$\texttt{XDRBG} - \texttt{512}$ Algorithm

Stephan Müller

September 18, 2025

smueller@chronox.de

Abstract

XDRBG is a deterministic random number generator whose specification is published, peer-reviewed and publicly presented during the ToSC 2024 conference. Furthermore, NIST announced that this algorithm is about to be standardized as part of the NIST Special Publication 800-90A. The XDRBG is specified for AsconXOF with a strength of 128 bits of security as well as SHAKE256 which provide a security strength of 256 bits.

This specification defines the $\texttt{XDRBG} - \texttt{512}$ algorithm which uses SHAKE512 as cryptographic primitive for XDRBG, leaving the actual algorithm of XDRBG unchanged. The newly defined SHAKE512 parameter set for the SHAKE algorithm is presented with a rationale that its security strength offers 512 bits of security. Therefore, the resulting $\texttt{XDRBG} - \texttt{512}$ offers 512 bits of security as well. In terms of NIST security categories, the newly devised $\texttt{XDRBG} - \texttt{512}$ algorithm exhibits a significantly stronger mechanism than the NIST security category 5 en par with the definition for $\texttt{SHA3} - \texttt{512}$. The selected parameters for $\texttt{XDRBG} - \texttt{512}$ offers a performance that is comparable to an SP800-90A Hash DRBG with a $\texttt{SHA2} - \texttt{512}$ core. Comparing with $\texttt{XDRBG} - \texttt{256}$ its performance is less than half, but compared with $\texttt{XDRBG} - \texttt{128}$ it offers a similar performance or may be a bit faster, depending on the platform. A reference implementation of the algorithm is given with leancrypto.

Contents

1 Introduction 2

2 SHAKE512 Algorithm Specification 3

3 $\texttt{XDRBG} - \texttt{512}$ Algorithm Specification 3

4 Reference Implementation 4

4.1 Performance of $\texttt{XDRBG} - \texttt{512}$ 4

List of Tables

1 Security strength of SHAKE512 3
2 Security strength of $\texttt{XDRBG} - \texttt{512}$ 4
3 Generation of 1 GB Data with XDRBG 5

1 Introduction

With the selection as candidate for the upcoming revision of the NIST Special Publication 800-90A [2], the XDRBG algorithm is a well-recognized algorithm. This is supported by the fact that it was specified with the peer reviewed document [3]. Also, the algorithm was publicly presented at the ToSC 2024 conference.

The XDRBG specification contains an deterministic random number generator mechanism based on eXtended Output Functions (XOF), specifically based on SHAKE and AsconXOF. The claimed security strength is directly based on the used primitives:

- the SHAKE256-based $\texttt{XDRBG} - \texttt{256}$ offers 256 bits of security and is recognized to be equivalent to the NIST security category 5 as outlined in [3] section 7.3,

- the AsconXOF-based $\texttt{XDRBG} - \texttt{128}$ offers 128 bits of security equivalent to the NIST security category 1 as outlined in [3] section 7.4.

In addition to the mentioned primitives, this document presents the XDRBG construction using the SHAKE512 primitive. As the SHAKE512 primitive is not yet defined, it is specified first. This specification shows that the security strength of this cryptographic primitive is equivalent to $\texttt{SHA3} - \texttt{512}$ and thus offers 512 bits of security as well as a significant higher security then NIST security category 5 following [5] appendix A.5.

After the presentation of SHAKE512, the integration of this primitive into the XDRBG definition is specified. The integration ensures that the security strength of the SHAKE512 is upheld giving the same security strength to the devised $\texttt{XDRBG} - \texttt{512}$ algorithm.

A reference implementation of the algorithm is given with leancrypto.

Before providing the algorithm specification, it first should be clarified why a DRBG with a security strength of 512 bits is considered to be relevant. The algorithm specification given in [4] is defined to offer an AEAD algorithm with a security strength of 512 bits of security. To support this algorithm, a random number generator of equal strength must be available as otherwise a key with 512 bits security may not immediately be generatable.

2 SHAKE512 Algorithm Specification

The NIST specification [1] defines the Keccak-based algorithm suite of SHA3 and SHAKE128 as well as SHAKE256. The algorithm specification defines the use of the Keccak sponge with different parameters for the capacity and rate segregation of the Keccak sponge.

The specification [1] interestingly defines the message digest of $\texttt{SHA3}-\texttt{512}$ with a security strength of 512 bits security where the strength is solely derived from the size of the selected capacity: the security strength of 512 bits is provided by a capacity of 1,024 bits.

