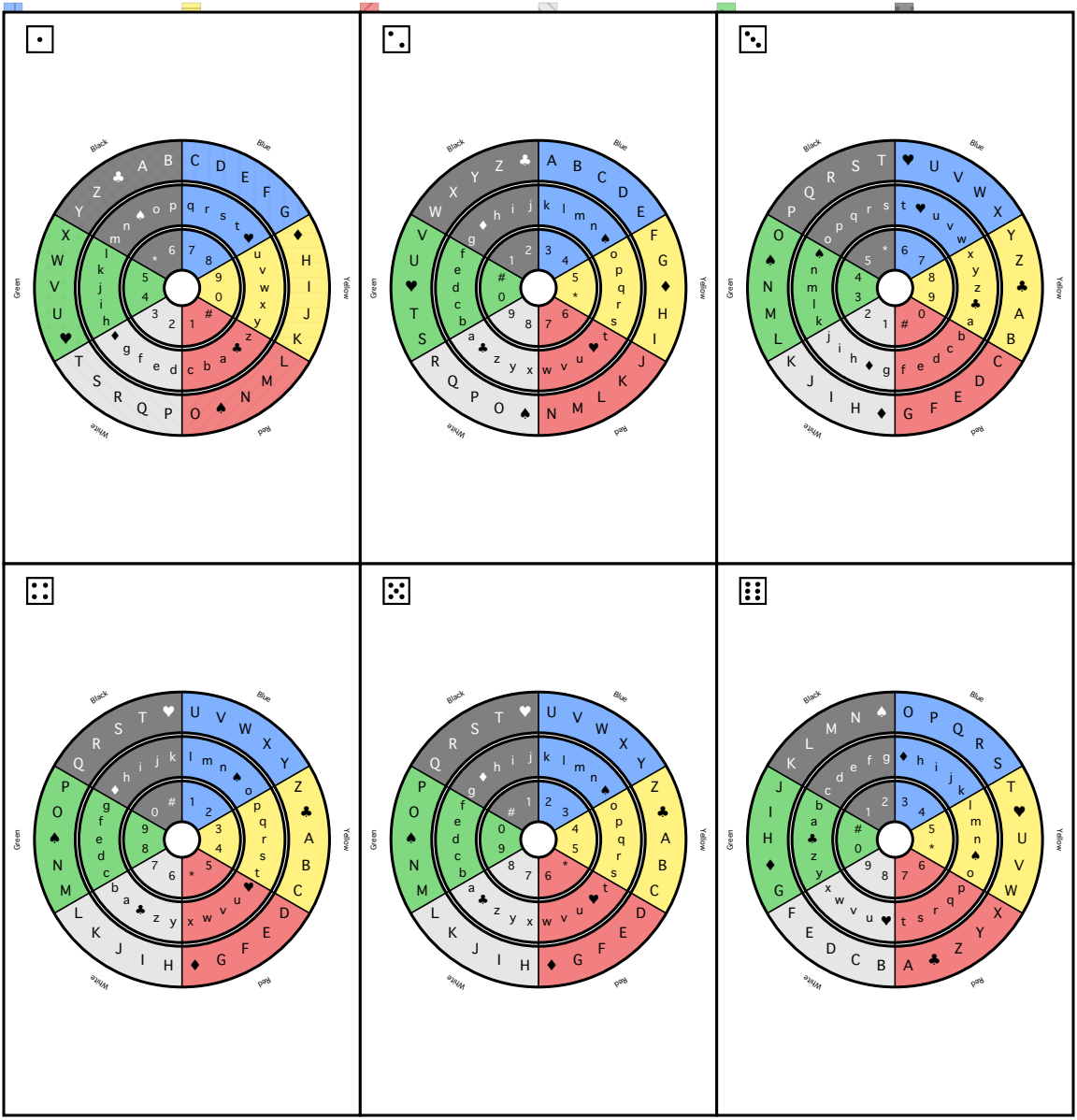


τ: 1785533985052867 | sha256(τ): f13f0411

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052868

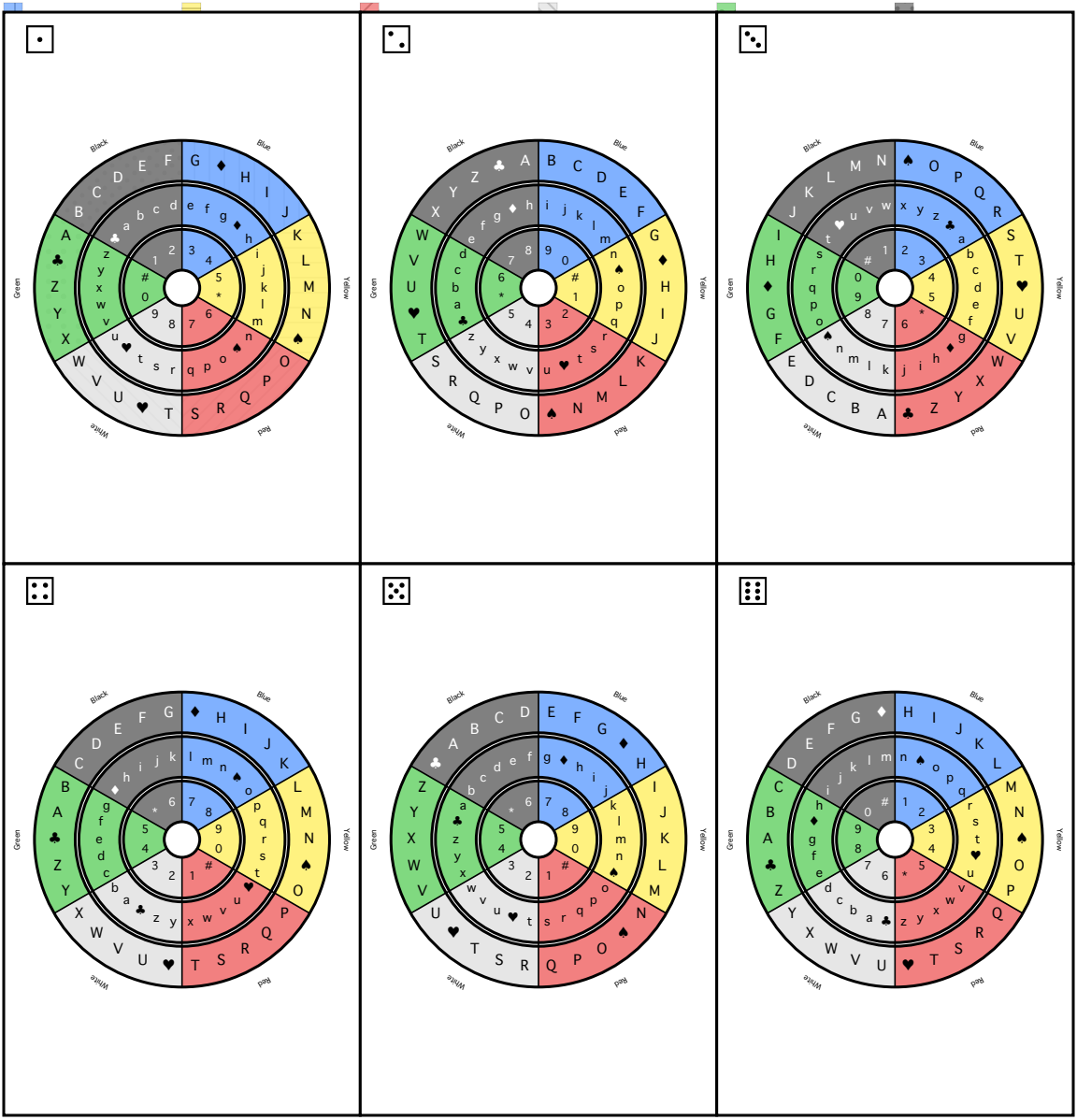


τ: 1785533985052868 | sha256(τ): cfa1f49f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052869

