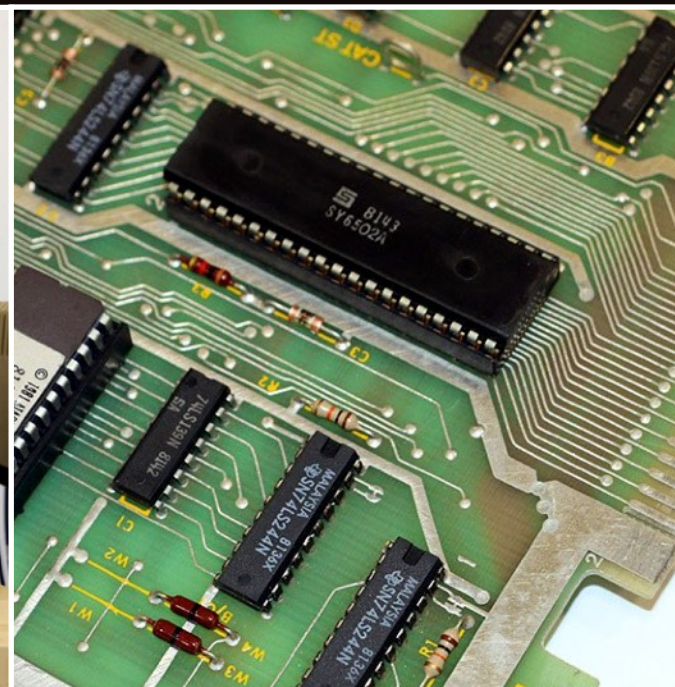
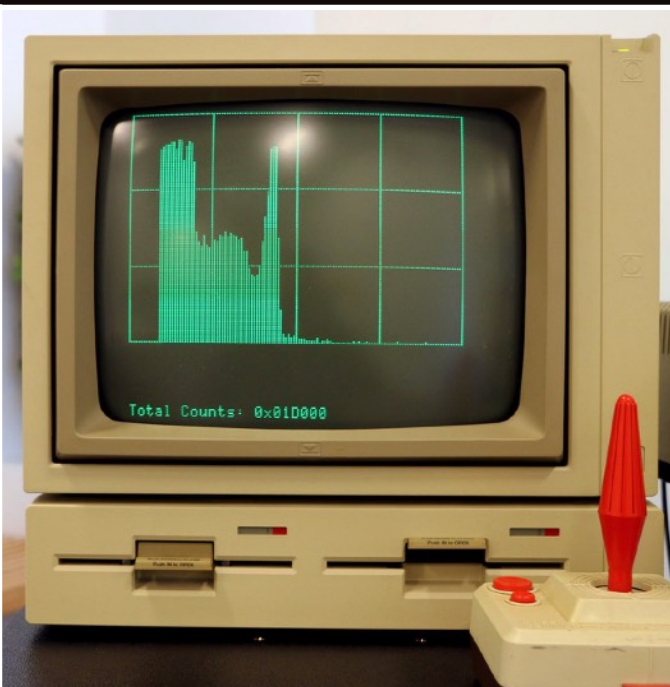




PUNCHED-OUT!!

