CODEX 32

THE SHAMIR SECRET SHARING CODEX

Andrew Poelstra — Director, Blockstream Research

Overview

Open workshop: feel free to come and go.
We will work through a complete SSSS+checksum process.

Topics in these slides:

Overview	Assembly	Future Work
Randomness	Checksumming	Deriving Shares
	Recovery	

[0] `https://www.secretcodex32.com`

Overview

First, a few definitions:

- volvelles are paper computers, because electronic computers are scary and unpredictable
- checksumming is a way to add redundant data to your secrets, such that errors are recoverable
- secret sharing is a technique to break your data into many pieces so that only a couple of them are needed to reconstruct

[0] `https://www.secretcodex32.com`

Overview

With volvelles,

- We can compute and verify checksums
- We can split and reconstruct secrets
- We can't do error correction (but we can blind e. computers)
- We can't heirarchical (BIP32) derivations (so far)
- We can't derive addresses (so far)

[0] `https://www.secretcodex32.com`

Overview

For more info:

Website: `https://www.secretcodex32.com`

Repo: `https://github.com/roconnor-blockstream/SSS32/`

Email: `pearlwort@secretcodex32.com`

Mathematics: `https://github.com/apoelstra/SSS32/blob/2021-12--math-intro/volvelles/main.tex`

Please email me, especially if you think you can do error correction or address derivation using volvelles.

Never enter secret data into `secretcodex32.com`, or any website!

[0] `https://www.secretcodex32.com`

Overview

Can I use this in practice? Not until we have hardware wallet support. Though I (Andrew) am using it, by converting BIP39 words with an extra ad-hoc worksheet. Not recommended.

What is the state of the project? We are putting together a website and formal doc, planning to get a BIP number, then will pitch the scheme to various wallet vendors.

How do I learn more? Check my MIT BItcoin Expo 2022 talk, or the website.

[0] `https://www.secretcodex32.com`

Assembly

Assembling volvelles:

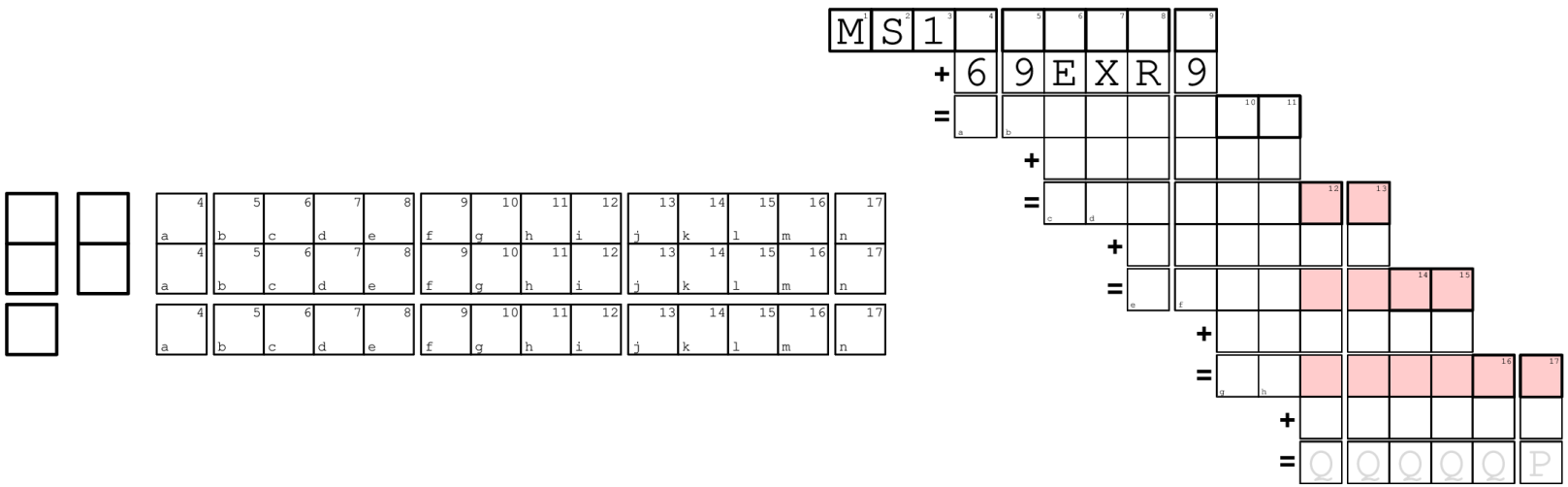
- With scissors, carefully cut out the wheels.
- Using a craft knife, cut out all the windows.

