Enthentica, Inc.

HELP Data Sheet, V2.1

Data sheet reporting implementation details and statistical results for HELP and a novel strong-PUF, privacy-preserving, mutual authentication protocol (version 2.1)

1. AREA OVERHEAD of HELP and Authentication Protocol

Area overhead is reported on each of the IP blocks individually to suit different application scenarios, e.g., TRNG, token authentication, verifier authentication, session encryption and KEK. A *4-sbox-1-mixedcol* component of the AES algorithm is used as the entropy source for HELP, implemented using a hazard-free logic style.

Table 1: Area Overhead of HELP

Component	MUX	Carry	LUTs	FFs
PUF: CollectPNs	15	9	288	79
PUF: ComputeModulus	0	18	194	67
PUF: ComputePNDiffs	0	27	212	101
PUF: DataTransferIn	8	4	513	202
PUF: DataTransferOut	0	0	12	10
PUF: DualHelpBitGen	4	31	346	117
PUF: EvalMod	96	0	299	773
PUF Entropy Source: (*sbox-mixedcol)*	0	0	3365 (nets 3564)	128
PUF: LaunchCaptureEngine	0	0	78	11
PUF: LCTest_Driver	1	7	40	17
PUF: LoadUnLoadMem	0	6	72	19
MstCtrl (master control module)	15	38	342	85
PUF: PhaseAdjust	0	7	58	30
PUF: SingleHelpBitGen	0	20	310	98
PUF: SecureKeyEncoder (SKE)	0	15	303	122
PUF: TVComp	0	49	421	155
Totals	**139**	**231**	**6855**	**2014**

Other resources: 16 KB on-chip Block RAM, 1 MMCM (w/ option to use time-to-digital-converter (TDC) instead), 1 dual channel, 32-bit GPIO and 1 26-bit multiplier.

* ‘nets’ are listed for the entropy source because they contribute to the amount of entropy available.

NOTE: Applications that require only a subset of the full-blown functionality, e.g., only TRNG, token authentication, verifier authentication, session encryption and/or KEK, will be smaller in size by 20% or more, depending on the function(s).

NOTE: Other more compact, key-generation-only versions of the entropy source are available, that reduce the footprint over that shown above.

NOTE: Version V2.1 is not optimized for area or speed, but rather is optimized for maintainability. The modular structure of V2.1 can be optimized to reduce speed and area over that shown in this datasheet.

2. RUNTIMES of HELP and Authentication Protocol

Runtimes are reported using a wired network implementation of the protocol and are average values.

Table 2: Timing Data

Operation	Time (milliseconds)
Token Authentication (with 10 tokens in the secure DB)	500 ms
Verifier Authentication	500 ms
Session Encryption Key Generation, 512 bits	575 ms
Key-Encryption-Key (KEK) Key Generation, Enrollment (2000 bits)	1400 ms
Key-Encryption-Key (KEK) Key Generation, Regeneration (2000 bits)	475 ms

NOTE: Runtimes are subject to the size of the challenges used in each operation. Larger challenge sets can increase runtimes by 2X over that shown above.

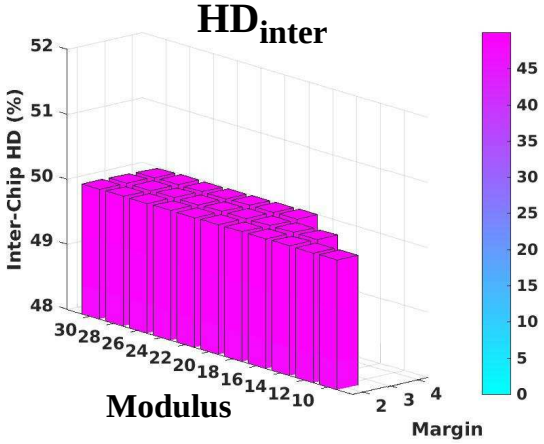
NOTE: Protocol requires a database search (to support the privacy preserving component). Each database element can be inspected in approx. 250 microseconds therefore runtimes of the protocol using databases of approx. 10K elements are less than 1 second.