PUBLIC TEMPLATES FOR NUCLEAR WARHEAD VERIFICATION

Boaz Barak, Alex Glaser, Moritz Kütt, Sébastien Philippe

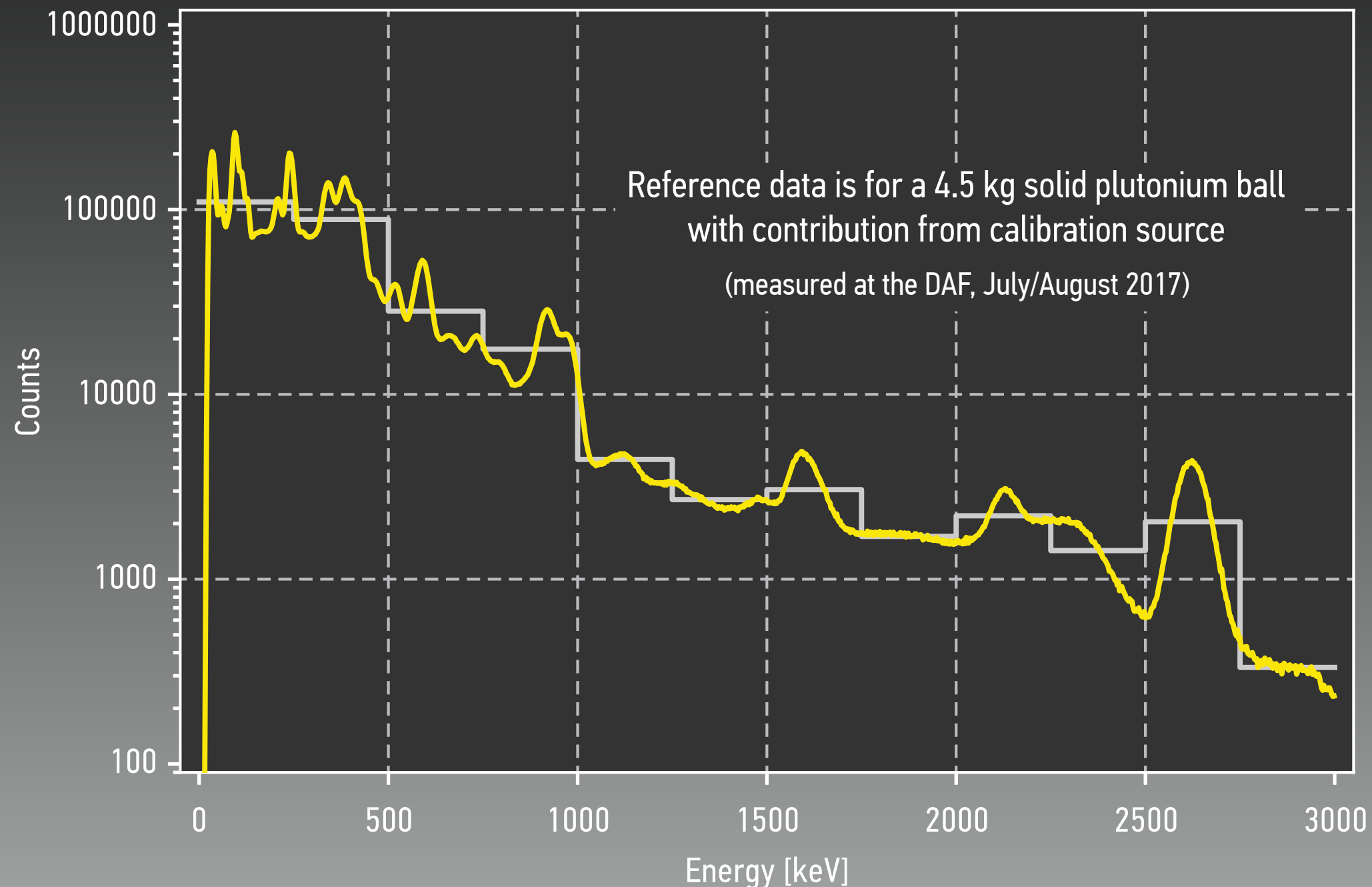
June 2018

Revision 3b