[0] https://www.secretcodex32.com

Assembly

For this workshop we will use reduced-size worksheets.

Talk to Andrew to get copies.



[0] https://www.secretcodex32.com

Tips for handwriting.

- Use a mechanical pencil, with the smallest lead you can find.
- Write on a hard surface to avoid leaving imprints.
- Cross your 0s, 7s, Zs, and Ss. Be careful not to draw 6s and Gs in similar ways.

[0] https://www.secretcodex32.com

Assembly

[0] https://www.secretcodex32.com

Assembly

[0] https://www.secretcodex32.com

Future Work

Tractable things we still need to do:

- Implement error correction and translation on the website.
- Hardware wallet support!
- Bring all the artistic changes into the main PostScript repo.

[0] `https://www.secretcodex32.com`

Future Work

Hard things we want to do:

- Implement error correction by hand
- Figure out how to do EC math by hand. (Seems very hard.)

[0] https://www.secretcodex32.com

Randomness

We can generate random data using dice rolls.

- (Cheap) dice are almost always biased
- But we can eliminate any passive bias! We use a **von Neumann entropy extractor** in the form of a worksheet
- The more sides your dice have, the faster you go

[0] `https://www.secretcodex32.com`

Randomness

For a 128-bit secret you need to generate 26 characters. For this workshop, only 2.

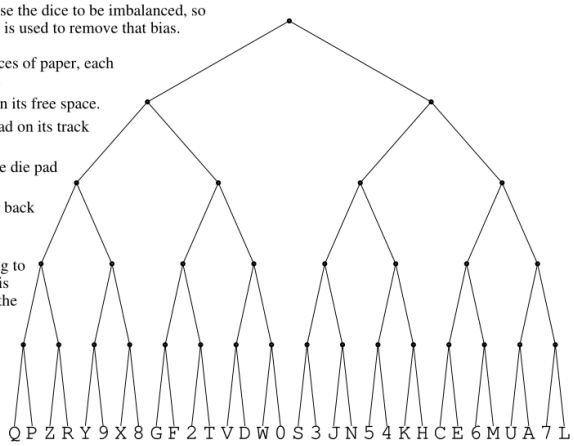
- Generating randomness is an annoyingly slow process.
- But if you take shortcuts the consequences may be catastrophic.
- Follow the instructions carefully.

Dice De-biasing Worksheet

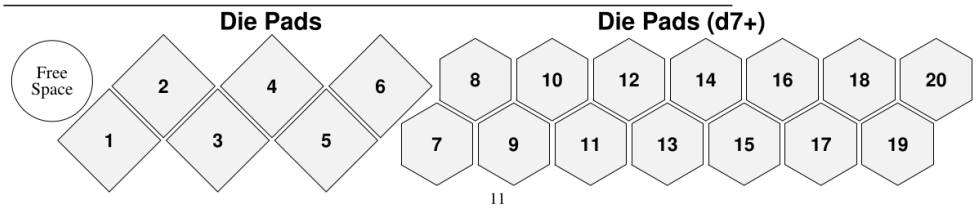
Most dice have small manufacturing imperfections that cause the dice to be imbalanced, so some values appear more often than others. This worksheet is used to remove that bias.

