Q15: How does a submission obtain secure randomness?

This question is still part of the FAQ, and was originally added 03/29/2017. The answer has been modified twice.

A15: The function `randombytes()` will be available to the submitters. This is a function from the SUPERCOP test environment and should be used to generate seed values for an algorithm. `randombytes` should only be used to seed a NIST-approved DRBG. If the algorithm needs additional randomness beyond the seed value a NIST-approved DRBG should be used. As stated in the call for algorithms, the DRBG should be NIST approved. If a non-approved DRBG is used “the submitter shall provide an explanation for why a NIST-approved primitive would not be suitable.” The length of the random value obtained from `randombytes()` should be selected to match one of the security categories in the call for algorithms. That is, if the call to generate a key pair is from category 1 the randomness value should be 192 bits (24 bytes), if the call is from category 2 or 3 it should be 256 bits (32 bytes) and if it is from category 4 or 5 it should be 320 bits (40 bytes). The DRBG will be used to expand that if necessary.

For functional and timing tests a deterministic generator is used inside `randombytes()` to produce the seed values. If security testing is being done simply substitute calls to a true hardware RBG inside `randombytes()`.

Function prototype for `randombytes()` is:

```c
// The xlen parameter is in bytes
void randombytes(unsigned char *x, unsigned long long xlen)
```

The following demonstrate the use of the KAT and non-KAT versions of the functions to generate a key pair for encryption:

```c
int crypto_encrypt_keypair_KAT(
    unsigned char *pk,
    unsigned char *sk,
    const unsigned char *randomness
)
```

```c
int crypto_encrypt_keypair(unsigned char *pk, unsigned char *sk) {
    unsigned char pk[CRYPTO_PUBLICKEYBYTES];
    unsigned char sk[CRYPTO_SECRETKEYBYTES];
    unsigned char seed[CRYPTO_RANDOMBYTES];
    randombytes(seed, CRYPTO_RANDOMBYTES);
    crypto_encrypt_keypair_KAT(pk, sk, seed);
}
```
Q: Why are hash functions assigned fewer bits of quantum security than classical security?

A: Bernstein\(^1\) is widely cited as demonstrating that the most efficient quantum algorithm for finding hash collisions is the classical algorithm given by Van Oorschot and Wiener\(^2\). NIST believes this analysis is correct. Nonetheless, NIST’s security goal, that schemes claiming \(s\) bits of quantum security be at least as secure against cryptanalysis as a \(2s\) bit block cipher leads to differing definitions for quantum and classical security. In particular, quantum search for a \(2s\) bit key does not parallelize well. It is NIST’s judgement that, since cryptanalysis in the real world tends to be most successful when it can take advantage of highly parallel implementations for attacks, finding collisions in a \(2s\) bit hash function must be considered easier than searching for the key of a \(2s\)-bit block cipher, even in a world with ubiquitous quantum computing. NIST therefore assigns fewer than \(s\) bits of quantum security against collision to \(2s\) bit hash functions.

Q: What is the rationale to convert time and space complexity of known attacks into a single number for quantum and classical security?

A: NIST’s definition of \(s\) bits of quantum security is “as hard to break as a block cipher with a \(2s\) bit key, assuming a relatively efficient and scalable quantum computing architecture is available.” According to the analysis of Zalka\(^3\) the best generic quantum attack on a \(2s\)-bit block cipher requires a quantum circuit with depth*(square root (space)) proportional \(2^s\). This would suggest that quantum security should be defined as the minimum possible value of \(\log(\text{depth} \times \text{square root (space)})\) plus a constant (to put the quantum security of AES 128 at precisely 64 bits of quantum security,) accross all quantum and classical algorithms. This formula should only be taken as a rough guess, though, as there are additional factors to consider: Extremely serial and extremely parallel attacks are likely to be of limited practical relevance, even if the above formula rates them as most efficient. Likewise, even under the assumption that a relatively scalable and efficient quantum computing architecture is available, it is still likely that purely classical algorithms will be easier to implement than the formula suggests, and quantum algorithms that, unlike parallel versions of Grover’s algorithms, cannot be divided into small, unentangled, subcircuits, will be harder to implement than the formula suggests. NIST plans to take these practical considerations into account when making its evaluations.

Similarly, NIST’s definition of \(s\) bits of classical security is “as hard to break as a block cipher with an \(s\) bit key, assuming quantum computers are not available.” This suggests that classical security should be estimated as the minimum value of \(\log(\text{depth} \times \text{space})\) plus a constant, over all classical attack algorithms.

---

\(^1\) Daniel J. Bernstein, Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? [https://cr.yp.to/hash/collisioncost-20090517.pdf](https://cr.yp.to/hash/collisioncost-20090517.pdf)