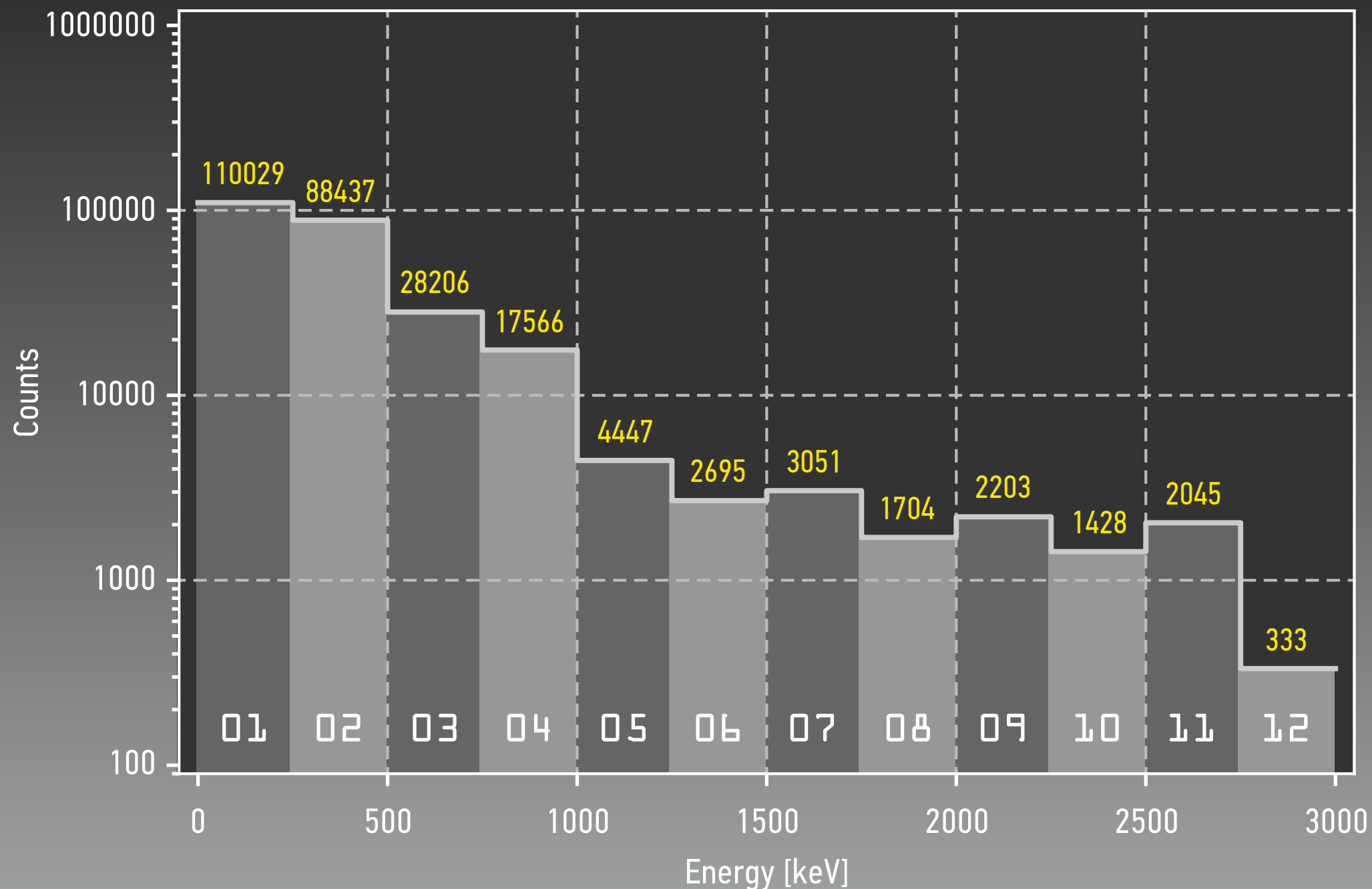
INSPECTION PROTOCOL

PRIVATE PHASE

GENERATING A SECRET TEMPLATE (TEMPORARY)

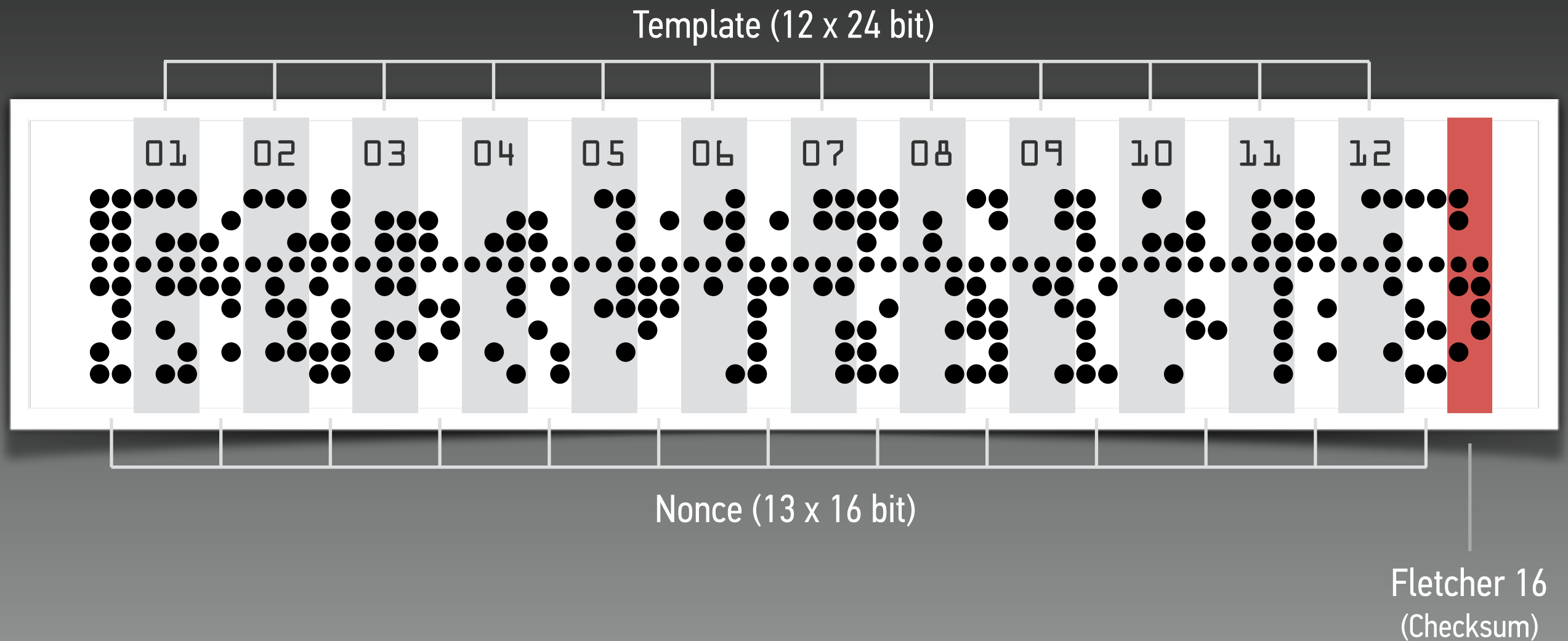


GENERATING A SECRET TEMPLATE (TEMPORARY)