You will need: five distinct dice, five die markers (e.g., pieces of paper, each labeled by which die it corresponds to), and this worksheet.

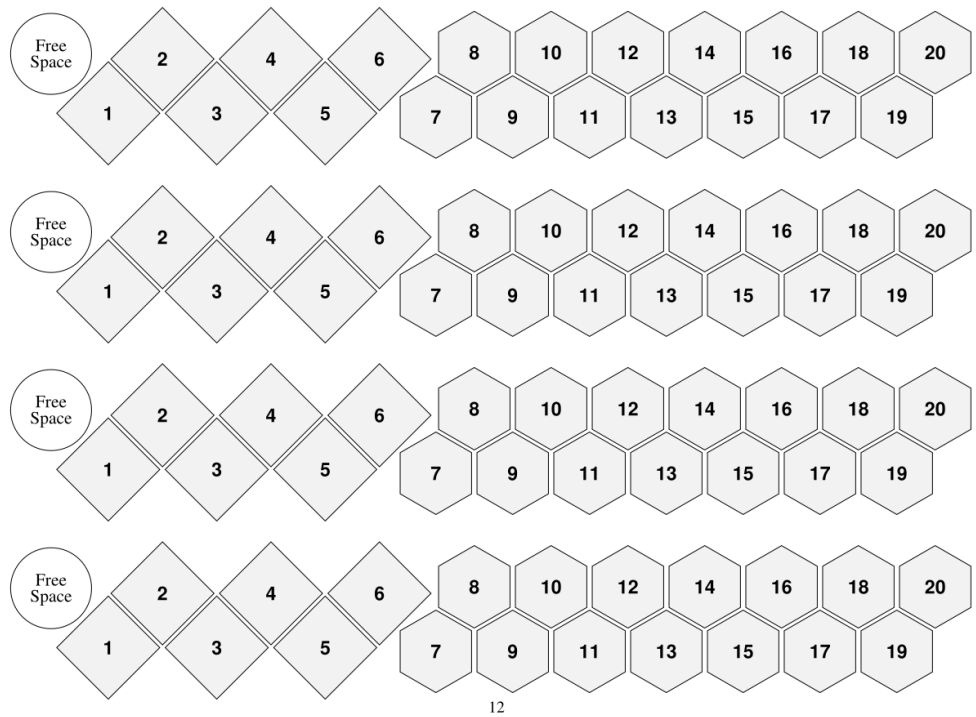
1. Choose a die track for each die. Put the die's marker on its free space.
2. Roll all five dice. Move each die's marker to the die pad on its track indicating its value.
3. Re-roll the same five dice again and set each **die** on the die pad indicating their second values.
4. If a die showed the same value twice, move its marker back to the free space and repeat steps two and three. *You must redo both rolls!*
5. Using your finger, follow the tree to the right according to the die tracks. Take the first left branch if the first die is to the left of its marker, and the right branch if it is to the right. Similarly, take the second branch based on the results on the second die track, and so on, until the bottom of the tree, which has the resulting character.
6. Repeat steps one through five for each character.