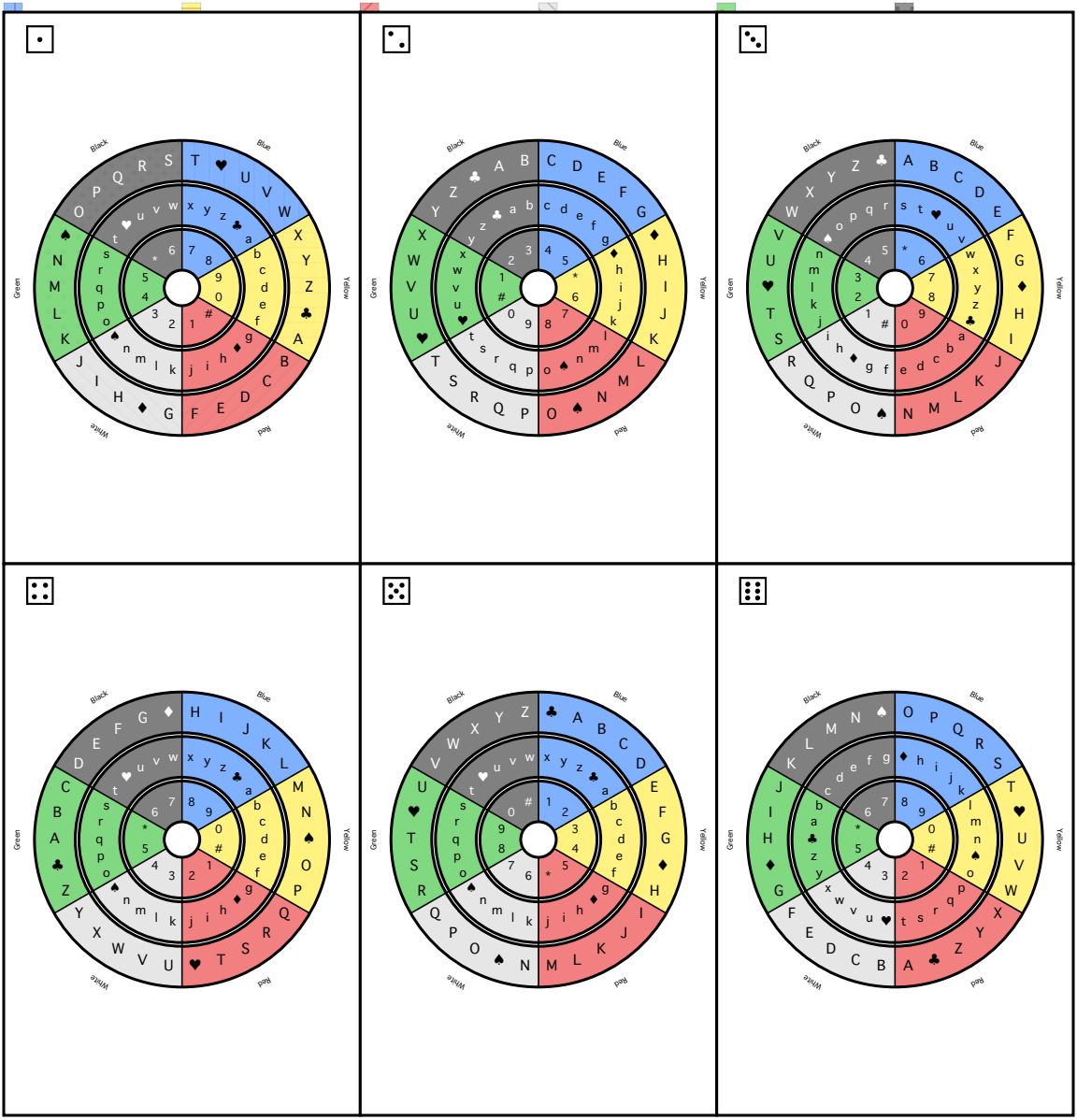


τ: 1785533985052869 | sha256(τ): 7577171d

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052870

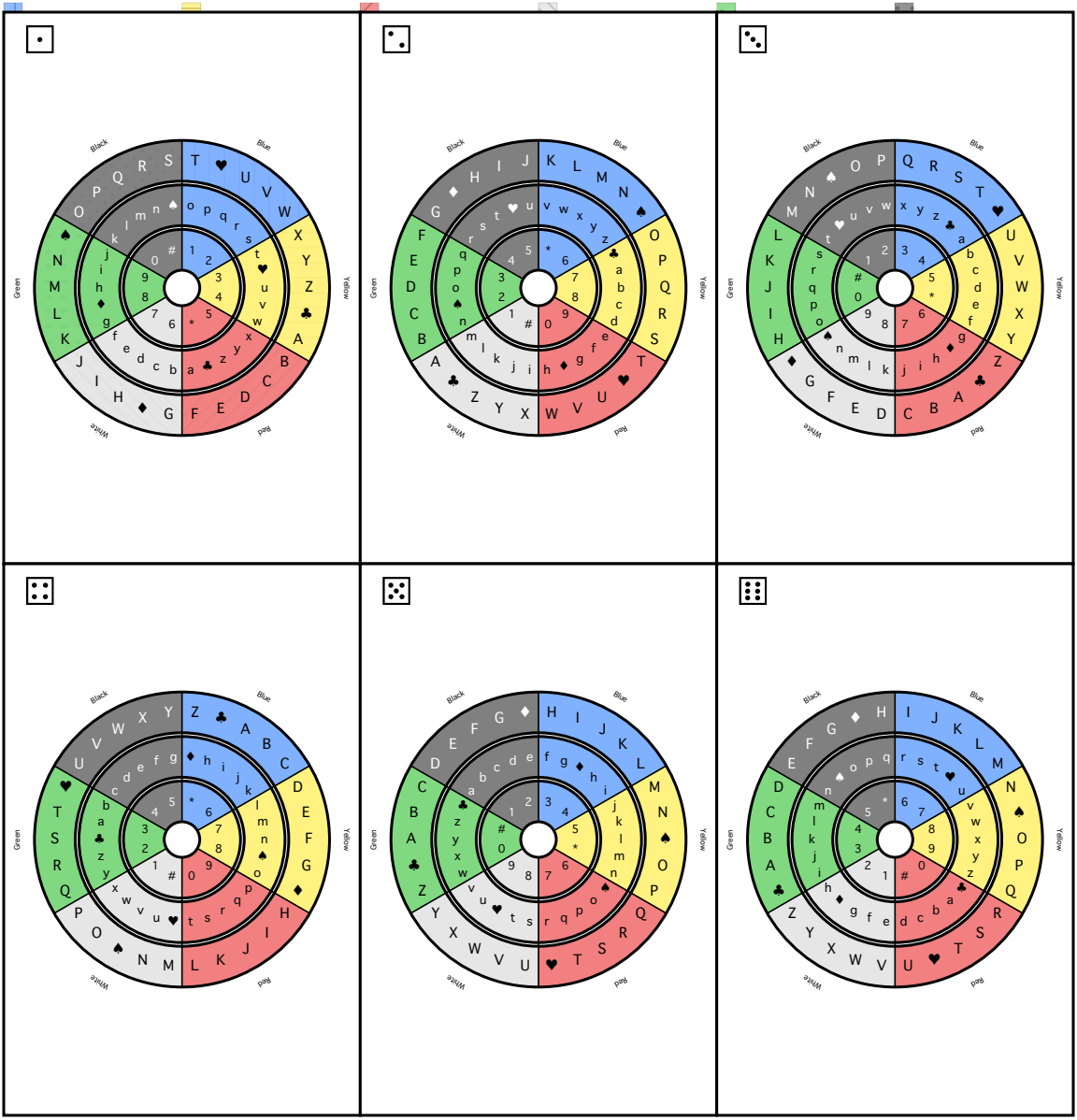


τ: 1785533985052870 | sha256(τ): 2c3525ed

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052871

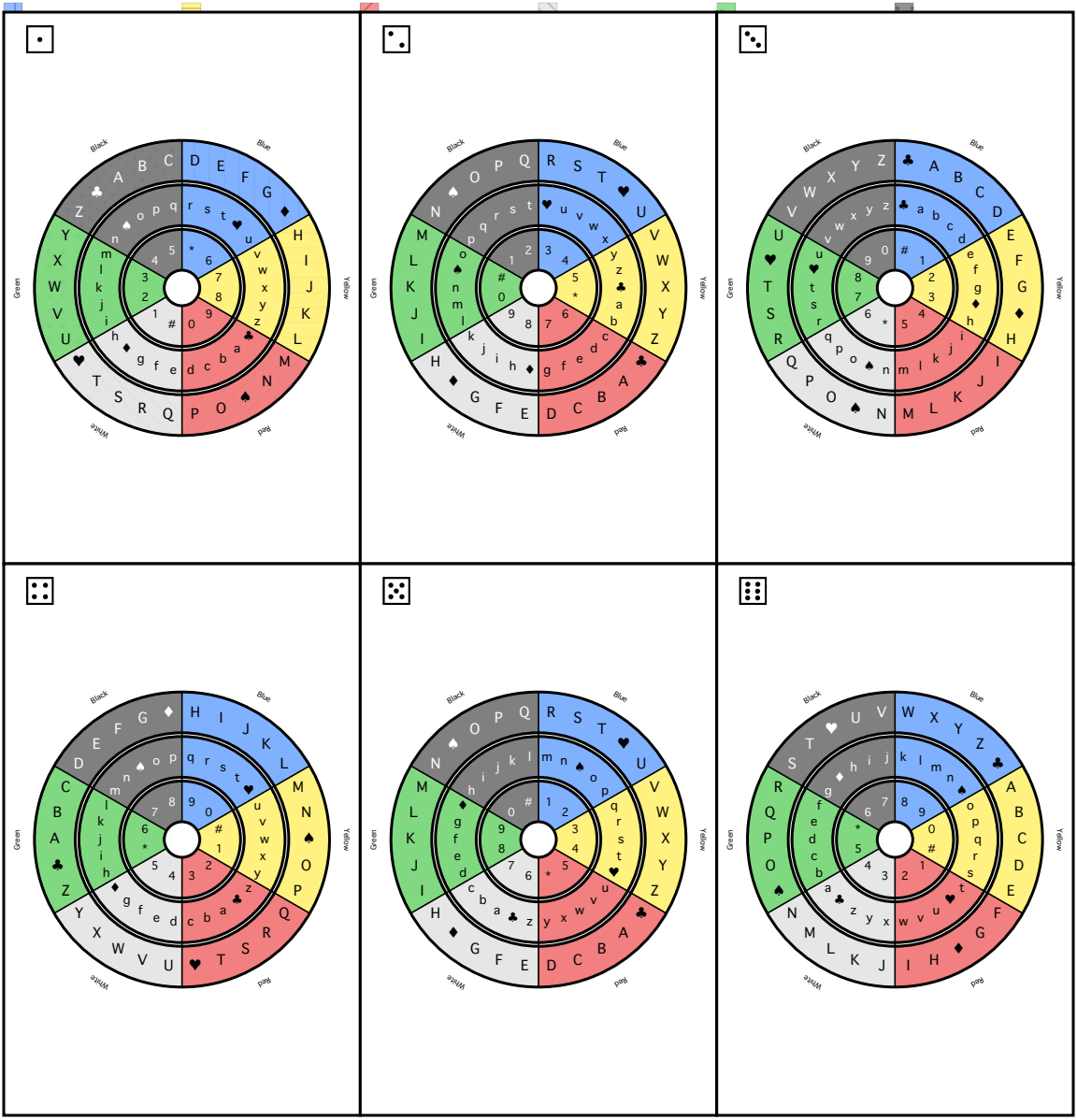


τ: 1785533985052871 | sha256(τ): b9d3afe6

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052872

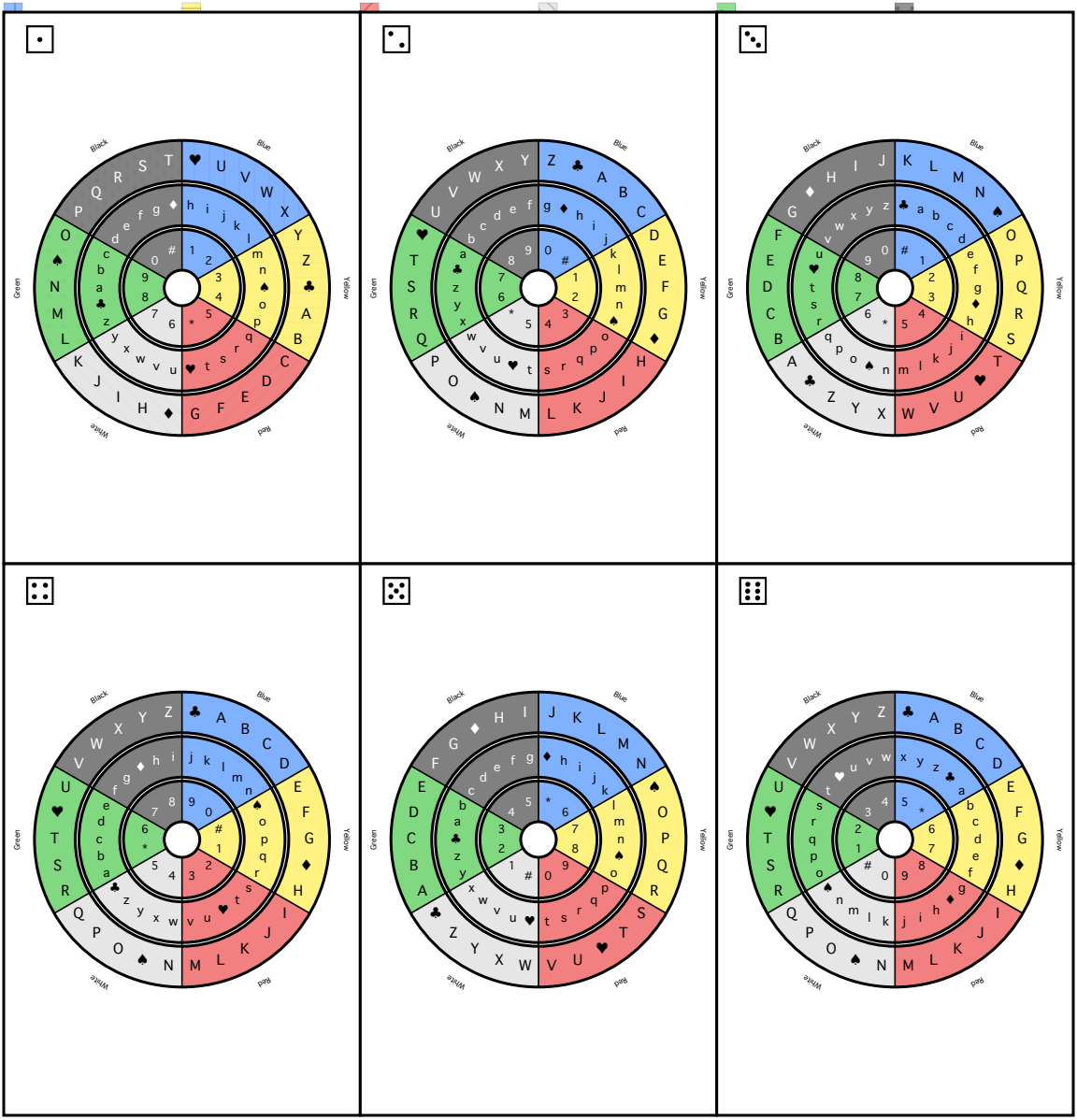


τ: 1785533985052872 | sha256(τ): 310f6623

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052873

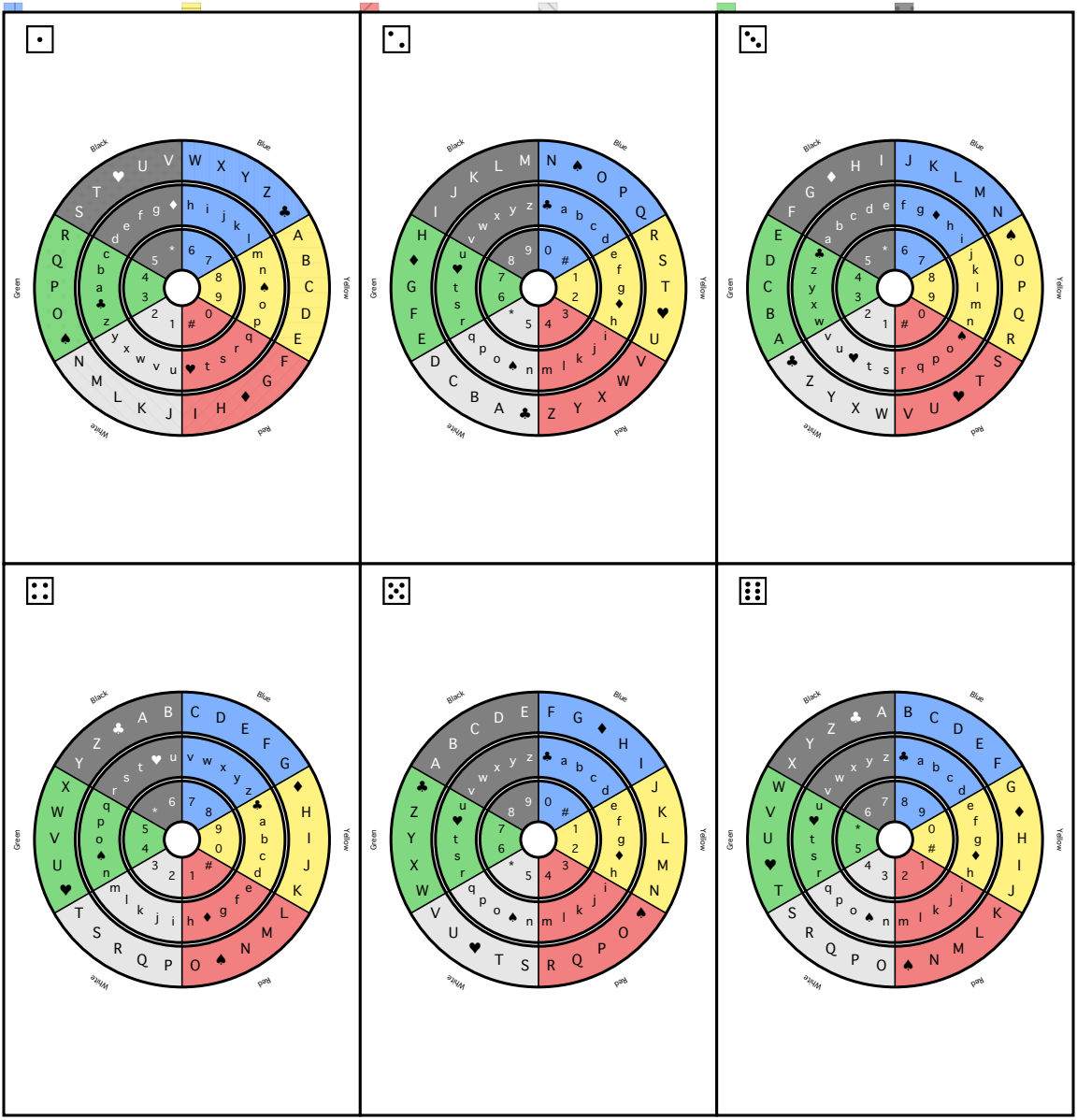


τ: 1785533985052873 | sha256(τ): 42a1c89a

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052874

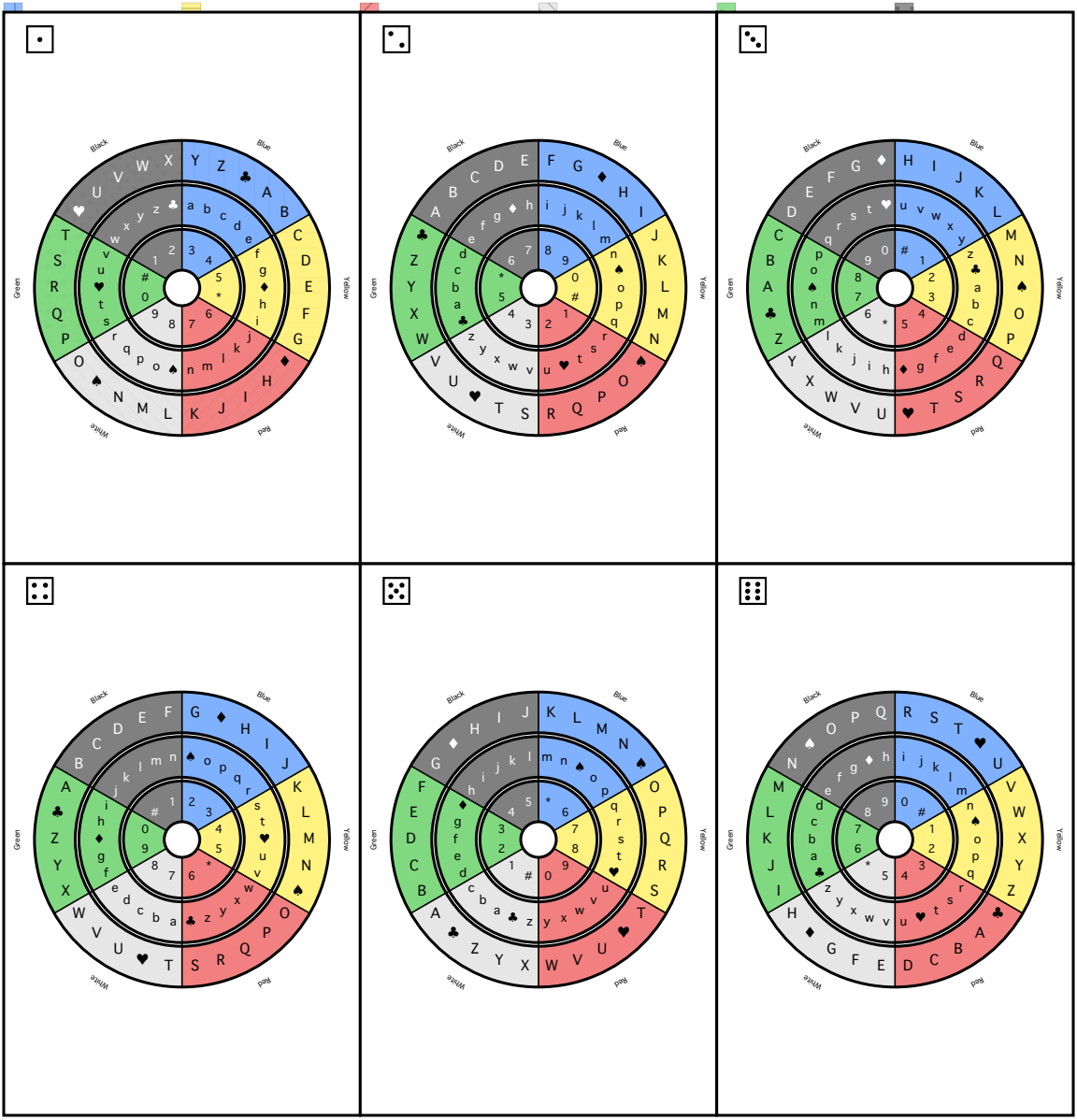


τ: 1785533985052874 | sha256(τ): d582af96

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052875