PRIVATE PHASE ¶ STEP 2

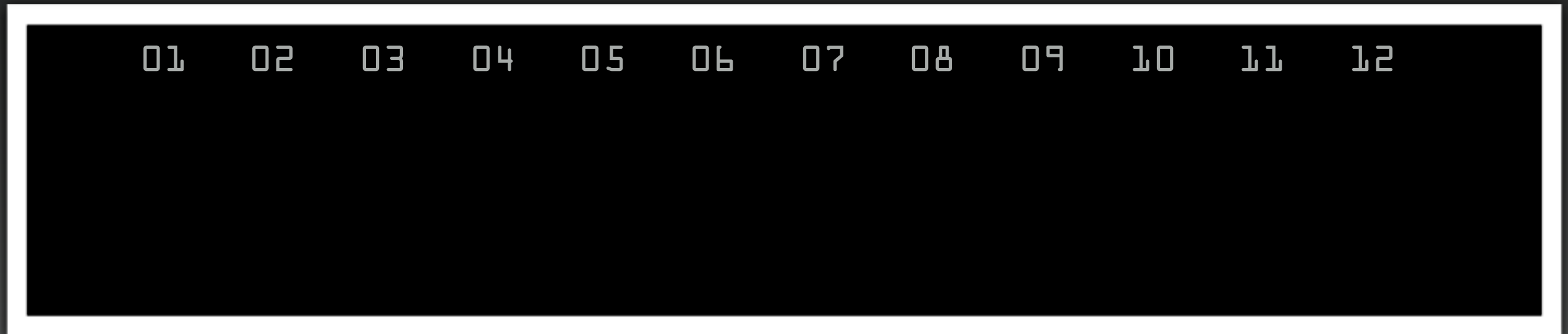
MAKING THE PUNCHED CARD WITH THE SECRET TEMPLATE



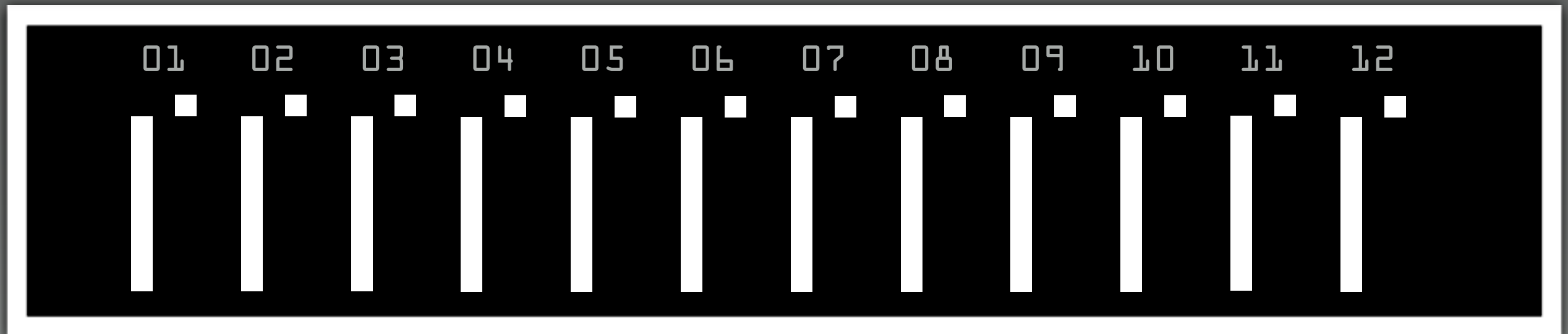
$$12 \times 24 \text{ bit (template)} + 13 \times 16 \text{ bit (nonce)} + 16 \text{ bit (checksum)} = 512 \text{ bit}$$