Die Tracks

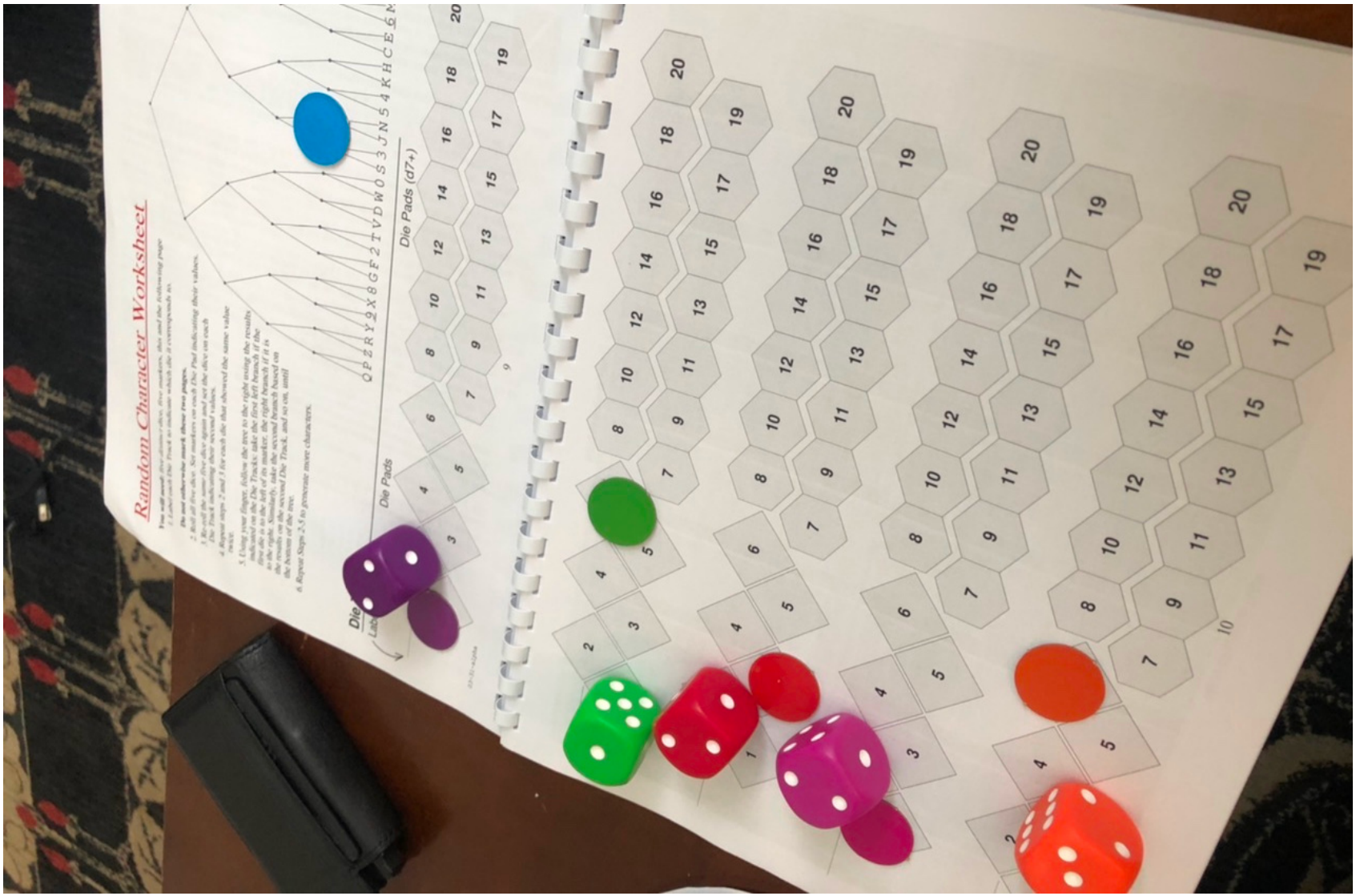


11



12

Randomness



[0] https://www.secretcodex32.com

Checksumming

Once we have random data, stick a header and checksum on it.

- The header is: your threshold, secret ID and share index
- The checksum is generated using the Checksum Worksheet.
- In this workshop we have a greatly-reduced-size worksheet. Talk to Andrew to get a copy.

