From: Nicholls, Tom <Tom.Nicholls@thalesesec.com>
Sent: Tuesday, July 22, 2014 2:55 PM
To: internal-hash
Subject: Comment on Draft FIPS 202
Attachments: FIPS 202 Comments-Thales e-Security.pdf

Comments on Draft FIPS 202 on behalf of Thales e-Security.

Best Regards,

Tom Nicholls
Security Engineer
THALES Information Systems Security
Phone: 954.888.6271
tom.nicholls@thalesesec.com

Confidentiality Classification: Thales e-Security OPEN

Legend (type of comment)

E = Editorial
G = General
T = Technical

ID	ORGANIZATION	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1	Thales e-Security	Section 3, 2nd paragraph	E	"The set of values for the b-bit input to the permutation, as it undergoes successive applications of the step mappings, culminating in the output, is called the state." This could be expressed more clearly. It starts off talking about the input, which is fixed, and ends up describing the state, which is mutable.	Recommend replacing the text with: "The permutation, as it undergoes successive applications of the step mappings, maintains a b-bit state, which is initially set to the input values."
2	Thales e-Security	Section 3.2.5, Algorithm 5, Step 3	E	The four 'plus' symbols should be 'xor' symbols.	Please amend.
3	Thales e-Security	Section 7, 2nd paragraph	E	"SHA3-224, SHA3-256, SHA3-384, SHA3-512 are approved hash functions …"	Missing "and" before "SHA3-512".

ID	ORGANIZATION	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
4	Thales e-Security	Section 6.2 (and elsewhere)	G	It would be preferable to name the XOFs 'SHAKE-128' and 'SHAKE-256' instead of 'SHAKE128' and 'SHAKE256'. This would be consistent with the naming of the hash functions 'SHA3-X'. Separation of the symbol and number with a hyphen gives a clearer indication that the number is not intrinsic to the symbol, but is a parameter of the construction.	Please amend.

ID	ORGANIZATION	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
5	Thales e-Security	All	G	This document defines: • Keccak[c], a family of sponge functions of width 1600 bits (parametrized by their capacity, 0 < c < 1600); • SHA3-X, a family of hash functions parametrized by their output length X in {224, 256, 384, 512}, defined in terms of Keccak[2X]; • SHAKE-X, a pair of extendable-output functions parametrized by their security level X in {128, 256}, defined in terms of Keccak[2X]. Suggest that this standard is decomposed into constituent primitives.	Recommend splitting this standard into three standards, one for each of the defined primitives: 1. a standard defining an approved family of sponge functions, namely Keccak[c]; 2. a standard defining an approved construction for hash functions in terms of arbitrary approved sponge functions, namely SHA3-X; 3. a standard defining an approved construction for extendable-output functions in terms of arbitrary approved sponge functions, namely SHAKE-X. This would allow greater flexibility in future. For example, NIST could then: • update the XOF standard without touching the hash standard, or vice versa; • approve a different sponge function and thereby get alternative hash and XOF functions for free; • define new primitives based on the sponge construction (in addition to hashes and XOFs) with minimal disruption to existing standards.