PRIVATE PHASE ¶ STEP 3

CHOOSING THE PUBLIC MASK

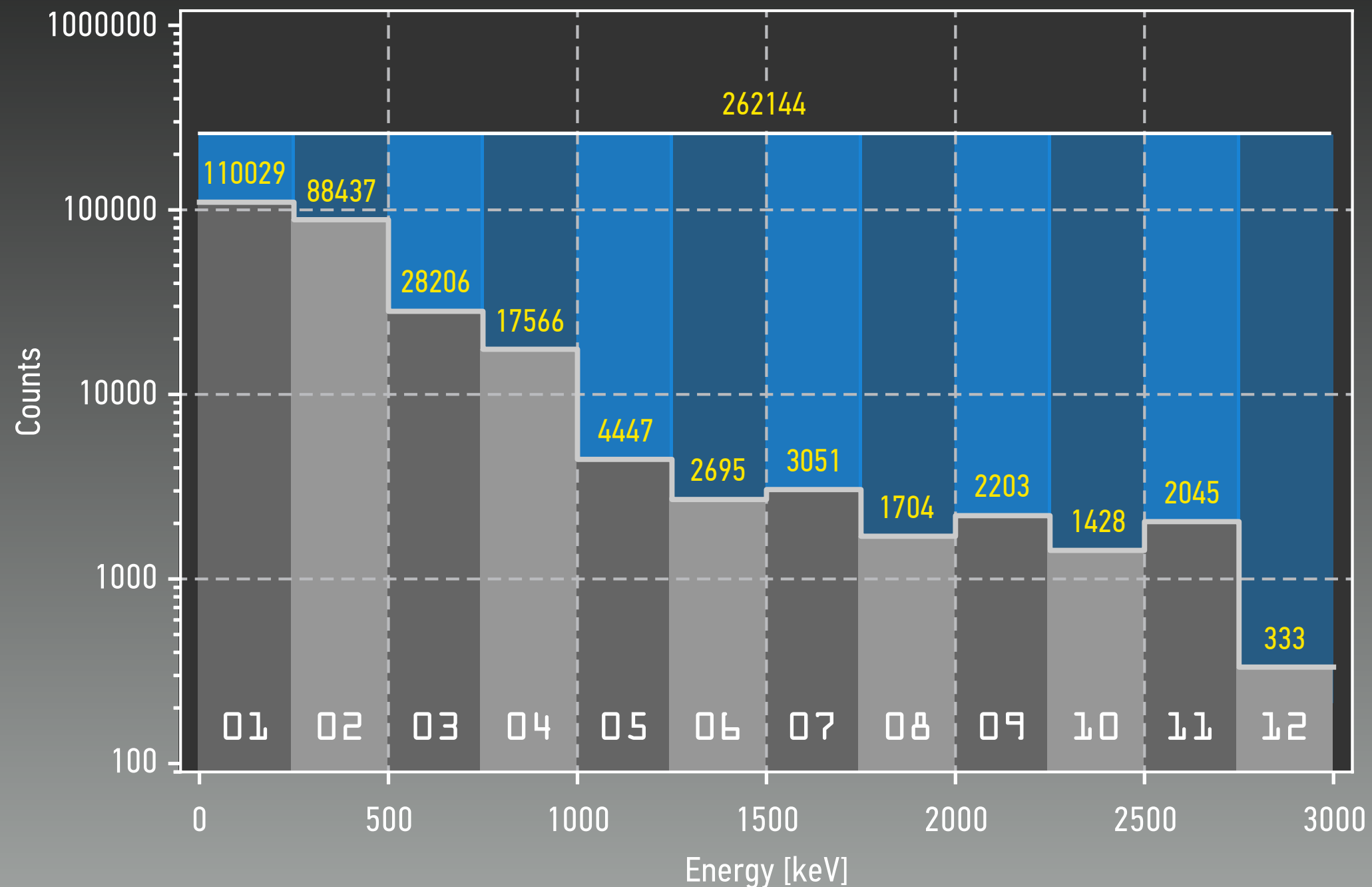


“Maximum secrecy mask”



Mask confirming that the counts in all bins are $< 2^{18} = 262,144$; also reveals the LSB for each bin