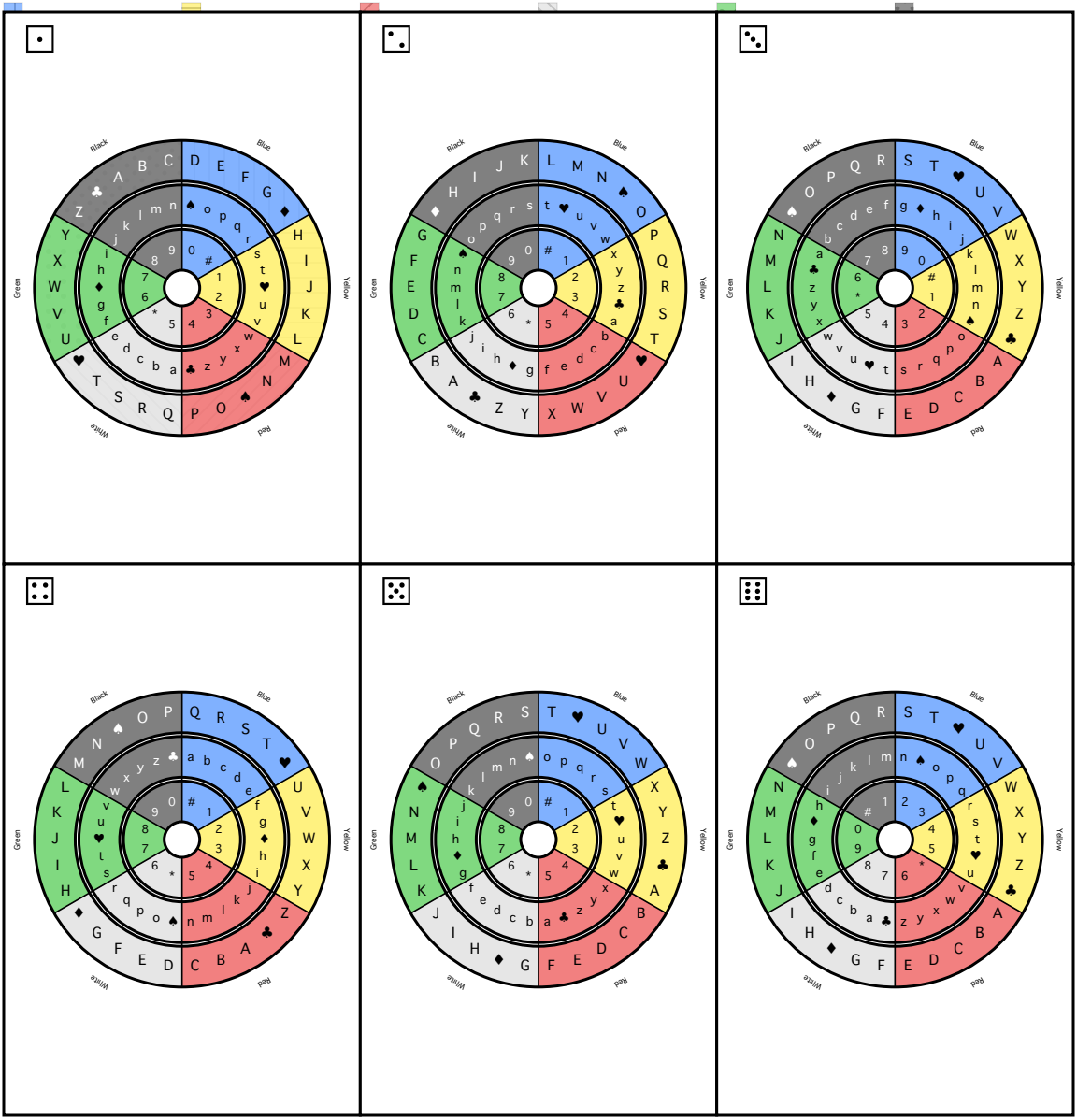


τ: 1785533985052875 | sha256(τ): a425c92c

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052876

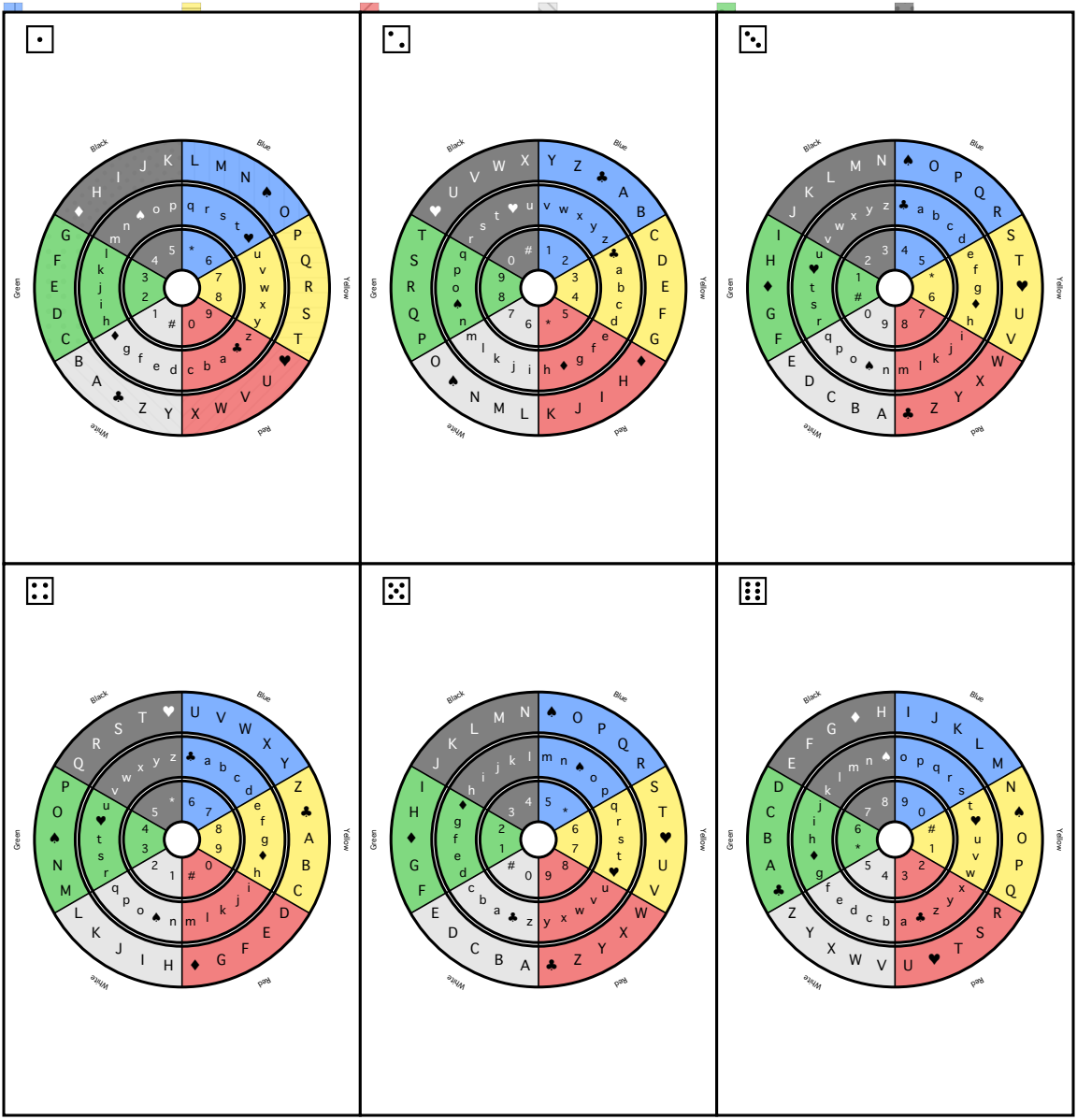


τ: 1785533985052876 | sha256(τ): bbf1894b

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052877

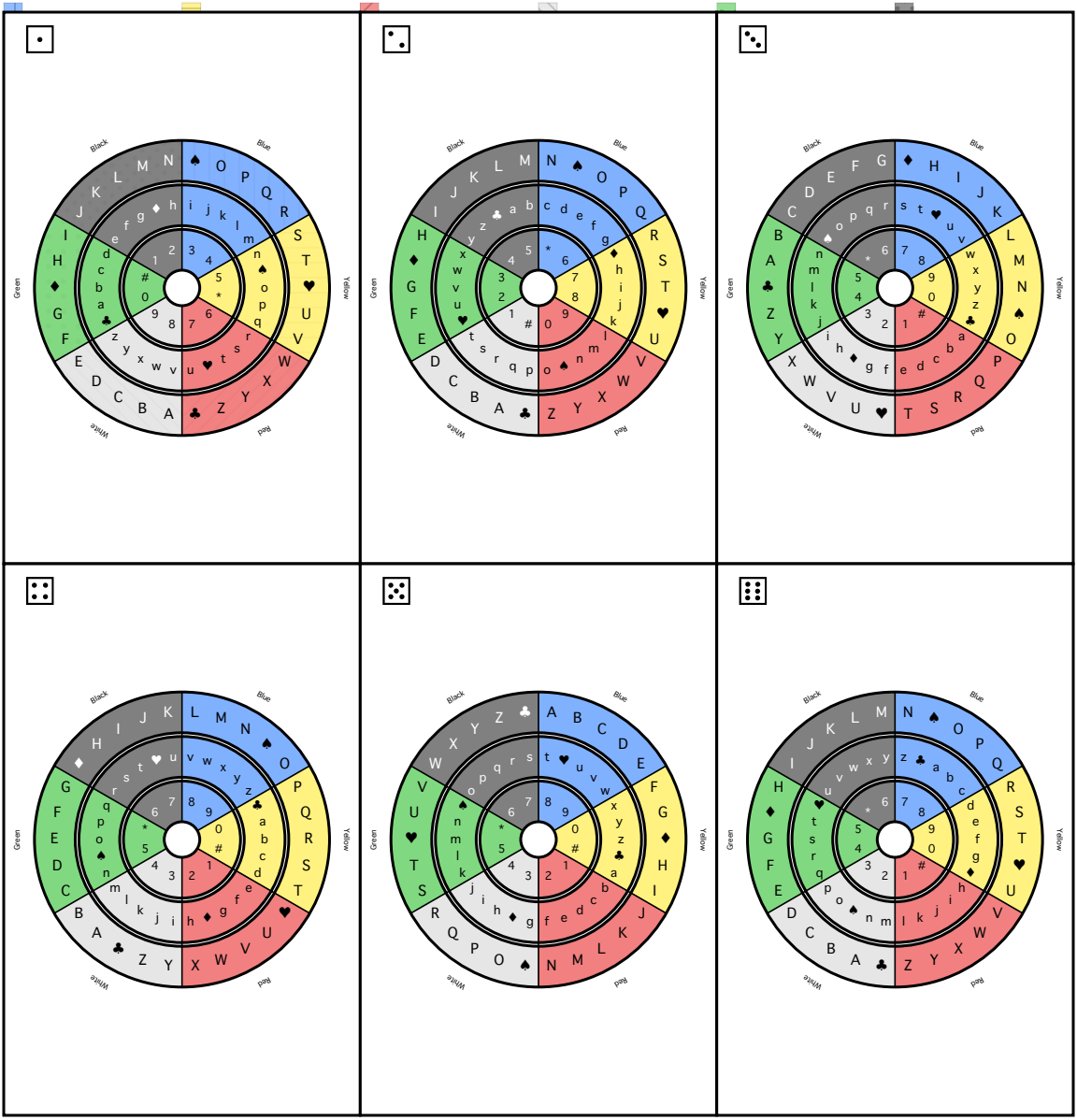


τ: 1785533985052877 | sha256(τ): 8d96a68e

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052878

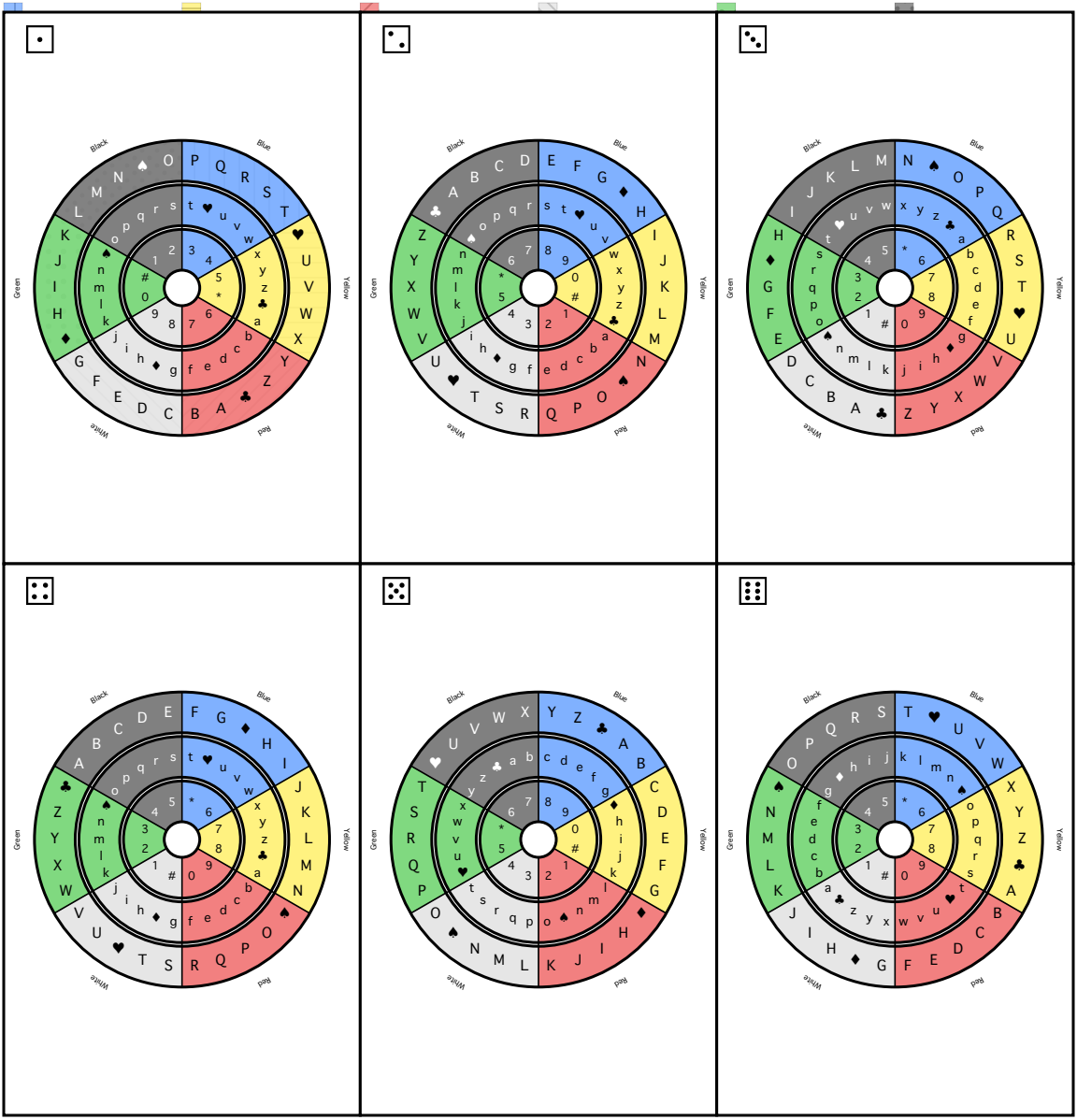


τ: 1785533985052878 | sha256(τ): 9f63a67f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052879

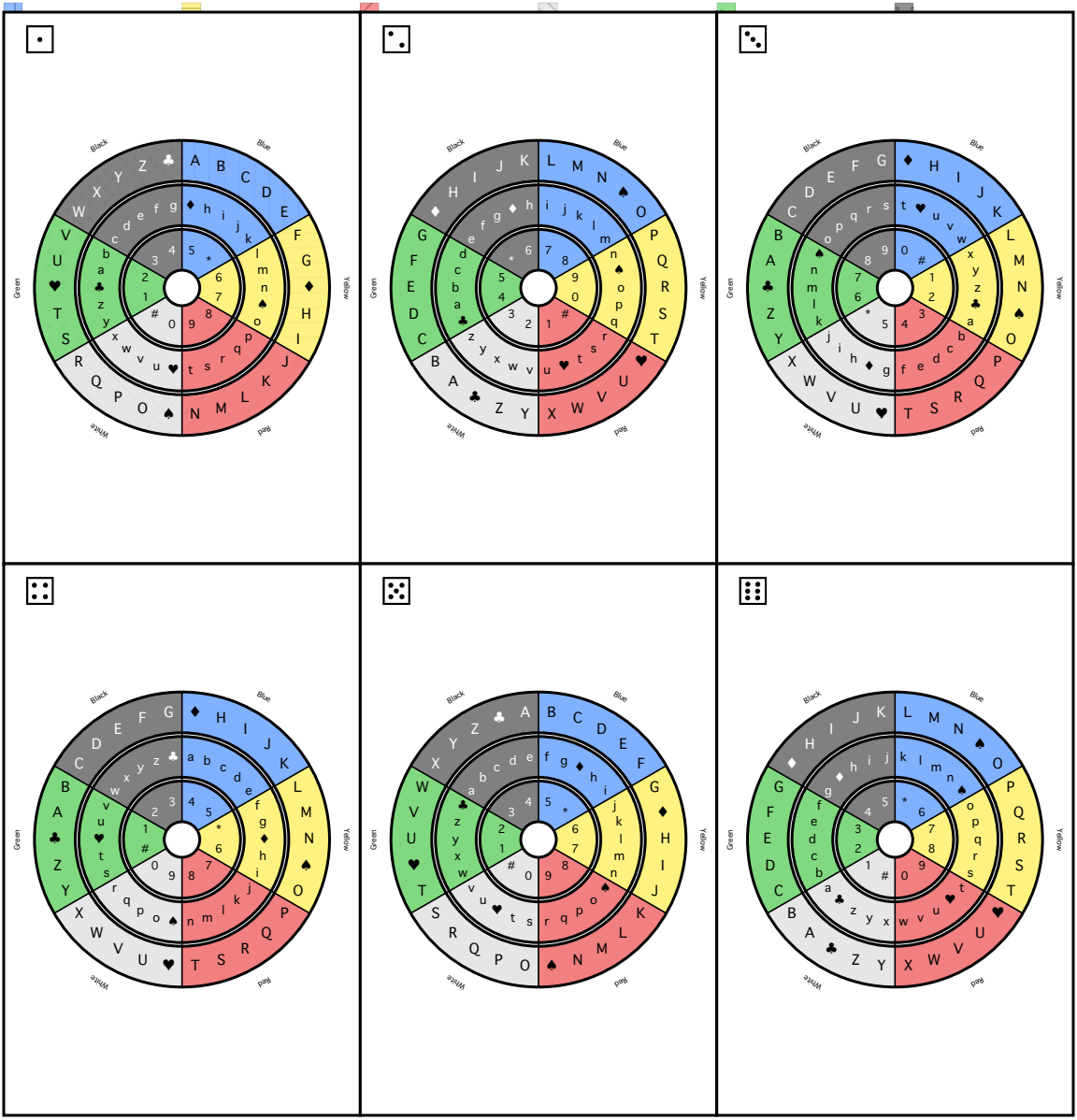


τ: 1785533985052879 | sha256(τ): 4d0c23da

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052880

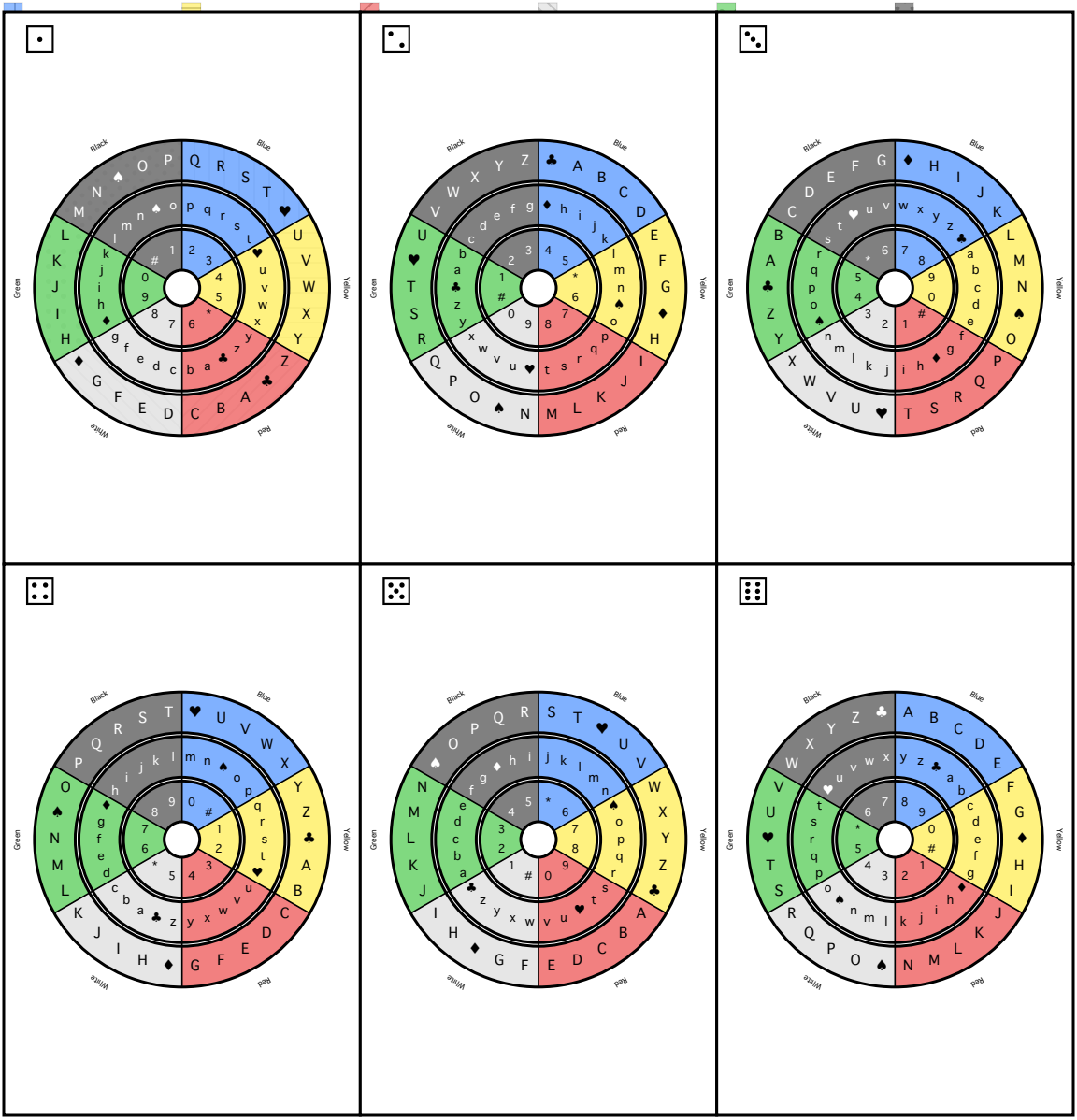


τ: 1785533985052880 | sha256(τ): d0eb679f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052881

