Part 3
DRBGs)

May 2004

Elaine Barker

- **[illegible] (8.2):** Separated the [illegible]ment from the FIPS 140-2
- **[illegible] DRBG Processes (8.3):** Provided [illegible]d diagrams for distributed DRBG processes.
- **DRBG Instantiation and the Internal State (8.4):** Usage class removed from the state; state pointer/handle now used to access a state.

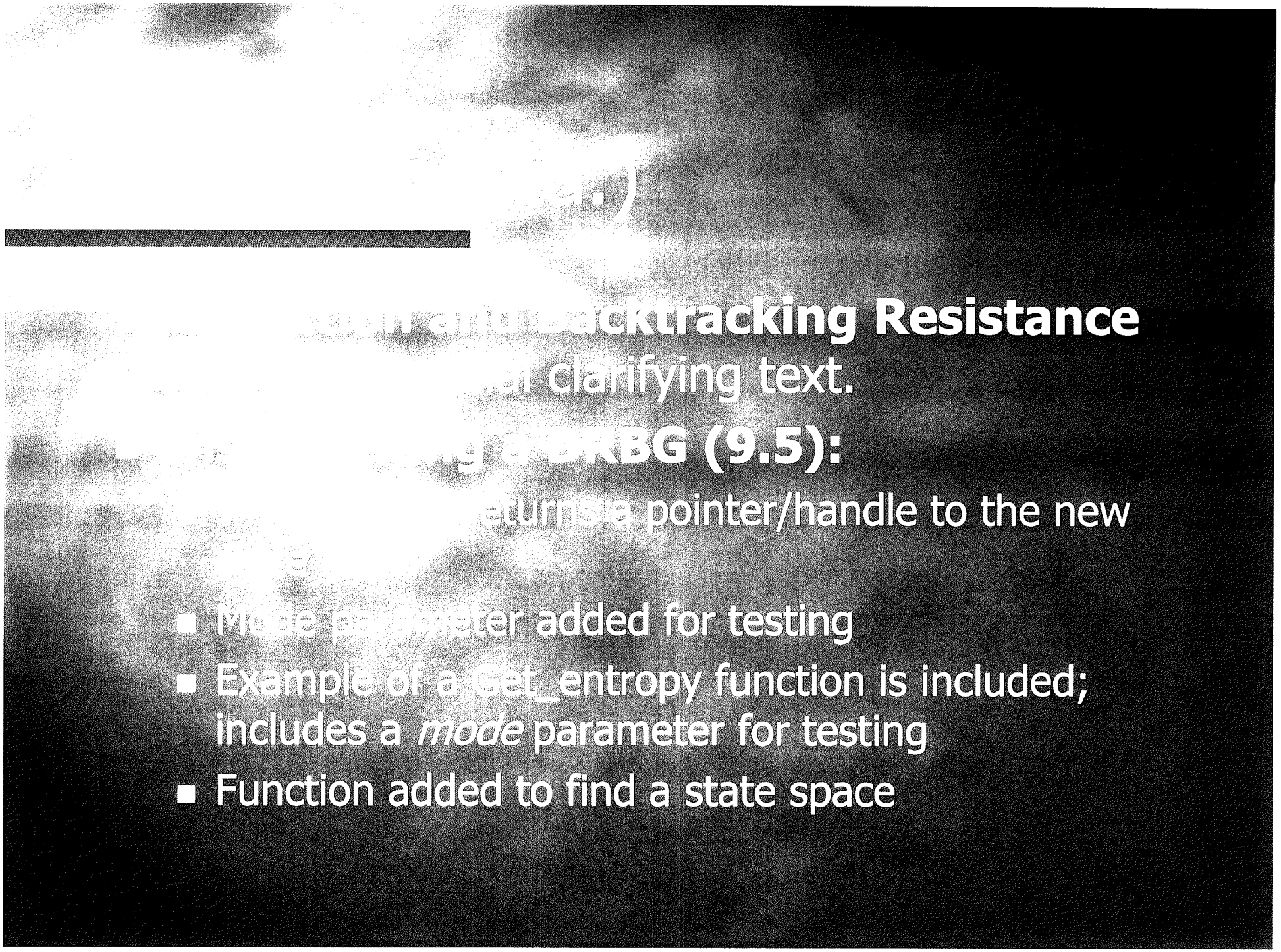
...7)

...andling of Seeds

...ption not required if no
...ction, or if full entropy & no
... string.