WHAT THE PUBLIC MASK TELLS

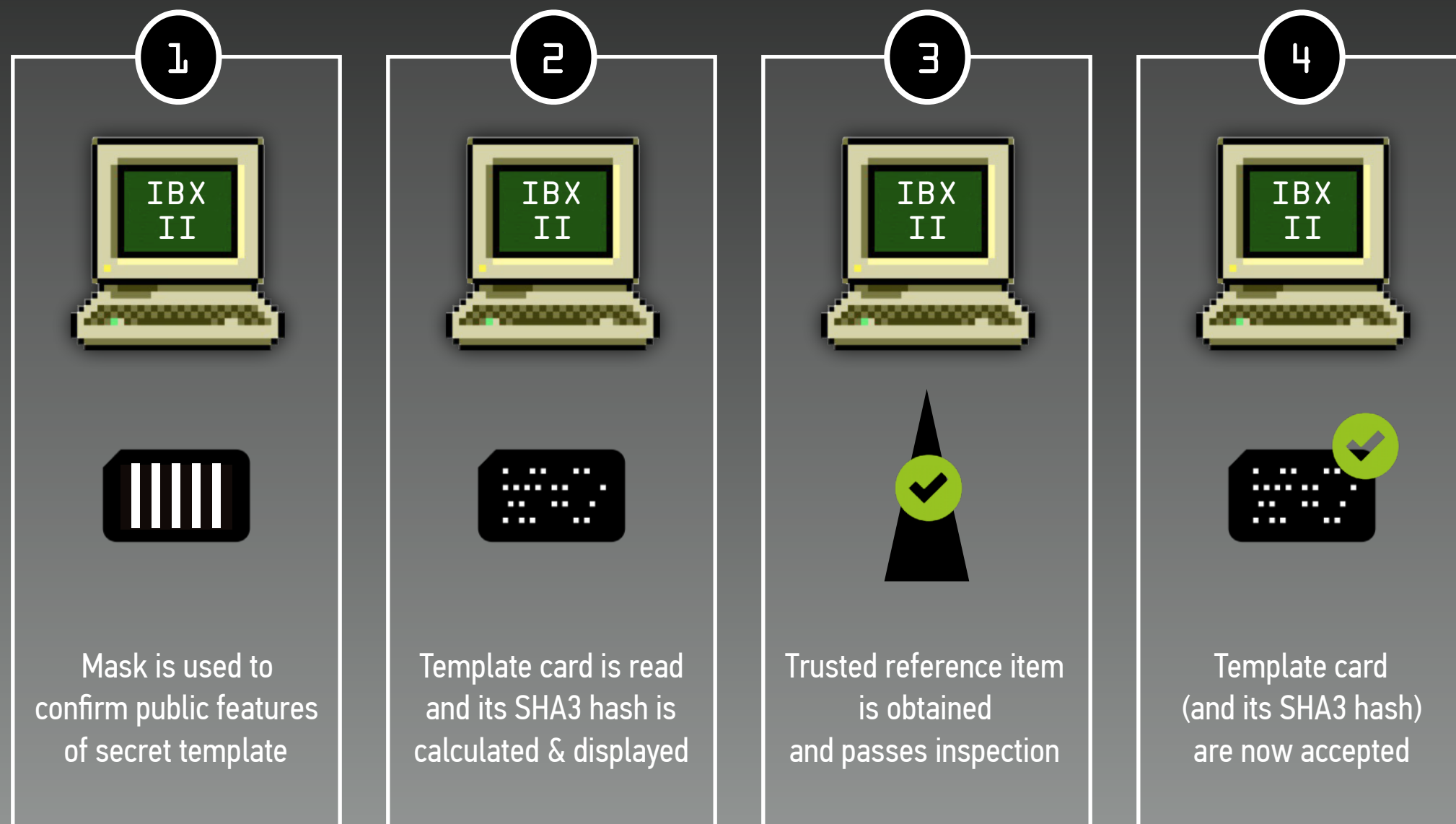


INSPECTION PROTOCOL

PUBLIC PHASE

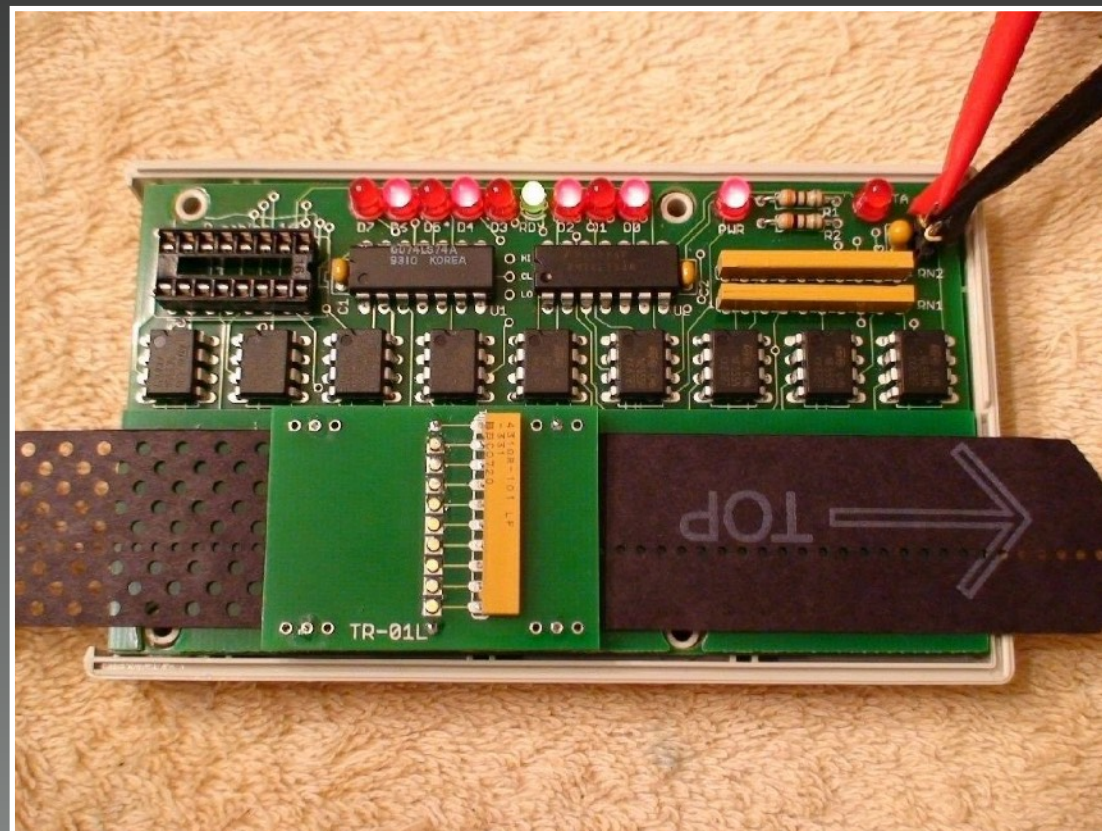
VALIDATING THE TEMPLATE CARD

USING A TRUSTED REFERENCE ITEM



PUBLIC PHASE ¶ STEP 4