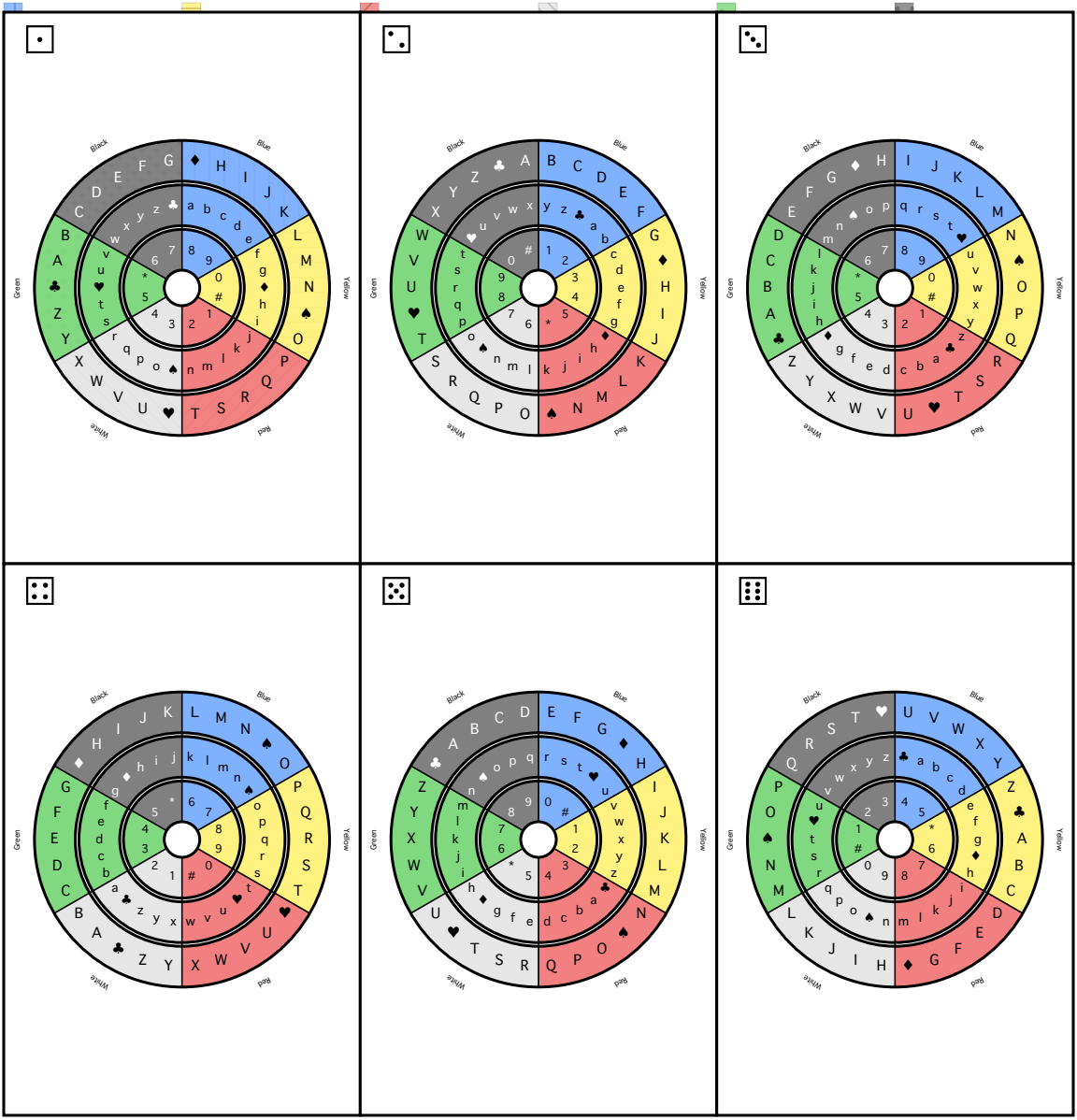


τ: 1785533985052881 | sha256(τ): 0d138b03

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052882

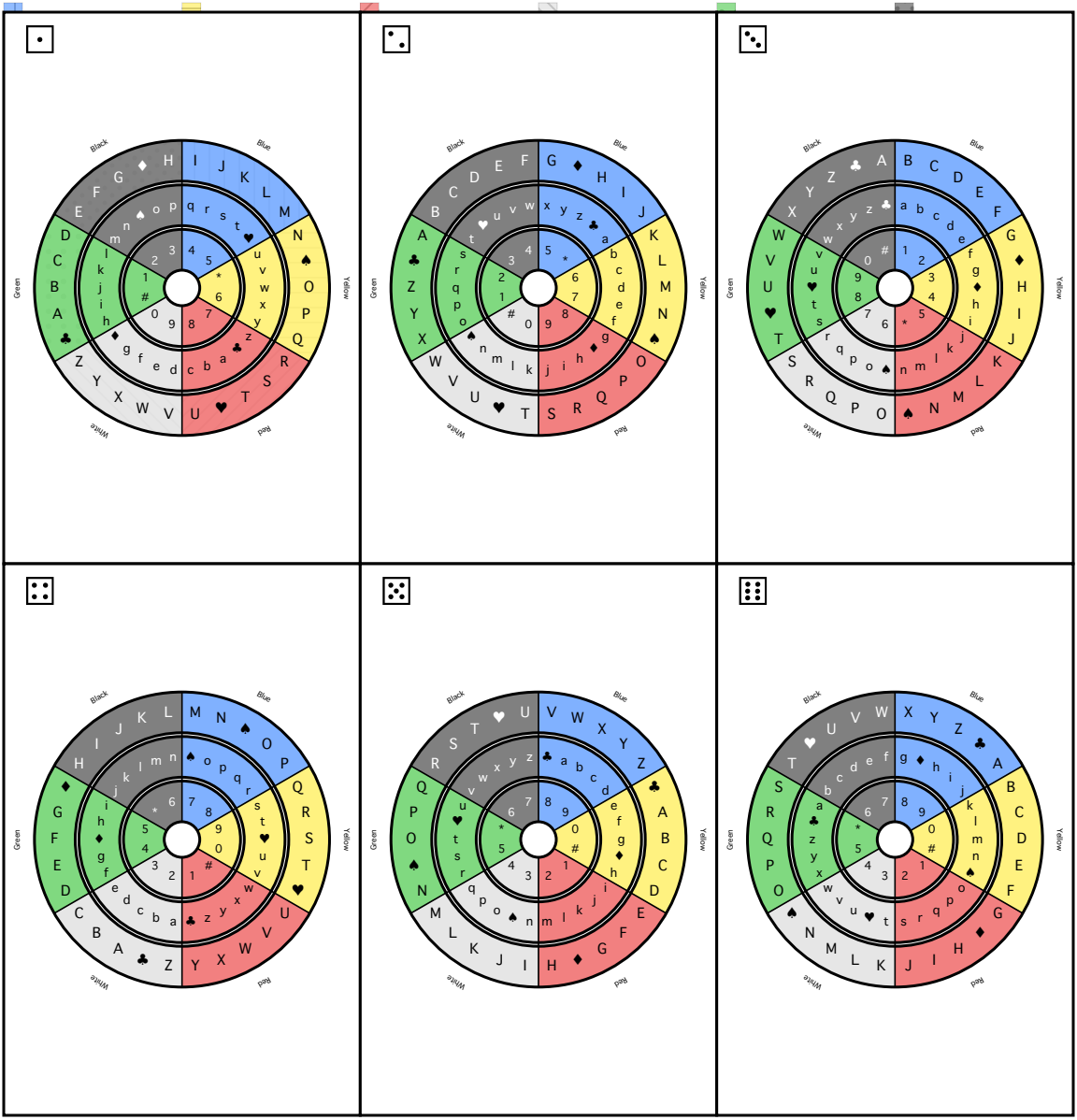


τ: 1785533985052882 | sha256(τ): 4e24803a

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052883

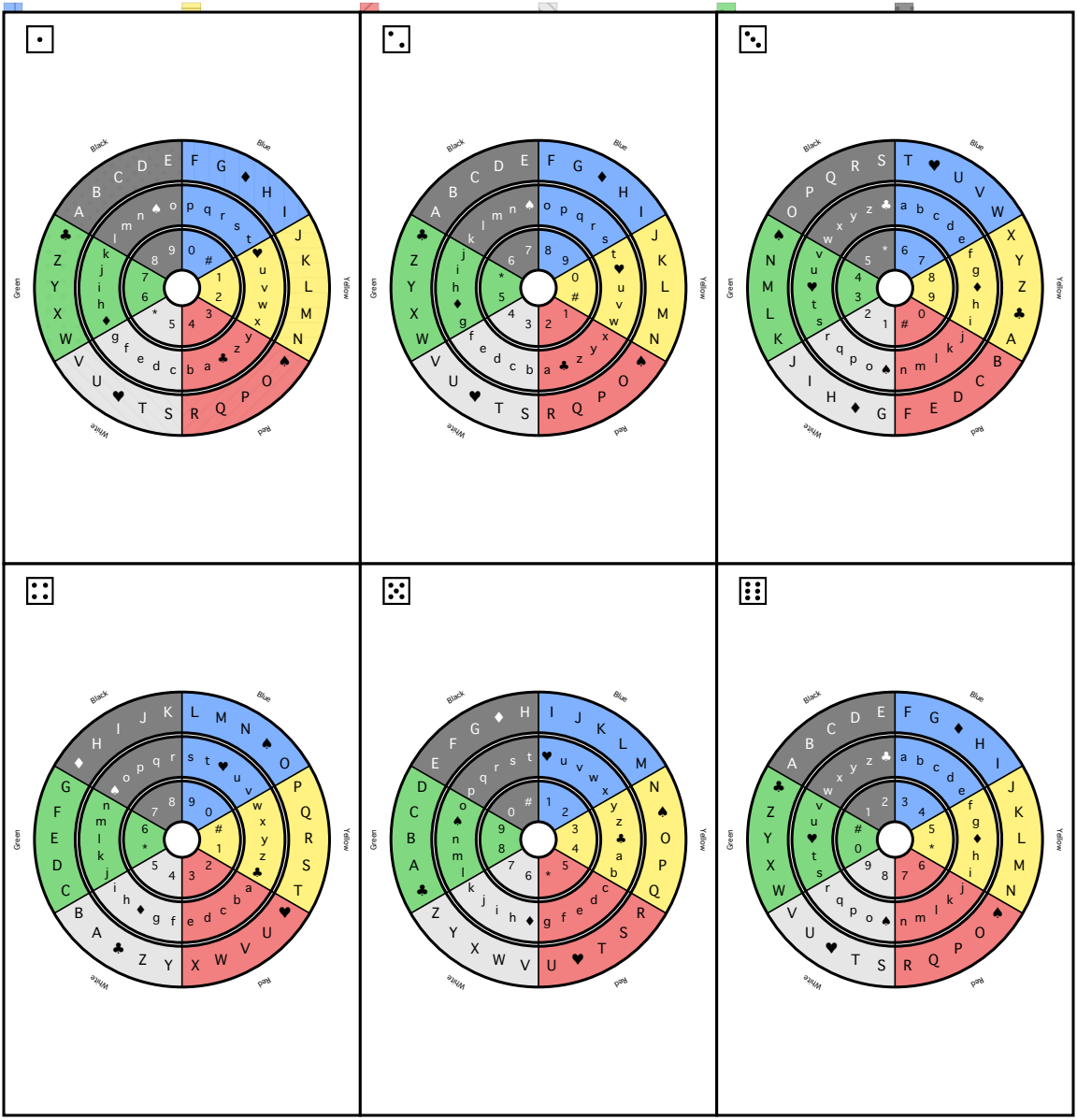


τ: 1785533985052883 | sha256(τ): 39db1e07

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052884

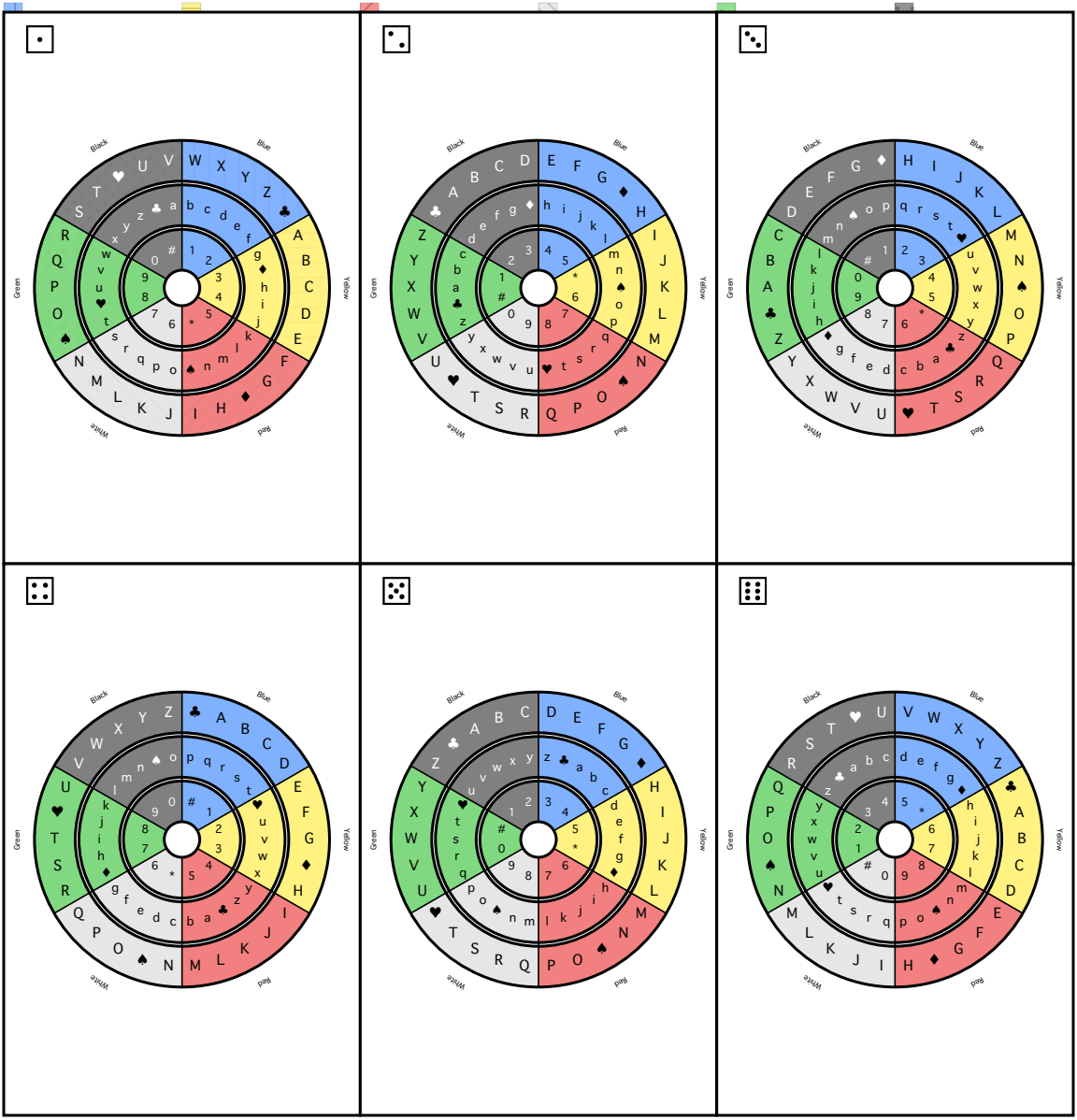


τ: 1785533985052884 | sha256(τ): 22eae224

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052885

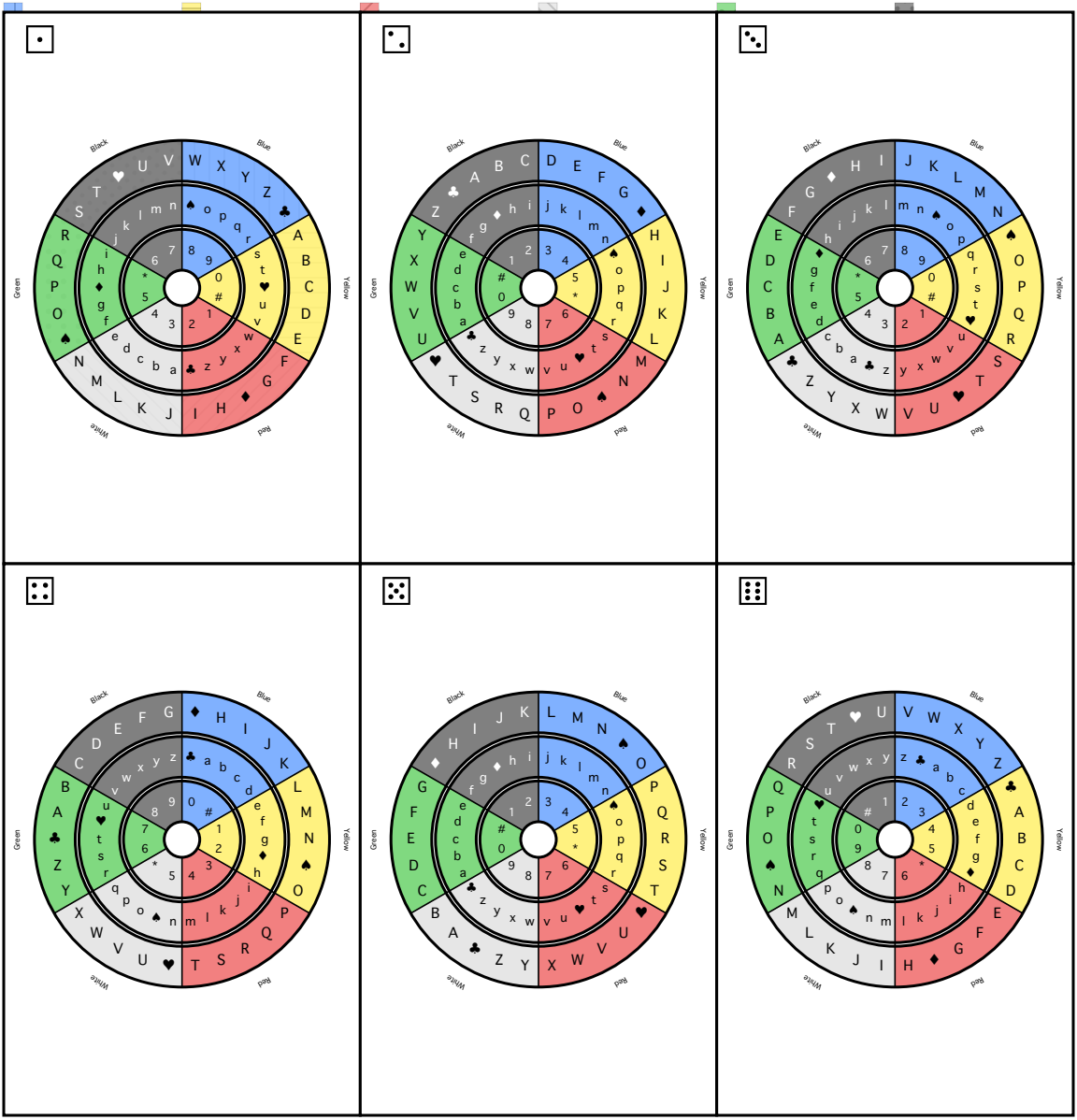


τ: 1785533985052885 | sha256(τ): c5c2200f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052886