- ... discussion and a diagram on entropy
  ... chain of DRBGs.

- **Other Input (8.7):**
  - Additional text on the use of a personalization string.


Backtracking Resistance
clarifying text.
DRBG (9.5):
pointer/handle to the new
Mode parameter added for testing
Example of a get_entropy function is included; includes a *mode* parameter for testing
Function added to find a state space

...)

...about when reseeding might be

...*tional_input* parameter to
... additional input for reseeding

- Added a *mode* parameter to allow testing
- Uses a *state_pointer* to access the correct state

.)

...orandom Bits Using a

...*pointer* to access the correct

...provided in the function

- **Removing a DRBG Instantiation (9.8):**
  - Provides the ability to remove/delete an instantiation (e.g., after testing the instantiation process)

...ed.)

...DRBG (9.9):

- ...pecify general known-answer ...DRBGs; each DRBG may ...al test code
- ...ct operation of each DRBG ...implemented
- Tests the error handling code

.)

.(10):

- ...sed DRBGs: KHF and HMAC
- ...to indicate security strengths, and
- ...requirements

.1.2):

- ...the application-specific constant *t*
- Instantiation (10.1.2.3.3):
  - *seedlen* = *strength* + 64
  - *entropy_input* saved, rather than the *seed*
  - C defined differently: *C* = Hash (0x00 || *V*).

...d.)

...d.)

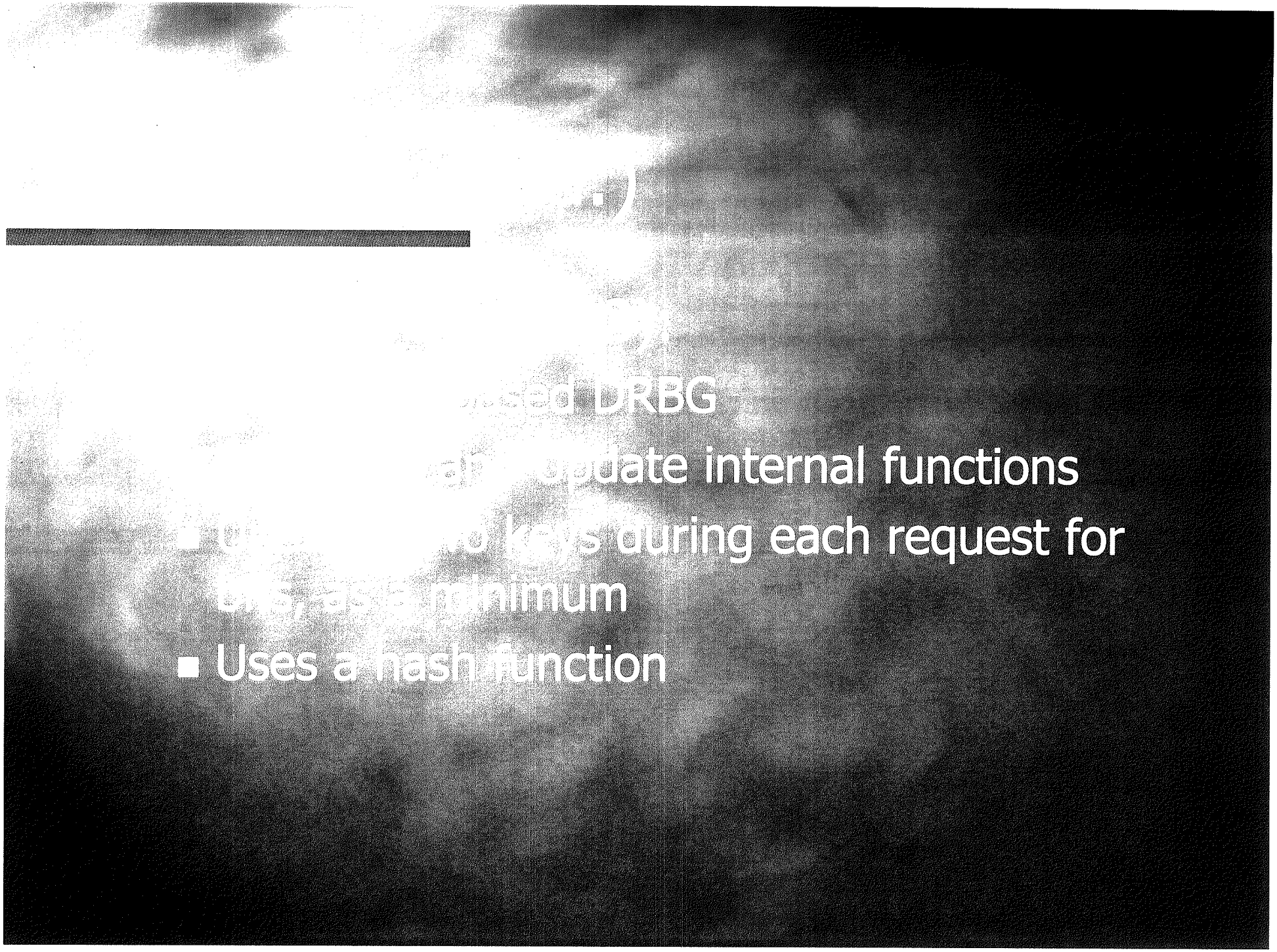
...1.2.3.4):