READING THE TEMPLATE CARD AND GENERATING ITS PUBLIC HASH

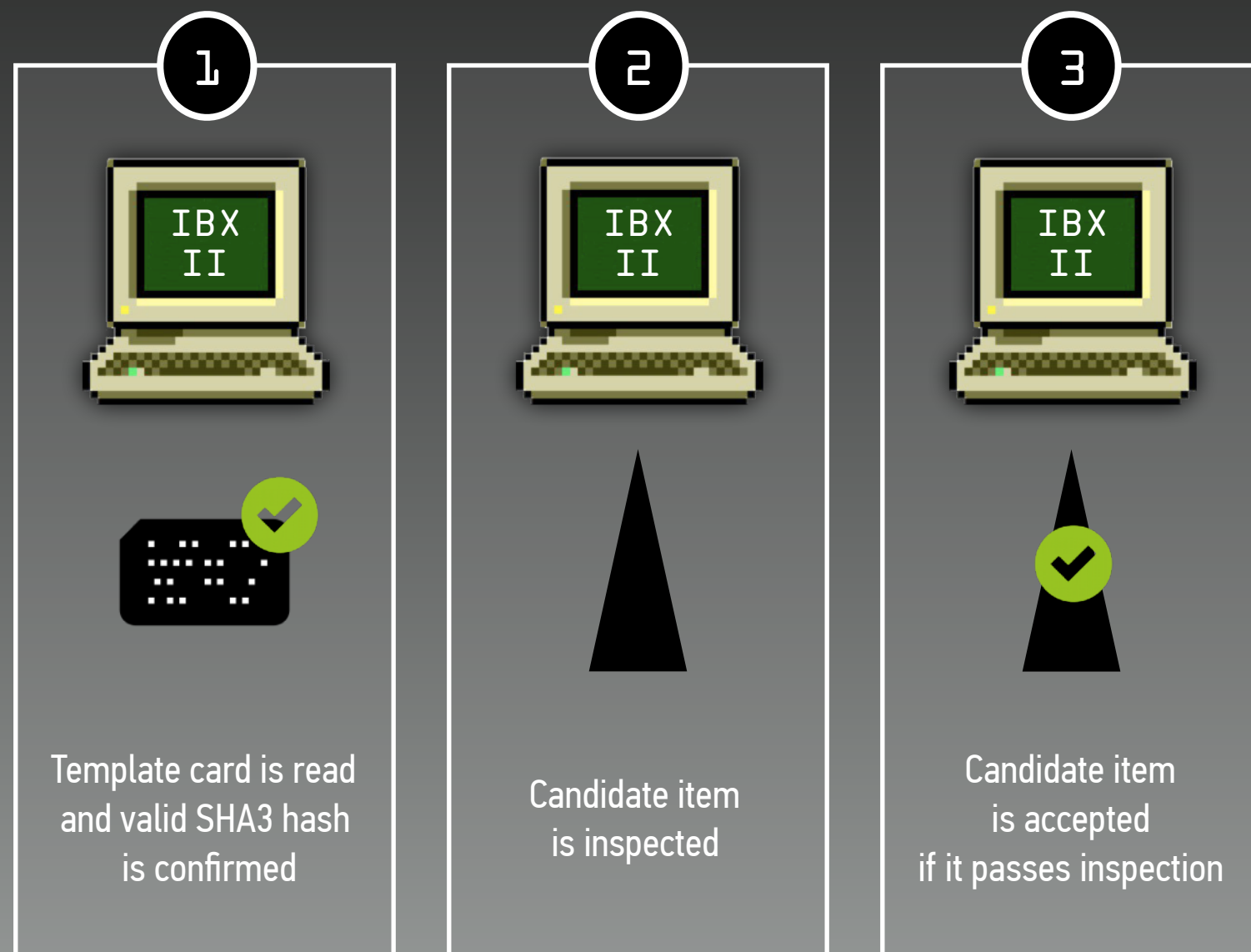


Manual punched card reader

```
3d05e4f4e1de1b19
a4075c6bd9107bda
93ebd94f4c9251db
1c9e1854afae0498
1666836f92502a30
b83eaeafa383d5d5
58cbd00ad149a0f3
d51002b1d0e7a8fd
```

