PUNCHED-OUT!!
PUBLIC TEMPLATES FOR NUCLEAR WARHEAD VERIFICATION

Boaz Barak, Alex Glaser, Moritz Kütt, Sébastien Philippe

June 2018
Revision 3b
INSPECTION PROTOCOL

PRIVATE PHASE
PRIVATE PHASE ¶ STEP 1

GENERATING A SECRET TEMPLATE

(TEMPORARY)

Reference data is for a 4.5 kg solid plutonium ball with contribution from calibration source

(measured at the DAF, July/August 2017)
PRIVATE PHASE ¶ STEP 1

GENERATING A SECRET TEMPLATE

(TEMPORARY)
PRIVATE PHASE ‖ STEP 2

MAKING THE PUNCHED CARD
WITH THE SECRET TEMPLATE

Template (12 x 24 bit)
Nonce (13 x 16 bit)
Fletcher 16 (Checksum)

12 x 24 bit (template) + 13 x 16 bit (nonce) + 16 bit (checksum) = 512 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
INSPECTION PROTOCOL
PUBLIC PHASE
VALIDATING THE TEMPLATE CARD

USING A TRUSTED REFERENCE ITEM

1. Mask is used to confirm public features of secret template
2. Template card is read and its SHA3 hash is calculated & displayed
3. Trusted reference item is obtained and passes inspection
4. Template card (and its SHA3 hash) are now accepted
PUBLIC PHASE ¶ STEP 4

READING THE TEMPLATE CARD
AND GENERATING ITS PUBLIC HASH

3d05e4f4e1de1619
a4075c6b9d91076da
93ebd94f4c9251db
1c9e1854afae0498
1669836f92502a30
b83eaeafa383d5d5
58c6d00ad149a0f3
d51002b1d0e7a8fd

Manual punched card reader
SHA3 hash of template card
PUBLIC PHASE ¶ STEP 5

INSPECTING CANDIDATE ITEMS

1. Template card is read and valid SHA3 hash is confirmed
2. Candidate item is inspected
3. Candidate item is accepted if it passes inspection
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)