NOTE: HELP implementations that leverage the time-to-digital-converter (instead of the Xilinx MMCM) improve runtimes by at least 50%, but also decrease bitstring reliability slightly over that shown in the following statistical report.

3. BITSTRING STATISTICAL PROPERTIES of HELP and Authentication Protocol

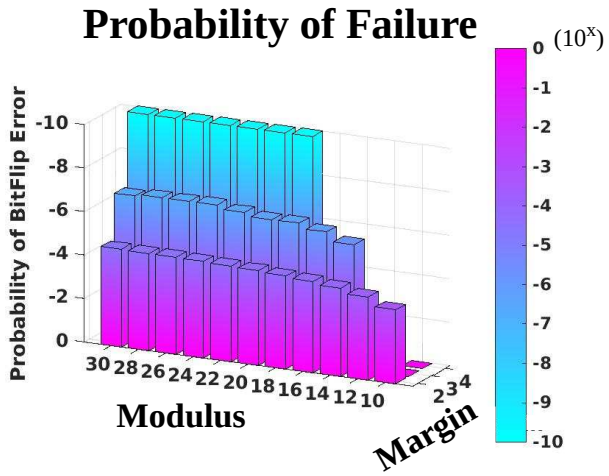
The characterization data from 20 commercial-grade Zynq 7020 chips with 25 instances/chip (500 chip-instances) is used to determine three statistical metrics, namely **uniqueness** (measured as Inter-chip Hamming Distance or HD_{inter}), **reproducibility** (measured using Intra-chip Hamming Distance or HD_{intra}) and **randomness** (measured using the NIST -- National Institute of Standards and Technology -- statistical tests). The total number of structural paths in the implementation is approx. 8 milliion of which more than 80% are testable. A small subset of 4096 paths are used in the statistical analysis presented in this report.

Uniqueness: The histogram presented below shows the HD_{inter} results for all combinations of enrollment-generated bitstrings from the 500 chip-instances, i.e., 500*499/2 = 124,750. Results are reported using HELP's population offset method. The ideal value is 50%.



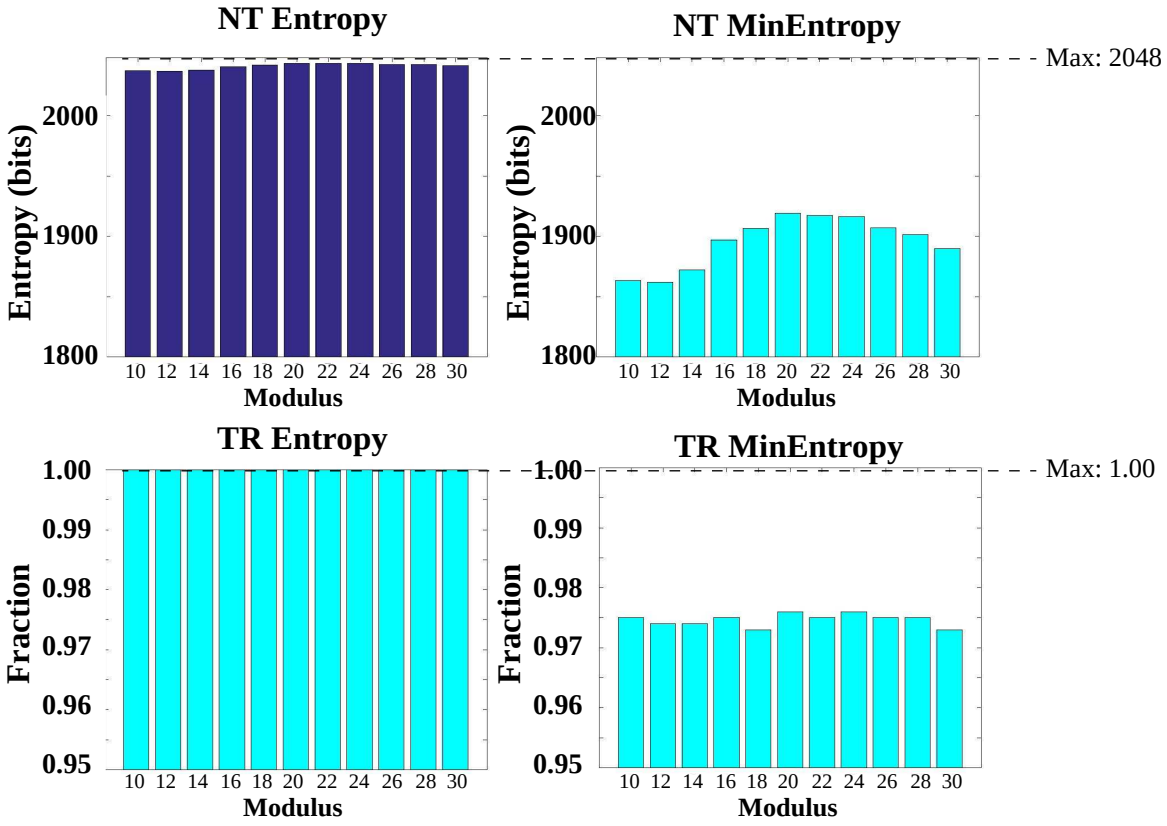
NOTE: Bars of height 0 in all histograms represent analyses not possible under the parameter values.