SHA3 hash of template card

INSPECTING CANDIDATE ITEMS

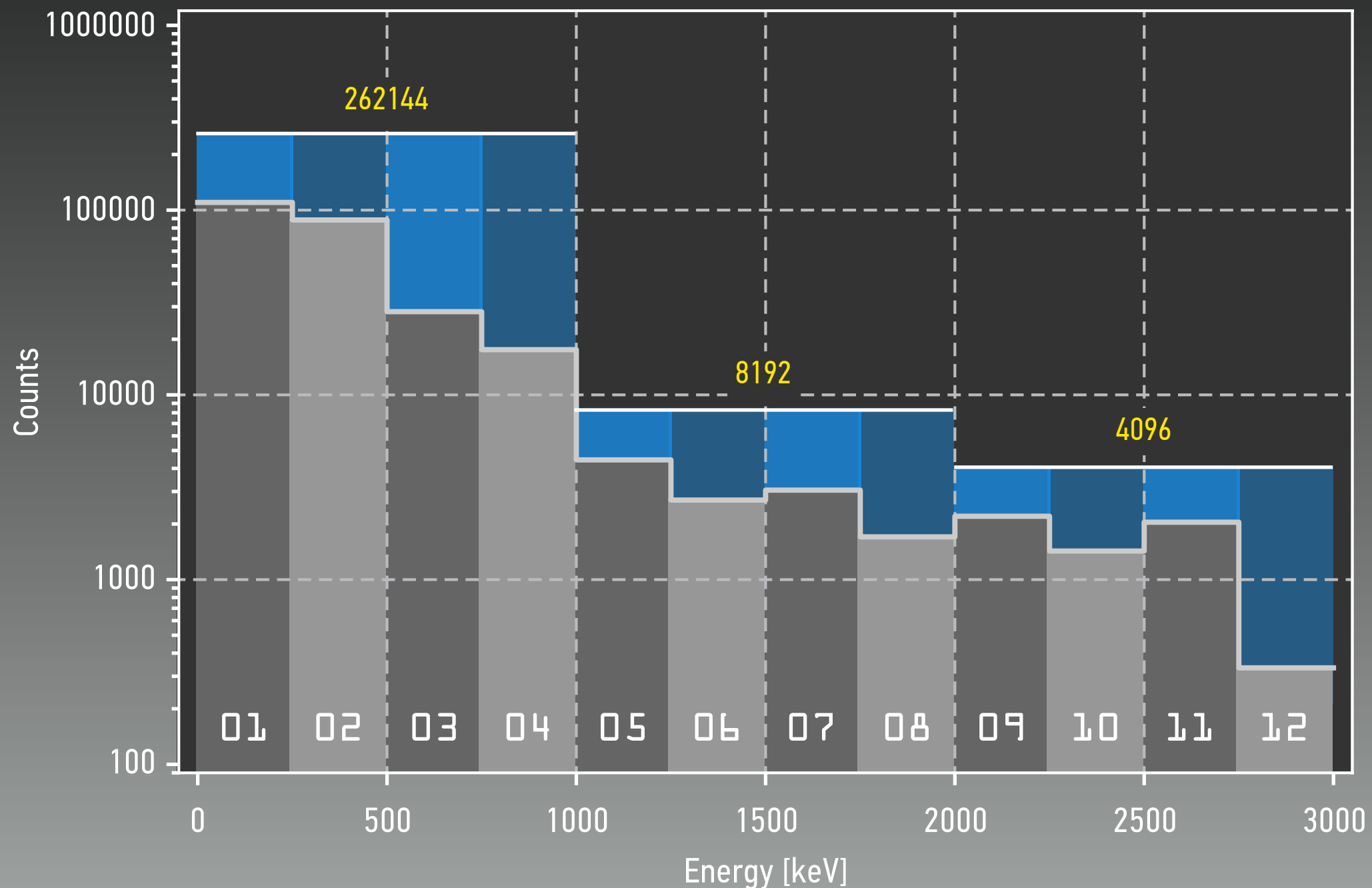


FEATURES

INCREASING TRANSPARENCY

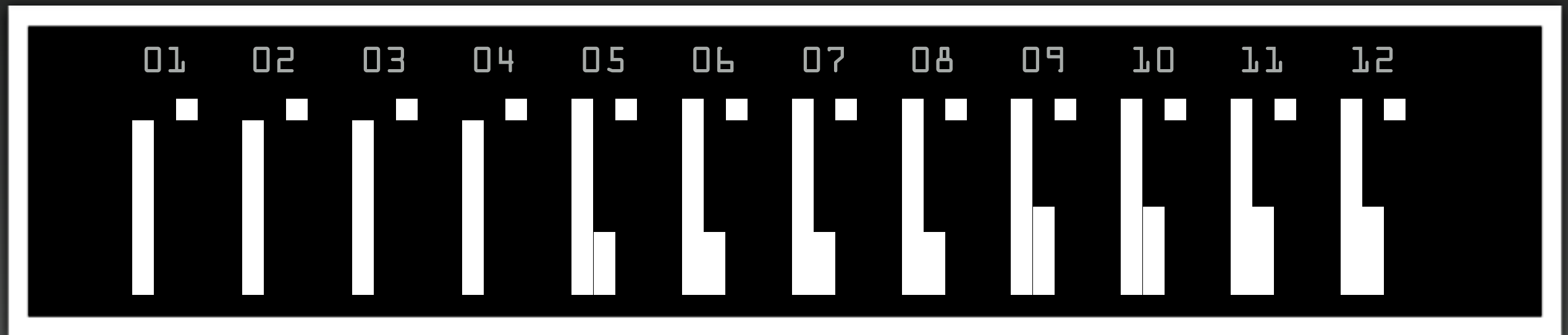
GRADUALLY LIFTING THE VEIL

(REVEALING UPPER LIMITS ON BIN COUNTS)

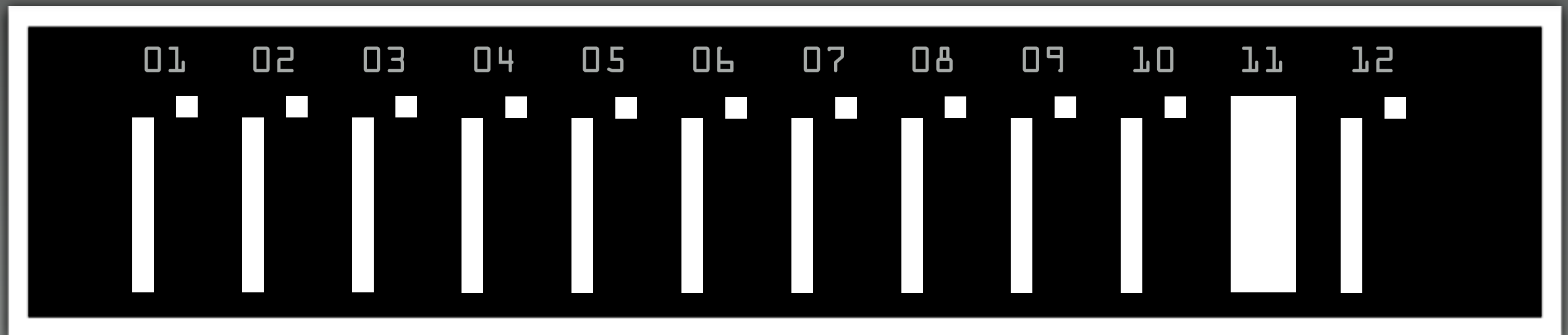


INCREASING TRANSPARENCY

GRADUALLY LIFTING THE VEIL



Mask confirming increasingly lower limits on counts as bin number increases



Mask revealing Bin 11 entirely (to provide confidence in calibration procedure)