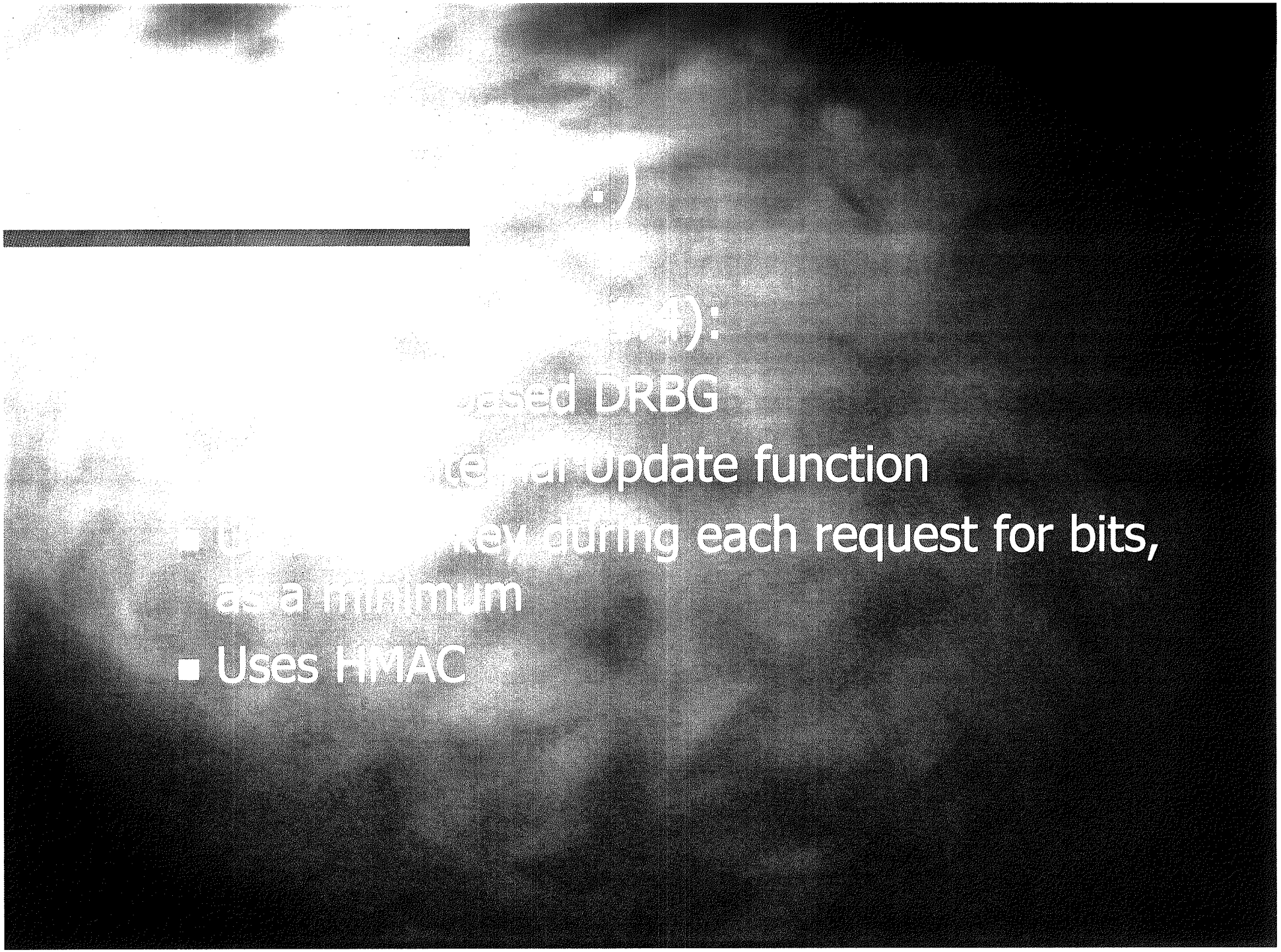
...now includes optional *additional_input*