On the other hand, [1] only applies a capacity of maximum 512 bits for the XOFs of SHAKE.

To obtain a SHAKE XOF algorithm that offers 512 bits of security, this paper proposes the use of the $\texttt{SHA3}-\texttt{512}$ parameter set, namely the capacity of 1,024 bits to the SHAKE algorithm definition as follows using the same terminology as given in [1] chapter 6:

$$\texttt{SHAKE512}(M, d) = \texttt{Keccak}[1024](M||1111, d)$$

Using the parameter set from $\texttt{SHA3}-\texttt{512}$, the newly devised SHAKE512 inherits that security strength. Following the specification of the security strength given in [1] appendix A.1, the security strength of SHAKE512 is therefore defined as given in table 1.

Function	Output Size	Security Strength in Bits		
		Collision	Preimage	2nd Preimage
SHAKE512	d	min(d/2, 512)	≥min(d, 512)	min(d, 512)

Table 1: Security strength of SHAKE512

3 $\texttt{XDRBG}-\texttt{512}$ Algorithm Specification

The XDRBG specification provided with [3] contains an algorithm specification that is agnostic of the used XOF. This specification is applied for the $\texttt{XDRBG}-\texttt{512}$ algorithm.

The state paramenter V is defined to be equal to the capacity of the used XOF function in [3] section 7.3. For the application of the $\texttt{XDRBG}-\texttt{512}$ algorithm, the size of V is therefore defined to be 1,024 bits. Following the parameter specification given in [3] section 7.3 $\texttt{XDRBG}-\texttt{512}$ is therefore defined with table 2.

capacity	H_{init}	H_{rsd}	$log_2(R)$	log_2 (R_{DEV})	promised security level		
					classical	quantum (Grover)	NIST category
XDRBG − 512	768	512	128	128	512	256	>5[1]

Table 2: Security strength of XDRBG − 512

4 Reference Implementation

A reference implementation of XDRBG − 512 is provided with leancrypto. To demonstrate also that its implementation matches the aforementioned specification, the following considerations are applied:

- The library implements XDRBG − 128 and XDRBG − 256 which are both demonstrated to match the implementation given in [3] by calculating the reference test vectors from a "manual" invocation of SHAKE.
- The SHAKE128 and SHAKE256 are implemented and verified against the NIST reference implementation by obtaining CAVP certificates.
- The SHAKE512 implementation uses the exact same SHAKE processing and Keccak sponge implementation as used by SHAKE128 and SHAKE256 with the only difference that it is initialized with a rate size of 576 bits and thus an implied capacity of 1,024 bits.
- The XDRBG − 512 implementation instantiates the generic algorithm implementation used for XDRBG − 128 and XDRBG − 256 but uses the aforementioned SHAKE512 implementation along with the enlarged V state size of 1,024 bits.

4.1 Performance of XDRBG − 512

Based on the reference implementation, the following performance data is obtained. The following tables show the performance data with the C implementation of both, the Keccak and Ascon sponge processing to make them comparable. Yet, the reference implementation also offers accelerated implementations of the sponges which significantly increase the performance.

[1] The strength definition given in [5] appendix A.5 provides the estimation of the NIST security category for SHA3 − 512 which is applicable here.

Hardware	Word size	XDRBG − 128	XDRBG − 256	XDRBG − 512
Apple M4 Max	64-bit	4.95s	1.49s	3.80s
Intel Core Ultra 7 155H	64-bit	7.59s	3.28s	8.02s

Table 3: Generation of 1 GB Data with XDRBG

References

[1] *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. NIST, August 2015. https://doi.org/10.6028/NIST.FIPS.202.

[2] John Kelsey Elaine Barker. *NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. Revistion 1 edition, June, 2015. https://doi.org/10.6028/NIST.SP.800-90Ar1.

[3] John Kelsey, Stefan Lucks, and Stephan Müller. Xdrbg: A proposed deterministic random bit generator based on any xof. *IACR Transactions on Symmetric Cryptology*, 2024(1):5–34, Mar. 2024.

[4] Stephan Müller. *Ascon-Keccak AEAD Algorithm*. June 19, 2024. https://leancrypto.org/papers/Ascon-Keccak.pdf.

[5] NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. Official Call for Proposals, National Institute for Standards and Technology, December 2016.