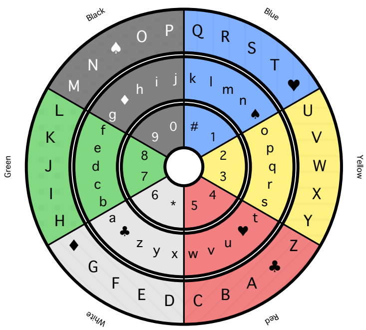


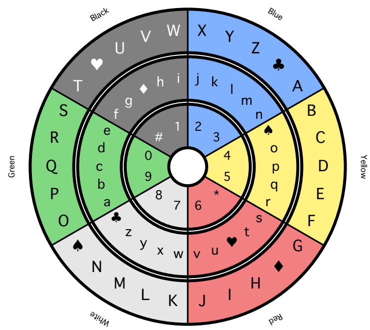
τ: 1785533985052886 | sha256(τ): a3577f6f

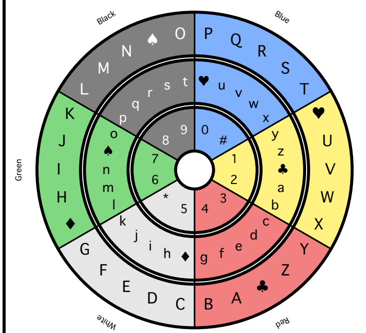
circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