Reproducibility: Overall HD_{intra} is less than 10^{-6} for most parameter combinations for *Margin* > 2, as shown by the histogram below. The Probability of Failure reported is the probability that a bit-flip error occurs in the regeneration of the bitstring, computed as log_{10}(*total number of bit flips/total number of strong bits*). Regeneration was carried out at 12 TV corners, i.e., all combinations of the industrial-grade temperature-voltage specification limits for the FPGAs, i.e., -40°C, 0°C, 25° and 85°C and voltages 0.95V, 1.00V and 1.05V. Cases in which no bit flips occurred are shown as e^{-10}. The ideal value is 0.



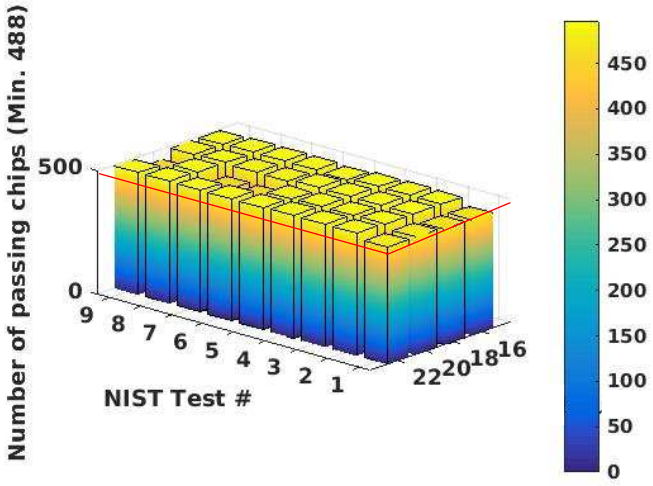
Enthentica, Inc.

Randomness: Entropy is measured in two ways: Across chips for each bit position called non-traditional or NT and across bitstrings for each chip called traditional or TR.



NIST statistical test results are reported on bitstrings generated by the KEK algorithm on bitstring sizes of more than 16,000 bits. The results indicate that 27 tests of the 36 tests are passed, where failing tests failed by at most 34 chips (of 500). NIST imposes a strict pass limit of 488 bitstrings passing of the 500 (97.6%).

NIST Statistical Results KEK 5



4. REVISION HISTORY

3/1/2018: Finalized this datasheet using ZED data collected from 500 chip-instances, with 20 Zedboards and 25 instances per Zedboard.
2/1/2018: Developed instuction videos for HELP (http://ece-research.unm.edu/jimp/HOST/index.html)
12/15/2017-1/2/2018: Developed TDC technique as alternative to Xilinx MMCM
10/1/2017: Developed SecureBoot techniques
6/15/2017: Bug fixes to Nonce Generator (in collaboration with Sandia)
3/1/2017-4/1/2017: Completed revisions to HELP Engine (KEK, Offset method, etc) for KG_EOA_V2.1
12/18/2016-1/10/2017: Collected data from 20 copies of Zedboard, with 25 instances on each board
10/1/2016: Developed Distribution Effect and Offset Methods
6/1/2016: Changed Entropy source to *sbox-mixedcol*