[0] `https://www.secretcodex32.com`

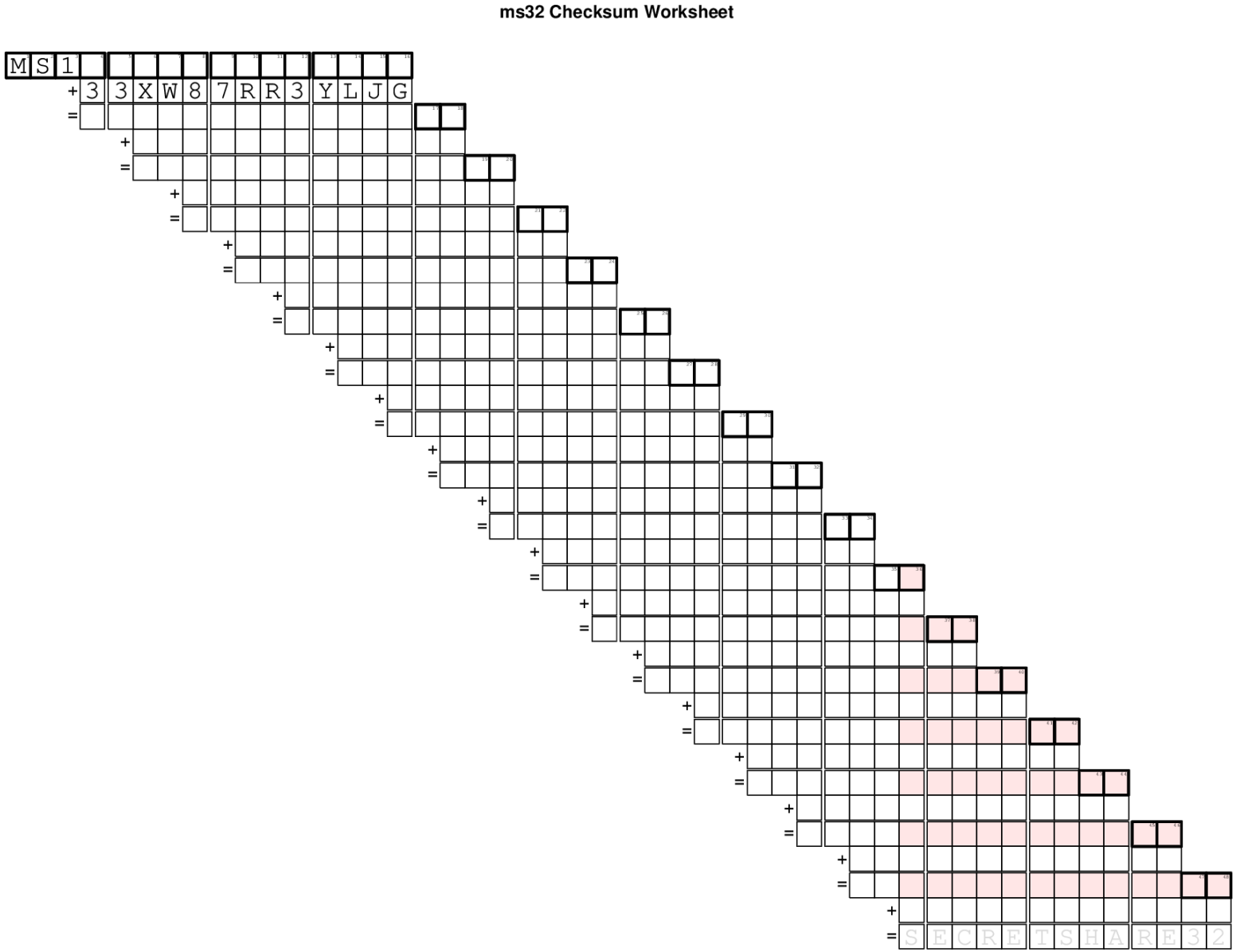
Checksumming

Checksumming is complicated and may be hard to notice mistakes.

- You can practice using the interactive tools on `secretcodex32.com`.
- But the checksum worksheet is (almost) entirely secret data; don't enter any part of your real data into a website!
- And if you trust a friend to help with the sheet... trust them!