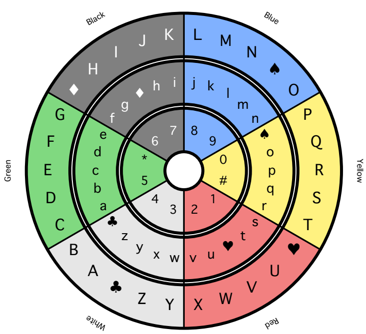
ENI6MA CHALLENGE SHEET

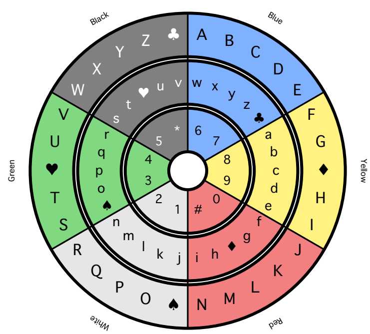
H=6 | τ: 1785533985052887

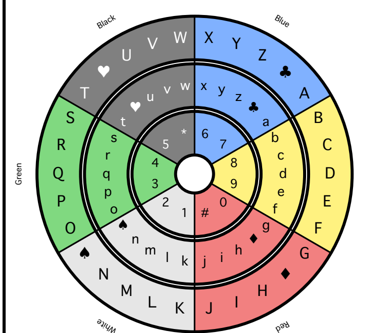










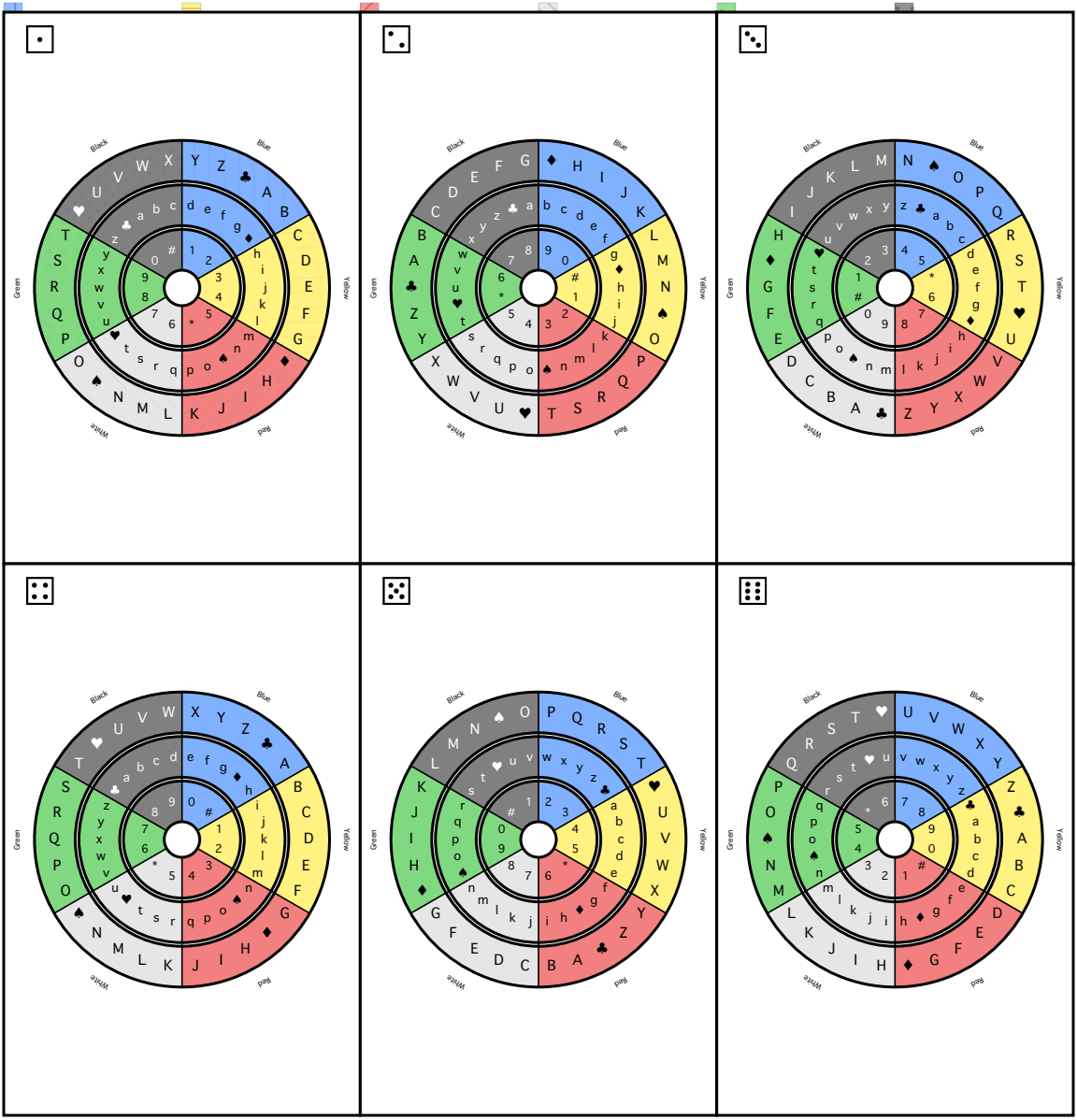


τ: 1785533985052887 | sha256(τ): c78259b0

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052888

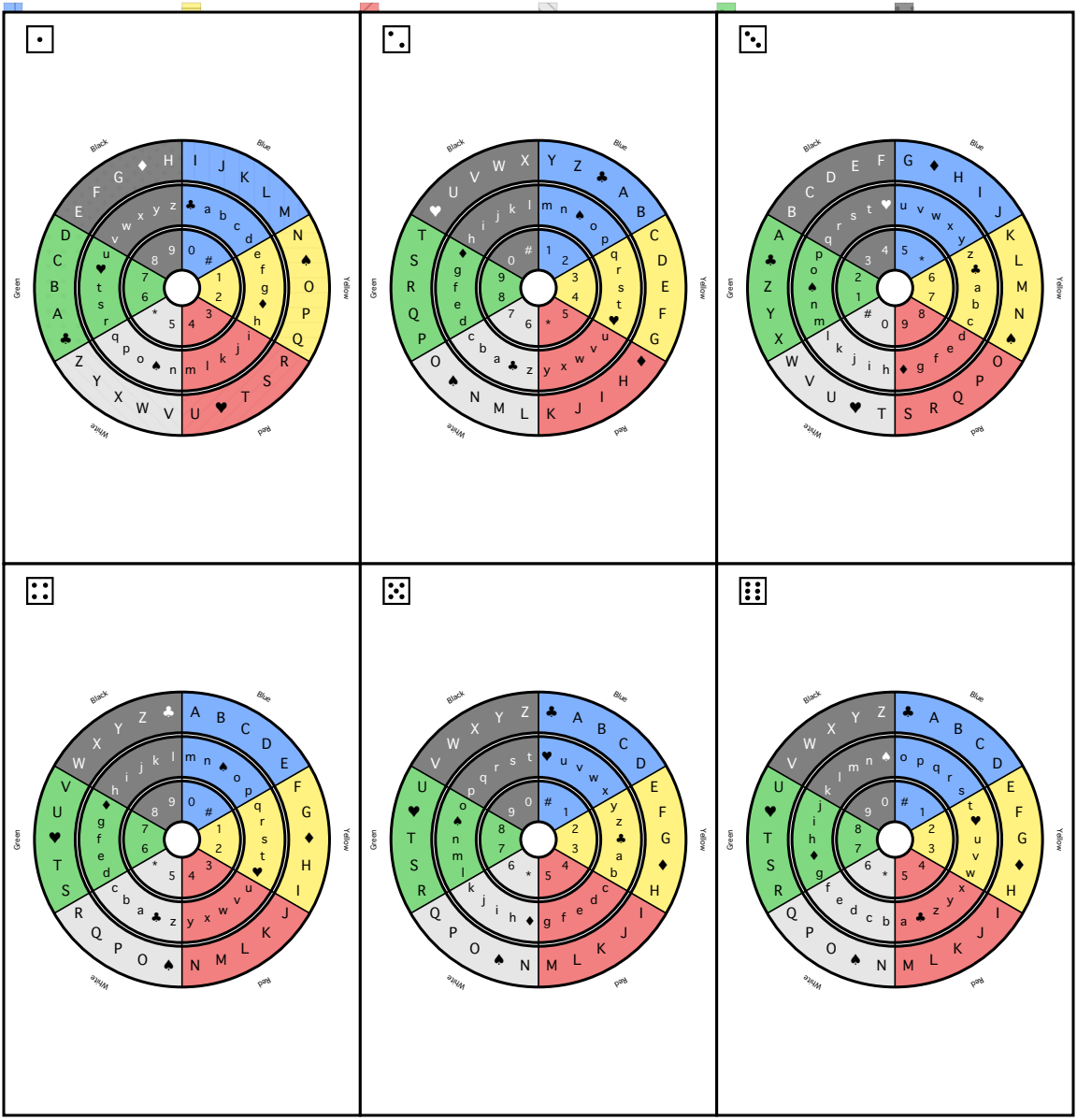


τ: 1785533985052888 | sha256(τ): 25e6bb4c

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052889

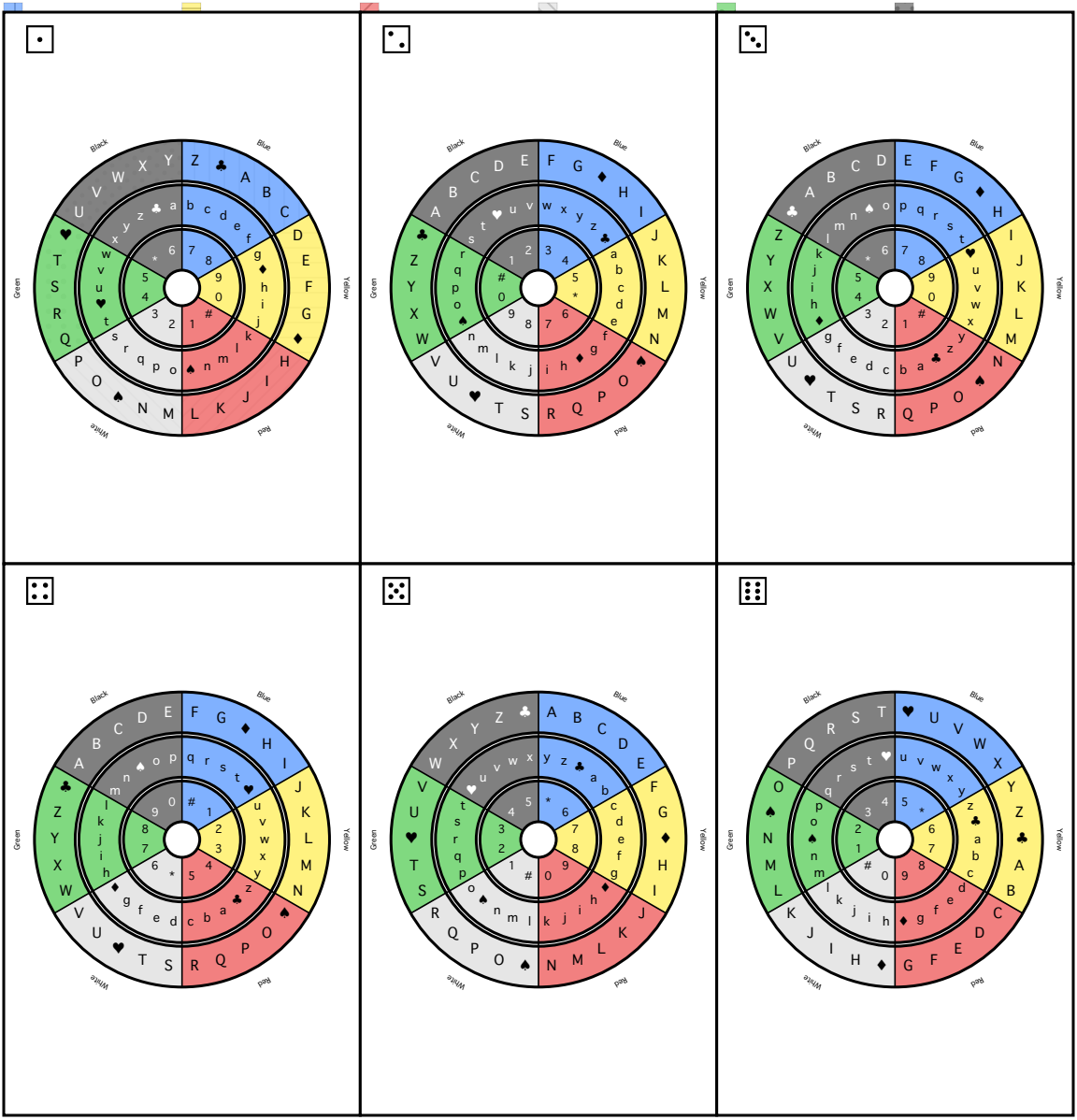


τ: 1785533985052889 | sha256(τ): 19b127a9

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052890

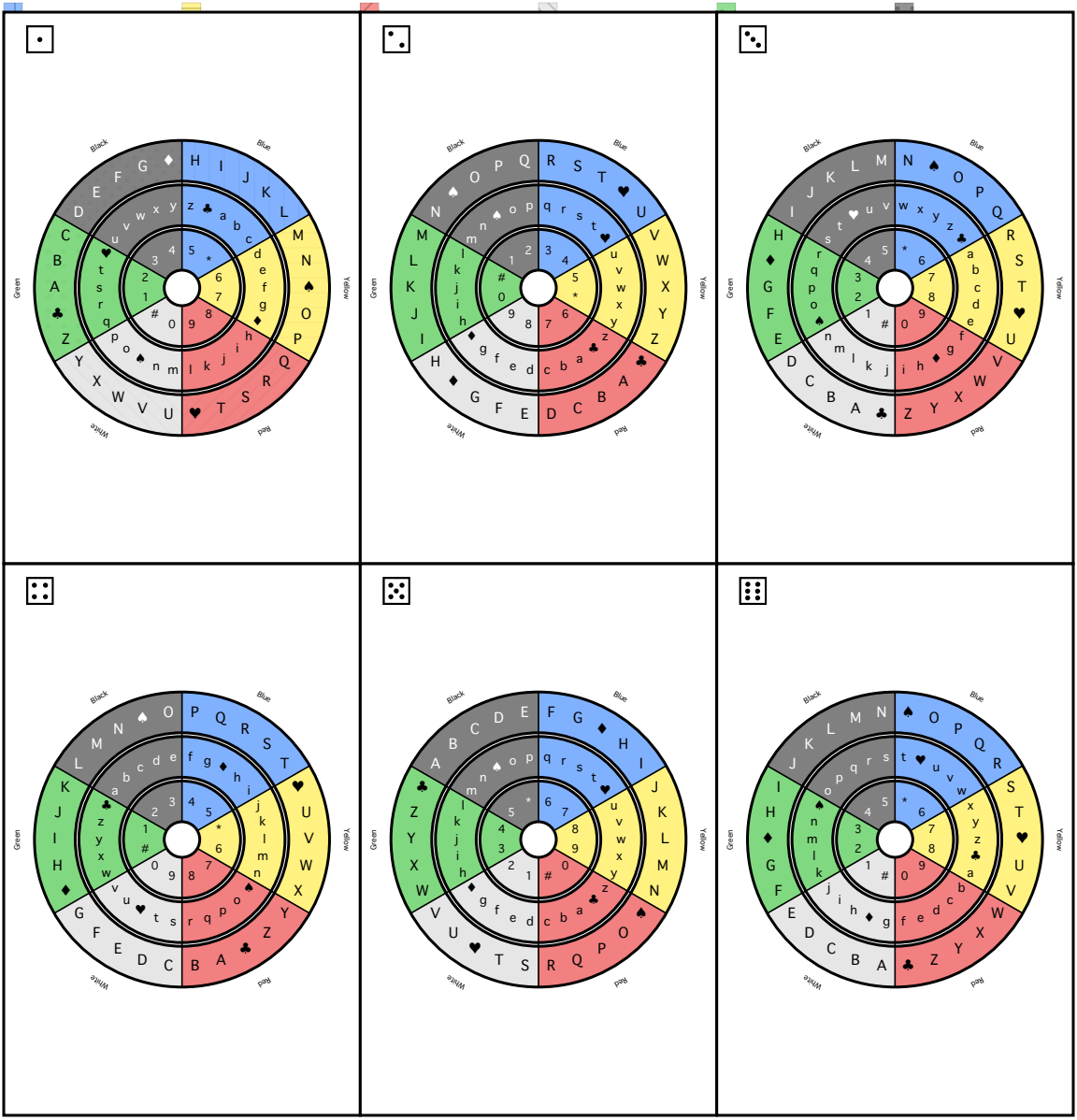


τ: 1785533985052890 | sha256(τ): db00bd3e

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052891

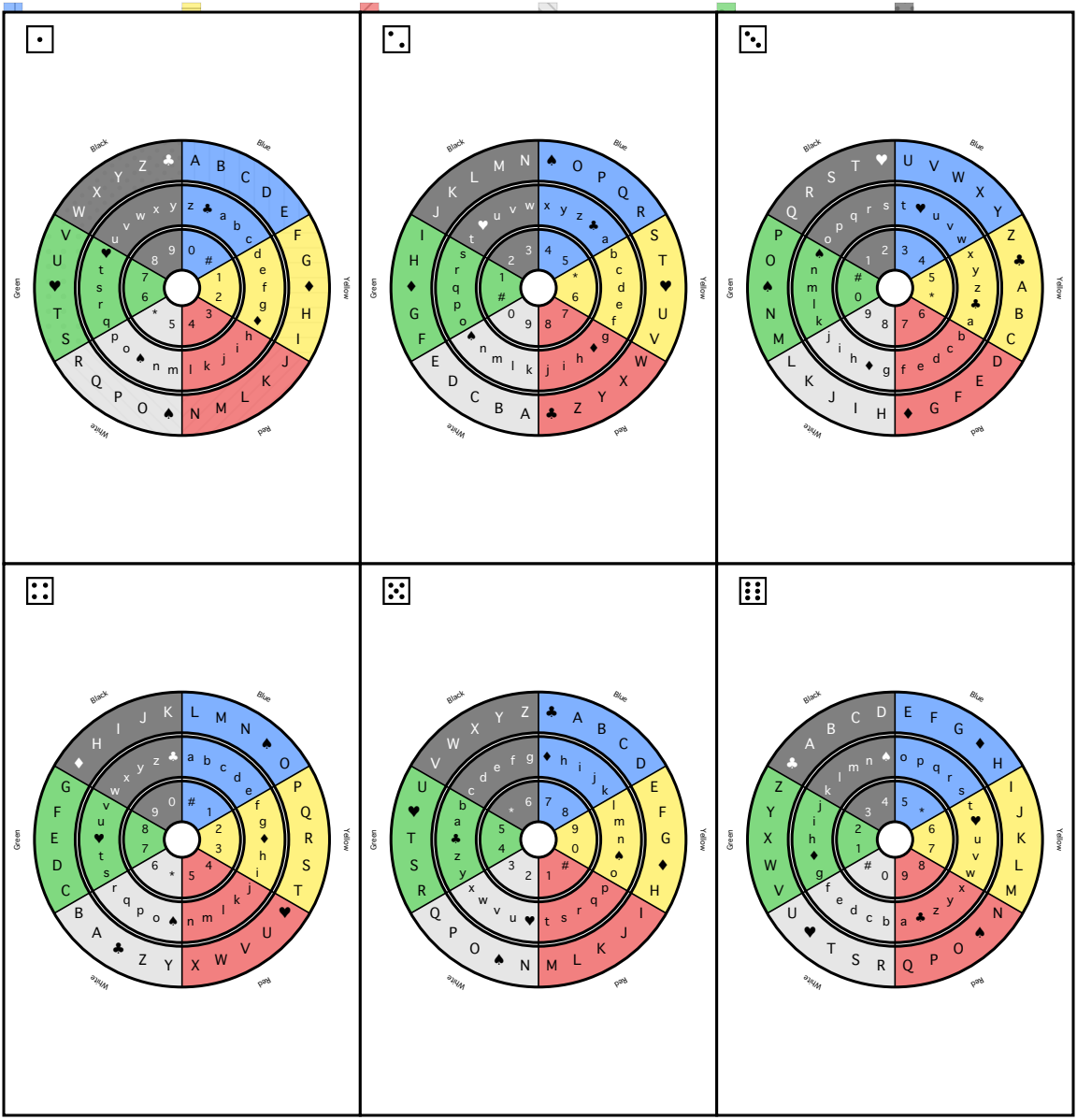


τ: 1785533985052891 | sha256(τ): 57c5b419

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052892

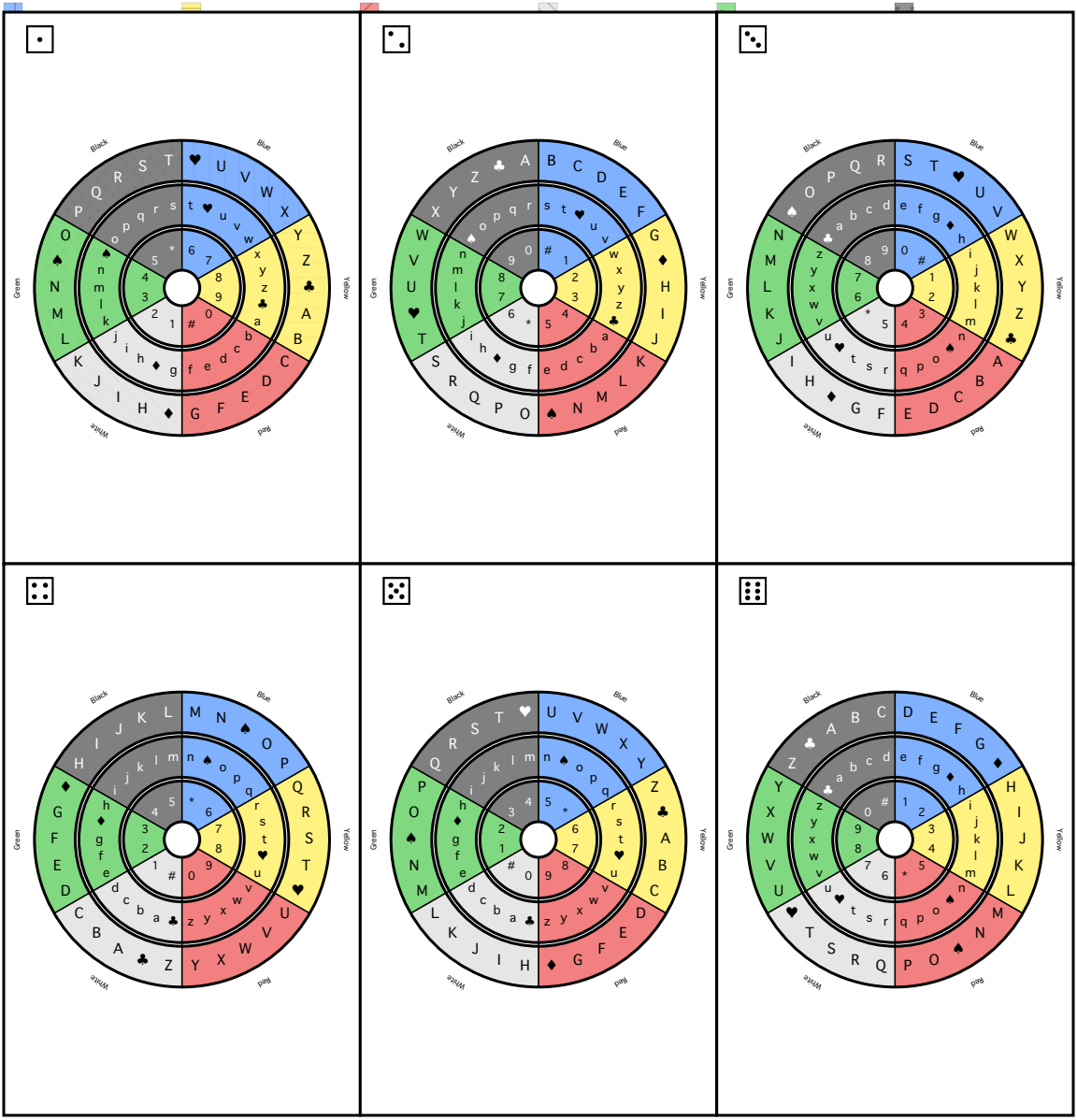


τ: 1785533985052892 | sha256(τ): 52f85ca6

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052893

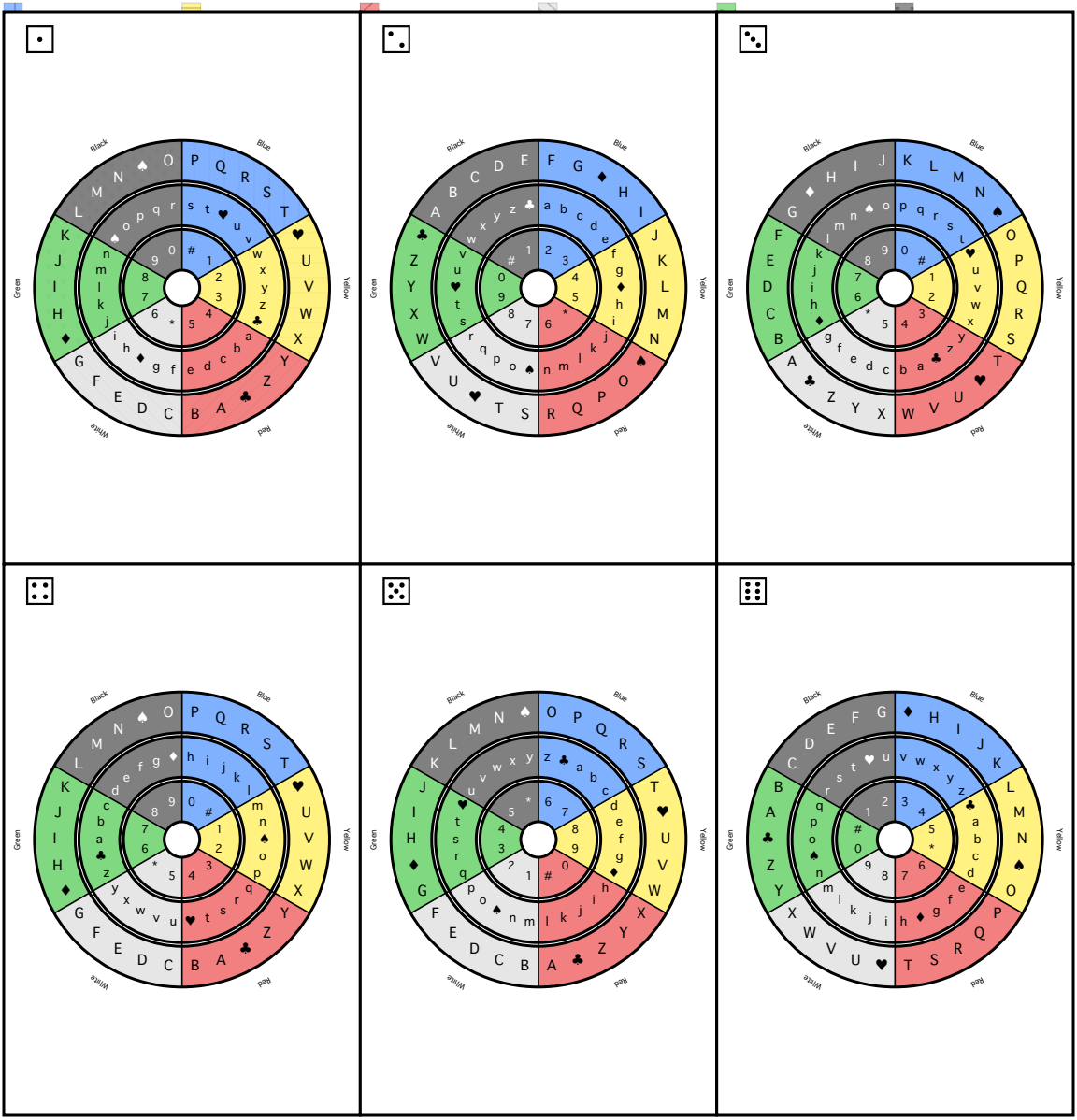


τ: 1785533985052893 | sha256(τ): 38f25017

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052894

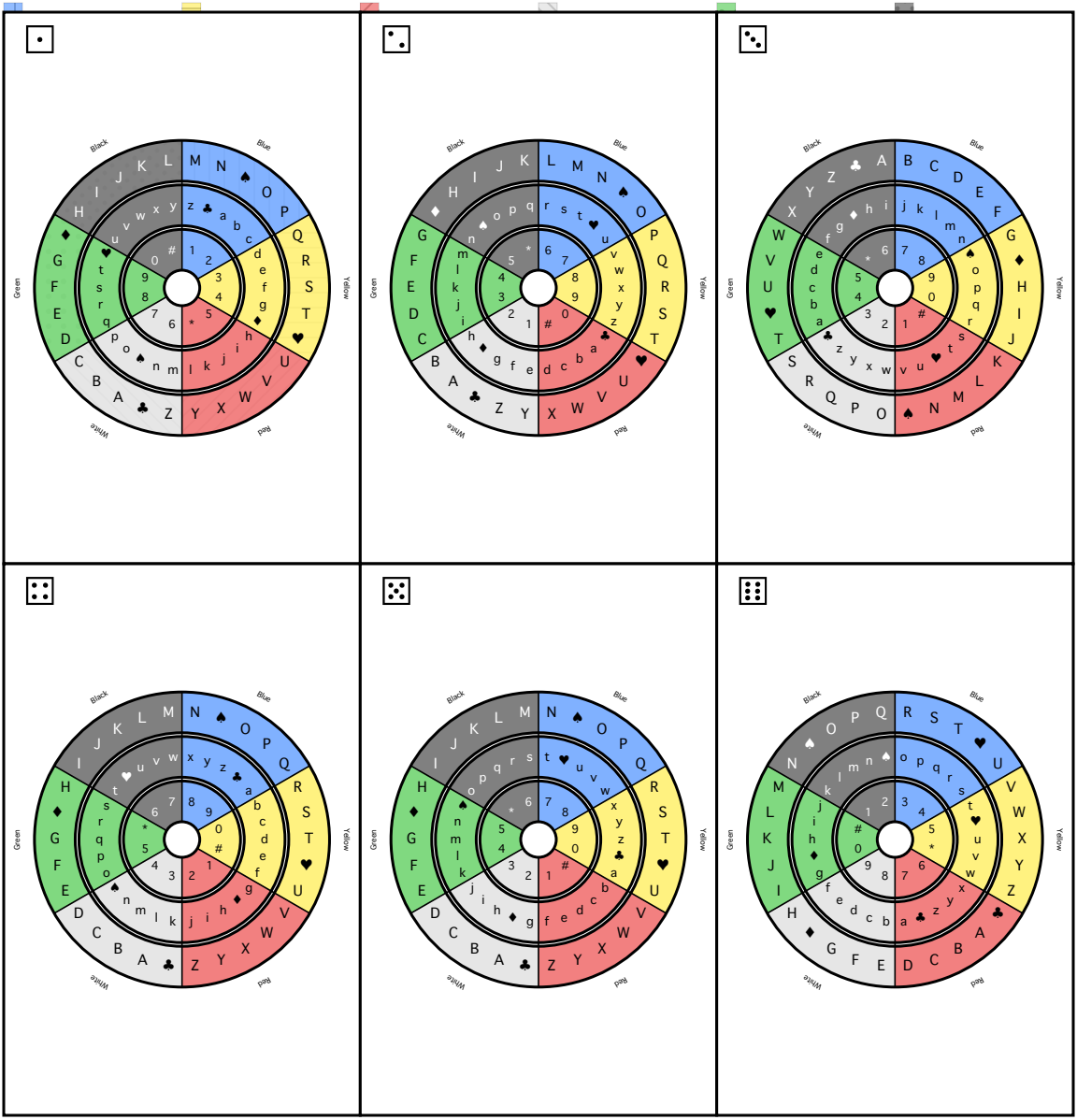


τ: 1785533985052894 | sha256(τ): c5b683fd

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052895

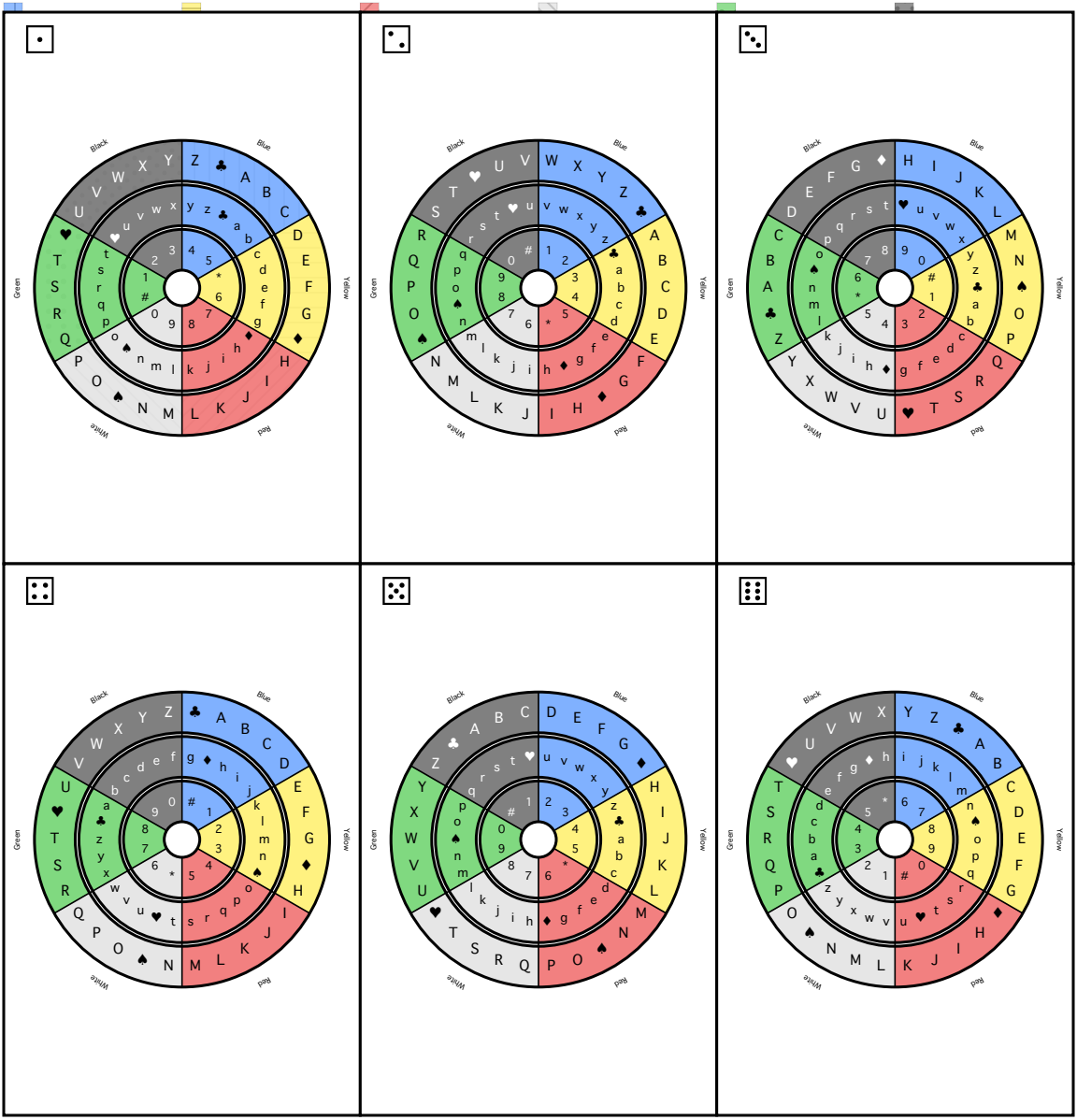


τ: 1785533985052895 | sha256(τ): ad31963f

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052896

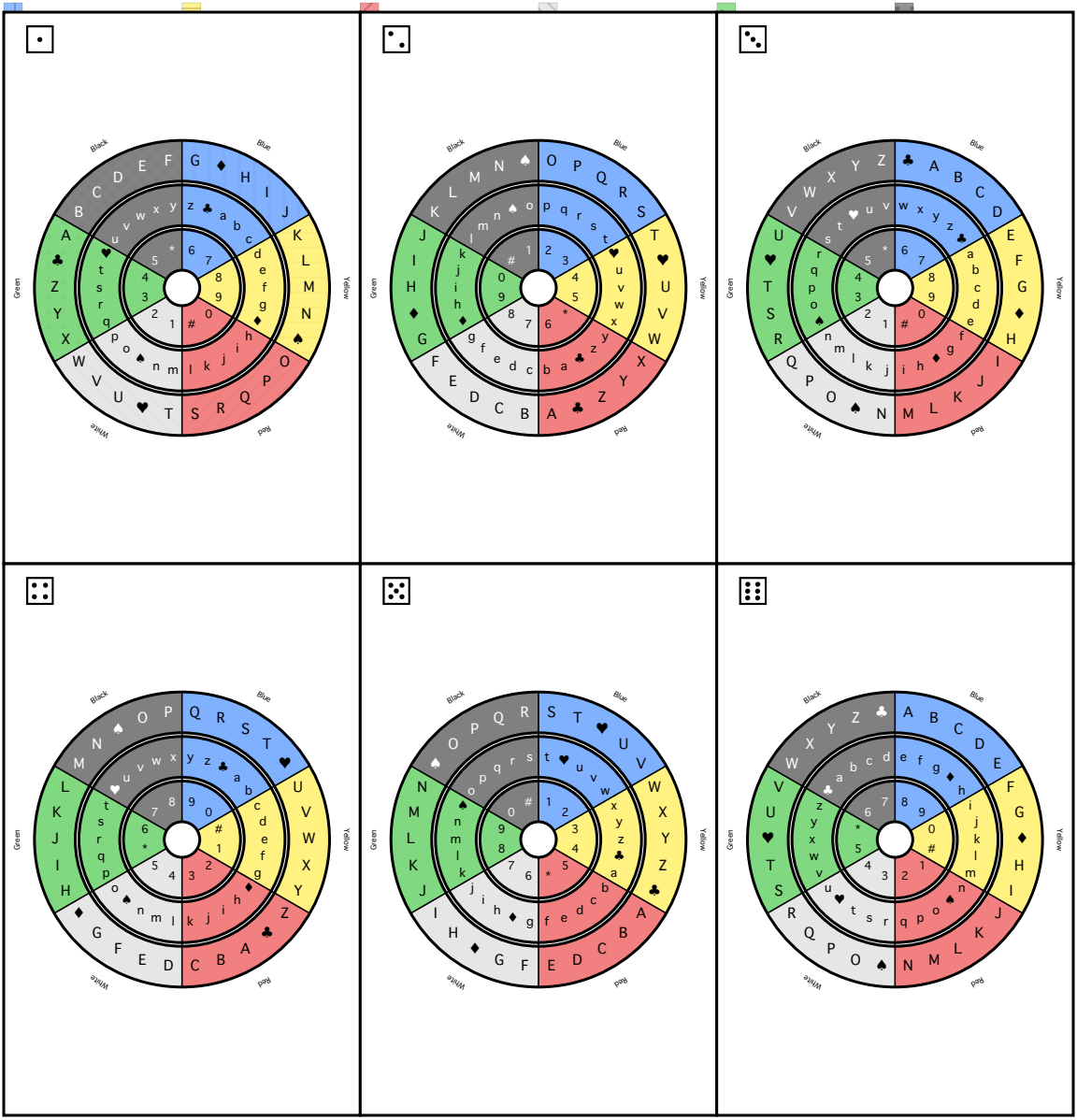


τ: 1785533985052896 | sha256(τ): 9bfba37c

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052897

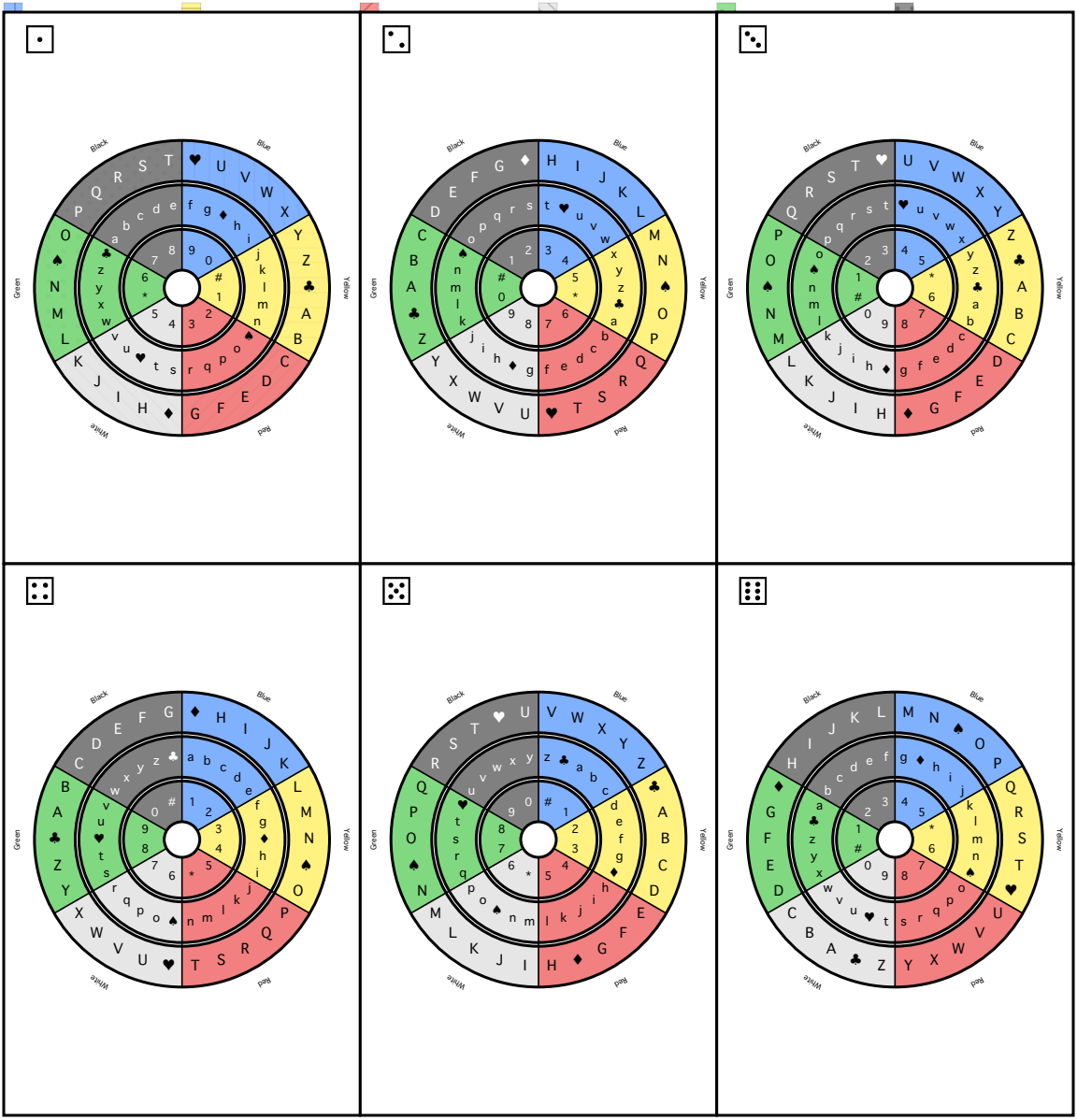


τ: 1785533985052897 | sha256(τ): 8c83cc43

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052898

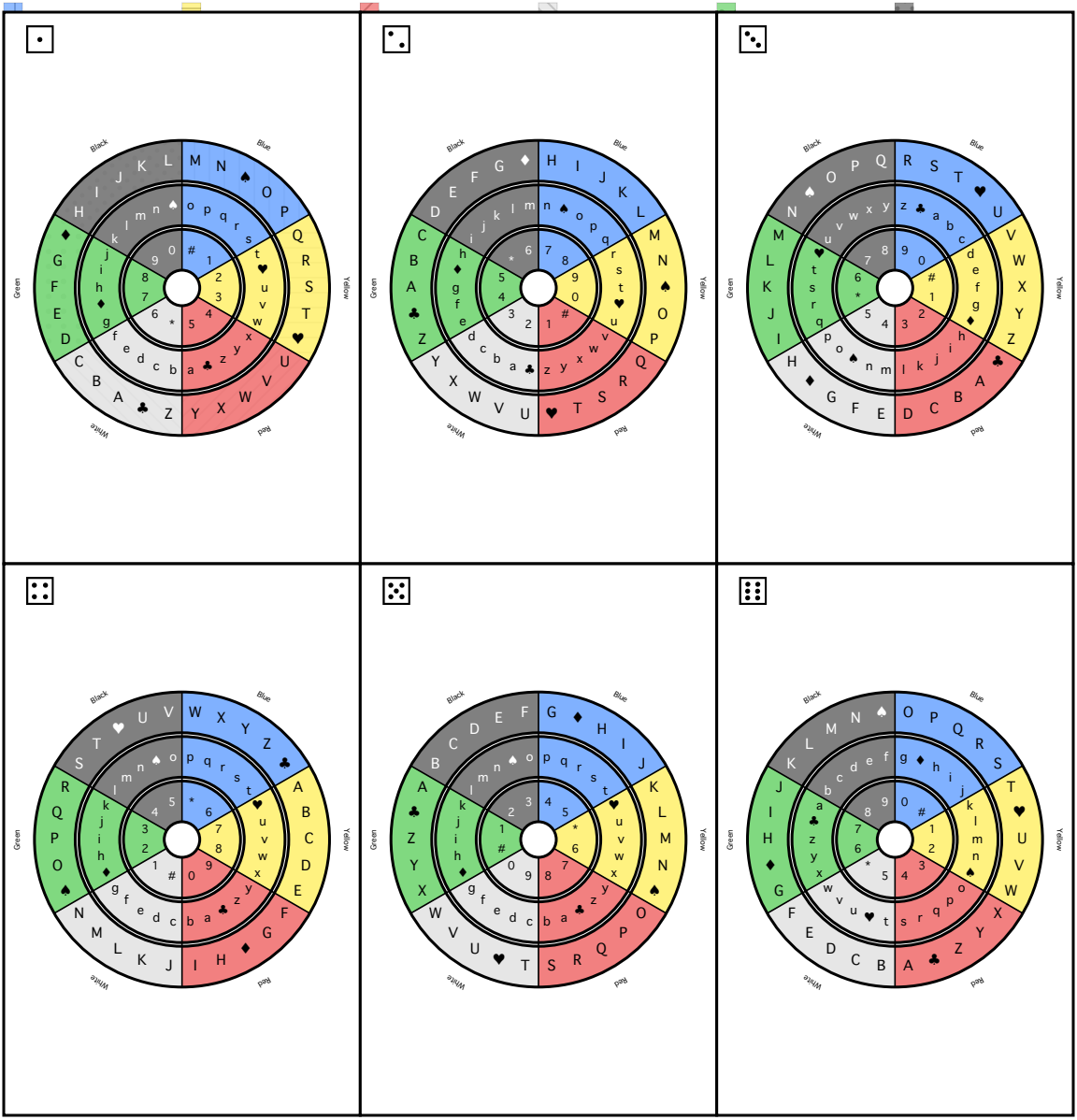


τ: 1785533985052898 | sha256(τ): d7c5534a

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052899

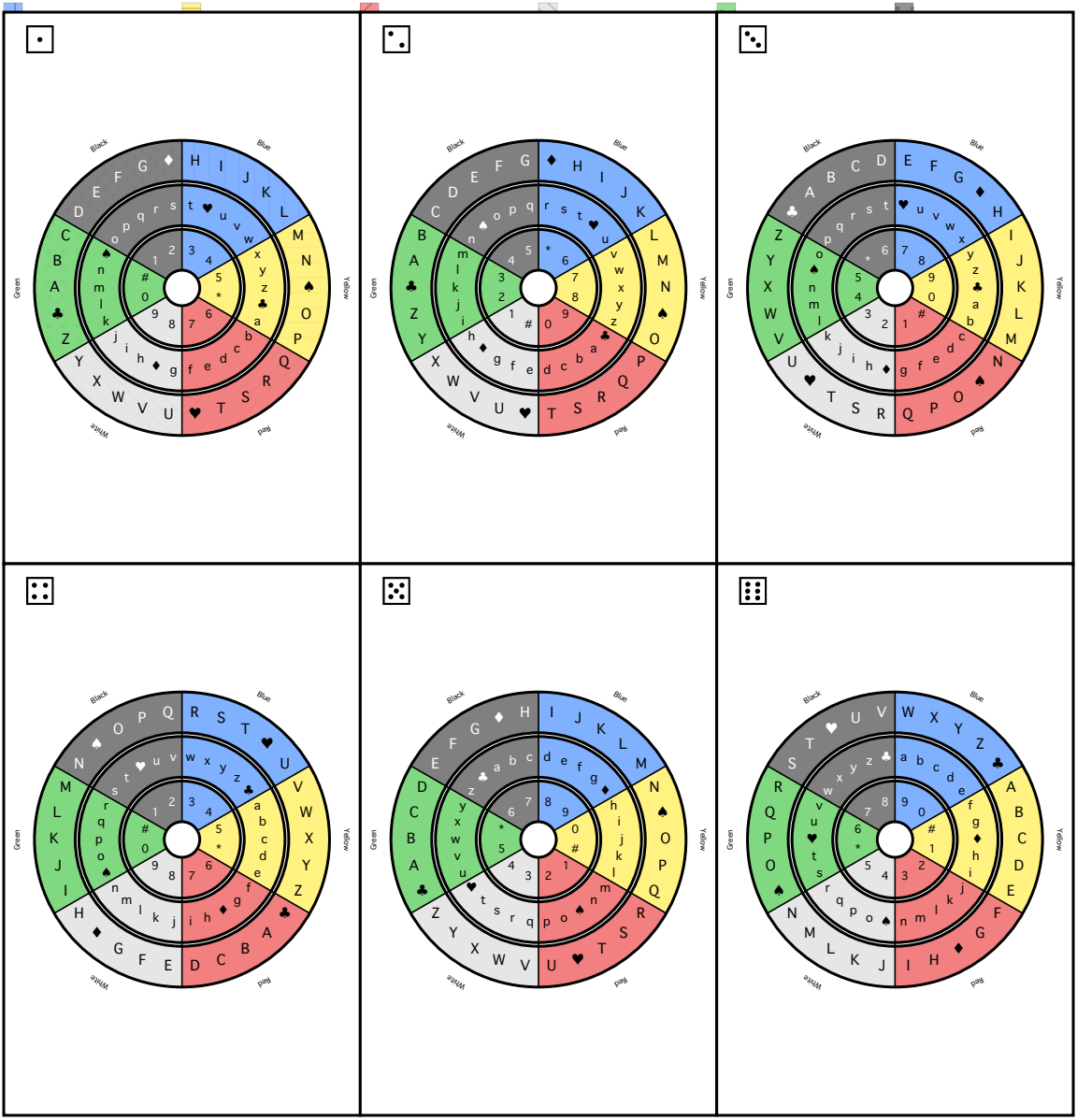


τ: 1785533985052899 | sha256(τ): ce886dac

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052900

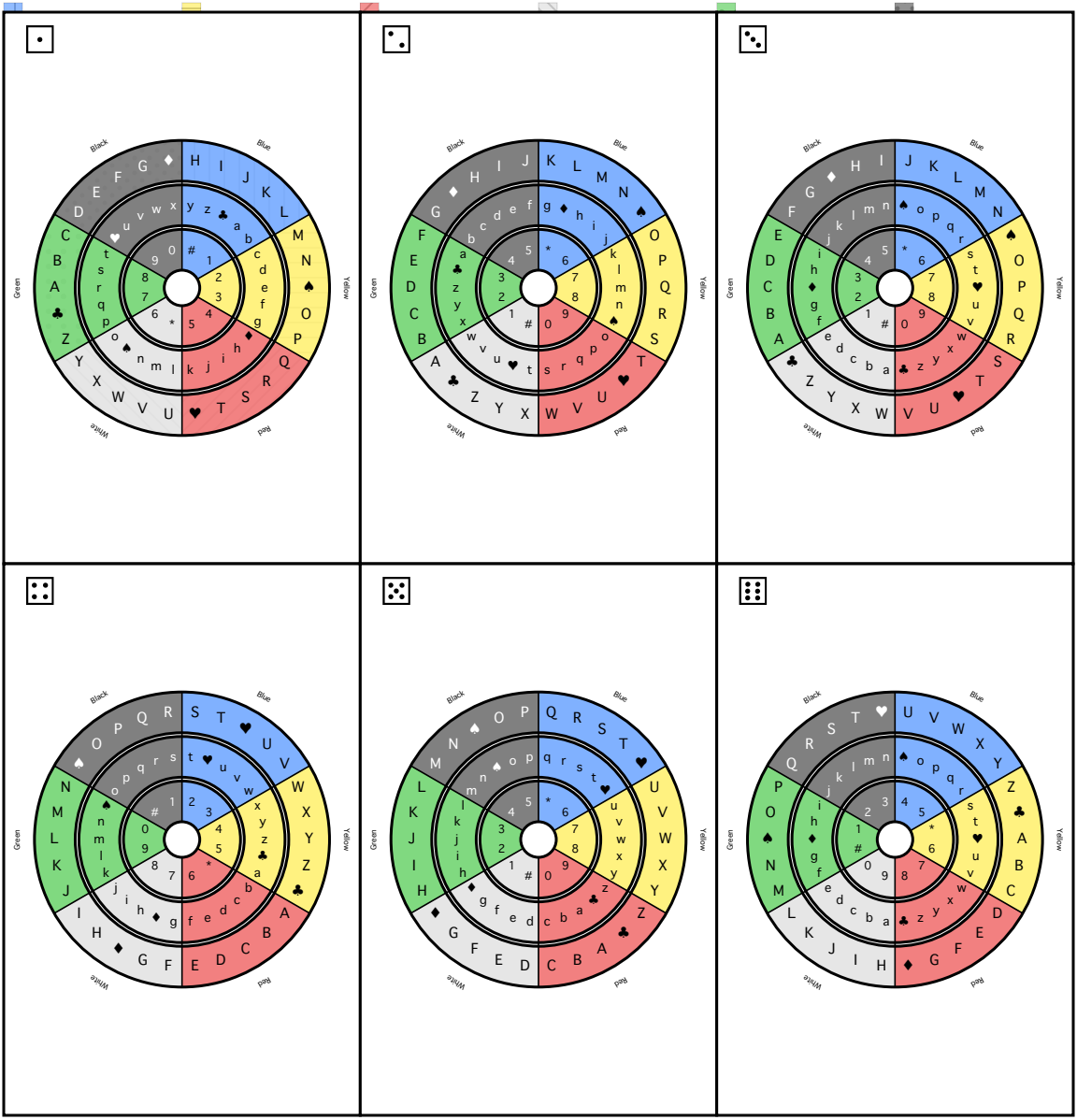


τ: 1785533985052900 | sha256(τ): a862217d

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052901

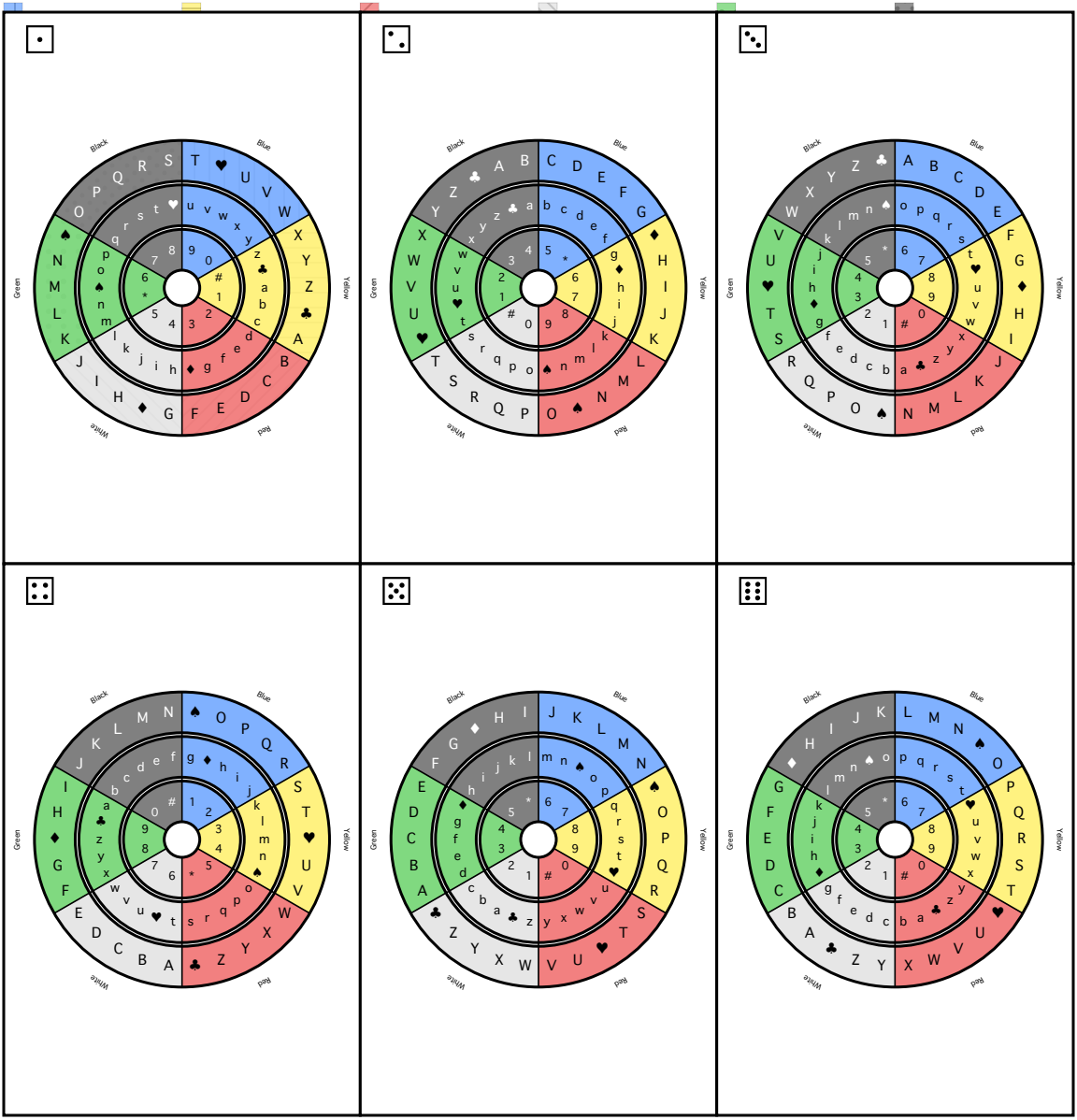