...as stored in the state

...ion of *C* (as in instantiation)

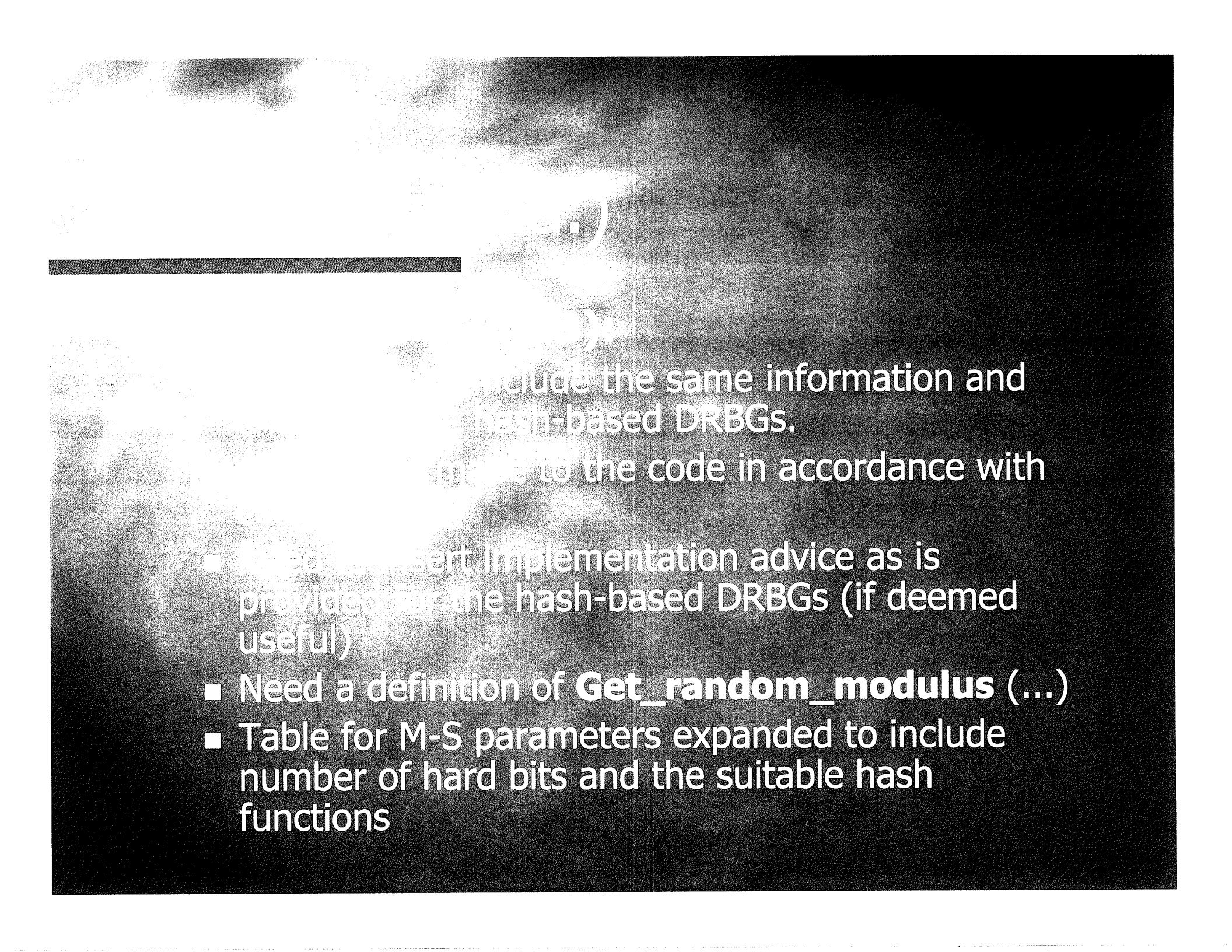
- **...g Pseudorandom Bits (10.1.2.3.5):**
  - ...*al_input* as provided from the calling ...parameters
  - Prediction resistance request gets entropy rather than reseeding (counter not reset)
  - Revised update process: $V = (V + \text{Hash}(0x03 \,||\, V) + C + \textit{reseed\_counter}) \bmod 2^{seedlen}$.


DRBG
update internal functions
during each request for
minimum
Uses a hash function


d)
ed):
ased DRBG
te an Update function
key during each request for bits,
as a minimum
Uses HMAC

8.3.2):

- to aid selection of appropriate
  ve, hash function, etc.)
- nclude the same information and
  based DRBGs.
- de to the code in accordance with
  comments
- Need to insert implementation advice as is provided for the hash-based DRBGs (if deemed useful)


include the same information and
hash-based DRBGs.
to the code in accordance with
insert implementation advice as is
provided for the hash-based DRBGs (if deemed
useful)
Need a definition of **Get_random_modulus** (…)
Table for M-S parameters expanded to include
number of hard bits and the suitable hash
functions

- ...on containing minimum
  - ...requirements
- ...ch normative annexes first
- Added an annex on Implementation Considerations (B)
  - Implementation within a FIPS 140-2 boundary (B.1)
  - Entry of entropy input into a DRBG boundary (B.2)
  - Transfer of state information between boundaries (B.3)

ed:

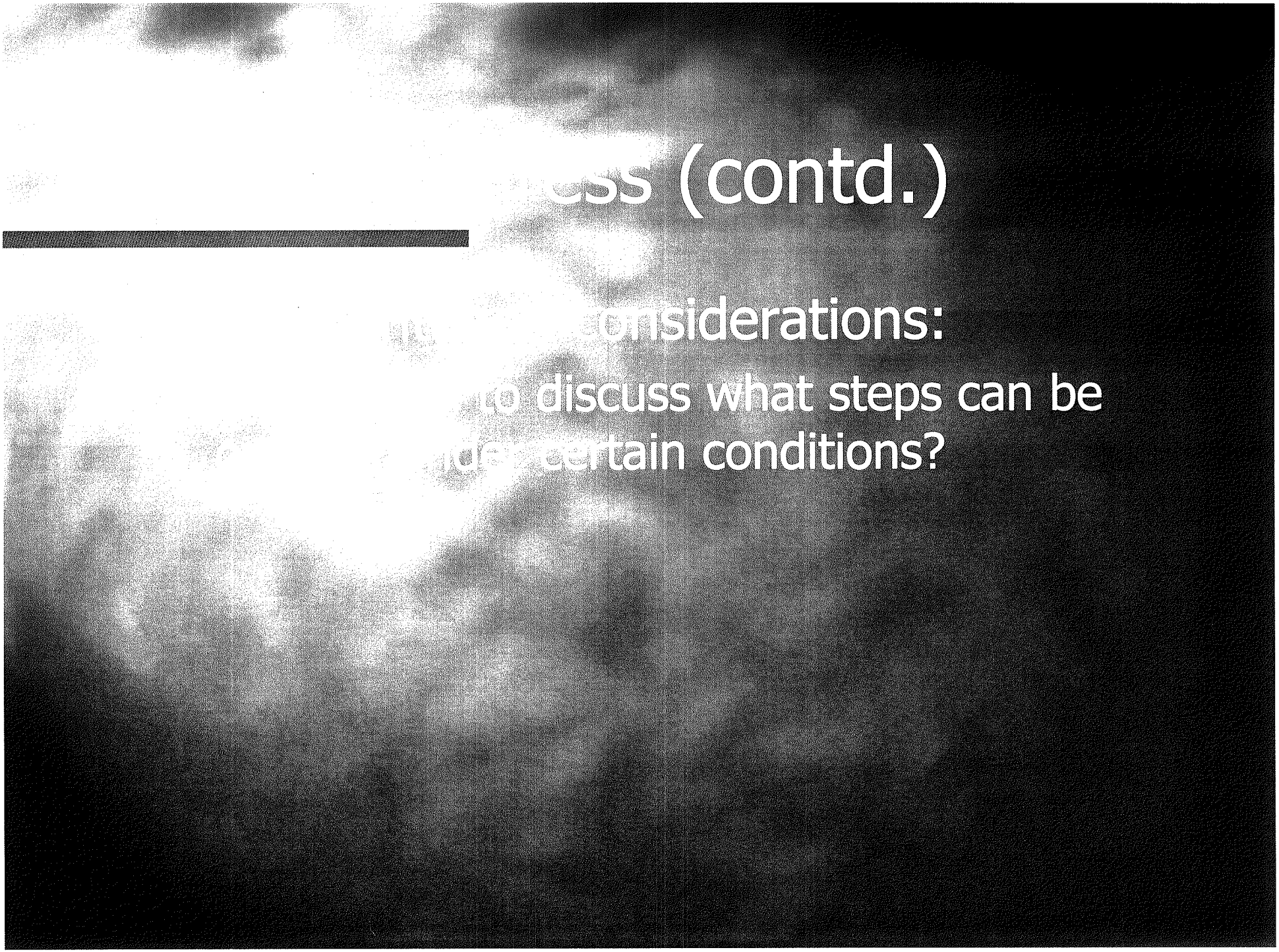
- discussion
- ecurity consideration text
- ner-based DRBG?
- Re/Seed block cipher-based derivation function