[0] `https://www.secretcodex32.com`

Checksumming



[0] https://www.secretcodex32.com

Deriving Shares

Deriving shares involves the translation worksheet and wheel.
It is (relativly) fast and probably the most fun part of the process.

- Essentially: look up your translation symbol in the appropriate table, translate your shares character-by-character using this symbol, then add the results.
- There isn't yet an interactive version to practice with online.
- Again: this worksheet contains secret data!

[0] `https://www.secretcodex32.com`

Translation Worksheet

The translation worksheet is used to derive shares, when splitting keys, and during key recovery. In all cases, the process is to translate a set of shares using the translation wheel, then to add the translated results using the addition wheel.

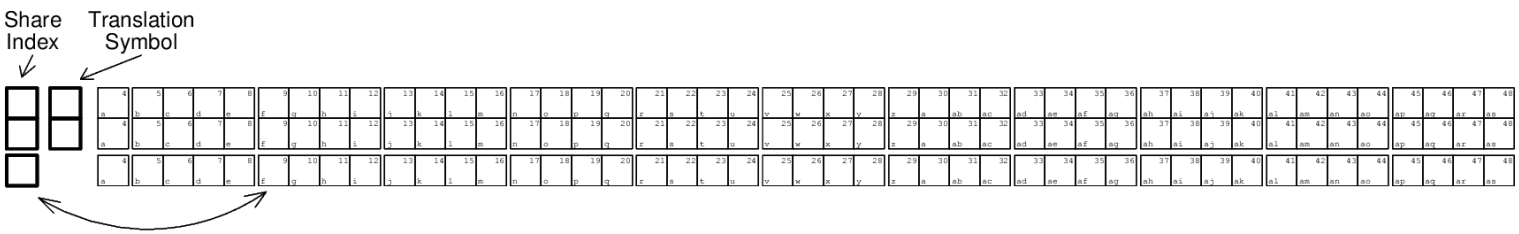
You will need: translation worksheet, translation/fusion wheel, addition wheel, recovery wheel (for key recovery), derivation table (page 7, for share derivation)

In all cases, the number of shares to combine is your *k* value, the number of required shares to reconstruct the secret. The process is:

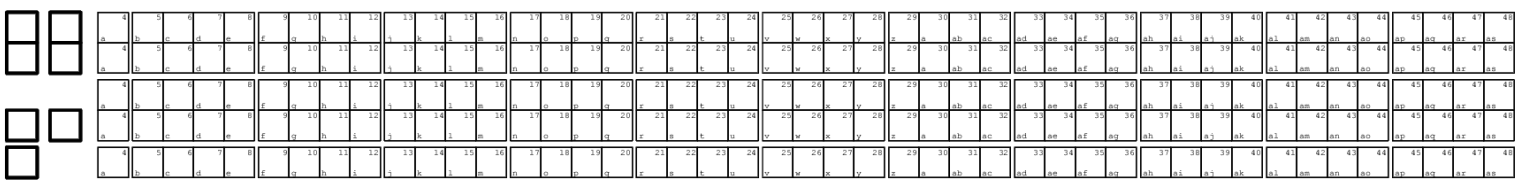
1. Make sure that you have completed checksum worksheets for all input shares.
2. Look up the translation symbols for each share, either in the derivation table or using the recovery wheel and fusion wheel.
3. Mark down each share's index (the sixth character of its header) and translation symbol in the appropriate squares.
4. Character by character, translate each share from its checksum worksheet to its row, using the translation wheel.
5. Using the addition wheel, add all rows together.

Notice that the resulting share will automatically have the correct share index in its header. **If not, you have likely misread the instructions.**

k=2 Example



k=3 Example



[0] https://www.secretcodex32.com

Recovery

Recovery is literally the same as deriving shares, except you always derive the S share, and you need the recovery wheel rather than a table to obtain the symbols.

If $k > 2$ you get to use the fusion side of the translation wheel.

[0] https://www.secretcodex32.com