τ: 1785533985052901 | sha256(τ): 3d8b2902

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052902

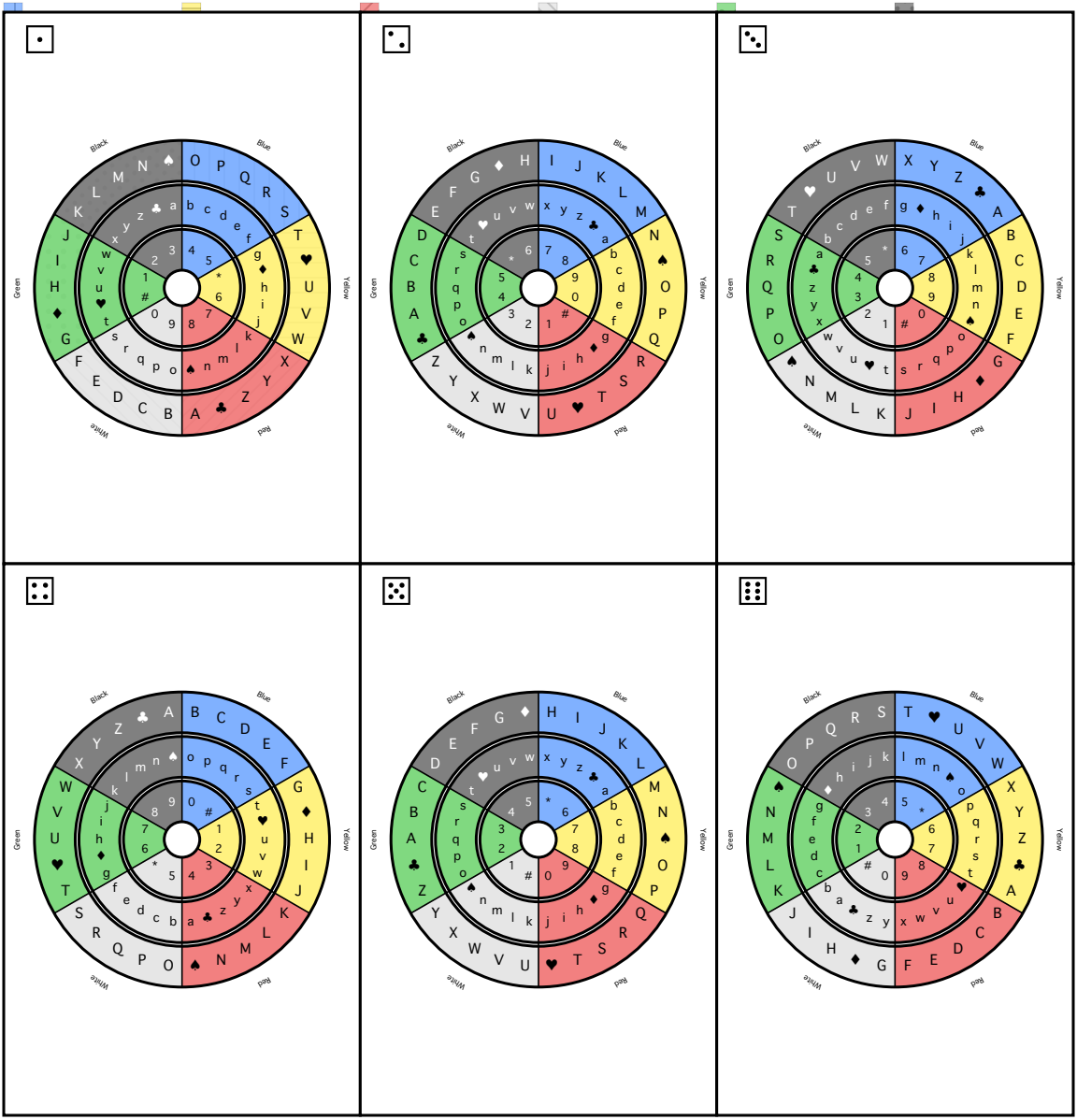


τ: 1785533985052902 | sha256(τ): b22e05e9

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA CHALLENGE SHEET

H=6 | τ: 1785533985052903



τ: 1785533985052903 | sha256(τ): c27ce88c

circuit sha256: 1777ee59292e42f5169491fcee59e51eaa68cad101a08521e848b36d4bda61af

ENI6MA Paper Identity Proof Appendices

Appendix A — Copyright and trademarks

Generated material

This booklet is **generated material**. Cover design, typography, sheet layout, and branding elements may be updated in later production editions. The identity guarantees of each sheet depend on the minting operator and the enrolled circuit, not on decorative artwork.

Notices

- Do not remove copyright notices from redistributed copies of this PDF.
- Do not represent a photocopy of a spent sheet as a fresh identity leaf.
- Questions about revocation, reissue, or circuit enrollment: contact your ENI6MA operator or ENI6MA support channel.

No patent claim language is included in this booklet.

Appendix B — Technology in plain language

ENI6MA paper sheets sit on three layers often abbreviated **SAC / EHP / SVE**. You do not need the equations to use the booklet; this page is orientation.

SAC — structured ambiguity channel

Public symbols on a sheet are arranged so an outsider's notebook fills with **surface bits** (marks you can photograph) while **effective bits**—mutual information with the secret—stay empty under the model. Capture is not knowledge.

EHP — ephemeral holographic proof

Each session (each sheet) is a short-lived manifold of balanced public leaves. The dice ceremony walks those leaves. Histograms stay flat so frequency attacks do not get a compass. The leaf is bound to a freshness window and a nonce.

SVE — spent verification event

Validation exports a **residue-only verdict**: PASS or FAIL for this spent event. It does not export a reusable credential. After burn-before-validate, the nonce is gone; success does not mint a lasting login.

Surface bits vs effective bits

Kind	What an observer gets
Surface bits	Ink, photos, footer text, ceremony marks
Effective bits	Mutual information with the authorizing secret