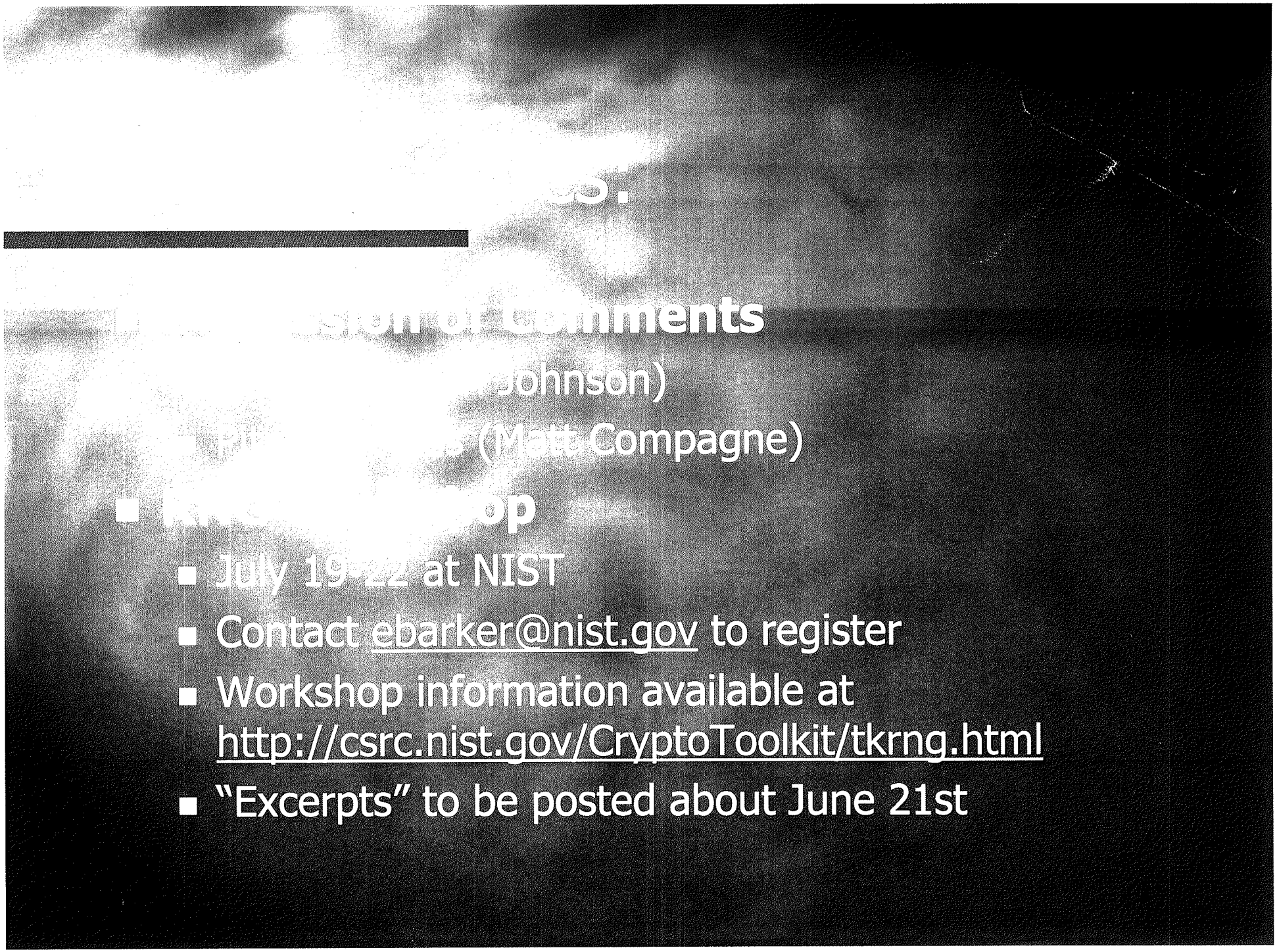
...ess

...ements:

...ed discussion of the functional
...om Part 1 be in Section 7 or in an

- ...
  - ...s this an appropriate approach for known-answer testing?
  - How many pseudorandom bit requests to make and of what length(s)?
  - Should the error handling code be tested?


ess (contd.)
considerations:
to discuss what steps can be
certain conditions?


Comments
Johnson)
(Matt Compagne)
op
July 19-22 at NIST
Contact ebarker@nist.gov to register
Workshop information available at http://csrc.nist.gov/CryptoToolkit/tkrng.html
"Excerpts" to be posted about June 21st