Signature proof sheets are designed so mailing and validating consume a one-shot event without turning the public channel into a recoverable password.

Appendix C — Shannon, unicity, and anti-unicity

Claude Shannon's perfect secrecy asks that an observer's posterior on the secret equal their prior even after seeing the ciphertext: mutual information ($I = 0$).

Classical unicity

Ordinary ciphers with redundant language eventually hit a **unicity distance**: enough ciphertext collapses ambiguity to one plausible key. More data helps the attacker.

Anti-unicity for authorization transcripts

ENI6MA authorization transcripts aim at the opposite under the stated model: more recordings still leave the secret uncollapsed—**anti-unicity**. Additional PASS/FAIL events and surface marks do not assemble into a recoverable long-lived credential.

For paper sheets:

- A spent leaf adds surface evidence (photo, marks) but not a reusable secret.
- A wrong-circuit or replayed nonce fails closed.
- The cover circuit SHA-256 identifies *which* enrolled system you validate against; it is not itself a password.

Formal statements, axioms, and bounds live in ENI6MA's Technology pages and white papers. This appendix is a field reminder: empty effective information is the design target; "I photographed the sheet" is not the same as "I can mint new authority."

Appendix D — Glossary

Term	Meaning in this booklet
tau	Server-minted timestamp identifying the sheet reservation
Nonce	One-time UUID (or equivalent) burned at validation
Circuit	Enrolled cryptographic system; identified by SHA-256 on the cover
Dice leaf / sheet	One physical identity page with dice ceremony card + footer
Book QR	Cover-only QR linking to the circuit / validate landing
Burn-before-validate	Nonce spent before PASS/FAIL is returned; no retry
SHA-256	Hash identifying circuit (cover) or leaf footer integrity
Surface bits	Observable marks and photos
Effective bits	Mutual information with the secret (target: empty)
PASS / FAIL	Only validator outcomes; no exported reusable credential
Custody log	Hand table tracking which blanks left the booklet

Validate path reminder

`/validate/<nonce_uuid>`

Scan the **book QR** on the cover when available; otherwise enter the circuit SHA-256 and the sheet nonce manually.